ISSN 2421-4442

Sicurezza Terrorismo Società

Security Terrorism Society

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

16

2022

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

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

16

ISSUE 2/2022

Milano 2022

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

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

ISSUE 2 – 16/2022

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: 978-88-9335-041-9

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Geopolitical spaces: frontiers

Meta spaces:
communities, threats and interactions

GEOPOLITICAL SPACES:
FRONTIERS

La nuova sicurezza europea tra Baltico e Artico

Luca Cinciripini

Luca Cinciripini: Ph.D. candidate in Institutions and Policies at UCSC in Milan, is research analyst and researcher at the Italian Team for Security Terroristic Issues and Managing Emergencies – ITSTIME. Prevously, he obtained a Master's Degree in Law at LUISS – Guido Carli and a Master in International Relations at ASERI – Postgraduate School of Economics and International Relations (UCSC). He specialised in EU Security and Foreign Policy and its interaction with NATO, terrorism and open-source intelligence (OSINT). His work includes, in particular, strategic analysis of crisis areas and scenarios focused on Islamic terrorism and national and international security threats.

Abstract

Following a geopolitical phase that has seen the Mediterranean at the center of European security studies, the northern part of the continent is assuming a new centrality. In particular, we are now witnessing the relevance of the Baltic Sea and the Arctic as new geopolitical scenarios of confrontation between great powers, in particular Russia and the member countries of NATO. The Ukrainian conflict, in fact, is producing serious consequences in these regions as well, as in the case of the request for accession by Sweden and Finland to NATO, with a consequent increase in international tensions. In addition, the multilateral governance that has so far governed the fate of the Arctic, both in terms of security and scientific research, is being severely tested by the tough confrontation between Russia and the West. Furthermore, climate warming opens new trade routes and provides access to huge deposits of raw materials, accelerating the competition between the players also thanks to the inclusion of powers such as China. In the light of their geographical, political and military characteristics, it is therefore useful to observe the Baltic and the Arctic as two regions of peculiarity, with points of contact that link their future security scenarios.

Dopo una fase geopolitica che ha visto il Mediterraneo al centro degli studi di sicurezza europei, la parte settentrionale del continente sta assumendo una nuova centralità. In particolare, si assiste ormai alla rilevanza del Mar Baltico e dell'Artico come nuovi scenari geopolitici di confronto tra grandi potenze, in particolare la Russia e i Paesi membri della NATO. Il conflitto ucraino, infatti, sta producendo serie conseguenze anche in queste regioni, come nel caso della richiesta di adesione di Svezia e Finlandia alla NATO, con conseguente aumento di tensioni internazionali. In aggiunta, la governance multilaterale che ha sin qui retto le sorti dell'Artico, sia in termini di sicurezza che di ricerche scientifiche, è messa a dura prova dal duro confronto tra Russia e Occidente. Il riscaldamento climatico, inoltre, apre nuove rotte commerciali e fornisce accesso a immensi giacimenti di materie prime, accelerando la competizione tra gli attori anche grazie all'inserimento di potenze come la Cina. Alla luce delle caratteristiche geografiche, politiche e militari, risulta pertanto utile osservare Baltico e Artico come due regioni con caratteristiche peculiari ma con punti di contatto che ne legano gli scenari di sicurezza futuri.

Keywords

Artico, Baltico, Russia, NATO, UE

1. Introduzione

Il sabotaggio al gasdotto Nord Stream avvenuto alla fine di settembre 2022 nel Mar Baltico,[1] ha portato ancor più alla ribalta i rischi per la sicurezza che si annidano nella parte più settentrionale del continente europeo. Accuse circostanziate sono state rivolte alla Russia che tuttavia ha sin qui declinato ogni responsabilità per l'accaduto.[2] A prescindere dalle responsabilità individuali circa il sabotaggio, ne emerge una chiara indicazione relativa alla crescente rilevanza di due aree specifiche nel quadro di sicurezza europeo e internazionale: il Baltico e l'Artico. Sebbene per motivi diversi, infatti, queste due aree rappresentano non solo cruciali hotspot di tensione e potenziale conflitto, ma stante l'attuale quadro geopolitico sono destinati a incrementare la loro rilevanza in tal senso. Ne deriva, dunque, la necessità di indagare e approfondire i caratteri specifici connessi a tali aree e le principali minacce alla sicurezza europea che ne derivano e che si proporranno in futuro, anche attraverso un approccio integrato delle due aree che studi i fenomeni riguardanti Baltico e Artico in maniera interconnessa.

2. Il Baltico

L'aggressione russa all'Ucraina ormai in corso da febbraio 2022 sta producendo importanti ripercussioni sul piano dell'architettura di sicurezza europea. Tale aspetto non concerne soltanto le sanzioni imposte a Mosca o il processo di allargamento della NATO, sebbene tali fattispecie siano strettamente connesse al conflitto. Oltre al pesante impatto che la guerra sta causando sull'Europa centro-orientale, si sta assistendo allo spostamento del baricentro geopolitico verso la parte settentrionale del continente europeo. Se infatti, nel corso degli ultimi anni, il Mediterraneo aveva rappresentato il fulcro delle principali minacce all'Europa, in particolare per quanto concerneva terrorismo internazionale, competizione tra potenze e processi migratori, ora l'attenzione si sta spostando verso nord, a partire dal Mar Baltico. Già da tempo luogo di stretta vicinanza tra Russia e paesi membri della UE e della NATO, il Baltico sta diventando sempre più cruciale nello scenario politico e

[1] https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/.

[2] https://www.bbc.co.uk/news/business-63084613.

di sicurezza internazionale in conseguenza del conflitto ucraino. L'invasione di Mosca ha infatti da un lato spinto Finlandia e Svezia ad abbandonare la loro storica politica di neutralità per formulare formale richiesta di adesione all'Alleanza Atlantica (Alberque e Schreer, 2022). Dall'altro, la penuria energetica che affligge l'Europa ha reso di importanza cruciale i gasdotti che trasportano gli approvvigionamenti energetici essenziali in vista dell'inverno. Il recente sabotaggio a Nord Stream, situato proprio nelle acque che affacciano su Danimarca e Svezia, e il conseguente rimpallo di responsabilità, hanno messo in mostra ancora una volta l'elevata conflittualità della zona e i rischi che ne derivano. In reazione all'attacco, la NATO ha incrementato massicciamente la propria presenza nella regione, schierando fino a 30 navi e ampliando il pattugliamento sottomarino.[3] La volontà di Finlandia e Svezia di accedere alla NATO, dunque, ha comportato l'inizio di un processo destinato a modificare gli equilibri regionali sul piano strategico ma ha avuto anche un forte impatto sul piano comunicativo. Una delle prime reazioni da parte di media, think tank e istituti di ricerca[4] è stata quella di definire il Baltico "*NATO lake*", alla luce della massiccia presenza di membri dell'Alleanza tra i Paesi che si affacciano sul bacino marittimo.[5] Sebbene tale definizione sembri adatta a riassumere lo spostamento consistente del baricentro strategico nel contesto regionale, frutto di una profonda integrazione non solo di mezzi ma anche di culture strategiche tra Paesi nordici e baltici, parte degli analisti sottolinea tuttavia la pericolosità di tale definizione.[6] Il conflitto ucraino, infatti, ha evidenziato la rilevanza della sfera comunicativa nel quadro dei conflitti, la quale si declina anche sul piano di una comunicazione in grado di proiettare una minaccia percepita dalla controparte. Nel caso del Baltico inteso come una sorta di *Mare Nostrum* in chiave occidentale e atlantista, infatti, vi è chi ritiene che si annidi il rischio di provocare ulteriori escalation con una Russia colta di sorpresa dall'improvvisa svolta atlantista di Svezia e soprattutto Finlandia, con la quale condivide un lungo confine. A tal proposito, occorre ricordare come al momento la procedura di adesione sia bloccata dall'ostruzionismo turco che ufficialmente richiede ai due Paesi misure decise contro i militanti curdi rifugiati in Scandinavia. Non sfugge, tuttavia, come tale manovra possa essere una sponda alla Russia, con la quale Ankara non ha di certo tagliato i legami economici, e come questa fase di

[3] https://foreignpolicy.com/2022/10/11/baltic-nato-russia-navy-nord-stream-sabotage/.

[4] https://www.fpri.org/article/2022/07/baltic-defense-after-madrid/; https://warontherocks.com/2022/05/will-finland-and-sweden-joining-nato-deepen-the-alliances-problems/; https://www.bbc.co.uk/news/world-61924778.

[5] https://warontherocks.com/2022/08/cooperation-can-make-the-nato-lake-a-reality/.

[6] https://www.rusi.org/explore-our-research/publications/commentary/no-dont-call-baltic-nato-lake.

incertezza rischi di lasciare spazi di manovra per operazioni ibride da parte di Mosca.[7] Questo processo interseca sempre più, inoltre, le dinamiche interne alla politica europea e comunitaria. Spicca infatti in particolar modo il ruolo svolto da Regno Unito e Polonia nel porsi come attori protagonisti in questo processo di riscoperta della strategicità baltica, a detrimento dei Paesi meridionali che sembrano assistere a un lento declino geopolitico attorno al Mediterraneo.[8] La traiettoria del Mar Baltico, dunque, sembra essere passata da quello che veniva definito "*sea of peace*"[9] da parte dell'Unione Sovietica ed esempio di *region-building*, a un'area di forte confronto e tensione militare, politica e strategica.

3. L'Artico

Se il Baltico ha assunto enorme rilevanza solo in tempi più recenti a causa della contiguità tra NATO e Russia, le attenzioni sull'Artico si concentrano da tempi più remoti. Ciononostante, la coesistenza tra le potenze occidentali e la Russia nella regione era stata considerata sufficientemente pacifica e moderatamente cooperativa (Kramnik, 2022). Da lungo tempo ormai, infatti, nella regione artica si assiste alla compresenza di numerosi Paesi membri della UE e della NATO, i quali hanno dato vita, assieme alla Russia, a una governance multilaterale sempre più istituzionalizzata volta non solo a garantire la pacifica coesistenza ma anche a promuovere forme di cooperazione in ambito scientifico e di sicurezza (Lagutina e al., 2022). L'istituzionalizzazione dei rapporti anche attraverso il Consiglio Artico ha contribuito a normalizzare la regione rendendola teatro di cooperazione soprattutto sul piano scientifico. Tuttavia, a partire dalla crisi del 2014 si è assistito a un processo di rallentamento del dialogo multilaterale, in parallelo con una crescente militarizzazione della regione. Svezia, Canada e USA hanno incrementato il loro budget di difesa, parallelamente all'accrescimento degli investimenti russi che sono stati giustificati dal Cremlino come investimenti difensivi, sebbene accompagnati da chiare manovre offensive e di disturbo nei confronti in primis di Norvegia e Finlandia.[10] A tali atteggiamenti da parte di Mosca si è replicato chiedendo un maggior intervento da parte della NATO, la quale già nel 2020 nel documento "NATO 2030 report" aveva espresso tra le raccomandazioni finali un invito a incrementare la propria "*situational awareness*

[7] https://foreignpolicy.com/2022/11/04/nato-nordic-expansion-turkey-sweden-finland/.

[8] https://www.limesonline.com/cartaceo/artico-e-baltico-i-mari-anti-italiani.

[9] https://www.centrumbalticum.org/files/5320/BSR_Policy_Briefing_7_2022.pdf.

[10] https://www.chathamhouse.org/2022/07/myths-and-misconceptions-around-russian-military-intent/myth-8-russias-military-build.

across the High North and the Arctic' as well as for the creation of a proper Arctic strategy [...] and should develop a strategy that takes into account broader deterrence and defence plans".[11] Una maggiore partecipazione della NATO all'architettura di sicurezza della regione era tuttavia vista con preoccupazione prima della recente crisi ucraina temendo, parte degli esperti, che potesse costituire il pretesto per un' escalation da parte di Mosca.[12] Sebbene tali preoccupazioni permangano, l'accesso di altri due Paesi regionali come Svezia e Finlandia nell'Alleanza Atlantica rende molto più probabile un maggior *engagement* della NATO nelle politiche artiche. A fronte di tali timori, infatti, non mancano le opinioni di chi ritenga che ormai un coinvolgimento della NATO nella regione sia inevitabile,[13] indicando dunque la necessità non di evitare tale presenza ma di individuarne per tempo le adeguate *policy recommendations*. Queste, infatti, sarebbero volte a indirizzarne le azioni nella maniera più efficace possibile considerando la limitata conoscenza dell'Alleanza di una regione un tempo considerata "a bassa tensione" (Lanteigne, 2019).

Uno dei principali fattori capaci di incidere sul quadro di sicurezza della regione, risulta essere quello ambientale a causa dei profondi sconvolgimenti naturali prodotti dal *climate change* (Hall e Webber, 2022). La progressiva erosione dei ghiacci polari, infatti, sta aprendo nuove rotte marittime impensabili solo fino a qualche anno fa. Ciò comporta da un lato la possibilità di aprire nuove arterie marittime di trasporto, oltre all'accesso a nuovi e immensi giacimenti di materie prime. Lo scenario di sicurezza è complicato però anche dalle insistenti mire di Pechino che, sebbene non risulti essere un Paese artico, da tempo manifesta la volontà di partecipare attivamente agli sviluppi della regione e alla corsa alle materie prime allocate (Odgaard, 2022). La sospensione dei lavori del Consiglio Artico a seguito dell'invasione russa dell'Ucraina, dunque, pone sostanziali problemi in termini di sicurezza della regione. Indebolisce economicamente la Russia, che aveva sin qui sostenuto pesanti investimenti infrastrutturali nella regione puntando appunto su giacimenti di materie prime e nuove rotte commerciali, investimenti che già prima del conflitto avevano dato magri ritorni. Ciò avvicina sempre più la Russia all'orbita cinese, la quale subisce anch'essa le dirette conseguenze dello stop al confronto multilaterale nella regione, spingendola sempre più a interessarsi dell'Artico come una sorta di "*near-arctic country*".[14] Già nel 2018 un report del Consiglio Artico aveva corroborato tale definizione, individuando

[11] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

[12] https://www.chathamhouse.org/2021/05/new-military-security-architecture-needed-arctic

[13] https://jsis.washington.edu/news/natos-role-in-securing-a-changing-arctic/.

[14] https://isdp.eu/publication/the-ice-silk-road-is-china-a-near-artic-state/#:~:text=Factually%20speaking%2C%20China%20is%20not,its%20attention%20toward%20the%20region.

nelle politiche di Pechino un tentativo di costituire una vera e propria "Polar Silk Road" destinata a supportare e complementare i progetti della Belt and Road Initiative (BRI), suscitando frizioni con Mosca che ne teme l'ingerenza nella propria sfera di influenza.[15] Inoltre, si assiste anche all'interruzione di importanti progetti di collaborazione scientifica riguardanti proprio gli effetti del cambiamento climatico, che incidono sulla regione a un ritmo ben più sostenuto del resto del pianeta.[16]

4. Prospettive future

L'illegale invasione russa dell'Ucraina sta producendo potenti ripercussioni sulla governance di sicurezza europea costruita a partire dalla fine della Seconda Guerra Mondiale e affermatasi nella sua forma attuale con la fine della Guerra Fredda. Se negli ultimi anni il Mediterraneo aveva rappresentato il fulcro delle principali minacce alla sicurezza europea, ora il baricentro si sta spostando verso nord. Ciò è dovuto alla compresenza di fattori naturali, militari ed economici, oltre che geografici. Il progressivo scioglimento dei ghiacci, infatti, apre nuove rotte commerciali e consente l'accesso a immensi giacimenti di materie prime, accelerando la competizione tra potenze e incrementando le frizioni tra loro. La sospensione di forme di cooperazione multilaterale come quella del Consiglio Artico, in conseguenza dell'aggressione russa, rende più difficile una pacifica coesistenza nella regione, la quale da tempo assiste a una progressiva militarizzazione. La richiesta di Svezia e Finlandia di accedere alla NATO, inoltre, non solo aumenta considerevolmente lo spazio geografico di confine tra l'Alleanza e la Russia, ma allarga anche il quadrante regionale consentendo ormai di poter considerare in maniera non separata Baltico e Artico. Sebbene diversi, infatti, i due contesti presentano similitudini e fattori di vicinanza, a partire dagli attori protagonisti. Alla luce di tale prospettiva, risulta utile un'osservazione non separata dei due contesti, quanto piuttosto uno studio che tenga in debita considerazione i numerosi punti di contatto esistenti tra Baltico e Artico, arrivando a comprendere la parte settentrionale del continente europeo come una sorta di macro-regione. Si assiste ormai da tempo, inoltre, a una dinamizzazione delle forme di cooperazione in campo militare in risposta all'assertività di Mosca, come nel caso del NORDEFCO (Nordic Defence Cooperation) che

[15] https://www.chathamhouse.org/sites/default/files/2022-06/2022-06-06-militarization-russian-polar-politics-boulegue_0.pdf.

[16] https://www.ssoar.info/ssoar/bitstream/handle/document/81694/ssoar-2022-paul-Arctic_repercussions_of_Russias_invasion.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2022-paul-Arctic_repercussions_of_Russias_invasion.pdf.

racchiude Danimarca, Finlandia, Islanda, Svezia e Norvegia, sempre più attivo nel dialogo con gli USA e in fase di possibile allargamento.[17] Ciò ha riflessi importanti anche per altri attori, come Regno Unito e Germania da un lato, sempre più coinvolte negli affari baltici e artici, e la Cina dall'altro, la quale insistentemente si propone da tempo come Paese quasi-artico e che guarda con interesse alle dinamiche in corso. Proprio l'indebolimento di Mosca può consentire in futuro un maggior inserimento di Pechino nella regione, avvicinando pericolosamente la traiettoria cinese a quella della NATO con il rischio che, in futuro, il Baltico ma soprattutto l'Artico possano diventare il nuovo territorio di confronto tra potenze e in cui misurare le politiche di contenimento verso la Cina.

Bibliografia

Ålander, M., Paul, M. (2022). Moscow threatens the balance in the High North: In light of Russia's war in Ukraine, Finland and Sweden are moving closer to NATO, SWP Comment, No. 24/2022, Stiftung Wissenschaft und Politik (SWP), Berlin, https://doi.org/10.18449/2022C24.

Alberque, W., Schreer, B. (2022). Finland, Sweden and NATO Membership, Survival, 64:3, 67-72, DOI: 10.1080/00396338.2022.2078046.

Bennet, M. (2020). NATO's role in securing a changing Arctic, The Henry M. Jackson School of International Studies, University of Washington. Retrieved from: https://jsis.washington.edu/news/natos-role-in-securing-a-changing-arctic/.

Boulègue, M., Depledge, D. (2021). New military security architecture needed in the Arctic. Mounting military pressure in the European Arctic can no longer be ignored. The US must address the issue and build proper mechanisms for dialogue on security, Chatham House, 4 may. Retrieved from: https://www.chathamhouse.org/2021/05/new-military-security-architecture-needed-arctic.

Boulègue, M. (2022). The militarization of Russian polar politics. Addressing the growing threat of tension and confrontation in the Arctic and Antarctica, Chatham House research paper, 6 June. Retrieved from: https://www.chathamhouse.org/2022/06/militarization-russian-polar-politics.

Descamps, M. (2019). The Ice Silk Road: Is China a "Near-Arctic-State"?, Institute for Security & Development Policy. Retrieved from: https://isdp.eu/publication/the-ice-silk-road-is-china-a-near-artic-state/#:~:text=Factually%20speaking%2C%20China%20is%20not,its%20attention%20toward%20the%20region.

Gardner, F. (2022). Nato summit: Five challenges for the military alliance, BBC News, 28 June. Retrieved from: https://www.bbc.co.uk/news/world-61924778.

Gramer, R. (2022a). NATO Doubles Naval Presence in Baltic, North Seas After Pipeline Sabotage, Foreign Policy, 11 October. Retrieved from: https://foreignpolicy.com/2022/10/11/baltic-nato-russia-navy-nord-stream-sabotage/.

[17] https://www.econstor.eu/bitstream/10419/256747/1/2022C24.pdf.

Gramer, R. (2022b). NATO's Nordic Expansion Stuck at Turkish Roadblock, Foreign Policy, November 4. Retrieved from: https://foreignpolicy.com/2022/11/04/nato-nordic-expansion-turkey-sweden-finland/.

Hall, G., Webber, M. (2022). Maritime security in the North Atlantic. In R-L. Boşilcă, S. Ferreira, & B.J. Ryan (Eds.), *Routledge Handbook of Maritime Security*.

Jonsson, M., Haggblom, R. (2022). Cooperation can make the NATO lake a reality, War On The Rocks, 29 AUGUST. Retrieved from: https://warontherocks.com/2022/08/cooperation-can-make-the-nato-lake-a-reality/.

Josephs, J. (2022). US suggests Russia could be behind Nord Stream gas leaks, BBC News, retrieved from: https://www.bbc.co.uk/news/business-63084613.

Kramnik, I. (2022). The Cold War in the Cold Region: A Return. In: Likhacheva, A. (eds) Arctic Fever. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-16-9616-9_2.

Lagutina, M.L., Eremina, N.V., Gadal, S. (2022). European Arctic Policy. In: Pak, E.V., Krivtsov, A.I., Zagrebelnaya, N.S. (eds) The Handbook of the Arctic. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-16-9250-5_5-1.

Lanteigne, M. (2019). The Changing Shape of Arctic Security, NATO Review, Nato Review, 28. Retrieved from: https://www.nato.int/docu/review/articles/2019/06/28/the-changing-shape-of-arctic-security/index.html.

Milevski, L. (2022). Baltic defense after Madrid, Foreign Policy Research Institute, Baltic bulletin, 28 July. Retrieved from: https://www.fpri.org/article/2022/07/baltic-defense-after-madrid/.

NATO. (2020). NATO 2030: United for a new era, Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General", Brussels, 25 November. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

Odgaard, L. (2022). Russia's Arctic Designs and NATO, Survival, 64:4, 89-104, DOI: 10.1080/00396338.2022.2103259.

Paul, M. (2022). Arctic repercussions of Russia's invasion: council on pause, research on ice and Russia frozen out. (SWP Comment, 39/2022). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2022C39.

Pawlak, J. (2022). No, don't call the Baltic a 'NATO lake', RUSI commentary, 5 September. Retrieved from: https://www.rusi.org/explore-our-research/publications/commentary/no-dont-call-baltic-nato-lake.

Petroni, F. (2022). Artico e Baltico, i mari anti-italiani, in Il mare italiano e la guerra, Limes, 8, 2022. https://www.limesonline.com/cartaceo/artico-e-baltico-i-mari-anti-italiani.

Plucinska, J. (2022). Nord Stream gas sabotage: who's being blamed and why?, Reuters, 6 Octiober. Retrieved from: https://www.reuters.com/world/europe/qa-nord-stream-gas-sabotage-whos-being-blamed-why-2022-09-30/.

Wittmann, K. (2022). NATO and Security in the Baltic Sea Region, centrum Balticum, BSR Policy Briefing 7/2022. Retrieved from: https://www.centrumbalticum.org/files/5320/BSR_Policy_Briefing_7_2022.pdf.

Zysk, K. (2022). Myth 8: 'Russia's military build-up in the Arctic is defensive'. In Myths and misconceptions around Russian military intent. How they affect Western policy, and what can be done, Chatham House, 14 July. Retrieved from: https://www.chathamhouse.org/2022/07/myths-and-misconceptions-around-russian-military-intent/myth-8-russias-military-build.

Renewed Kyrgyz-Tajik Border Conflict – Cui Bono?

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. In capacity of multiple Government Advisory positions, he has counselled both government agencies and investing international corporates on issues of direct investment, energy security and counter-terrorism.

Abstract

Following the July 2022 4th Consultative Meeting of the heads of state of Central Asian Countries at the Lake Issyk-Kul, hosted by Kyrgyzstan, and literally on the eve of a high-level summit of the Shanghai Cooperation Organization in Samarkand, where among other agenda, the regional powerhouse Iran, so far active as an observer state, formally submitted an application to join the regional geopolitical organization increasingly aspiring to become a global one, and Turkey, an invited guest, announced its preparedness to join the alliance in the future, fierce fighting flared up in the Batken Region of Kyrgyzstan, following a military incursion from the side of Tajikistan. Not only were the presidents of Kyrgyzstan and Tajikistan sitting around the same table sipping tea when young Kyrgyz soldiers were losing their lives defending their homeland, the whole idea behind the summit hosted by Uzbekistan was originally prepared to increase the regional cooperation perspectives, not to watch such efforts disintegrate before the very eyes of the Central Asian and wider regional nations. Moreover, in less than a week, the 77th United Nations General Assembly gathering was to take place, bringing to New York the leaders of the very nations embroiled in another round of Central Asian border conflict – compelling the Kyrgyz President Sadyr Japarov to dedicate his address entirely to the renewed border dispute with Tajikistan.

Obviously, with the ongoing Russia-Ukraine confrontation and the situation around the Nagorno-Karabakh recently aggravating to another level of military clashes between Azerbaijan and Armenia, a question needs to be asked whether this new Kyrgyz-Tajik engagement is to be seen and analyzed on its own, or whether some other global mechanisms in the backdrop should be identified. The border dispute between Kyrgyzstan and Tajikistan is certainly an issue in force for the past twenty years, having attained its very hot phase in April 2021, and a complex mix of causes needs to be addressed to understand the matter in question – from a lack of proper governance on both sides, decades long competition over water resources in the Fergana Valley, socioeconomic disparities in the geographical area far from their respective national capitals, proliferating organized crime including drug trafficking, and, not the least, the ever contrasting ethnic divide among the several nations of the region.

The article will put less emphasis on historical data and perspectives, while maintaining a certain measure of a chronological frame of reference, and instead will attempt to place the current Kyrgyz-Tajik border crisis into both regional context (as part of the ongoing phenomenon where currently all of the Central Asia gains significance among various global affairs) as well as the context of increasingly crucial global issues, including a proper use of water resources, food security and inter-ethnic symbiosis.

Dopo il 4° incontro consultivo dei capi di stato dei paesi dell'Asia centrale nel luglio 2022 presso il lago Issyk-Kul, ospitato dal Kirghizistan, e letteralmente alla vigilia di un vertice ad alto livello dell'Organizzazione per la cooperazione di Shanghai a Samarcanda, dove, tra l'altro, la potenza regionale Iran, finora attiva come stato osservatore, ha formalmente presentato domanda per entrare a far parte dell'organizzazione geopolitica regionale sempre più aspirante a diventare globale, e la Turchia, un ospite invitato, ha annunciato la sua disponibilità ad aderire all'alleanza in futuro, aspri combattimenti sono divampati nella regione di Batken del Kirghizistan, a seguito di un'incursione militare dalla parte del Tagikistan. Non solo i presidenti del Kirghizistan e del Tagikistan erano seduti intorno allo stesso tavolo a sorseggiare il tè quando i giovani soldati kirghisi stavano perdendo la vita per difendere la loro patria, l'intera idea alla base del vertice ospitato dall'Uzbekistan era originariamente preparata per aumentare le prospettive di cooperazione regionale, e non vedere tali sforzi disintegrarsi davanti agli occhi stessi delle nazioni dell'Asia centrale e della regione più ampia. Inoltre, in meno di una settimana, si sarebbe tenuta la 77a riunione dell'Assemblea Generale delle Nazioni Unite, portando a New York i leader delle stesse nazioni coinvolte in un altro round di conflitti di confine dell'Asia centrale, costringendo il presidente kirghiso Sadyr Japarov a dedicare interamente il suo discorso al rinnovato conflitto di confine con il Tagikistan.

Ovviamente, con il conflitto Russia-Ucraina in corso e la situazione intorno al Nagorno-Karabakh che si è recentemente aggravata a un altro livello di confronto militare tra Azerbaigian e Armenia, è necessario porsi una domanda se questo nuovo impegno kirghiso-tagiko debba essere visto e analizzato da solo, o se dovrebbero essere identificati altri meccanismi globali sullo sfondo. La disputa di confine tra Kirghizistan e Tagikistan è certamente una questione in vigore negli ultimi vent'anni, avendo raggiunto la sua fase molto calda nell'aprile 2021, e per comprendere la questione in questione è necessario affrontare un insieme complesso di cause – dalla mancanza di un buon governo da entrambe le parti, dalla concorrenza decennale per le risorse idriche in Val Fergana, disparità socioeconomiche nell'area geografica lontana dalle rispettive capitali nazionali, proliferazione della criminalità organizzata compreso il traffico di droga, e, non ultimo, la sempre contrastante divisione etnica tra le diverse nazioni della regione.

L'articolo porrà meno enfasi sui dati storici e sulle prospettive, pur mantenendo una certa misura di un quadro di riferimento cronologico, e cercherà invece di collocare l'attuale crisi del confine tra Kirghizistan e Tagikistan in entrambi i contesti regionali (come parte del fenomeno in corso in cui attualmente tutta l'Asia centrale acquista importanza tra i vari affari globali) così come il contesto di questioni globali sempre più cruciali, tra cui un uso corretto delle risorse idriche, la sicurezza alimentare e la simbiosi interetnica.

Keywords

Kyrgyzstan, Tajikistan, Central Asia, Regional Security, post-USSR Conflict Zone, Water Resources

1. Introduction – The 100-year Old Soviet Legacy Reflected in the Current Border Dispute

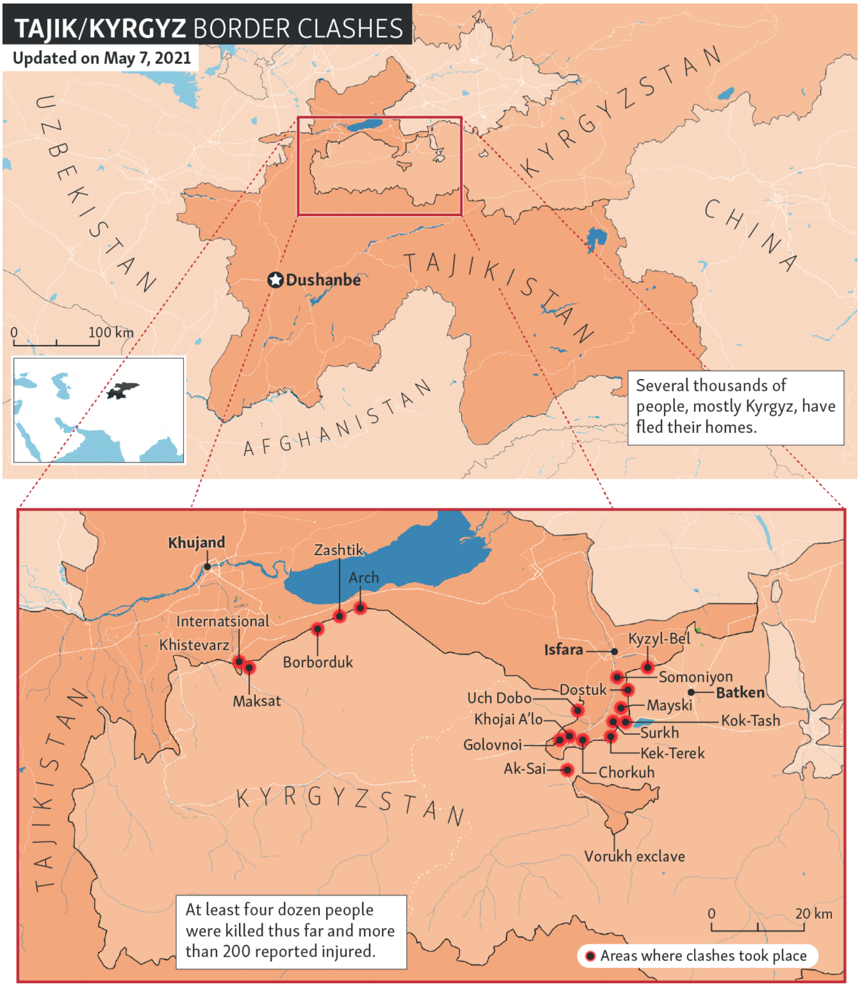
In order to understand the current border dispute between Kyrgyzstan and Tajikistan, which in September 2022 intensified in the form of open military incursions from the side of Tajikistan into Kyrgyzstan, one needs to simply look at the regional map and perhaps make a short excursion into the history of the Soviet Union. As displayed in the map below, the three nation-states of Kyrgyzstan, Tajikistan and Uzbekistan are intertwined almost in a symmetric vortex around the fertile Fergana Valley, with the border delineation as if each of the countries was firmly embedded into the neighboring one. Furthermore, the existence of multiple exclaves (Sarvan – the Tajikistan exclave in Uzbekistan, Vorukh – the Tajikistan exclave in Kyrgyzstan, Kayragach – less than 1 km^2 Tajik exclave inside Kyrgyzstan, Shakhimardan – an Uzbekistan exclave in Kyrgyzstan, Sokh – another Uzbekistan exclave in Kyrgyzstan, Barak – a Kyrgyz exclave within the Uzbek province of Andijan, Chon-Qora – two Uzbek village exclaves in Kyrgyzstan, and similarly Jani-Ayil – an Uzbek exclave within Kyrgyzstan) makes the region difficult to navigate when it comes to determining which ethnic group controls the local lands. While the exclaves usually denote the predominance of the motherland ethnic group within the small territory inside its neighbor, there are also some anomalies, such as the Uzbek exclave of Sokh within the Batken Province of Kyrgyzstan, which is almost entirely populated by ethnic Tajiks with Uzbek citizenship. Apart from the complexities of the national exclaves, historically the Kyrgyz Osh Region (with the city of Osh – the second largest megalopolis in Kyrgyzstan) has been home to a large Uzbek diaspora (by percentage almost equal to that of local Kyrgyz population), and similarly the Samarqand Region in south-west Uzbekistan with its second largest city Samarkand is the home to ethnic Tajiks, who in fact count for 70% of the local population.

Rashid Gabdulhakov provides perhaps the most comprehensible overview of the Fergana Valley enclaves/exclaves, as well as the historical perspective on the reasoning around their original formation:

> The emergence of Ferghana Valley enclaves is usually explained via the assumption that during the formation of the USSR land units were allocated to a country based on the language spoken by its inhabitants. For instance, since the majority of the people in Barak village spoke Kyrgyz, the land unit was given to the administration of the Kyrgyz Republic, despite the fact that this land unit is located inside Uzbekistan. Border demarcation between the

"brotherly" Soviet republics was carried out in a manner that complicates border negotiations today.[1]

Tajik-Kyrgyz border clashes as of May 2021.
©Radio Free Europe/Radio Liberty[2]


TAJIK/KYRGYZ BORDER CLASHES
Updated on May 7, 2021

Several thousands of people, mostly Kyrgyz, have fled their homes.

At least four dozen people were killed thus far and more than 200 reported injured.

RadioFreeEurope RadioLiberty
C. Coelho | Sources: RFE/RL's Tajik and Kyrgyz services

[1] Gabdulhakov R. (2021), Geographical Enclaves of the Fergana Valley: Do Good Fences Make Good Neighbors?, p. 2.

[2] https://www.zois-berlin.de/en/publications/spiralling-violence-on-the-borders-in-the-fergana-valley.

Separately from the issues of national exclaves, the existing road and utilities infrastructure in the border regions de facto transform some of the sovereign villages into pene-enclaves/pene-exclaves, where the local population needs to choose between physically using its own national services or for the purposes of convenience it would rely on the services of its neighboring country. A typical example can be drawn by looking at the functioning of a Kyrgyz village Dostuk close to the Tajik border – a Bishkek-based expert on border issues between Kyrgyzstan and Tajikistan, Asel Murzakulova, describes the situation clearly:

> The only road through which the residents of Dostuk village could reach the administrative center of the District [= Kyrgyzstan], and the wider region, ran through Tajikistan's territory. Thus, Dostuk village was a peni-enclave: a territory that can only be accessed via the roads of the neighboring state. Dostuk village was not only dependent on Tajikistan's road infrastructure, but was also widely integrated into other infrastructures belonging to Tajikistan. For example, before 2003, the village was connected to Tajikistan's electricity system via Tajikistani electric lines, the only cell phone reception available for Dostuk village is provided by Tajikistani companies, and the irrigation and drinking water is supplied from Tajikistan. Kyrgyzstani television channels are not broadcast to the village, and the most accessible way to learn news of what is happening in the outside world is through media from Tajikistan.[3]

The gradual establishment of strict border posts between Kyrgyzstan and Tajikistan make it difficult for the local populace to tend to their livelihood – farming – as the cadastral delineations between the actual villages and the agricultural land belonging to the village population are disconnected from each other by the neighboring country territory:

> Dostuk has limited agricultural land, only covering the basic household need for vegetables, not enough to produce crops for sale. During the privatization of land following independence, the collective farm employees each received 11 acres of land, and all the other villagers were allocated 8 acres each. Fields of Dostuk residents were, however, disconnected from the village because they were located beyond the neighboring Tajik village. To irrigate their fields nowadays, farmers from Dostuk either have to cross a border post and enter into Tajik territory, walking only 200 meters along an asphalt road, or if wishing or needing to stay within Kyrgyzstan, they must travel 15 km on a mountain road further in order to reach a water source. The choice was obvious, before border posts were erected next to the village.[4]

[3] Murzakulova A. (2018), Challenges of Social Cohesion and Tensions in Communities on the Kyrgyz-Tajik Border, pp. 12-13.

[4] Ibid, p. 14.

The aforementioned border area idiosyncrasies between Kyrgyzstan and Tajikistan have deep roots in the 1920's and early 1930's, when the process of a so-called national-territorial delimitation for the Soviet Central Asia was finalized and borders between then Soviet Socialist Republics were demarcated (for the discourse of Kyrgyz-Tajik relationship and their territorial division, the date of February 1924 – when the Soviet Central Committee commenced the process of final delineation – is usually referenced, hence in the minds of contemporary geopolitical experts it is 98-year history still in the making. The end of 1936 which saw a final form of border demarcation among the five Soviet Central Asian republics also laid foundation for 1991 inter-country border lines when the Soviet Union disintegrated.

The process in the period between the first two world wars that led to demarcation of sovereign borders among the countries of Central Asia is a complex one, and today's Kyrgyzstan was created only in 1936. In both its previous local precursors, the Kara-Kirghiz Autonomous Oblast (established in October 1924) and the Kirghiz Autonomous Socialist Soviet Republic (established in February 1926), the Kyrgyz national entity existed as part of the Russian Soviet Federative Socialist Republic. Only in December 1936, after the adoption of the Soviet Constitution, it became a fully-fledged constituent of the Soviet Union – but the borders were not delineated along the ethnic or linguistic lines, and instead the intermixed form putting together the major regional ethnic groups – Kyrgyz, Uzbeks, and Tajiks – remain to this day. As for the Tajik ethnic population of the area, they also feel unjustly "carved up" or "mixed in", as the original Turkestan Autonomous Soviet Socialist Republic, spanning from the shores of the Caspian Sea to China, was initially divided between Turkmen and Uzbek Soviet entities. The Tajik SSR was subsequently created from within the Uzbek SSR, to accommodate the Tajik (= non Turkic) population inhabiting the area, but the three regions dominantly populated by Tajiks – Samarkand, Bukhara and Surkhandarya – remained within the Uzbek SSR.

The individual historical milestones within the history of Kyrgyz-Tajik relations, be it during the Soviet Union or as part of past 30 years of independence of respective Central Asian republics notwithstanding, the current stalemate around the obvious unwillingness to conclude any permanent solutions to the problem highlights a broad spectrum of imminent concerns that need to be addressed on a micro-economic level before any all-inclusive peaceful resolution is achieved.

2. Kyrgyz-Tajik Conflict within the Last 30 years of Independence

In the wake of September 2022 border clashes, which during the first day reported 24 dead and 200 injured on the Kyrgyz side, with almost 150,000 local population fleeing the Batken Region towards the capital Bishkek, a former Kyrgyz Government official in a private conversation clearly stated that the conflict is about 98 years in the making (referring to the 1924 original USSR border delineation process) and that the issue can, must and will be resolved only within bilateral relationship between Kyrgyzstan and Tajikistan. He also categorically excluded any possibility of CSTO, OSCE, UN or even NATO intervening in the conflict or mediating it – the border issue has been set long before the existence of any of these regional or multinational organizations, and they have no right to be involved.[5]

Tajikistan on its part was too preoccupied most of the 1990's with her own bitter and devastating Civil War which essentially ended in a stalemate and Dushanbe is still not in full control of the Badakhshan Mountainous Autonomous Region (or Gorno-Badakhshan, often abbreviated as GBAO). The status of the largest of the Tajik enclaves inside Kyrgyzstan, Vorukh, is much less consequential to the overall well-being of Tajikistan, compared to that of internal territorial issues, nevertheless in the renewed 2022 border conflict the enclave of Vorukh seems to be the focal point of the dispute, with reported objectives to link it territorially with "motherland" Tajikistan by a corridor.

The Batken Region where the enclave of Vorukh is located is a no stranger to clashes between the armed forces of Kyrgyzstan and external militant forces from the late 1990's – in a series of confrontations the members of the Islamic Movement of Uzbekistan (IMU) intruded into Uzbekistan and Kyrgyzstan from the Tajik territory in summer 1999, the situation eventually witnessing the Uzbek armed forces joining their Kyrgyz counterparts in expelling the militants (the events collectively dubbed the "Batken Conflict"). While some of the radical elements retreated to Tajikistan, the incursion ended in both political and reputational fiasco for the Uzbeks and the Kyrgyz, with far reaching international implications when the Japanese government reportedly resolved to paying the ransom for a Japanese geologist abducted during the original incursion.[6]

[5] By the account of S.B.B., a former Colonel in the Soviet KGB and Kyrgyz GKNB, who also participated in a Kyrgyz Government committee in 2000's on the border issue resolution with neighboring countries.

[6] Details on the Islamic Movement of Uzbekistan with the instance of a Japanese national kidnapping are outlined in "Security Terrorism Society" No. 14 from November 2021, in the

While the Batken Conflict was not instigated by Tajikistan per se, it showcased the utilization of the Tajik territory as a safe haven for radicalized militants posing the threat to all neighbors, and also the fact that two years after the nominal end of the Tajik Civil War, the Government in Dushanbe was still not in control of many of its border territories. The Batken Region itself was created in October 1999 (by carving out the western Osh Region) as a response to the IMU incursion, and as one of the consequences, the Kyrgyz-Uzbek relations became strained, especially when the Uzbeks started to seal off the border area and openly declared their readiness to launch military operations into Kyrgyzstan if needed (ostensibly to preempt any future attacks from rebel hotbeds in the region).

Towards the end of April 2021, following the local Kyrgyz and Tajik residents' skirmishes around a water supply facility in Batken Region, the dispute quickly turned deadly with heavy military equipment used, leaving 55 casualties on both sides after the four days of infighting. Just with the September 2022 military clashes in the same region, occurring during the Shanghai Cooperation Organization summit in Samarkand, the April-May 2021 confrontation happened during a CSTO meeting of national Security Council Secretaries under the Tajikistan's chairmanship.

While the use of water resources for agricultural purposes was contested between the Kyrgyz and Tajik farmers in the Soviet era too, for the period prior to the most serious military clashes in 2021 and 2022, respectively, Kemel Toktomushev of the University of Central Asia in Bishkek recapitulates that:

> In general, the years of independence for both Kyrgyzstan and Tajikistan have been marred by conflicts on the borders of their Batken and Sughd prov-inces, respectively (for instance, in 2000, 2003, 2005, 2008, 2011, 2014, 2015). Per some reports, in the period from 2011 to 2013, there were 63 incidents on the Kyrgyz-Tajik border, ranging from small fights to hostage taking.[7]

3. The Blame-Game – a New Name of the Game?

While the original address to the United Nations General Assembly by the Kyrgyz President Sadyr Japarov was exclusively focused on sustainability issues surrounding high mountain economies, the actual speech delivered on September 20, 2022 in New York reflected almost exclusively the ongoing Kyr-

article "Regional Ramifications for Taliban-Controlled Afghanistan – Role and Position of Uzbekistan on Islamic Fundamentalism 1991-2021" by the author.

[7] Toktomushev K. (2018), Understanding Cross-Border Conflict in Post-Soviet Central Asia: The Case of Kyrgyzstan and Tajikistan, p. 27.

gyz-Tajik relationship crisis.[8] President Japarov briefed the General Assembly of historical milestones regarding mutual agreements among ex-Soviet republics since the Kyrgyz Republic gained independence in 1991, emphasizing those agreed upon with Tajikistan. For the April 2021 and September 2022 military incursions into the Kyrgyz territory by Tajik armed forces, Japarov placed the blame entirely on its neighbor. While further negotiations, using international intermediaries if needs be, are apparently a preferred method of the Kyrgyz leadership to resolve the issue, Japarov made it clear that Kyrgyzstan does not intend to surrender any of its sovereign territory.

The United Nations General Assembly address by the Tajikistan's representative, the Foreign Minister Sirojiddin Muhriddin, delivered four days later, was more multi-lateral in nature, making a mention of terrorism in general, water security, climate issues. A great emphasis in the Foreign Minister's speech was put on the issue of Afghanistan. Referring to the nation as a "fallen state" and elaborating on multiple socio-economic issues, including lack of respect for basic human rights, emergence of new terrorist groupings vis-à-vis inept Taliban government, and essentially the country becoming a "new hotbed of tensions" near Central Asian nations' borders, the Minister demonstrated a possibility that Afghanistan is already on the path of Tajikistan in early 1990's when the Tajik nation entered a devastating Civil War.[9]

Only then the Tajik Minister turned to the question of the current border conflict with Kyrgyzstan, first criticizing the very address of the Kyrgyz President who raised the issue at the General Assembly. Continuing with further criticism of its neighbor for "deviating from the reached agreements", he actually openly accused Kyrgyzstan of being the aggressor in the ongoing dispute. While drawing some comparison to the Tajik-Chinese and Tajik-Uzbek border issues that have already been resolved, the Tajik representative concluded by referring to the 1924-27 Soviet era decisions on national-territorial delimitation as the only legal framework for further negotiations, giving some limited leeway to the Kyrgyz propositions made in 1989 as part of parity commission deliberations.

The former Member of the Kyrgyz Parliament and the country's Ombudsman, Dr. Toktokuchuk Mamytov, in a televised interview on September 19 focused on the many details of the September 14-16 border clashes that were either omitted in general media reporting, or were brought to the attention of the public only superficially. He underlined that the military

[8] As per the Presidential Adviser in charge of Mountain Issues who personally notified the author on changes in the President's UN address.

[9] Address by the Minister of Foreign Affairs of the Republic of Tajikistan Sirojiddin Muhriddin at the General Debates of the 77th Session of the General Assembly of the United Nations, September 24, 2022, p. 5.

incursion from the side of Tajikistan could not have been spontaneous, but carefully prepared, citing the fact of an obvious mobilization of the Tajik armed forces. He also mentioned the presence of seasoned fighters (not the young conscripts that on the Kyrgyz side were called to arms to defend the territorial integrity) – apparently witnesses spoke of "older men, with long beards, in black military outfits not displaying clear marks of adhering to any particular national army".[10]

Responding to a question why the losses on the Kyrgyz side were relatively heavy (more than 60 people dead on the Kyrgyz side, and close to 150,000 local Batken Region inhabitants being evacuated, in effect instantly becoming internally displaced population), Dr. Mamytov stresses the circumstances where the country was taken by surprise and was not able to mobilize the corresponding army units (for such mobilization, at least 48 hours would have passed by), and that even the information possessed by the State Committee for National Security of the Kyrgyz Republic (GKNB) was scarce and incomplete. The Kyrgyz scholar also highlights the very fact that the Fergana Valley – where most Central Asian territorial disputes occur – also happened to be a place not so far from another Tajik-majority populated Uzbek city of Samarkand, where the Shanghai Cooperation Organization summit was taking place during the border skirmishes. He added ironically that while some global questions are being addressed and perhaps solved at the summit, new conflicts are being set up in the neighborhood.

Displays of mutual distrust between Kyrgyzstan and Tajikistan can be seen everywhere – in the summer 2022, five post-Soviet Central Asian nations convened for a consultative summit at the Lake Issyk-Kul in Kyrgyzstan, and the media following the event must have noticed from the onset of the meeting that most photo opportunities were zoomed in onto the leaders of Uzbekistan, Kazakhstan and the hosting Kyrgyzstan, with the presidents of Tajikistan and Turkmenistan ostentatiously missing. An observation was provided in the interview of Dr. Mamytov – directing attention to some of the obvious precursors of the September military clashes. At this July 2022 Fourth Consultative Meeting of the Leaders of Central Asian States in picturesque city of Cholpon-Ata, on the shores of the Kyrgyz Lake Issyk-Kul, it was namely Tajiki-

[10] Televised interview of Dr. Toktokuchuk Mamytov in "Real View with Rita Mukalaeva", September 19, 2022, https://youtu.be/_moAZk4KNY8. The implied message regarding the physical description of the deployed fighters from the Tajik side was that these may have been non-Tajik mercenaries – given the porous borders between Tajikistan and Afghanistan, it cannot be excluded that foreign radical fighters for hire are being used in the Kyrgyz-Tajik border conflict. While the Taliban-controlled Kabul may not want to be associated with any regional non-Afghan related conflicts, the real threat, according to Dr. Mamytov, stems from the extremist groupings within Afghanistan that are not controlled by the Taliban.

stan and Turkmenistan that declined to sign the "Agreement on Friendship, Good-Neighborliness and Cooperation for Development of Central Asia in the 21st century" (envisaged as a meeting's hallmark declaration, proposed by the Kazakh president Tokaev during the previous consultative summit), with Tajikistan referring to the "need to consult the Parliament" in order to sign the document. While the position of Turkmenistan not to enter any particular conflicts in the region, but also any special friendship frameworks either, as part of their "Bitarap" (neutral foreign policy) stratagem may be understandable (on top of the fact that the new Turkmen president, the son of the previous head of state, was installed into position only in March 2022), Tajikistan's position was both the slap in the face of the summit's host, as well as laughable excuse. As Mamytov put it bluntly, "the Tajik Parliament is the more rubber-stamp body than ours", and the outright refusal of the Tajik President Rahmon to join the declaration should have raised the red flags in the eyes of the Kyrgyz leadership already in the summer 2022.

4. The Vector of a "Third Party" at Play?

Given the centuries of world superpower's interference in the Central Asian affairs, it is understandable that every conflict, whether a reoccurring old one or a newly created one, draws various theories regarding a "third party" stirring up the decades old animosities into the open confrontations. While the local population's finger pointing vaguely at the "West" can be frequently encountered without providing any specific evidence, the mere issue of such accusations merits some examination. Certainly, Dr. Mamytov in his televised interview was also asked whether he sees any other player present at the roots of the current hostilities, but he restrained himself to noting that the role of the regional Shanghai Cooperation Organization continuously grows to more global dimensions, and "perhaps someone does not like it".

Another Kyrgyz political analyst, commenting on the issue privately, spoke in a more direct fashion, showing in the direction of the USA and United Kingdom. For one, he says, the US troops conducted military exercises in Tajikistan just a month before the September 14 clashes, hinting on a possibility that the Tajik armed forces may have been given opportunities to "rehearse" the incursion. As another indication, the expert mentions the long-term presence of one of the Tajik president's daughters, Ozoda in the United Kingdom (herself a career diplomat having served, among others at the Tajik Embassy in Washington, as well as the Head of Presidential Administration and the country's parliamentarian), from where she wages a successful information war beneficial to the Tajik cause "with the corresponding local counterparts".[11]

The expert also goes further in depicting the (lack) of power play surrounding the current Kyrgyz president Japarov – and as such, he (and consequently also his country) is susceptible to third party manipulations aimed at general instability in all of the Central Asian region, also hinting at a possibility of another "color revolution" that may already be overdue in Kyrgyzstan. While most of the other post-Soviet Central Asian republics essentially took almost 30 years to change their leadership originally installed after the break-up of the Soviet Union[12], Japarov is a leader who came in by revolution, a phenomenon being an idiosyncrasy in Central Asia everywhere except for Kyrgyzstan. In all other "Stans", the leader is firmly embedded in his presidential position and most of opposition is either in jail, detention centers or in exile. Japarov is, according to the political analyst, a proverbial white crow – and because he did not come to power by usurping the government, he is not recognized by the others "as one of their own". In other words, Japarov is an exception (which probably can be applied to every Kyrgyz president who came to lead the country after Askar Akaev, and whoever will eventually replace Japarov), and as a such, the other Central Asian leaders have very little to offer to him to bring stability to the border region with Tajikistan. The expert is not afraid to voice a concern that whatever the original cause for the border hostilities may have been, the other Central Asian leaders may see the situation even as an opportunity to conspire against Japarov, and perhaps replace him with someone "more acceptable to the club". As an unofficial adviser to the president Japarov, the expert already suggested to the president to be closer to the Russian president Putin back in February 2022, with the unfolding situation around strained Russia-Ukraine relations in the background. Instead, Japarov started to take internally, and declare publicly, a rather neutral position regarding the Russia-Ukraine conflict (with more than one million Kyrgyz citizens working in Russia as temporary workers, it may have been at least a logical step to voice some support for Putin), and as a result, Putin may have chosen not to get involved personally in the Kyrgyz-Tajik border issues. According to

[11] By the account of L.B.S., an official of the Administration of the former president Almazbek Atambayev. As a prominent Kyrgyz political analyst he has close relations to the current presidential administration, and while most of the Atambayev former staff (including Atambayev himself) have been indicted on various charges related to that period of Presidency, L.B.S. has never been implicated in any accusations of wrongdoing.

[12] Tajikistan is essentially ruled by the same president that came into power in early 1990's, Uzbekistan and Kazakhstan changed their leaders relatively recently, and Turkmenistan cosmetically exchanged the person in the top post in 2022 within the family succession of the previous president.

the expert, one phone call placed from Vladimir Putin to Emomali Rahmon would have at least stopped the military actions, and Russia could have successfully brokered some kind of provisional agreement between the Kyrgyz and the Tajiks. The consequences of a diplomatic stalemate between the two countries may have some specific ramifications – in the process of regulating the conflict the Tajiks cling onto the Soviet era border delineation of the 1920's, and the extreme consequence could be that by spring 2023, Tajikistan will overtake the territory of all Batken Region.[13]

While the Kyrgyz border situation did receive some limited international media attention (less than ongoing Azeri-Armenian conflict, and much less than the Russo-Ukrainian war), the problem, according to the expert, also lies in the fact that the US does not fully believe the Japarov's supposedly neutral stance towards Russia. Therefore it will not be the USA, nor Turkey, nor any Western alliance such as NATO that could come "to the rescue", and if Japarov is not taken to the "Club of the Stans" by Putin, Russia also has very little to offer in terms of long-term solutions to the issue. In effect, Japarov is an individual "alienated among his own" and very little is being envisaged to change while he is in the top country position. China may be the only regional power that could hypothetically assist in regulating the permanent demarcation of Kyrgyz-Tajik border, the question is whether she wants to. The last, but not least, an important factor is in Tajik side's military preparedness for any offensive or defensive maneuvers, given their comparatively high degree of "war experience" through their own civil war. The expert concludes that just like the hybrid war in Ukraine's Donbass region, the current conflict can essentially be described as an undeclared war by Tajikistan towards Kyrgyzstan.[14]

Now a very public political commentator and a former Kyrgyz intelligence officer, Colonel Taalaybek Djumadylov, does not shy from pointing a finger directly at the United Kingdom (as one of the long-term players in Central Asia's Great Game of the 19-20th centuries), and very specifically at its foreign intelligence service MI-6, calling the newest Tajik military incursion into Kyrgyzstan as the "greetings from MI-6 to SCO, CSTO and first of all – Russia".[15]

[13] From the numerous private conversations with L.B.S. in the days following September 14 Tajik incursion into Batken region.

[14] L.B.S. who knows the Tajik president Rahmon personally, also asserts that Putin is the only remaining authority in the Central Asian region that could instigate changes in inter-regional relationships, and the only one whose advice or suggestion would be taken seriously by Rahmon.

[15] https://kundemi.kg/index.php?newsid=9849.

Djumadylov lays out in a way intriguing plan of action on part of the British intelligence seemingly not related to Kyrgyzstan at all, whereby the United Kingdom aims at utilizing the post-August 2021 power vacuum in Afghanistan by fragmenting the remnants of the republic into at least four parts, based on their respective ethnic composition – its western part with ethnic Hazaras to fall under the influence of Iran, Pashtus to be controlled by Pakistan, the Uzbek-populated north of the country to become Uzbekistan dominated and the north-eastern part to be embedded into Tajikistan's control. The legacy of the regionally celebrated anti-Taliban fighter leader, the "Lion of Panjshir" – an ethnic Tajik Ahmad Shah Massoud – and his United Front (now headed by Massoud's son) are one of the best instruments how to eventually diminish Taliban's control of Afghanistan and its vile influence in the neighborhood, and according to Djumadylov the MI-6 succeeded in convincing Emomali Rahmon that only he can unite the 12 million ethnic Tajiks living in Afghanistan with the 8 million in Tajikistan (which could then prove to be the only united formidable force to resist the Taliban). From the larger perspective, the new so-called Great Game 2.0, would eventually allow the British to confront Russia in the region of Central Asia. Then a legitimate question is – why is Kyrgyzstan being attacked by Tajikistan? Just as other Kyrgyz political observers, Djumadylov also underscores that the process of handing over the country's control to a family heir in Tajikistan faces certain problems, and by creating an illusion of the "external enemy", Rahmon was advised by his British handlers that he can smooth the task of power transition.[16]

5. Water as a Possible Focal Point of the Conflict

Tajikistan's relations have been tense within the last 30 years not only with Kyrgyzstan, but also with the other neighbor – Uzbekistan. And it is the water which is one of the contested issues – the author recalls a car trip from Uzbek Tashkent to Tajik Khujand in August 2013 over the land border – which was at that time still off limits to civilians of the both countries, and the only option to be able to cross the border by car was to make use of a vehicle with consular number plates. It takes a little less than an hour from Tashkent to reach the Uzbek side of the border – and at the height of the summer most

[16] Ibid. The ex-GKNB officer also illustrates that on the post-Soviet area, the succession into the hands of family members is nothing new, but there were "successful" examples as well as "failures". Azerbaijan or Turkmenistan count for more fortunate instances of straightforward transition of the country's control, while Kyrgyzstan's first President Akaev or Kazakhstan's Nazarbaev did not manage to transfer their control onto their relatives.

of the land that one passes through before reaching the border crossing is parched and dry. Right after crossing the border, however, a phenomenal sight opened – roads surrounded by the lush greenery, and any visitor would soon be greeted by the emerald color Kayrakkum water reservoir on the Tajik side. It did make one wonder why in a span of less than 50 km, one side of the border struggles to provide enough water resources to secure the agricultural needs, while on the other side the abundance of clean fresh water even makes it possible to provide the local population with a summer aqua-park.

Kayrakkum Reservoir near Khujand, Tajikistan[17]

A predominant reliance on agriculture and livestock breeding as local livelihoods in border areas between Kyrgyzstan and Tajikistan, where the coexistence of the two distinct ethnic groups is already exacerbated by the complex border demarcation and inclusion of several ethnic exclaves, gives way to a constant competition for water resources – used either for irrigation or the animal farms. A Kyrgyz expert on pasture resource management, Gulzana Kurmanalieva, observes that it is namely the relationship of upstream-living Tajiks (having abundance of water) and downstream-living Kyrgyz (being dependent on how much water is left for them) – the seasonally shared water channels are used at times of conflict to escalate the tensions:

> Further, water resources often serve as an instrument to put pressure on each other among the Tajik and Kyrgyz communities. Whenever there are other conflicts at the border territories, the communities block water canals to each other which causes new tensions and escalates the situation.[18]

Furthermore, the complicated Pasture Reforms in Kyrgyzstan in 1990's and the Land Reform in Tajikistan in early 2000's with their respective pro-

[17] Photo of the author, August 2013.

[18] Kurmanalieva G. (2019), Kyrgyzstan and Tajikistan: Endless Border Conflicts, p. 8.

visions aimed at protecting their own ethnic groups have resulted in mutual limitations as to the optimal use of the grazing land to which both communities may have an access, given the geographical composition of exclaves and overall form of the current border demarcation. While the certain legal frameworks have been enacted on both sides of the border, practical mechanisms on sharing of the water resources are lacking, and there seems to be no willingness on either side to address the issue.

> Water resources in the Kyrgyz – Tajik border regions are managed by the state, province and district levels. However, despite of existing institutions, many water conflicts remain due to a lack of precise mechanisms of transboundary water management.[19]

The Batken Region on the Kyrgyz side (where both 2021 and 2022 Tajik military incursions occurred) and the Sughd Province on the Tajik side rely on livestock and farming, with the Tajiks being dependent on water resources controlled by the neighboring Kyrgyzstan. The April 2021 clashes, deadliest in the 30 years of the post-Soviet period of independence, also caused over 30,000 Kyrgyz inhabitants to flee the region, making them effectively internally displaced. Most observers agree that in this instance, the source of Isfara River water used by the three communities around the Fergana Valley alike – Uzbeks, Kyrgyz and Tajiks, was the cause of the dispute when the Kyrgyz inhabitants spotted the Tajik personnel installing surveillance equipment around the water intake facility. The local Kyrgyz villages coming under the military attacks from Tajikistan, resulting in the houses and the local school burned down and looted, drew even calls by the international community to investigate the alleged war crimes perpetrated by the Tajik armed forces.

6. Issues of Tajik Presidential Accession and Other Internal Factors at Play

Keeping the members of the leaderships of the five post-Soviet Central Asian countries “in a Club” (and from the historical superpower point of view to keep this Club revolving around Moscow leadership) always poses one question – how to keep the internal national influence within one clan, one family, and one succession line. With Uzbekistan, Kazakhstan and Turkmenistan having recently changed their respective nominal heads of the state, and with Kyrgyzstan permanently prone to a periodic change of guard, only Tajikistan finds itself today within a strong grip of a man who came to the country’s presidency in 1994. While officially the third President of the

[19] Ibid, p. 8.

independent Tajikistan after the break-up of the USSR, Emomali Rahmon has been in charge of the country almost from the onset of independence in 1992, having presided over all the period of Tajik Civil War. Having succeeded to "constitutionally designate" his eldest son Rustam as an official successor to the presidency (Rustam currently holds the title of the Chairman of the National Assembly of Tajikistan as well as the Mayor of Tajikistan's Capital Dushanbe), Rahmon Senior probably starts to feel the limitations of his age and accompanying health. The obvious obstacle to a smooth succession process, should Rustam be put in charge today, is Rustam's tender age of 34 – although he has been groomed for the top post long enough by the virtue of being the family's eldest son (including having been promoted to the rank of Major General of the country's armed forces), he may not smoothly fit into the "Club" as a leader supported by all sections of Tajik society. One thorny issue that the Tajik leadership has not coped with in the past 30 years is the status of the Badakhshan Mountainous Autonomous Region which makes up almost half of the country's territory, and the ethnic strife between its indigenous Pamiris and the Tajiks that was at the core of Tajik Civil War of 1992-1997. While the war nominally ended in June 1997, in practice it resulted in a military stalemate, with Dushanbe unable to control the GBAO region and its socio-economic development. The autonomous region serves to this day as the bastion of opposition, and many of its prominent political figures direct its actions from exile in Western Europe. Together with the issue of Tajik exclave of Vorukh in Kyrgyzstan's Batken Region, it represents a serious challenge to the Tajik leadership in the sense of both territorial integrity as well as national cohesion.

In the view of the political analyst Dr. Mamytov, one way to hand over the power in Tajikistan from the father to son in an unhindered fashion would be to artificially (and temporarily) unite the country's opposing factions around an "international" issue – with this issue being the border conflict with the neighboring Kyrgyzstan. According to Dr. Mamytov, one of the ways to try to solve these internal Tajik issues is to find a common enemy that will in part deflect some attention from these pressing questions, and in part could be to blame should an internal national dissent become visible. Tajikistan clearly cannot afford to designate Afghanistan, Uzbekistan or China as its perceived enemy, and the regionally weakest Kyrgyzstan takes on this position. Both the GBAO and Vorukh exclave are local barrels filled with gunpowder, ready to explode at any moment.[20]

[20] Televised interview of Dr. Toktokuchuk Mamytov in "Real View with Rita Mukalaeva", September 19, 2022, https://youtu.be/_moAZk4KNY8.

7. New Approaches towards the Problem Resolution Needed

Dr. Mamytov emphasizes that coming to the negotiations table with own versions of the delineated maps does not help anymore, and a new methodology needs to be adopted should both parties wish to come closer to resolution of the conflict. In his view, a "hot phase" of the Kyrgyz-Tajik border dispute started in 2002 when the two sides commenced a process by which they hoped they would finally demarcate the border to mutual satisfaction. This was also the time when the Kyrgyz-Uzbek, Kyrgyz-Kazakh and Kyrgyz-Chinese border demarcation issues had more or less been completed.[21] The Kyrgyz-Tajik undertakings regarding the border delineation were relatively problem-free until 2010 – during that time the borders in the mountain area with minimum population on both sides were being agreed upon (around 511 km). The difficulties arose when the 460+ km section of the border going through the populated valley started to be negotiated – this is where the talks entered a dead-end and the political stalemate ensued. In the period of 2013-2014 when the CSTO offered to become an intermediary in the conflict following a round of violence at the border, the Kyrgyz side was content to have this regional organization arbitraging the situation, but the Tajiks found it impossible to accept. Therefore, Dr. Mamytov concludes, before any third party is introduced as a facilitator or mediator, the two sides need to ratify within their respective Parliaments the acceptance of the international arbiter and also the modus by which they would accept the ultimate decision. The expert is also considering a notion that the Batken Region, being the constant target of Tajik military incursions, should be fortified with some kind of permanent armed outpost set up there – but the militarization of the Kyrgyz side of the border is not a solution in itself, and continuation of peaceful diplomatic approaches, without Kyrgyzstan becoming a perpetrator in international relations, needs to be secured. And to avoid more bloodshed in the future, some non-standard approaches need to be adopted, including the launching of the information offensive, making sure that "the world sees the true face and intentions of the opponent".[22]

A Kyrgyz political commentator, Bakyt Baketaev, in May 2021 after the military scuffle at the Kyrgyz-Tajik border in April, drew a parallel between the never-ending Israeli-Palestinian territorial conflict and the escalating si-

[21] Out of 1,400 km of the border shared between Kyrgyzstan and Uzbekistan, about 15% is still subject to a definitive agreement on demarcation. The future of the Kempir-Abad water reservoir, between the Uzbek Andijan Province and the Kyrgyz Osh region, was being discussed by the two sides in late September 2022, as it remains one of few disputed territories between Kyrgyzstan and Uzbekistan.

[22] Ibid.

tuation at one of the Central Asian borders – noting that the violent approach towards the solving of each other's territorial claims in Palestine started after the demise of the Ottoman Empire, clearly suggesting the similar fate was waiting the post-Soviet nations as well. He also stresses the (in)effectiveness of involvement of international organizations in resolving the bilateral issues if the interests of the involved states do not overlap with those of international arbiters. That way, he considers it a grave mistake to allow the United Nations establish the enclaves of Gaza and the West Bank, calling them the "political appendicitis" – their formation did not contribute to solving any post-Second World War issues, and to the contrary created new problems that cannot be solved for decades. He also provides his political formula for solving international conflicts as follows:

$$P = (NI - Gov) \times (II + St)$$

where P – Peace, NI – National Interest, Gov – Government, II – International Institutes, St – States.[23]

8. Conclusions

The freshly revived border conflict in the Kyrgyz Batken Region is nowhere near a solution, and the effects of the September 2022 military incursion from the side of Tajikistan will linger for some time to come. The Kyrgyz President Japarov decided not to attend the CIS summit in St. Petersburg on October 7 (following the decision of the Kyrgyz Head of State not to organize planned CSTO drills on the territory of Kyrgyzstan), giving way to several speculations what made him suddenly distance himself from the regional organizations that the country has been so far firmly embedded in. While the official explanation of the Presidential Administration pointed to Japarov "being too busy to attend", most observers immediately saw a most likely cause – just a few days ago on October 4, on the eve of the Tajik President's birthday, Vladimir Putin decreed to award Emomali Rahmon with a Russian state order "For Merit to the Fatherland". While the 70th anniversary of the nation's chieftain may have been celebrated by the Tajik society and such an award may have been in place to recognize Rahmon's "loyalty" towards the ideas of the Commonwealth, the wording for the reason of the award citing the Tajik President's "personal contribution towards the regional stability and security" triggered an outright discontent throughout the Kyrgyz political le-

[23] https://www.vb.kg/doc/401482_kluch_k_resheniu_kyrgyzsko_tadjikskogo_prigranichnogo_konflikta_v_ierysalime.html.

adership.[24] Japarov's absence at the CIS summit in Russia (where even the Azerbaijani and Armenian leaders sat behind the table) also further added insult to injury as the summit was set on the day of Putin's own birthday, and in this way most certainly the Kyrgyz President managed to display a symbolic gesture of disaffection with both the regional "leader", as well as his current neighborhood nemesis. The Kyrgyz political analyst Bakyt Baketaev summarized the circumstances of Japarov's absence at CIS Summit as:

> There is a period of cooling down of the Kyrgyz-Russian relations. But I would not recommend to Bishkek to force the decreasing of this "temperature". The history shows that no post-Soviet republic found it useful to engage in a similar process. In diplomacy, emotions need to be set aside.[25]

The region of Central Asia has been at the crossroads of several civilizations, empires and hegemonies for centuries, and both its geographical and cultural importance increases even more during the new global conquests for influence and control. It would be naïve to assume that any bilateral relations derive its root causes and principles only from those two respective nation-states – the history indicates over and over again that the multiple factors playing their role often include even the most geographically distant contenders. The Kyrgyz-Tajik border issue, being only a segment of a wider spectrum of Kyrgyz-Tajik national affairs, is in itself a solidification of problems that need both regional and international attention to solve. As a prime example and indication of what shape and form can seemingly a local thorny issue take when left untreated, a border skirmish leaving 60 young people dead today may become a fatality of several thousand tomorrow.

A former Kyrgyz Government official watches the re-emerged border conflict through the prism of potential destabilization of the Kyrgyz internal political order, referring to a potential need to reach out to other superpowers should the current Kyrgyz-Russian relationship not suffice for satisfactorily ensuring the Kyrgyz territorial integrity. Clearly, the only other superpower in question would be the United States, with the expert noting a possible conclusion of new Kyrgyz-US friendship treaty with a provision for re-instating the US military base in the country. The current Kyrgyz Ambassador to the

[24] A climax of the situation emerged on October 14 in Astana, where the Russian and Central Asian leaders (this time with the Kyrgyz President Japarov participating) met at the "Central Asia-Russia Summit" – at the round table the Tajik President Rahmon decided to give a very public and loud lecture addressed at the Russian President Putin, demanding "respect" for his nation and reminding the visibly humiliated Russian leader of the root causes of the fall of the USSR – the lack of attention to "small" republics, nations and their people – making even sure to add "the same as today there was no regard for cultures and traditions, with a willingness to assist in development", eerily forecasting the events that may be about to arrive.

[25] https://kundemi.kg/index.php?newsid=9974.

United Kingdom Edil Baisalov or the former Kyrgyz president Roza Otunbayeva are mentioned as the most prominent pro-Western individuals of the Kyrgyz national politics, who also studied and worked in the West. However, given the equal number of pro-Russian Members of the Parliament and strong pro-Russian links by the current administration, the expert cautions for a remote possibility of creating root causes for the civil war within Kyrgyzstan, should the internal political interests clash on the background of Kyrgyz-Tajik bilateral relations.[26]

It may be tempting to succumb to accusations of the one culprit most visible for causing the suffering of the local population, and the work of scholars and diplomats needs to focus on exposing the myriad of hidden factors that lie underneath the surface of obvious evidence. At times when the food and water security becomes paramount in particular to those states that are both capable as well as willing to sustain their own population with sufficient provisions, natural resources needed to support the national economies will be fiercely guarded and defended. At the same time it should not be forgotten that at times of global crisis it is the bold and shameless that usually come out of a conflict victorious, regardless of the apparent violations of international practice, and the weak and silent are the ones giving in. Instead of indicating which scenario may be the most probable in outlining the causes of the current border issues in Central Asia, the author will invite the readers to make their own judgment.

Acknowledgements

While Kyrgyzstan with its parliamentary mechanism and sometimes too frequently changing leadership comes closest to the Western notion of democracy, it is still a country where the echo of Soviet-era general oppression, cults of personalities, and the invisible hand of the national security apparatus lingers well into the present. Much of the ongoing border issue would have been impossible to fully comprehend from the Kyrgyz viewpoint without an individual input on part of several former national security officers and experts with their first-hand experience in several presidential administrations within the past 30 years. Even they would not have shared their most intimate inside knowledge on the issue without first establishing a certain level of comradeship – which takes both time and effort by establishing mutual credentials first. I am greatly indebted for their extended friendship and their

[26] By the account of L.B.S., an official of the Administration of the former president Almazbek Atambayev, following his own visit to the Batken Region with destructed villages at the beginning of October 2022.

willingness to speak on the subject-matter openly, albeit in the references they sometimes remain anonymous to protect their well-being at home. It is an earnest wish to find similarly brave individuals willing to share their views and analysis also on the Tajik side – the process of gaining similar friends will take time, but I believe in the sincere approach from both sides of the conflict towards the gradual peaceful resolution.

References

Abazov R. (1998), Practice of Foreign Policy Making: Formation of Post-Soviet Politics of Kazakhstan, Kyrgyzstan, and Uzbekistan, NATO Research Fellowship supported Paper.

Abdullaev K. and Barnes C. (eds.) (2001), Politics of Compromise – The Tajikistan Peace Process, Conciliation Resources, London, United Kingdom.

Address by the Minister of Foreign Affairs of the Republic of Tajikistan Sirojiddin Muhriddin at the General Debates of the 77th Session of the General Assembly of the United Nations, September 24, 2022, New York, USA.

Address by the President of the Kyrgyz Republic Sadyr Zhaparov at the General Debates of the 77th Session of the General Assembly of the United Nations, September 20, 2022, New York, USA.

Agreement between the Russian Federation, the Republic of Kazakstan, the Kyrgyz Republic, the Republic of Tajikistan and the People's Republic of China on confidence building in the military field in the border area (1996), the Document provided to the United Nations General Assembly, Shanghai, China.

Arynova A. and Schmeier S. (2021), Conflicts over Water and Water Infrastructure at the Tajik-Kyrgyz Border – A Looming Threat for Central Asia?, a Report by Water, Peace and Security.

Azizian R. (2006), Countering Islamic Radicalism in Central Asia, Article in Quarterly Journal, Winter Supplement 2006.

Baizakova Z. (2017), Border Issues in Central Asia: Current Conflicts, Controversies and Compromises, Revista UNISCI, No. 45 (221-234), Universidad Complutense de Madrid, Madrid, Spain.

Baldakova O. et al. (2021), Central Asia Forecasting 2021 (Results from an Expert Survey), Friedrich Ebert Foundation, OSCE Academy in Bishkek, SPCE Hub.

Bisig N. (2002), Working with Conflicts in Kyrgyzstan (Peace and Conflict Impact Assessment based on an Analysis of the Conflict Situation in Southern Kyrgyzstan), Helvetas Kyrgyzstan.

Bitabarova A. (2015), Contested Views of Contested Territories: How Tajik Society Views the Tajik-Chinese Border Settlement, Eurasia Border Review Volume No. 6, Issue 1 (63-81), Hokkaido University, Sapporo, Japan.

Blackwood M.A. (2021), Central Asia: Background and U.S. Relations, Congressional Research Service, Washington D.C., USA.

Brattsev I. et al. (2020), Media and Social Media Analysis on Religious Freedom and Violent Extremism in Central Asia: Cases of Kazakhstan, Tajikistan and Uzbekistan, Search for Common Ground. Washington D.C., USA and Brussels, Belgium.

Chekirova A. (2022), Social Media and Cross-Border Political Participation: A Case Study of Kyrgyz Migrants' Online Activism, Social Sciences Journal No. 11 (370), MDPI, Basel, Switzerland.

Chesterman S. (2002), Does Central Asia Exist? – Regional Politics after a Decade of Independence, a Paper to 32nd IPA Vienna Seminar on Peacemaking and Peacekeeping, International Peace Academy.

Chmykh E. et al. (2021), Mapping Fragile Areas: Case Studies from Central Asia, Geneva Centre for Security Sector Governance, Geneva, Switzerland.

Civil Society Briefs – Tajikistan (2011), Tajikistan Resident Mission, Asian Development Bank, Dushanbe, Tajikistan.

Colville R. (ed.) (2006), After Andijan – Tensions Mount in Central Asia, Journal "Refugees", Number 143, Issue 2, UNHCR, Milan, Italy.

Country Strategy for Development Cooperation – The Kyrgyz Republic and Tajikistan 2018 – 2021, Ministry for Foreign Affairs, Finland.

Cross-border Cooperation for Sustainable Peace and Development (Kyrgyzstan) (2016), a Project Report by United Nationa Peacebuilding Support Office and Peacebuilding Fund, Bishkek, Kyrgyzstan.

Dadabaev T. and Komatsu H. (eds.) (2017), Kazakhstan, Kyrgyzstan and Uzbekistan – Life and Politics during the Soviet Era, Politics and History in Central Asia Series, Palgrave Macmillan, New York, USA.

Engvall J. (2014), Kyrgyzstan and Tajikistan: Next in Line (as part of the book "Putin's Grand Strategy: The Eurasian Union and Its Discontents"), Central Asia-Caucasus Institute, Washington, USA & Stockholm, Sweden.

Epkenhans T. (2016), The Origins of the Civil War in Tajikistan – Nationalism, Islamism and Violent Conflict in Post-Soviet Space, Lexington Books, Lanham, USA.

Fergana Valley Five Year Humanitarian Trends Assessment – Aging Leadership, Economic Shocks, Decreased Funding and Reduced Resilience to Environmental Hazards (2017), An Analysis commissioned by Inter-Agency Regional Analysts Network.

Gabdulhakov R. (2021), Geographical Enclaves of the Fergana Valley: Do Good Fences Make Good Neighbors?, Central Asia Security Policy Briefs No. 14, OSCE Academy, Bishkek, Kyrgyzstan.

Grogan L. (2021), Civil War, Famine and the Persistence of Human Capital: Evidence from Tajikistan, IZA Institute of Labor Economics, Bonn, Germany.

Heathershaw S. and Mullojonov P. (2018), Elite Bargains and Political Deals Project: Tajikistan Case Study, Stabilisation Unit, United Kingdom.

Heathershaw S. and Roche S. (2011), Islam and Political Violence in Tajikistan, Ethnopolitics Papers, Exeter Centre for Ethno-Political Studies, University of Exeter, United Kingdom.

Hiro D. (2011), Inside Central Asia – A Political and Cultural History of Uzbekistan, Turkmenistan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkey, and Iran, Duckworth Overlook, London and New York.

Human Rights in Tajikistan – In the Wake of Civil War (1993), a Report by Human Rights Watch, USA.

Huttova J. et al. (2002), Education Development in Kyrgyzstan, Tajikistan and Uzbekistan: Challenges and Ways Forward, Open Society Institute – Education Support Program, Budapest, Hungary.

Iji T. (2010), Negotiating an End to the Conflict in Tajikistan, Ritsumeikan Asia Pacific University, Beppu, Japan.

Kassenova N. (2009), China as an Emerging Donor in Tajikistan and Kyrgyzstan, Russia/NIS Center, Institut Français des Relations Internationales, Paris, France.

Khalid A. (2007), Islam after Communism – Religion and Politics in Central Asia, University of California Press, Berkeley, USA.

Kuchins A.C. et al. (2015), Central Asia in a Reconnecting Eurasia – Tajikistan's Evolving Foreign Economic and Security Interests, Center for Strategic and International Studies, Washington D.C., USA.

Kuehnast K. et al. (2008), Whose Rules Rule? – Everyday Border and Water Conflicts in Central Asia, The World Bank Group, Washington D.C., USA.

Kurmanalieva G. and Crewett W. (2019), Institutional Design, Informal Practices and International Conflict: The Case of Community-based Pasture Management in the Kyrgyz-Tajik Border Region, Springer Open.

Kurmanalieva G. (2019), Kyrgyzstan and Tajikistan: Endless Border Conflicts, "The EU, Central Asia and the Caucasus in the International System" Online Paper No. 4, Berlin, Germany.

Kyrgyz-Tajik Border Conflict: Mutual Concessions Needed (2019), a Report by Central Asian Bureau for Analytical Reporting.

Kyrgyz-Tajik Border Disputes: Reasons and Ways of Solution (2020),a Report by Central Asian Bureau for Analytical Reporting.

Kyrgyzstan: Border Conflict (2022), Final Report by International Federation of Red Cross and Red Crescent Societies.

Malashenko A. (2012), Tajikistan: Civil War's Long Echo, Briefing Vol. 14, Issue 3, Carnegie Moscow Center, Moscow, Russian Federation.

Mankoff J. (2009), Russian Foreign Policy – The Return of Great Power Politics, A Council on Foreign Relations Book, Rowman & Littlefield Publishers, Inc., USA.

Matveeva A. (2009), Tajikistan – Stability First, Taiwan Journal of Democracy, Volume 5, No.1 (163-186), Taipei, Taiwan.

Matveeva A. (2009), The Perils of Emerging Statehood: Civil War and State Reconstruction in Tajikistan – An Analytical Narrative on State-making, Working Paper No. 46, Crisis States Research Centre, Development Studies Institute, London, United Kingdom.

Matveeva A. (2016), Divided We Fall... or Rise? Tajikistan – Kyrgyzstan Border Dilemma, Cambridge Journal of Eurasian Studies, London, United Kingdom.

McGlinchey E. (2021), The April 2021 Kyrgyz-Tajik Border Dispute: Historical and Causal Context, Crossroads Policy Brief No. 2, Crossroads Central Asia, Bishkek, Kyrgyzstan.

Migacheva K. and Frederick B. (eds.) (2018), Religion, Conflict, and Stability in the Former Soviet Union, RAND Corporation, Santa Monica, USA.

Minaeva Y. (2012), Research Report on a fact finding survey of the Vorukh-Shurab drinking water supply system conducted in the framework of the OSCE project "Towards sustainable water usage and management in southern Kyrgyzstan", OSCE Centre, Bishkek, Kyrgyzstan.

Murzakulova A. (2018), Challenges of Social Cohesion and Tensions in Communities on the Kyrgyz-Tajik Border, Research Report No. 2, The Mountain Societies Research Institute, University of Central Asia, Bishkek, Kyrgyzstan.

Ni V. et al. (2021), The Impact of Climate Change on the Dynamics of Conflicts in the Transboundary River Basins of Kyrgyzstan, Kazakhstan and Tajikistan, International Alert Kyrgyzstan.

Omelicheva M.Y. (2010), The Ethnic Dimension of Religious Extremism and Terrorism in Central Asia (a Study published in International Political Science Review 31(2)), SAGE Publications, USA.

Peña-Ramos J.A. et al. (2021), Water Conflicts in Central Asia: Some Recommendations on the Non-Conflictual Use of Water, Sustainability Journal No. 13 (3479), MDPI, Basel, Switzerland.

Rahimov M. and Urazaeva G. (2005), Central Asian Nations & Border Issues, Defence Academy of the United Kingdom, Surrey, United Kingdom.

Rashid A. (2000), Taliban – Islam, Oil and the New Great Game in Central Asia, I.B. Tauris, London and New York.

Reljić D. (2008), Political Extremism, Terrorism, and Media in Central Asia – The Examples of Kazakhstan and Kyrgyzstan, International Media Support, Copenhagen, Denmark.

Schmitz A. (2021), Revolution Again in Kyrgyzstan: Forward to the Past?, SWP Comment No. 8, German Institute for International and Security Affairs, Berlin, Germany.

Schmitz A. (2019), Tajikistan on the Road to Totalitarianism, SWP Comment No. 10, German Institute for International and Security Affairs, Berlin, Germany.

Slipchenko V.I. (1997), Russia's Political and Military Problems in Central Asia [Excerpt on Tajikistan], European Security Vol 6, No. 1, Lawrence, USA.

Stein M. (2015), Undemarcated Borders and Incidents of Violent Conflict in Central Asia, The Foreign Military Studies Office, Fort Leavenworth, USA.

Stronski P. (2016), Tajikistan at Twenty-Five, Carnegie Endowment for International Peace, Washington D.C., USA.

Tadjbakhsh S. (2008), International Peacemaking in Tajikistan and Afghanistan Compared: Lessons Learned and Unlearned, Les Études du CERI, No. 143, Sciences Po, Paris, France.

Tadjbakhsh S. (1995), National Reconciliation – The Imperfect Whim (Tajikistan), Columbia University, USA.

Tajikistan (2013), a Country Section from “Nations in Transit 2013”, Freedom House, Washington D.C., USA.

Tani O. (2008), Understanding the Civil war in Tajikistan through the Lens of Localism, Text of the Intervention at the 2008 ASIAC Conference: Central Asia and the Caucasus, Levico Terme, Italy.

Taylor S.C. (2009), Aral Sea Summit Highlights Water Impasse (Water Management: a Central Asian Security Concern), George C. Marshall European Center for Security Studies.

Toktomushev K. (2018), Understanding Cross-Border Conflict in Post-Soviet Central Asia: The Case of Kyrgyzstan and Tajikistan, Connections: The Quarterly Journal 17, No. 1 (21-41), Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, Garmisch, Germany.

Toshmuhammadov M. (2004), Civil War in Tajikistan and Post-Conflict Rehabilitation, Center of Slavic Researches, Hokkaido University, Sapporo, Japan.

Umarov A. (2021), Recent Border Clash between Kyrgyzstan and Tajikistan and Its Implications on Regional Cooperation in Central Asia, University of World Economy and Diplomacy, Tashkent, Uzbekistan.

UNHCR Global Report 2008: Central Asia – Operational Highlights.

Valieva S. (2014), Kyrgyzstan, Tajikistan: Land and Water Conflicts, Briefer No. 20, The Center for Climate and Security, World Bank Development Group.

Zenn J. and Kuehnast K. (2014), Preventing Violent Extremism in Kyrgyzstan, United States Institute of Peace Special Report 355, Washington D.C., USA.

Zhaimagambetov S. (2015), The Protracted Border and Territorial Disputes between Kyrgyzstan and Its Neighbors (a Master’s Thesis), U.S. Army Command and General Staff College, Fort Leavenworth, USA.

Websites

https://cabar.asia/.
https://www.drishtiias.com/eng.
https://eurasianet.org/.
https://fergana.ru/.
https://www.longwarjournal.org/.
https://www.voanews.com/.

Web-based Resources

https://youtu.be/fVwv3KEmg44.
https://youtu.be/_moAZk4KNY8.
https://iigsa.org/ukraine-war-the-central-asian-summit-disagreement/.
https://www.iwpr.net/global-voices/kyrgyz-tajik-border-violence-spurs-calls-compromise.

https://kabar.kg/news/politolog-v-konflikte-mezhdu-kyrgyzstanom-i-tadzhikistanom-nuzhen-posrednik-v-vide-kitaia/.

https://kabar.kg/news/zdes-zameshany-tret-i-sily-politolog-o-konflikte-na-granitce/.

https://kundemi.kg/index.php?newsid=9974.

https://kundemi.kg/index.php?newsid=9849.

https://www.vb.kg/doc/401482_kluch_k_resheniu_kyrgyzsko_tadjikskogo_prigranichnogo_konflikta_v_ierysalime.html.

https://eurasianet.org/kyrgyzstan-the-dashed-dreams-of-a-man-who-loved-his-land.

https://eurasianet.org/kyrgyzstan-looming-border-deal-with-uzbekistan-causing-discontent.

META SPACES:
COMMUNITIES, THREATS AND INTERACTIONS

Vetting e processi di radicalizzazione come pratiche di comunità digitali: dai TRA-I al metaverso

Barbara Lucini

Barbara Lucini (phd in Sociology and Methodology of Social Research), is Senior Researcher at the Italian Team for Security Terroristic issues and Managing Emergencies – ITSTIME.
She is coordinating the research activities of the EU Project – H2020 – CounteR – *Countering Radicalisation for a Safer World Privacy-first situational awareness platform for violent terrorism and crime prediction, counter radicalisation and citizen protection*.
She is adjunct professor of risk management and crisis communication at the Catholic University. 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 relation 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

This paper focuses on key findings emerged from the research activities conducted within the H2020 European project CounteR – Countering Radicalisation for a Safer World Privacy-first situational awareness platform for violent terrorism and crime prediction, counter radicalisation and citizen protection.
The central theme concerns vetting processes and their methodologies applied in multiple ecosystems for both Islamic and far-right radicalisation processes.
The theoretical perspective that we want to focus on is related to the cultural-narrative approaches and the declinations that these can operationally have in the field of socio-cultural intelligence.
The methodological perspective instead relates to the understanding of the context and operational ecosystem of such processes and of those weak signals or risk factors that can be useful to Law Enforcement Agencies to adapt and adjust TRA-I (Terrorism Risk Assessment Instruments) models to the contemporary and varied radicalisation processes.
The result is a work of primary importance for national security in a global context of strong radicalisation, for its methodological-operational implications and for the theoretical reflections that make it worthy of further study.

Il presente articolo si focalizza su alcuni risultati emersi dalle attività di ricerca condotte nell'ambito del progetto europeo H2020 – CounteR – Countering Radicalisation for a Safer World Privacy-first situational awareness platform for violent terrorism and crime prediction, counter radicalisation and citizen protection.

Il tema centrale riguarda i processi di vetting e le loro metodologie applicate in molteplici ecosistemi sia per i processi di radicalizzazione islamica sia per quelli relativi all'estrema destra.

La prospettiva teorica che si vuole porre all'attenzione è relative agli approcci culturali – narrativi e alle declinazioni che questi possono operativamente avere nell'ambito della socio-cultural intelligence.

La prospettiva metodologica invece si relaziona con la comprensione del contesto ed ecosistema operativo di tali processi e di quei segnali deboli o risk factors che possono essere utili alle Law Enforcement Agencies per adattare e adeguare i modelli di TRA-I (Terrorism Risk Assessment Instruments) ai contemporanei e variegati processi di radicalizzazione.

Ne risulta un lavoro di primaria importanza per la sicurezza nazionale in un contesto globale di forte radicalizzazione, per le ricadute metodologiche-operative, per le riflessioni teoriche che lo rendono meritevole di ulteriori approfondimenti.

Keywords

Radicalisation, Extremism, Vetting, Islamic, Right – Wing, Socio-Cultural Intelligence, Radicalizzazione, Estremismo, Islamico, Estrema Destra, Socio-Cultural Intelligence

1. Introduzione

Alla fine di Ottobre 2022 la Polizia di Bari ha arrestato un giovane di 23 anni Luigi Antonio Pennelli contestandoli di reati di terrorismo internazionale, propaganda, istigazione con finalità di discriminazione razziale, etnica e religiosa.

Il giovane tramite il canale Telegram Sieg Heil era in contatto con il gruppo di suprematisti bianchi e neo-nazista americano The Base. Il suo ruolo era quello di fare proselitismo e diffondere materiali video e volantini ad altre persone potenzialmente reclutabili. In questo contesto radicale, si era dimostrato anche disposto a compiere un sacrifico estremo a difesa della razza bianca.

Questo fatto è solo uno degli ultimi esempi di radicalizzazione transnazionale che travalicano confini geografici e culturali e che utilizzano l'ormai vasto panorama degli ambienti digitali, per creare contatti e diffondere visioni estremiste.

Nell'ambito del progetto europeo H2020 *CounteR – Countering Radicalisation for a Safer World Privacy-first situational awareness platform for violent terrorism and crime prediction, counter radicalisation and citizen protection* questo fenomeno è stato indagato ed esplorato nelle sue molteplici sfumature con particolare riferimento agli ambiti della radicalizzazione di estrema destra e quella islamica.

La riflessione teorica e metodologica che qui si vuole porre all'attenzione concerne la specifica attività di vetting ovvero di valutazione per fine di reclutamento che i membri di comunità radicali ed estremiste devono affrontare, per poter operare nell'ambito di quell'organizzazione.

Un fenomeno questo che si è osservato essere trasversale alle tipologie di radicalizzazione islamica e di estrema destra, in questo caso accomunate da alcuni elementi di interazione sociale e comunicazione mediale che poi diventano tipici nel momento di incontro con la cultura caratteristica sia essa islamica o di estrema destra. Esplorare e comprendere queste dinamiche sociali e i loro contesti di sviluppo e azione è un'attività fondamentale per la prevezione e il contrasto della radicalizzazione da parte delle varie agenzie nazionali e internazionali.

2. Processi di vetting, radicalizzazione islamica ed estrema destra

Il focus teorico sui processi di vetting colma un gap interpretativo che ha radici storiche lontane nell'ambito dei terrorism studies e degli studi sui processi di radicalizzazione.

L'attenzione iniziale su questi temi ha preso avvio con le analisi sulle dinamiche di radicalizzazione islamica per la quale due componenti fondamentali sembrano essere caratteristiche di questo processo: la componente ideologica – religiosa come driver per il proselitismo e la propaganda; la familiarità e i network familiari come componente operativa e di vetting nei processi di reclutamento e di filtro per la partecipazione ad organizzazioni estremiste.

Questo tipo di radicalizzazione aveva anche solide basi nei processi legati al fenomeno conosciuto come migrazione a catena e la loro applicazione nel campo delle organizzazioni terroristiche internazionali.

La sempre maggiore diffusione delle piattaforme social ha però inciso su questi fenomeni e portato allo sviluppo di forme sempre più complesse di radicalizzazione e delle sue dinamiche (Lucini, 2020). Inoltre, nel corso dell'ultimo ventennio i cambiamenti economici, politici e sociali di molte società hanno contribuito alla diffusione e alla pervasività di altre tipologie di radicalizzazione come quella di estrema destra, sempre più presente in vari ambiti della vita sociale, culturale e politica di molti Paesi europei e non.

In questo contesto anche la pandemia da Covid-19 ha inciso in modo preciso sia sulle modalità operative di tali fenomeni e la loro prevalente collocazione nei domini virutali sia sulla compressione temporale che ha cristallizzato, nell'urgenza, la nuova normalità così definita.

Nello scenario generale così caratterizzato, le piattaforme social sono state lo strumento più efficace e resiliente per la diffusione di contenuti estremisti, le possibilità di reclutamente ma anche per la capacità di mantenere attivi i network creati adattandoli e ristrutturandoli in seguito a cambiamenti endogeni al gruppo oppure esogeni come le varie regolamentazioni relative al contrasto alla radicalizzazione. Questa capacità intrinseca dei social è stata ben compresa e utilizzata proprio dallo Stato Islamico e poi adottata con quasi altrettanto successo dai gruppi di estrema destra come sottolinea Hutchinson et al. (2022).

I processi di vetting dell'una e dell'altra forma di radicalizzazione sono fondamentali per la comprensione delle dinamiche di selezione dei potenziali futuri radicalizzati e possono fornire indicazioni utili per l'identificazione di segnali deboli, fattori di rischio e vulnerabilità che possono condurre a questa condizione.

Un elemento importante emerso dalle attività di analisi e ricerca condotte concerne la possibilità di colmare il gap teorico nello studio e nell'analisi dei processi di vetting, considerando i gruppi estremisti e radicali non soltanto come gruppi sociali presenti nelle dimensioni online e offline ma come comunità di pratiche, originariamente identificate da Jean Lave e Etienne Wenger (Lave, 1991; Wenger, 2011).

Inoltre, considerando l'evoluzione tecnologica, è possibile identificare i gruppi estremisti come comunità di pratiche digitali (Archetti, 2015) per le quali la doppia dimensione di contesto – online e offline – non deve essere identificata come una modalità dicotomica oppositiva, quanto una digitalizzazione di modalità culturali e comunicative che possono avvenire ed essere presenti sia nella dimensione reale sia in quella virtuale.

In accordo a questa prospettiva le pratiche di vetting assumono caratteristiche culturali e identitarie precise ad un secondo livello di interazione, quando le persone assumono ruoli e funzioni più precise, mentre al un primo livello con una funziona più ampia di filtro, il vetting assume caratteristiche trasversali ai differenti orientamenti ideologici, come ricordano Davey et. al (2020) per il caso di Fascist Forge:

> Questa omogeneità ideologica tra gli utenti è probabilmente un riflesso della struttura e del processo di selezione del sito, che premia il conformismo. Inoltre, suggerisce che, sebbene abbia una piccola base di utenti, Fascist Forge può essere importante per rafforzare la visione del mondo di individui impegnati, il che, combinato con la sua attenzione all'ideologia accelerazionista, suggerisce che potrebbe rappresentare un rischio per la sicurezza.[1]

[1] In lingua inglese nel testo originale: *This ideological homogeneity across users is likely a reflection of the site's structure and vetting process, which rewards conformity. Importantly it suggests*

Davey et. al (2020) mostrano come queste dinamiche siano perfettamente comprese ed adattate alla cultura e sub – culture dell'estrema destra in modo da raggiungere gli scopi di reclutamento prefissati.

Questo è quanto viene sottolineato anche da Jones et. al (2020):[2]

> In terzo luogo, gli estremisti di destra hanno adottato alcune tattiche di organizzazioni terroristiche straniere, sebbene anche Al-Qaeda e altri gruppi abbiano adottato tattiche sviluppate da movimenti di destra.[3] In un post online del giugno 2019, un membro della Atomwaffen Division (AWD) ha dichiarato che "la cultura del martirio e dell'insurrezione all'interno di gruppi come i Talebani e l'ISIS è qualcosa da ammirare e riprodurre nel movimento del terrore neonazista".[4] Allo stesso modo, la Base – un movimento acceleratore neonazista vagamente organizzato che condivide il nome in lingua inglese di al-Qaeda – utilizza un processo di selezione per vagliare le potenziali reclute, simile ai metodi di al-Qaeda.[5]

Nei processi di vetting di qualsiasi tipologia di radicalizzazione contano le dimensioni identitarie, il convincimento ideologico che può essere poi forgiato secondo precise attività di formazione, i codici linguistici, la cultura di riferimento, il sistema valoriale, gli atteggiamenti e le concezioni della socie-

that although it has a small user base, Fascist Forge may be important in reinforcing the world view of committed individuals, which, combined with its focus on accelerationist ideology, suggests that it may pose a security risk.

[2] In lingua inglese nel testo originale: *Third, right-wing extremists have adopted some foreign terrorist organization tactics, though al-Qaeda and other groups have also adopted tactics developed by right-wing movements.In a June 2019 online post, a member of the Atomwaffen Division (AWD) stated, "the culture of martyrdom and insurgency within groups like the Taliban and ISIS is something to admire and reproduce in the neo-Nazi terror movement."1Similarly, the Base—a loosely organized neo-Nazi accelerationist movement which shares the English-language name for al-Qaeda—uses a vetting process to screen potential recruits, similar to the methods of al-Qaeda.*

Le note seguenti sono riportate per la versione del paper in lingua italiana.

[3] See, for example, Bruce Hoffman, "Back to the Future: The Return of Violent Far-Right Terrorism in the Age of Lone Wolves," War on the Rocks, April 2, 2019, https://warontherocks.com/2019/04/back-to-the-future-the-return-of-violent-far-right-terrorism-in-the-age-of-lone-wolves/.

[4] New Jersey Office of Homeland Security and Preparedness, *2020 Terrorism Threat Assessment* (Trenton, NJ: February 2020), 18, https://static1.squarespace.com/static/54d79f88e4b0db3478a04405/t/5e9f332ff92d080928b942f9/1587491645834/2020+Terrorism+Threat+Assessment.pdf.

[5] The Base limits membership to men of European descent of a certain age and those who attend in-person meetings, similar to how al-Qaeda introduced potential recruits to a family member of an imam. See, for example, New Jersey Office of Homeland Security and Preparedness, *2020 Terrorism Threat Assessment*, 18.

tà e i network nei quali si è inseriti che possono fungere da primo approccio ad un ecosistema radicale.

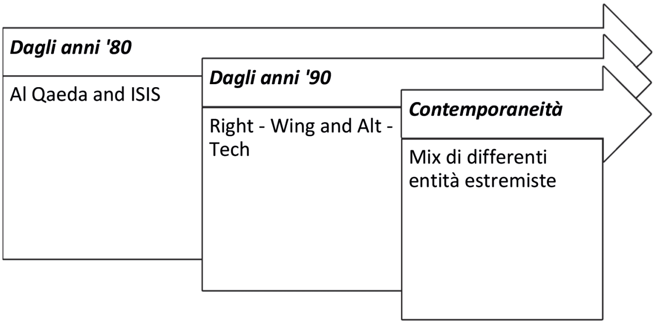
3. Vetting ed ecosistemi offline, online, digitali

L'evoluzione temporale dei processi di vetting e le loro iniziale aderenza a precisi costrutti ideologici estremisti e radicali può essere posta in relazione con l'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione proposta da Williams (2021), il quale individua le seguenti fasi:

1. Bulletin Board Systems and the World Wide Web 1983-2003
2. The Emergence of Social Media; Harassment and Trolling Prompt Limited Self-Regulation 2003-2014
3. Increased Platform Self-Regulation Is Followed by Extremist Use of Fringe Platforms and the Weaponization of Social Media 2015-2017
4. Far-Right Spaces, Market Pressure for Self-Regulation, Cell Proliferation and Infiltration, and Violent Action 2017-2019
5. Sustained Online Organized Mass Movements, the Reconstitution of Extremist Cells, and Government Focus on Domestic Terrorism 2020–Present

La figura sottostante sistematizza l'evoluzione temporale in funzione delle differenti prospettive culturali, ideologiche e organizzative, per poi giungere alla contemporaneità nella quale differenti forme di entità estremiste sono presenti simultaneamente e adottano anche una similare attività di vetting che può essere ampiamente influenzata dalle modalità comunicative che le piattaforme social permettono e garantiscono (Pauwels e Schils, 2016; Lucini, 2022).

Fig. 1 – *Evoluzione temporale delle diverse entità estremiste*


Dagli anni '80
Al Qaeda and ISIS
Dagli anni '90
Right - Wing and Alt - Tech
Contemporaneità
Mix di differenti entità estremiste

Questo approccio che pone in relazione i processi e i metodi di vetting nei differenti ecosistemi digitali e con le molteplici modalità comunicative messe a disposizione dalle piattaforme social porta ad un'estensione di quella cultura ideologica "*culling and cherry picking*" descritta da Hoffman e Ware (2020) con riferimento principale all'estrema destra.

Dalle analisi condotte su alcuni casi studio di ecosistemi sia di radicalizzazione islamica sia di estrema destra nell'ambito del progetto EU H2020 *Counter* è emerso che il vetting è un processo socio-culturale attraverso il quale non soltanto si selezionano futuri membri e radicalizzati, ma si plasmano queste persone attraverso pratiche mediali e comunicative tipiche di ogni piattaforma social utilizzata.

Infatti, come ricordano Maretti et al. (2022):[6]

> Lo spazio virtuale condiviso dai social network può avere diverse piattaforme digitali. Si tratta di Reddit, gruppi Facebook, gruppi WhatsApp, Wiki, canali e gruppi Telegram e hashtag popolari su Twitter, Instagram o TikTok. Ogni social network ha caratteristiche algoritmiche che influenzano il modo in cui vengono aggregati i dati. Infatti, ogni piattaforma sociale ha le proprie caratteristiche di comunicazione individuale e collettiva, per cui sviluppa un linguaggio particolare, definisce una struttura specifica delle informazioni e determina in modo diverso le polarizzazioni delle opinioni. In alcuni casi, le relazioni all'interno dei gruppi virtuali possono rimanere focalizzate nell'ambito digitale, mentre in altri casi si interfacciano tra il mondo online e quello offline.

Per sottolineare l'influenza e le capacità di orientamento che le piattaforme social hanno sulle interazioni sociali attraverso pratiche comunicative adattate al contesto del loro sviluppo Maretti et. al. (2022) pongono all'attenzione che:

> [...] secondo la teoria dell'elaborazione dell'informazione sociale (SIP), i soggetti che tendono a sviluppare relazioni interpersonali all'interno di contesti mediati tendono anche ad adattare le loro strategie comunicative alle opportunità offerte dal mezzo utilizzato (Walther, 2011; Walther & D'Addario, 2001).[7]

[6] In lingua inglese nel testo originale: *The virtual space shared by social networks can have different digital platforms. This includes Reddit, Facebook groups, WhatsApp groups, Wikis, Telegram channels and groups, and popular hashtags on Twitter, Instagram, or TikTok. Each social network has algorithmic characteristics that influence the way in which it is aggregated. In fact, each social platform has its own characteristics of individual and collective communication, whereby it develops a particular language, defines a specific structure of information, and determines polarisations of opinions in a different way. In some cases, the relationships within virtual groups may remain focussed in the digital realm, while in other cases they interface between the online and offline worlds.*

[7] In lingua inglese nel testo originale: "*In fact, according to social information processing theory (SIP), subjects who tend to develop interpersonal relationships within mediated contexts also tend to adapt their communicative strategies to the opportunities offered by the medium used (Walther, 2011; Walther & D'Addario, 2001).*"

È proprio la modalità di interfacciarsi in modo continuo fra l'una e l'altra dimensione che porta gli ecosistemi radicali ad assumere sempre più una forma digitale, di sintesi fra l'ambito online e quello offline, e sempre meno una distinzione netta fra queste due dimensioni.

Queste caratteristiche comunicative e di interazione sociale presenti negli ecosistemi digitali, per i quali il passaggio dall'ambiente online a quello offline è contemporaneo, reciproco e continuo, incide anche sui metodi di vetting.

Ciò lo si è appreso per esempio dal caso di Ilias Panagiotaros, leader del partito di estrema destra Alba Dorata, ponendo in evidenza che la reciprocità delle forme di vetting si situa in relazione a a quello che può essere sintetizzato come uno schema di pratiche e metodi di vetting nel quale agiscono differenti elementi combinati fra loro:

- il riconoscimento dei gruppi estremisti come comunità digitali di pratiche socio – culturali per le quali la dimensione online e offline si fonde in quella del digitale (Valentini et al., 2020). Ognuna di queste pratiche è in relazione con altre e i propri membri assumono ruoli e funzioni per la permanenza in tali comunità e la sopravvivenza del loro ecosistema digitale;
- a seconda del tipo di organizzazione estremista e del suo orientamento prevalente – religioso, politico, para-militare, militare, culturale – emergono pratiche e metodi di vetting specifici ma che possono accomunare gruppi estremisti di differente orientamento ideologico;
- i processi di vetting si caratterizzano per la presenza delle componenti simbolica, identitaria, narrativa che si intersecano e si influenza reciprocamente nella dimensione digitale;

In questo quadro, i processi di vetting si concretizzano in rituali che possono essere più o meno strutturati indipendentemente dal livello di strutturazione dell'organizzazione estremista: per esempio The Base presenta una struttura organizzativa piuttosto flessibile ma i processi di vetting seguono norme di selezione che si fondano su rituali precisi e normati anche in modo latente.

4. Conclusioni

Le analisi condotte e per le quali è stato possibile identificare i gruppi estremisti come comunità digitali di pratiche hanno portato anche ad alcuni risultati metodologici importanti per il futuro della digital humint, della socio-cultural intelligence e le policy di contrasto alla radicalizzazione da parte delle agenzie di Law Enforcement.

Un primo risultato è che i metodi di vetting che si traducono in pratiche socio – culturali e si declinano in comportamenti digitali specifici sono simili per gli ecosistemi digitali di radicalizzazione islamica e di estrema destra, in quanto come ricordano Maretti et al. (2022) le piattaforme social producono comportamenti, interazioni sociali e comunicazioni simili in quanto il modo stesso con il quale sono stati progettati e sviluppati orienta le azioni degli utenti. C'è quindi una componente di modellazione attuata dagli stessi strumenti messi a disposizione dalle piattaforme social.

Da una prospettiva di processo invece, il vetting si dimostra plasmato in funzione degli orientamenti ideologici e del contesto socio – culturale di riferimento.

Questa considerazione basata sull'evidenza delle analisi dei casi porta alla consapevolezza che la dimensione digitale, sintesi di quella online e offline, crea nuovi sistemi di relazioni nei quali il vetting agisce e che sono interdipendenti fra loro andando a formare comunità di comunità ovvero ecocistemi digitali permeabili e in relazioni fra loro che si spostano anche su molteplici piattaforme contemporaneamente.

In questo ambito diventa quindi essenziale riuscire a tradurre operativamente le componenti socio – culturali dei processi di vetting prima illustrate in segnali deboli e fattori di rischio che possono essere trasferiti alle agenzie di Law Enforcemente in modo da creare un conteso comune di azione fondato su elementi concreti, osservabili e che possono essere ricondotti ad un sistema di relazioni, potendo quindi giungere alla loro comprensione da un punto di vista più ampio e preciso.

I TRA-I ovvero gli strumenti per la valutazione del rischio terrorismo ed estremismo sviluppati in seguito all'attentatto dell'11 Settembre presentano ormai alcune vulnerabilità che dovrebbero essere colmate attraverso un loro aggiornamento e in funzione dei cambiamenti tecnologici, sociali, politici e culturali. A questo riguardo non deve essere dimenticato che per quanto concerne il fenomeno dell'estrema destra le agenzie di Law Enforcement sono chiamate anche ad operare secondo una prosepttiva sia interna sia esterna per l'idividuazione di potenziali segnali deboli anche al loro interno (Jacques, 2022), come il caso tedesco insegna.

Purtroppo come spesso accade i fenomeni estremisti anticipano le possibilità di contrasto perché per esempio per il processo di vetting, i vari gruppi estremisti sono stati più resilienti nel comprendere le opportunità tecnologie insite nelle nuove piattaforme social e adattate ai loro scopi di selezione dei membri e reclutamento in mdo da poter garantire la sopravvivenza e la resilienza del proprio ecosistema radicale.

Una vulnerabilità questa tipica delle varie agenzie di contrasto e dovuta a limiti politici e di visione strategica ma anche di lacune nella comprensione che per esempio il fenomeno dei lupi solitari meriterebbe più attenzione nella sua comprensione e nella determinazione dei rapporti che singoli estremisti hanno con l'ecosistema radicale al quale, in modi differenti operativi e/o culturali, aderiscono.

Il futuro quindi si fonda su una duplice direzione:

- includere le analisi dei processi dei vetting nella metodologia di valutazione del rischio estremismo e dei suoi fattori mediante gli strumenti della digital humint e la socio – cultural intelligence;
- promuovere una riflessione sul ruolo che le piattaforme social hanno e avranno nella determinazione delle attuali forme di radicalizzazione

È notizia recente che META lancerà le community su whatsapp e metterà a disposizione degli specifici strumenti per la gestione dei gruppi (Nisi, 2022) e ancora più interessante saranno le possibilità aperte sul Metaverso.

Infatti quest'ultimo è già stato oggetto di domande sul suo potenziale ruolo nei processi di radicalizzazione ed estremismo come per esempio identificava Isaac Kfir (2021) riflettendo sulla possibilità che il metaverso possa aprire ad ulteriori forme di radicalizzazione soprattutto con riferimento alla toxic masculinity che già si è vista in atto nelle comunità ICEL e dei suprematisti bianchi[8]:

> Gli aspetti del metaverso esposti da Stephenson risuonano con molti estremisti di destra, in particolare con i neoreazionari come Curtis Yarvin, Nick Land, Peter Thiel, Patri Friedman e la comunità Incel. Membri, sostenitori e affiliati di questi movimenti e pensatori sostengono una forma di cyber-idealismo che riconosce le possibilità dell'anarco-capitalismo e della mascolinità tossica. Quando le idee neo-reazionarie e accelerazioniste vengono infuse nell'etica "pilled", questi individui cercano di costruire un nuovo ordine mondiale – che rifletta i loro valori e interessi, rifiutando il femminismo, l'immigrazione, la globalizzazione e tutte le forze responsabili di quello che ritengono essere un persistente assalto alla mascolinità. Queste idee vengono esplorate e testate ai margini (anche nelle piattaforme di gioco online mainstream) perché non hanno modo di verificare adeguatamente le loro idee, ma con il metaverso le cose potrebbero cambiare.

[8] In lingua inglese nel testo originale: *Aspects of the metaverse as expounded by Stephenson resonate with many right-wing extremists, particularly within neoreactionists such as Curtis Yarvin, Nick Land, Peter Thiel, Patri Friedman, and the Incel community. Members, supporters, affiliates of these movements and thinkers advocate for a form of cyber-idealism that recognizes the possibilities of anarcho-capitalism and toxic masculinity. When neo reactionist and accelerationist ideas are infused within the 'pilled' ethos, these individuals look to construct a new world order — one that reflects their values and interests while rejecting feminism, immigration, globalization, and all the forces responsible for what they believe is the persistent assault on manhood. These ideas are explored and tested at the margins (including in mainstream online game platforms) as they do not have a way to properly test their ideas, but with the metaverse, things could change.*

Le potenzialità del metaverso per alimentare forme nuove di radicalizzazione con specifici metodi di vetting relativi alle stesse tipicità tecnologiche del metaverso appaiono come passibili di concretizzazione come sottolineano Elson et al. (2022) e Schori Liang (2022).

Ciò significa che, in considerazione dei mutamenti tecnologici, sociali, culturali e politici, sono necessari ulteriori approfondimenti nella relazione esistente fra processi e metodi di vetting, forme molteplici di radicalizzazione, strumenti di valutazione, contrasto, digital humint e nuove strategie di policy.

5. Introduction

At the end of October 2022, police in Bari arrested a 23-year-old young man, Luigi Antonio Pennelli, charging him with offences of international terrorism, propaganda, and incitement to racial, ethnic and religious discrimination.

Through the Telegram channel Sieg Heil, the young man was in contact with the American white supremacist and neo-Nazi group The Base. His role was to proselytise and disseminate video materials and leaflets to other potentially recruitable people. In this radical context, he was also willing to make an extreme sacrifice in defence of the white race.

This fact is just one of the latest examples of transnational radicalisation that crosses geographical and cultural boundaries and uses the now vast landscape of digital environments to create contacts and spread extremist views.

Within the framework of the European H2020 project CounteR – Countering Radicalisation for a Safer World Privacy-first situational awareness platform for violent terrorism and crime prediction, counter radicalisation and citizen protection, this phenomenon has been investigated and explored in its multiple nuances with particular reference to the areas of extreme right-wing and Islamic radicalisation.

The theoretical and methodological reflection that we wish to draw attention to here concerns the specific activity of vetting, i.e. the assessment for recruitment purposes that members of radical and extremist communities must face, in order to operate within that organisation.

This is a phenomenon that has been observed to be transversal to Islamic and extreme right-wing types of radicalisation, in this case united by certain elements of social interaction and media communication that then become typical at the moment of encounter with the characteristic culture, be it Islamic or extreme right-wing. Exploring and understanding these social dynamics and their contexts of development and action is a fundamental activity for the prevention and countering of radicalisation by the various national and international agencies.

6. Vetting processes, Islamic and right – wing radicalisation

The theoretical focus on vetting processes fills an interpretative gap that has distant historical roots in terrorism studies and studies on radicalisation processes.

The initial focus on these issues began with analyses on the dynamics of Islamic radicalisation for which two fundamental components seem to be characteristic of this process: the ideological-religious component as a driver for proselytism and propaganda; familiarity and family networks as an operational and vetting component in the processes of recruitment and filtering for participation in extremist organisations.

This type of radicalisation also had solid foundations in the processes related to the phenomenon known as chain migration and their application in the field of international terrorist organisations.

However, the increasing spread of social platforms has affected these phenomena and led to the development of increasingly complex forms of radicalisation and its dynamics (Lucini, 2020). Moreover, over the last two decades, economic, political and social changes in many societies have contributed to the spread and pervasiveness of other types of radicalisation such as the extreme right, which is increasingly present in various spheres of social, cultural and political life in many European and non-European countries.

In this context, the Covid-19 pandemic has also had a definite impact on both the operational modalities of these phenomena and their prevalence in viral domains, and on the temporal compression that has crystallised, in urgency, the new normality thus defined.

In the general scenario thus characterised, social platforms have been the most effective and resilient tool for the dissemination of extremist content, the possibilities of recruitment, but also for the ability to keep the networks created active by adapting and restructuring them following endogenous changes to the group or exogenous ones such as the various regulations concerning the fight against radicalisation. This intrinsic capacity of social networks was well understood and utilised by the Islamic State itself and then adopted with almost equal success by extreme right-wing groups as Hutchinson et al. (2022) point out.

The processes of vetting of both forms of radicalisation are fundamental to the understanding of the dynamics of selection of the potential future radicalised and can provide useful indications for the identification of weak signals, risk factors and vulnerabilities that can lead to this condition.

An important element that emerged from the analysis and research conducted concerns the possibility of bridging the theoretical gap in the study and analysis of vetting processes, considering extremist and radical groups not only as social groups present in online and offline dimensions but as communities of practices, originally identified by Jean Lave and Etienne Wenger (Lave, 1991; Wenger, 2011).

Furthermore, considering the technological evolution, it is possible to identify extremist groups as communities of digital practices (Archetti, 2015) for which the double contextual dimension – online and offline – should not be identified as an oppositional dichotomous modality, but rather a digitisation of cultural and communicative modalities that can occur and be present in both the real and virtual dimensions.

In accordance with this perspective, vetting practices take on precise cultural and identity characteristics at a second level of interaction, when people take on more precise roles and functions, while at a first level with a broader filtering function, vetting takes on characteristics across different ideological orientations, as Davey et. al (2020) recall for the case of Fascist Forge:

> This ideological homogeneity across users is likely a reflection of the site's structure and vetting process, which rewards conformity. Importantly it suggests that although it has a small user base, Fascist Forge may be important in reinforcing the world view of committed individuals, which, combined with its focus on accelerationist ideology, suggests that it may pose a security risk.

Davey et. al (2020) show how these dynamics are perfectly understood and adapted to the culture and sub-culture of the extreme right in order to achieve the intended recruitment goals.

This is also emphasised by Jones et. al (2020):

> Third, right-wing extremists have adopted some foreign terrorist organization tactics, though al-Qaeda and other groups have also adopted tactics developed by right-wing movements.In a June 2019 online post, a member of the Atomwaffen Division (AWD) stated, "the culture of martyrdom and insurgency within groups like the Taliban and ISIS is something to admire and reproduce in the neo-Nazi terror movement."1Similarly, the Base—a loosely organized neo-Nazi accelerationist movement which shares the English-language name for al-Qaeda—uses a vetting process to screen potential recruits, similar to the methods of al-Qaeda.

In the vetting processes of any type of radicalisation, identity dimensions, ideological conviction, which can then be forged according to precise training activities, linguistic codes, culture of reference, value system, attitudes and conceptions of society and the networks in which one is embedded that can serve as the first approach to a radical ecosystem, count.

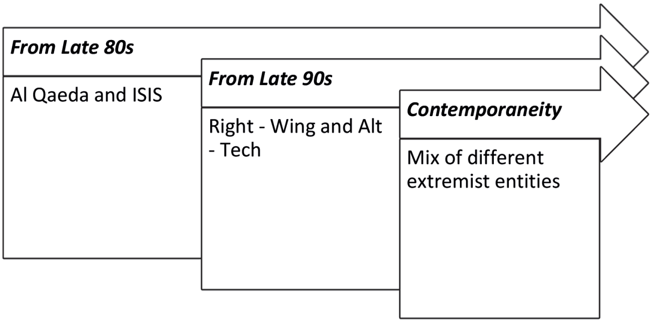
7. Vetting and offline, online and digtital ecosystems

The temporal evolution of vetting processes and their initial adherence to precise extremist and radical ideological constructs can be related to the evolution of information technology and media proposed by Williams (2021), who identifies the following phases:

1. Bulletin Board Systems and the World Wide Web 1983-2003
2. The Emergence of Social Media; Harassment and Trolling Prompt Limited Self-Regulation 2003-2014
3. Increased Platform Self-Regulation Is Followed by Extremist Use of Fringe Platforms and the Weaponization of Social Media 2015-2017
4. Far-Right Spaces, Market Pressure for Self-Regulation, Cell Proliferation and Infiltration, and Violent Action 2017-2019
5. Sustained Online Organized Mass Movements, the Reconstitution of Extremist Cells, and Government Focus on Domestic Terrorism 2020–Present

The figure below systematises the temporal evolution as a function of different cultural, ideological and organisational perspectives, and then arrives at the contemporary time in which different forms of extremist entities are simultaneously present and also adopt a similar vetting activity that can be largely influenced by the communicative modes that social platforms allow and guarantee (Pauwels and Schils, 2016; Lucini, 2022).

Fig. 1 – *Temporal evolution of the different extremist entities*


From Late 80s
Al Qaeda and ISIS
From Late 90s
Right - Wing and Alt - Tech
Contemporaneity
Mix of different extremist entities

This approach, which relates the processes and methods of vetting in different digital ecosystems and with the multiple communication modes made available by social platforms, leads to an extension of the 'culling and cherry picking' ideological culture described by Hoffman and Ware (2020) with main reference to the extreme right.

The analyses conducted on some case studies of both Islamic and extreme right-wing radicalisation ecosystems within the EU H2020 Counter project showed that vetting is a socio-cultural process through which not only future members and radicalised people are selected, but these people are shaped through media and communication practices typical of each social platform used.

Indeed, as Maretti et al. (2022) recall:

> The virtual space shared by social networks can have different digital platforms. This includes Reddit, Facebook groups, WhatsApp groups, Wikis, Telegram channels and groups, and popular hashtags on Twitter, Instagram, or TikTok. Each social network has algorithmic characteristics that influence the way in which it is aggregated. In fact, each social platform has its own characteristics of individual and collective communication, whereby it develops a particular language, defines a specific structure of information, and determines polarisations of opinions in a different way. In some cases, the relationships within virtual groups may remain focussed in the digital realm, while in other cases they interface between the online and offline worlds.

In order to emphasise the influence and orientation capabilities that social platforms have on social interactions through communicative practices adapted to the context of their development, Maretti et. al. (2022) point out that:

> In fact, according to social information processing theory (SIP), subjects who tend to develop interpersonal relationships within mediated contexts also tend to adapt their communicative strategies to the opportunities offered by the medium used (Walther, 2011; Walther & D'Addario, 2001).

It is precisely the way in which one and the other dimension are continuously interfaced that leads radical ecosystems to increasingly assume a digital form, a synthesis between the online and offline spheres, and less and less a sharp distinction between these two dimensions.

These communicative and social interaction characteristics present in digital ecosystems, for which the transition from the online to the offline environment is simultaneous, reciprocal and continuous, also affect vetting methods.

This was learnt, for instance, from the case of Ilias Panagiotaros, leader of the extreme right-wing party Alba Dorata, highlighting that the reciprocity of the forms of vetting is situated in relation to what can be summarised as a pattern of vetting practices and methods in which different elements act in combination:

– the recognition of extremist groups as digital communities of socio-cultural practices for which the online and offline dimensions merge (Valentini et al., 2020). Each of these practices is related to others and their members assume roles and functions for the permanence in these communities and the survival of their digital ecosystem;

– depending on the type of extremist organisation and its prevailing orientation – religious, political, para-military, military, cultural – specific vetting practices and methods emerge that may unite extremist groups of different ideological orientation;
– vetting processes are characterised by the presence of symbolic, identity and narrative components that intersect and influence each other in the digital dimension

Within this framework, vetting processes take the form of rituals that can be more or less structured regardless of the level of structuring of the extremist organisation: for instance, The Base has a rather flexible organisational structure but vetting processes follow selection rules that are based on precise rituals that are also latently normalised.

8. Conclusions

The analyses conducted and for which it has been possible to identify extremist groups as digital communities of practices have also led to some important methodological results for the future of digital humint, socio-cultural intelligence and policies to counter radicalisation by law enforcement agencies.

A first result is that vetting methods that translate into socio-cultural practices and translate into specific digital behaviours are similar for Islamic and extreme right-wing radicalisation digital ecosystems, since as Maretti et al. (2022) point out, social platforms produce similar behaviours, social interactions and communications because the very way they are designed and developed orients users' actions. There is thus a modelling component implemented by the very tools provided by social platforms.

From a process perspective, on the other hand, vetting proves to be shaped by ideological orientations and the socio-cultural context of reference.

This consideration based on the evidence of the case analyses leads to the realisation that the digital dimension, a synthesis of the online and offline dimensions, creates new systems of relationships in which vetting acts and which are interdependent on each other, going on to form communities or permeable digital ecocystems that also move across multiple platforms simultaneously.

In this context, it is therefore essential to be able to operationally translate the socio-cultural components of the vetting processes illustrated above into weak signals and risk factors that can be transferred to law enforcement agencies in order to create a common context of action based on concrete, observable elements that can be traced back to a system of relations, thus being able to understand them from a broader and more precise point of view.

The TRA-I, i.e. the tools for assessing the risk of terrorism and extremism developed in the aftermath of the 11 September attack, now present certain vulnerabilities that should be addressed by updating them in line with technological, social, political and cultural changes. In this regard, it should not be forgotten that with regard to the phenomenon of the extreme right, law enforcement agencies are also called upon to operate according to both an internal and external prosepttiva for the identification of potential weak signals also internally (Jacques, 2022), as the German case shows.

Unfortunately, as is often the case, extremist phenomena anticipate the possibilities of law enforcement because, for example, in the process of vetting, the various extremist groups have been more resilient in understanding the technological opportunities inherent in the new social platforms and adapting them to their purposes of member selection and recruitment so as to ensure the survival and resilience of their radical ecosystem.

A vulnerability this typical of the various law enforcement agencies and due to political limitations and strategic vision but also gaps in understanding that for example the lone wolf phenomenon deserves more attention in its understanding and determination of the relationships individual extremists have with the radical ecosystem to which, in different operational and/or cultural ways, they adhere.

The future is therefore based on a twofold direction:

- include analyses of vetting processes in the methodology for assessing the risk of extremism and its factors using digital humint and socio-cultural intelligence tools;
- promote a reflection on the role that social platforms have and will have in determining current forms of radicalisation

It is recent news that META will launch communities on whatsapp and provide specific tools for group management (Nisi, 2022) and even more interesting will be the possibilities opened up on the metaverse.

In fact, the latter has already been the subject of questions about its potential role in the processes of radicalisation and extremism, as Isaac Kfir (2021) identified, reflecting on the possibility that the metaverse may open up further forms of radicalisation, especially with reference to the toxic masculinity already seen in the ICEL and white supremacist communities:

> Aspects of the metaverse as expounded by Stephenson resonate with many right-wing extremists, particularly within neoreactionists such as Curtis Yarvin, Nick Land, Peter Thiel, Patri Friedman, and the Incel community. Members, supporters, affiliates of these movements and thinkers advocate for a form of cyber-idealism that recognizes the possibilities of anarcho-capitalism and to-

> xic masculinity. When neo reactionist and accelerationist ideas are infused within the 'pilled' ethos, these individuals look to construct a new world order — one that reflects their values and interests while rejecting feminism, immigration, globalization, and all the forces responsible for what they believe is the persistent assault on manhood. These ideas are explored and tested at the margins (including in mainstream online game platforms) as they do not have a way to properly test their ideas, but with the metaverse, things could change.

The potential of the metaverse to nurture new forms of radicalisation with specific methods of vetting related to the metaverse's own technological peculiarities appears to be in the realisation as Elson et al. (2022) and Schori Liang (2022).

This means that, in view of technological, social, cultural and political changes, further insights are needed into the relationship between vetting processes and methods, multiple forms of radicalisation, assessment tools, counteraction, digital humint and new policy strategies.

Reference

Archetti, C. (2015), Terrorism, communication and new media: explaining radicalization in the digital age, Perspect. Terror. 9, 49-59.

Davey, J., Hart, M. and Guerin, C. (2020), An Online Environmental Scan of Right-wing Extremism in Canada, Edited by Jonathan Birdwell, ISD Report Retrieved online: https://www.isdglobal.org/wp-content/uploads/2020/06/An-Online-Environmental-Scan-of-Right-wing-Extremism-in-Canada-ISD.pdf.

Elson, J.S. (2022), *The Metaverse offers a future full of potential – for terrorists and extremists, too*, Retrived online: https://www.voxpol.eu/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too/.

Hoffman, B. and Ware, J. (2020), *The Challenges of Effective Counterterrorism Intelligence in the 2020s*, Lawfare Retrieved online: https://www.lawfareblog.com/challenges-effective-counterterrorism-intelligence-2020s.

Hutchinson et al. (2022), Violent Extremist & REMVE Online Ecosystems: Ecological Characteristics for Future Research & Conceptualization, Research Brief, Retrieved online: https://resolvenet.org/research/violent-extremist-remve-online-ecosystems-ecological-characteristics-future-research.

Jacques, P. (2022), *Concerning police vetting process' risks 'insider threat' from extremism, warns report*, Retrieved online: https://www.policeprofessional.com/news/concerning-police-vetting-process-risks-insider-threat-from-extremism-warns-report/.

Jones, S.G., Doxsee, C. and Harrington, N. (2020), *The Escalating Terrorism Problem in the United States*, Retrieved online: https://www.csis.org/analysis/escalating-terrorism-problem-united-states.

Kfir, I. (2021), *The Metaverse and the Prospect of Toxic Masculinity — A Storm Is Brewing*, Retrieved online: https://eeradicalization.com/the-metaverse-and-the-prospect-of-toxic-masculinity-a-storm-is-brewing/.

Lave, J. (1991). Situating learning in communities of practice. In L.B. Resnick, J.M. Levine, & S.D. Teasley (Eds.), Perspectives on socially shared cognition (pp. 63-82). American Psychological Association.

Lucini, B: (2022), *Social Network, la sicurezza e l'intelligence: prospettive metodologiche*, in Intelligence C4 Conoscenza, Comprensione, Consapevolezza, Comunicazione, BTT Editori, Lomazzo (CO).

Lucini, B. (2020), Extremisms, viral violence and pandemic: Fusion Extreme Right and future perspectives, SICUREZZA, TERRORISMO E SOCIETÀ INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies Issue 2, Vol. 12 Retrieved online: https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2020/11/SicTerSoc-12-2020%20_%20Barbara%20Lucini%20-%20Extremisms%2C%20viral%20violence%20and%20pandemic_Fusion%20Extreme%20Right%20and%20future%20perspectives.pdf.

Maretti, M., Russo, V. and Lucini, B. (2022): Resilience in online communities of practice during the COVID-19 pandemic: an Italian case study, *International Review of Sociology*, DOI: 10.1080/03906701.2022.2114871.

Nisi, A. (2022), *Meta lancia le Community su Whatsapp e nuovi strumenti per i gruppi*, Retrieved online: https://www.agi.it/innovazione/news/2022-11-03/meta-lancia-community-whatsapp-nuovi-strumenti-gruppi-18693118.

Pauwels, L., and Schils, N. (2016). Differential online exposure to extremist content and political violence: testing the relative strength of social learning and competing perspectives. Terror. Polit. Viol. 28, 1-29. doi: 10.1080/09546553.2013.876414.

Schori Liang, C. (2022), *The Technology of Terror: from Dynamite to the Metaverse*, Retrieved online: https://www.gcsp.ch/publications/technology-terror-dynamite-metaverse.

Valentini D, Lorusso AM and Stephan A (2020) Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization. Front. Psychol. 11:524. doi: 10.3389/fpsyg.2020.00524.

Walther, J.B., & D'Addario, K.P. (2001). The impacts of emoticons on message interpretation in computer-mediated communication, *Social Science Computer Review*, 19(3), 324-347. https:// doi.org/10.1177/089443930101900307.

Walther, J.B. (2011). Theories of computer-mediated communication and interpersonal relations, in M.L. Knapp, & J.A. Daly (Eds.), The handbook of interpersonal communication (pp. 443-479), Sage, USA.

Wenger, E. (2011). Communities of practice: A brief introduction. Retrieved online: http://www.ewenger.com/theory/index.htm.

Williams et al. (2021), The Online Extremist Ecosystem, Rand corporation Retrieved online: https://www.rand.org/pubs/perspectives/PEA1458-1.html.

A comparative analysis of ISIS Channels On Telegram

Kamil Yilmaz – Farangiz Atamuradova

Dr. Kamil Yilmaz: works as a post-doctoral researcher at the Cyber Threats Research Centre (CyTREC), Swansea University. He holds a PhD in applied (political) anthropology from Columbia University and multiple master's degrees in criminal justice, international affairs, and anthropology. He is the author of "Disengaging from Terrorism: Lessons from the Turkish Penitents" (Routledge 2014) and numerous articles related to counterterrorism.

Farangiz Atamuradova[1]**:** is a Program Officer at the Research and Analysis Department. She joined Hedayah in February 2018. Prior to Hedayah, Farangiz worked at Delma Institute as a political analyst covering various regional issues. Farangiz holds a Master of Letters in Terrorism Studies from the University of St. Andrews and a Bachelor of Arts in Politics with International Studies from the University of Warwick.

Abstract

With the increased presence of social media and online messaging platforms in daily lives of individuals came the threat of its appropriation by terrorist groups to spread their narratives, recruit individuals, and serve as a communication channel among members of the group. This research focuses on comparing two Islamic State of Iraq and Syria (ISIS)Telegram channels – an interactive and broadcast channel – to compare the tactics and strategies employed by the two channels. In particular, the research assesses the discursive strategies presented in both channels, especially those pertaining to the representation of the in- and out-group by the channel moderators as well as followers. The combined analysis of the posts on two ISIS-channels is beneficial for researchers, practitioners, as well as policy makers as it sheds light to how one single group employs different tactics and strategies to communicate their message, polarize followers' viewpoint, and maintain the existence of and support for the terrorist group as a whole, despite its territorial defeat.

Keywords

ISIS, Telegram, terrorism, critical discourse analysis, CDA

[1] Opinions expressed in this paper are of the author and do not necessarily reflect the views of Hedayah.

1. Introduction

Terrorists' use of the Internet has been a focus of scientific inquiry for more than two decades. In recent years, however, the use of social media platforms and online messaging applications by terrorist groups has received significant attention from researchers, practitioners, and policymakers. This is because these platforms and applications have become entrenched in the daily lives of civilians – and they simultaneously shape and are shaped by our experiences and expectations. Moreover, the dichotomy of agency versus structure in making sense of human behaviour is becoming increasingly blurred, as it is a process that goes *pari passu* with the rapid development of platforms and applications. All this is to say that today nobody can be impervious to the effects of the vortex created by such rapid developments. This applies to ordinary law-abiding citizens, as well as members of various terrorist organizations. While these effects manifest themselves both positively and negatively, terrorist groups seem to be adroit in adapting themselves to these developments and benefiting from the affordances they provide. Accordingly, they consistently use these tools to communicate with existing members and the world, to find new recruits, to claim their attacks, and to disseminate their messages, among other things.

In this study, we focused on two Islamic State of Iraq and Syria (ISIS) channels on Telegram to explore how and why the group uses these channels on this platform. One of these channels is interactive, while the other is used as a broadcasting channel that disseminates information about ISIS attacks and other world events. The main emphasis will be placed on the contents of the texts to discover the discursive strategies by which various groups are constructed as in-groups or out-groups within these channels. In this respect, this study aims to contribute to a small body of work that combine Terrorism Studies and Discourse analysis. Deciphering these strategies has significant implications for counterterrorism efforts in relation to understanding both traditional and innovative methods of terrorist recruitment, communication, propaganda, and ideological indoctrination. To achieve these tasks, the remainder of this paper is split into four parts. The first part will focus on the relevant literature, which includes the use of Telegram by terrorist groups. The second part will provide a brief overview of the data collection and methodology used throughout this study. Through the use of Critical Discourse Analysis (CDA), in the third part we will present our findings by explicating what discursive strategies were used in these channels. The fourth part will conclude with final thoughts and recommendations.

2. Previous Research

There is currently an ample amount of studies that look at terrorist organizations' general use of online platforms and the ways through which they leverage it to polarize their followers. However, there is a lack of literature studying how terrorist organizations and their supporters employ various tactics and strategies to communicate through the same social media platforms. Reviewing previous literature that broadly analyses the strategic communications of ISIS, the objective here is to touch upon key factors and tactics studied to further delve into the specific narratives inside each channel. This will help to advance research and knowledge on how messaging tactics differ, even when the messaging and communication channels are from members or supporters of the same group.

2.1 Terrorist Use of Online Social Networks

The importance of the Internet and the way terrorist organizations leverage it for communicating propaganda and other related information, and as a "support mechanism" for terrorist networks is thoroughly covered in various studies and literature reviews.[2] The opportunities that the Internet created for terrorist groups to build and maintain "global support, spread their messages and recruit new members" are evident.[3] In addition to the Internet as a means of communication, the emergence of online social networks, media, and messaging platforms, as a tool of globalization that helps people across the world to communicate, was also leveraged by terrorist organizations for the same reasons. As studies show, terrorist organizations have been quick to adapt to new digital platforms and emerging technologies to achieve their goals – be it to recruit new followers, communicate between existing members, share propaganda, or to carry out the day-to-day processes by diversifying tactics and digital processes.[4]

[2] Alexander Meleagrou-Hitchens and Nick Kaderbhai. (2017). "Research Perspectives on Online Radicalization: A Literature Review, 2006-2016." *VOXPol*. Accessed at: https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf.

[3] Amarnath Amarasingam, Shiraz Maher, and Charlie Winter. (2021). "How Telegram Disruption Impacts Jihadists Platform Migration." *CREST Report*. p. 15. Accessed at: https://crestresearch.ac.uk/resources/how-telegram-disruption-impacts-jihadist-platform-migration/.

[4] Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald, and Lella Nouri. (2017). "Terrorists' Use of Internet," in *NATO Science for Peace and Security Series*. Vol. 136. (IOS Press: Amsterdam, Netherlands).; Adam Dolnik. (2007). *Understanding Terrorist Innovations: Technology, Tactics, and Global Trends*. (Routledge: New York).; and, Amarasingam, et al., "How Telegram Disruption Impacts."

In the study of how ISIS used social media to communicate their narratives, Pambayun suggests that the most prevalent mainstream social media networks leveraged by the terrorist groups were Twitter, Facebook, and YouTube; encrypted social messaging services such as Telegram were used for peer-to-peer messaging; and JustPaste.it was leveraged for content sharing.[5] Although the explicit content was strategically used by ISIS to create fear in society and gain younger adventure-seeking recruits – a large sum of the messages presented stories of human emotion, grievances, struggles, values, and motivations to construct a fake-reality that diverse groups of people around the world could relate to and sympathize with. For instance, content tends to narrate the desire to see the expansion of a Muslim empire – helping to legitimize and emphasize ISIS's slogan, "*Baqiya wa Tatamadad*," which translates to, "Remaining and Expanding."[6]

A 2020 study by Dillon et al. analyzed pro-ISIS supporters and ISIS foreign fighters on social media to compare the differences and similarities between their narratives and how they utilized content across multiple social media platforms.[7] The qualitative findings showed that five key narrative themes were prevalent in the messages that circulated on the social media websites among pro-ISIS supporters and foreign fighters: 1) threat to in-groups; 2) societal grievances; 3) pursuit of significance; 4) religion; and 5) commitment issues.[8] Furthermore, one of the messaging methods that ISIS used to reach out to communities on Twitter was to post tweets in trending or unrelated hashtags. To reach a wider array of users on social media, in this case namely Twitter, ISIS utilized these types of approaches as a part of its strategic communications framework. One of the interesting findings from the study's analysis of retweets was that majority of the retweets and engagement with posts were actually from accounts un-related to ISIS – meaning those users barely had any other ISIS-related posts on their accounts.[9]

[5] Ellys Lastari Pambayun. (2018). "The Construction of Terror Communicating of ISIS News in Social Media." *ESENSIA: Jurnal Ilmu-Ilmu Ushuluddin*. Vol. 19: 1, p. 97-116. Accessed at: https://doi.org/10.14421/esensia.v19i1.1490.

[6] Ibid, p. 112.

[7] Leevia Dillon, Loo Seng Neo, and Joshua D. Freilich. (2020). "A Comparison of ISIS Foreign Fighters and Supporters Social Media Posts: An Exploratory Mixed-Method Content Analysis." *Behavioral Sciences of Terrorism and Political Aggression*. Vol. 12: 4, p. 268-291. Accessed at: https://doi.org/10.1080/19434472.2019.1690544. The main platforms discussed in this study were Twitter, Facebook, Ask.fm, Tumblr, and Instagram – the data collected was from January to mid-June 2015.

[8] Ibid.

[9] Majid Alfifi, Parisa Kaghazgaran, James Caverlee, and Fred Morstatter. (2019). "A Large-Scale Study of ISIS Social Media Strategy: Community Size, Collective Influence, and Beha-

According to a study by Lissaris et al., terrorist groups' communication strategy varied based on the platform used – with more open and surface-level platforms such as Twitter, Facebook, and YouTube used to disseminate "public communications." Religion-abusing terrorist organizations, such as ISIS, leveraged surface web platforms to spread propaganda, recruit new supporters, and justify the group's violent actions. Conversely, many of these same terrorist groups leveraged the anonymity that the Dark Web and encrypted platforms provide to establish more discreet lines of communication which allowed them to stay undetected by law enforcement agencies and avoid content removal or account suspension.[10]

With the onset of stricter policies on terrorism-related content on Twitter and Facebook in 2014 and 2015 came a mass effort to monitor users, remove swarms of extremist content, and ban users/accounts constantly flagged for violations. These efforts forced terrorist organizations to seek haven elsewhere and re-establish communications on more private networks. At that point in time, the most convenient platform available was Telegram.[11] Moreover, in 2015, ISIS provided its followers with a ranking of various social messaging platforms and the level of 'safety' each platform offered. As per the ranking, Telegram was categorized as 'safe;'[12] however, this assessment may have changed since there have been increased efforts to take down terrorist content even on Telegram.

2.2 Terrorist Use of Telegram

Telegram became popular among and widely used by terrorist organizations, and their members and followers in 2015. As a platform, Telegram, which is a cloud-based instant messaging site,[13] provided an array of new op-

vioral Impact." *Proceedings of The International AAAI Conference on Web and Social Media*. Vol. 13, p. 58-67. Accessed at: https://ojs.aaai.org/index.php/ICWSM/article/view/3209.

[10] Euthimios Lissaris, Georgios Giataganas, Dimitrios Kavallieros, Dimitrios Myttas, and Emmanouil Kermitsis. (2021). "Terrorist Activities in the Dark and the Surface Web." In *Dark Web Investigation*: Security Informatics and Law Enforcement. Eds. Babak Akhgar, Marco Gercek, Stefanos Vrochidis, and Helen Gibson. (Springer: Cham), p. 49-84. Accessed at: https://doi.org/10.1007/978-3-030-55343-2_3.

[11] Maura Conway, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson, and David Weid. (2019). "Disrupting Daesh: Measuring Takedown of Online Terrorist Materials and Its Impacts." *Studies in Conflict & Terrorism*. Vol. 42: 1-2, p. 141-160. https://doi.org/10.1080/1057610X.2018.1513984.

[12] The Counter Extremism Project. (2017). "Terrorists on Telegram." Accessed at: https://www.counterextremism.com/sites/default/files/Terrorists%20on%20Telegram_052417.pdf.

[13] Rubi Acherjya Manna and Shyamal Ghosh. (2018). "A Comparative Study between Telegram and Whatsapp in Respect of Library Services." *International Journal of Library & Infor-*

portunities for terrorist organizations. While not as user-friendly and, at the time, popular as mainstream platforms like Twitter and Facebook, terrorists quickly learnt the advantages of Telegram. The platform offered encrypted services and the possibility of hosting channels that "allows hosts to 'broadcast' messages to subscribers in a unidirectional format, making it attractive to those who have a message to disseminate," as well as allowing them to monitor and restrict users.[14] Within their specific groups, Telegram users are able to chat with other users, "with each member of the group having the right to participate in the discussion."[15] Through such functionalities, terrorist groups could broaden their strategic communication and diversify it through use of the platform to have broader discussions with their followers, or to recruit new followers through polarization tactics.

As Manna and Ghosh assert, Telegram's ability to send large files like e-books, e-articles, and audio video lectures between users makes it a prime choice for sharing information and an important medium for communication amongst users without any limitations.[16] Furthermore, in a separate study conducted by Lissaris et al., ISIS was found to often use various messaging platforms to share outlinks to hidden servers or websites, for instance, links that are only accessible via the Tor browser ("the onion router").[17] Additionally, Lissaris et al. found that social media messaging services like Telegram were used as "core disseminators and bots and dedicated to the regular re-uploading of older productions."[18] These procedures helped ensure that the same information was shared on other related channels, and that even if one channel was taken down, other channels would have a chance of 'surviving.'[19]

A study by Amarasingam, Maher and Winter looked at how ISIS related channels reacted to the 2018 and 2019 Europol Action Days terrorist content takedown and elaborated on the communication strategies of the groups, as

mation Science. Vol. 7: 2. Accessed at: http://sbp-brims.org/2020/proceedings/papers/working-papers/SBP-BRiMS_2020_paper_17.pdf.

[14] Amarasingam et al., "How Telegram Disruption Impacts," p. 15.

[15] Ibid, p. 16.

[16] Manna and Ghosh, "A Comparative Study," in Tuja Khaund, Mainuddin Shaik, and Nitin Agarwal. (2020). "Data Collection and Sensemaking from Telegram: A Case Study of Ukrainian Political Leaders Channels and Chat Groups." *2020 International Conference on Social Computing, Behavioral-Cultural Modeling, & Prediction and Behavior Representation in Modeling and Simulation*, p. 2. Accessed at: http://sbp-brims.org/2020/proceedings/papers/working-papers/SBP-BRiMS_2020_paper_17.pdf.

[17] Lissaris et al., "Terrorist Activities," p. 49-84.

[18] Ibid, p. 52.

[19] Bennet Clifford and Helen Powell. (2019). "Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram." *Program on Extremism*. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/EncryptedExtremism.pdf.

well as their migration from one platform to another.[20] Within their study, the authors implemented Gill et al.'s conceptual framework to explain how ISIS adapted their strategy based on the restrictions imposed on their means of communication to migrate to more encrypted platforms.[21] One of the points highlighted in the conclusion of the study was that lexicon, use of particular language, and content background lures like-minded people to join groups and channels that support or hold similar worldviews and systems of beliefs.

2.3 Terrorist Content and Discourse Analysis

Researchers and scholars have examined terrorist groups' discourse, but to our knowledge there are only a few studies that combine Terrorism Studies (TS) and Discourse Analysis (DA) to study jihadist discourse. While the latter field focused on language used by other terrorist groups operating in Europe and the US,[22] much research in the field of TS employed content analysis.[23] In one notable study combining TS and DA, Lorenzo-Dus and Macdonald examined how Al-Qaeda and ISIS discursively constructed the West as an 'alien', aberrant 'other' in their online propaganda magazines *Inspire* and *Dabiq* and found that 'othering' is a key discursive strategy they use via "homogenization, suppression (stereotyping) and pejoration."[24] Our findings supports this study in the sense that jihadist groups like ISIS, just like in their online propaganda magazines, use various discursive strategies in their messaging on Telegram to define certain individuals and groups as in-group or out-group.

As demonstrated above, while a number of studies are dedicated to assessing how terrorists leverage various online magazines, social media networks and messaging platforms for their own benefits, there is not much literature or research that cross-analyses the different strategies and methods of communication among followers from the same terrorist group and its supporters.

[20] Amarasingam et al., "How Telegram Disruption Impacts."

[21] Paul Gill, John Horgan, Samuel T. Hunter, and Lily D. Cushenbery. (2013). "Malevolent Creativity in Terrorist Organizations." *The Journal of Creative Behavior*. Vol. 47: 2, p. 125-151. Accessed at: https://doi.org/10.1002/jocb.28.

[22] See, for example, Reisgl, Martin and Ruth Wodak. (2001). *Discourse and Discrimination: Rhetorics of Racism and Anti-Semitism*. London and New York: Routledge; Bowden, Zachary A. (2008). "Poriadk & Bardak (Order and Chaos): The Neo-fascist Project of Articulating a Russian 'People'." *Journal of Language and Politics* 7 (2): 231-247.).

[23] See, for example, Chertoff. Michael. (2008). "The Ideology of Terrorism: Radicalisation Revisited." *Brown Journal of World Affairs*, 15(1): 11-20.; Stern, Jessica and Berger, J.M. (2015). *ISIS: The State of Terror*. London: William Collins.

[24] Lorenzo-Dus, N. & Macdonald, S. (2018). Othering the West in the online Jihadist propaganda magazines Inspire and Dabiq. *Journal of Language Aggression and Conflict*, 6(1), 79-106.

2.4 Competitive System of Meaning

Studying ISIS's tactics on messaging and communications with its followers, Haroro Ingram coined the concept of "competitive system of meaning," which "acts as a lens through which supporters are compelled to perceive and judge the world."[25] Ingram further asserted that "these powerful mental models – or perhaps more accurately a network of mental models – are designed to fundamentally shape its audiences' perception by strategically leveraging and interplaying identity, solution, and crisis constructs via a combination of narratives and imagery."[26] Evaluating ISIS's communication through the concept of "competitive system of meaning" allows us to dismantle the group's tactics and to explain how through establishing a reputation as a 'trusted' source of information, ISIS was able to leverage its status to form new "meanings" for their followers. As stated by Pambayun, "[for ISIS] trustworthiness is a decisive factor to ensure the persuasive communication."[27] As a result, through such manipulation of information, ISIS could easily instil their divisive categorization between the in-group and out-group and mobilize it in an advantageous manner. Similarly, the "competitive system of meaning" has been leveraged as a framework to assess how ISIS was internalizing and normalizing ideas among its followers through educational material used by ISIS in Iraq.[28]

3. Methodology

3.1 The Rationale

This research was part of a broader project titled "Comparative Analysis of Islamic State and Atomwaffen Division Activity on Telegram" conducted by colleagues from Swansea University's Cyber Threat Research Centre (CYTREC) and seconded colleagues from various institutions including Moonshot, Swansea University, Hedayah, and University of North Carolina,

[25] Haroro J. Ingram. (2016). "Deciphering the Siren Call of Militant Islamist Propaganda: Meaning, Credibility & Behavioural Change," *The International Centre for Counter-Terrorism – The Hague*. Vol. 7: 9, p. 4. Accessed at: http://dx.doi.org/10.19165/2016.1.12.

[26] Ibid. p. 4.

[27] Pambayun. "The Construction of Terror Communicating of ISIS News in Social Media." p. 114.

[28] Sara Zeiger, Farangiz Atamuradova, Lilah ElSayed, and Muna Chung. (2021). "Planting the Seeds of the Poisonous Tree: Establishing a System of Meaning Through ISIS Education." *The ISIS Files*. Accessed at: https://www.hedayahcenter.org/wp-content/uploads/2021/02/Planting_the_Seeds_of_the_Poisonous_Tree__Establishing_a_System_of_Meaning_ThroGMXh_ISIS_Education.pdf.

Chapel Hill. For this sub-project, the research examined two ISIS-related Telegram channels that used different tactics to communicate with their followers. Among these channels, the Channel X acted as an interactive platform for followers to hold discussions, namely over the specific issue of so-called "Muslim struggles;" while the Channel Y was used to broadcast information, seeking to establish itself as a legitimate source of current affairs and news covering world events. Moreover, the Channel X is ISIS sympathizers, who are not formally speaking on behalf of the group; whereas Channel Y is different – it is not user-generated content as such. It is hard to know what the relationship of the channel administrator to the ISIS leadership is – but it is not intended to be understood as being user-generated content. So, to some extent, the difference in their strategies and methods is not surprising. The following comparison will assess the narratives used within the two channels and the way certain elements, such as the in-group, ineligible in-group and out-group, were established throughout the communications.

3.2 Ethics

Before embarking on the data collection, the project received institutional ethics approval. In order to safeguard the welfare of the research team, the entirety of the data was collected by Open-Source Intelligence Analysts at Tech Against Terrorism and then transferred to the research team via a secure file transfer service. For additional security and privacy protection, the collected data was not shared with individuals outside of the project team and no channel names are identified in this paper.

3.3 Data Collection

Data collection took place from 30 July 2021 to 12 September 2021. Since Tech Against Terrorism has a policy of non-engagement with channel administrators, the dataset was limited to public channels and private channels with publicly available join-links. For a channel to be considered an ISIS channel, the channel had to have a pro-ISIS slant and meet one or more of the following four criteria: (1) it posted official ISIS content (such as claims of attacks, video/photo propaganda, or *nasheeds*); (2) it published unofficial pro-ISIS media that praised the group and its efforts, and/or promoted its ideology; (3) the channel administrator published official ISIS content or content in support of ISIS on another platform; and/or, (4) the channel was promoted by ISIS on other platforms.

Given the significant disruption experienced by ISIS channels on Telegram, data were extracted daily throughout the collection period. The channels were downloaded using Telegram's built-in channel download feature and all datasets were extracted in HTML format. Telegram's export chat history function was also used to export all other available data, including photos, videos, voice messages, video messages, stickers, GIFs, and files. Although data collection commenced on 30 July 2021, for both Channel X and Channel Y it was possible to collect posts from an earlier date (20 May 2021 and 15 June 2021 respectively). As of September 2021, both channels were live.

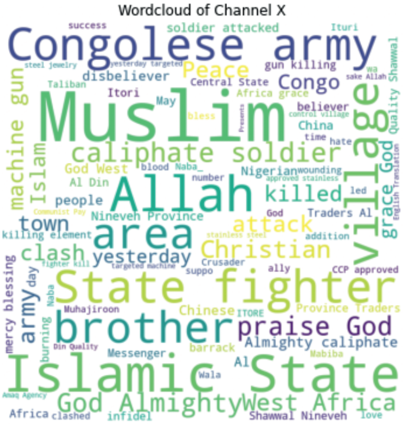
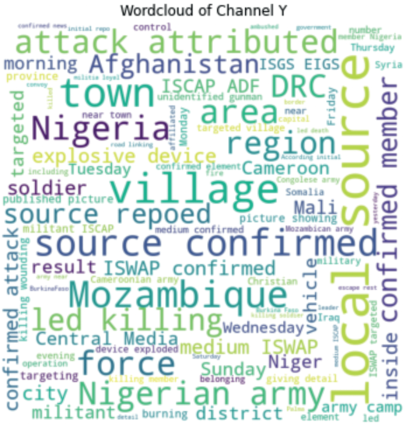
4. Findings

The analysis of the two channels is based on qualitative techniques. We will particularly delve into the 'content' (i.e., 'narratives') of the messages posted in these channels by focusing on three specific discursive strategies commonly used in CDA, namely: i) referential-nomination strategies, ii) perspectivation, framing, and discourse representation strategies; and iii) intensifying strategies. The determination of these three strategies was a semi-inductive process that was informed by two textual analysis techniques: word clouds (Figure 1) and topic-modelling (Appendices 1 and 2). The former is based on the frequency of words, which helps researchers understand what the text generally looks like. The latter, topic-modelling, exemplified by Latent Dirichlet Allocation (LDA), is a practical tool for discovering groups of words that often appear together in documents.[29] By revealing clusters of co-occurring words through various algorithms, topic modelling allows researchers to uncover the latent themes in large datasets of text.[30] In a nutshell, we employed these two techniques at the beginning of the research and determined the issues discussed in the channels which were represented by unigrams (words) in the word cloud and topic-modelling figures. We then looked at each individual item in the texts to understand the context in which they appeared. After reading and rereading these, we were able to categorize the items based on the aforementioned discursive strategies.

[29] Yuening Hu, Jordan Boyd-Graber, Brianna Satinoff, and Alison Smith. (2014). "Interactive Topic Modelling." *Machine Learning*. Vol. 95, p. 424. Accessed at: https://doi.org/10.1007/s10994-013-5413-0.

[30] Anton Törnberg and Petter Törnberg. (2016). "Combining CDA and Topic Modeling: Analyzing Discursive Connections Between Islamophobia and Anti-Feminism on an Online Forum." *Discourse & Society*. Vol. 27: 4, p. 401-422. Accessed at: https://doi.org/10.1177%2F0957926516634546.

Figure 1 – *Wordclouds*

Channel X	Channel Y
	

As shown in Figure 1, most frequently used words in the Channel X, as evidenced by the size of the words, are: *Muslim*, *Allah*, *Islamic*, *state*, *fighter*, *Christian*, *Congolese army*, *village*, *killed*, *caliphate*, *soldier* and so on. Leveraging other existing "hashtags" is what we call 'concept hijacking,' as it is employed as a tactic to use existing ideas to push forward their own narratives. The greater portion of the channel's content was related to ISIS's activities/attacks against Christians in West Africa (see words like *Congolese*, *army*, *West Africa*, *Christian*, *killed*, *attack*, *ituri*, *etc*), in Iraq (see the word Nineveh) and in Afghanistan (Taliban). In the Channel Y, most frequently used words include *local*, *source*, *village*, *region*, *reported*, *targeted*, *killing*, *Mozambique*, *Nigerian*, *Nigeria*, *force*, *soldier*, *army* and so on. It's important to note that the words *Islamic*, *state* or *ISIS* do not appear in the corpus; instead, we observed that a majority of posts contained words like *iswap* (Islamic State West African Province) or *iscap* (Islamic State Central African Province). In a nutshell, Channel Y seems to be dedicated to amplifying ISIS attacks especially in Africa, but also in the Middle East, by portraying itself as a legitimate news reporting outlet.

4.1 Discursive Strategies

For the purposes of this research, the term 'discourse' is defined, in the most abstract sense, as "an analytical category describing the vast array of meaning-making resources available to everybody."[31] Discursive practices, on the other hand, may have ideological effects in terms of helping, for example, the production and reproduction of unequal power relations between "social classes, women and men, and ethnic groups."[32] It is the main purpose of CDA to clarify these aspects of discourse as social practices that are otherwise opaque and not easily visible. One manifestation of such practices can be detected in political discourses that function in ways that "naturalize certain statements as self-evident."[33] For this reason, CDA helps individuals to be critical about this naturalization and recognize their misconception of real situations produced by the ideological effects of constructed discourses.[34] Another important aspect of discourse is linked to using various linguistic indictors in a strategic way to construct in- and out-groups, which are deemed to be essential for "political (and discriminatory) discourses in all kinds of settings."[35] One of the most important and commonly used settings in recent years has been social media – especially since it seems to be in strong competition with traditional media outlets (i.e., 'the fourth estate') for its instrumentalization of control and domination on a global spectrum, as well as in communication strategies of terrorist organizations.

In the CDA literature, the construction of in- and out-groups implies the use of *strategies of positive self-presentation* and the *negative presentation of others*. There is also minimizing the in-group's negative traits (as well as emphasizing their positive ones) and minimizing the out-group's positive traits (as well as emphasizing their negative ones). This research primarily focused on three types of discursive strategies that are all involved in positive self- and negative other- presentation:

1. Referential and nomination strategies;
2. Perspectivation, framing and discourse representation strategies; and,
3. Intensifying strategies.[36]

[31] Ruth Wodak. (2011). "Critical Discourse Analysis," in *Continuum Companion to Discourse Analysis*. Eds. Ken Hyland and Brian Paltridge. (London and New York: Continuum International Publishing Group), p. 39.

[32] Wodak, "Critical Discourse Analysis," p. 40.

[33] Norman Fairclough. (1989). *Language and Power*. (London: Longman).

[34] Kamil Yilmaz and Alper Sozer. (2015). "17/25 December Graft Probe in Turkey and Understanding Erdogan's Invincibility: A Critical Discourse Analysis (CDA)." *Security, Terrorism and Society*. Vol. 1: 1, p. 55-79.

[35] Wodak, "Critical Discourse Analysis," p. 46. In addition, construction of in- and out-groups chimes with the concepts of 'boundary formation,' 'boundary activation' and 'boundary deactivation,' which refers to us-them distinction between two political actors. For more information, see: Dough McAdam, Sidney Tarrow, and Charles Tilly. (2001). *Dynamics of Contention*. (Cambridge: Cambridge University Press).

[36] Wodak, "Critical Discourse Analysis," p. 49.

These discursive strategies underpin the justification/legitimization of inclusion and exclusion, as well as the constructions of identities. The breakdown of these strategies is presented in Table 1 below. The next couple of pages will explicate each strategy by providing several examples from our dataset.

Table 1 – *Discursive Strategies*

Channel X			**Channel Y**		
Discursive Strategies	Count	%	Discursive Strategies	Count	%
Referential/nomination	17	13.7	Referential/nomination	2	0.4
Framing/Discourse Representation	77	62.1	Framing/Discourse Representation	492	98.6
IS's strength & relevance	50	40.3	IS's strength & relevance	376	75.4
Plight of Muslims	27	21.8	Legitimation	114	22.8
Intensifying	71	57.3	Intensifying	492	98.6
Posts with text	124/255	49	Posts with text	499/805	62

4.2 Referential and Nomination Strategies

According to Wodak, *referential and nomination strategies* are used in constructing in-groups and out-groups by way of various categorization devices such as "memberships categorization; biological, naturalizing and depersonalizing metaphors and metonyms."[37] In the given assessment, these strategies were more visible in Channel X than Channel Y, given that around 13.7 percent of posts in the former contained referent terms about the out-group, whereas only a few instances of this strategy (0.4 percent) appeared in Channel Y(see Table 1).

Users in Channel X used referent-nomination terms like *infidel*, *crusader*, *atheist* and *communist* about non-Muslims in general, as well as Chinese people and the Chinese government, all of which invoke indelibly negative memories among Muslims around the world. More importantly, negative representations of the out-group went beyond non-Muslims in Channel X – it also included various Muslim people and states, which the channel depicted as being 'infidels.' For instance, regarding the recent victory of the Taliban in Afghanistan, one user posted a photo with the following message: "The Victory of the Taliban (American) and they are engaged behind the rostrum. God

[37] Ruth Wodak, (2001). The discourse-historical approach. In *Methods of critical discourse analysis* (pp. 63-94). SAGE Publications, Ltd. Accessed at: https://dx.doi.org/10.4135/9780857028020.

help Taliban's (American) victory. Here they already preaching behind a Shia minbar." Here, the user not only other-ed the Taliban by associating it with the word 'American,' but s/he also presented the Shia as an out-group, even though Shia is a recognized sect of Islam. The subsequent example about a depiction of Shiites in Channel X is more telling, as one user's caption under a photo had said: "Taliban members join the Shiah and offer their condolences at one of the Husayniyyat during the month of Muharram. Allahumma ihdeehum ila siratika al mustaqeem." The last sentence in the quote reads in English as "May God lead them to the straight path," which implies that Shiites are not on the right path, or that they are simply deviants. Another example was related to the ISIS-Khorasan attack at Kabul airport on 26 August 2021, which resulted in the death of 12 American servicemen and 60 Afghan civilians. One user in the channel wrote: "the blood of the infidels mixed with the blood of their dogs, the Taliban," – thereby, othering the Taliban more explicitly. In these examples, Shiites and the Taliban are viewed as part of the out-group, or as what Berger called the "ineligible of the in-group,[38] and presented as such. Using the "competitive system of meaning" we can see how leveraging some information, such as the withdrawal of American troops from Afghanistan, the group discussions present a narrative to categorize the in- and out- group.

In the Channel Y, the use of referent-nomination terms to define the out-group was almost non-existent. It appeared only in a small number of posts, in which the strategy was used indirectly by quoting the spokesperson of the ISIS Al-Qurashi, with the user saying:

> He talked about fighting the Kharijites and their leader Shekou, who was killed and blessed in the pledge of allegiance to those who repented from joining Shekou and joined the ISIS and recommended that they eliminate those who remained if they did not repent.

Here, the word Kharijites means 'seceders' or 'those who exit the community,' for their belief that it was forbidden to live among those who did not share their views, and those who disagreed with their position were deemed apostates deserving of capital punishment.[39] As such, 'Kharijite' is perhaps one of the most profound predicates that jihadist extremist groups use to label certain Muslims as part of the out-group, or as mentioned above, ineligible to be among the in-group. On the other hand, the fact that referential-nomi-

[38] J.M. Berger. (2021). "A Paler Shade of White: Identity & In-group Critique in James Mason's Siege." *RESOLVE Network*. Accessed at: https://doi.org/10.37805/remve2021.1.

[39] Tamara Sonn and Adam Farrar. (2009). "Kharijites." *Oxford Bibliographies*. Accessed at: https://www.oxfordbibliographies.com/view/document/obo-9780195390155/obo-9780195390155-0047.xml.

nation strategies were not used directly in Channel Y had to do with their conspicuous efforts to portray themselves as a legitimate pseudo news agency.

4.3 Perspectivation, Framing and Discourse Representation Strategies

In the observed posts, both channels used another strategy called *perspectivation, framing and discourse representation*, by means that "speakers express their involvement in discourse and position their points of view in the reporting, description, narration, or quotation of relevant events or utterances."[40] Once again, the use of this strategy in Channel X was direct and tended to revolve around framing the channel's discourse toward pro-ISIS narratives; whereas it was indirect and tailored more towards discourse representation in Channel Y. To specify, 62.1 percent of the posts in Channel X used this strategy, which was split up into two categories: messages around the promotion of ISIS's strength and relevance (40.3 percent) and messages related to the perceived plight of a specific group of Muslims (21.8 percent). In Channel Y, this strategy was used in 98.6 percent of the posts and manifested itself also in two ways: messages around the promotion of ISIS's strength and relevance (75.4 percent) and messages around the portrayal of the channel as a legitimate news outlet – legitimation (22.8 percent). (See Table 1). To better contextualize, one user in the Channel X said the following over the recent victory of the Taliban:

> #Taliban. They announce their fake victory but they are back to square one, after the Islamic State came out to them from where they did not count, amid their fortifications at Kabul Airport. But this time the flavor was different thankfully. The blood of the infidels mixed with the blood of their dogs, the Taliban. This is a small part and the sweetness has not yet begun.

In saying this, the user not only expresses his own point of view but also glorifies violence, belittles the enemy (i.e., 'infidels' and the 'Taliban'), and threatens to commit future attacks – thereby framing the discourse in such a way that the ISIS narrative is still powerful and the Taliban's victory is doomed to be ephemeral. The same user also posted a similar message about an ISIS attack in Central Africa stating:

> Central African State. By the grace of God Almighty, the soldiers of the Caliphate ambushed two trucks of unbelieving Christians, in the village of (Ofai) in the (Ituri) region yesterday, as they targeted them with machine guns, which led to their burning and the killing of one of the Christians, praise be to God.

[40] Wodak, "Critical Discourse Analysis," p. 49.

Phrases like "By the grace of God Almighty,' and 'praise be to God,' were referents for the glorification of the attacks and clearly demonstrated the user's own point of view in the ISIS's discourse which seeks to amplify the "strength" of the group on Telegram.

As mentioned earlier, in Channel Y this strategy manifested itself mostly as discourse representation. Discourse representation refers to "the language used in a text or talk to assign meaning to groups and their social practices, to events, and to social and ecological conditions and objects."[41] In this view, the implicit role of the language in social life is that "meaning is not embedded in the reality that is perceived but rather that it is construed by linguistic representation."[42] What we saw in Channel Y is that the channel first tried to represent itself as a legitimate news outlet by maintaining neutral language, seemingly distant from the content of the messages that it disseminated – the channel owed its successes, to a great extent, to this strategy. Given that Channel Y's accounts have been active for a long time, the channel's success was apparent on Telegram, as well as other platforms like Twitter and Facebook – notwithstanding the fact that almost 90 percent of the channel's content is about ISIS attacks in various regions around the world, namely in the African continent. The following example, which is the only message in the channel that shows the author's involvement in the discourse, however, clearly reveals the real opinion of the channel administrators about ISIS as a terrorist organization, even though they make enormous efforts to be seen as a legitimate news platform:

> "#Mozambique. The commander of the Rwandan army deployed in Cabo Delgado province is called "Innocent Kabandana", a war criminal notorious for causing crimes inside and outside Rwanda. *I think IS militants (ISCAP) love this breed:)*" [Emphasis added].

4.4 Intensifying Strategies

Both channels have consistently used intensifying strategies, which "help to qualify and modify the epistemic status of a proposition by intensifying the illocutionary force of utterances."[43] In other words, these strategies are an important aspect of presentation in terms of sharpening the narratives,

[41] Norman Fairclough. (1989:1995); Teun van Dijk (2002), cited in Anita. L. Wenden. (2005). "The Politics of Representation: A Critical Discourse Analysis of An Aljazeera Special Report." *International Journal of Peace Studies*. Vol. 10: 2, Autumn/Winter, p. 90. Accessed at: https://www.jstor.org/stable/41852931.

[42] Wenden, "Politics of Representation," p. 90.

[43] Wodak, "Critical Discourse Analysis," p. 49-50.

both real and constructed ones. Moreover, the intensification strategies can be used in at least two ways: 1) intensifying quantitatively, which means that an argument is uttered repetitiously; and 2) intensifying qualitatively, which refers to making a seemingly convincing fallacious argument and sharpening it when one is expected to tone it down."[44]

In Channel X, 57.3 percent of the posts contained intensifying strategies (see Table 1), which were most visible in users' narratives related to a specific group of Muslims, which was done both quantitatively, by repeating similar messages regarding the reported number of deaths, and qualitatively, by increasing the emotional weight of those narratives. The qualitative aspect of intensification was undergirded by attaching one or more visuals, such as photos, audios, or videos relating to the topic. The main issue at hand is the idea of 'concept hijacking,' i.e., the exploitation of the plight of specific Muslim groups around the world in this channel to promote and glorify ISIS by amplifying pro-ISIS messages and narratives.

In Channel Y, we observed this strategy in 98.6 percent of the messages (see Table 1), mostly in the form of quantitative intensifying in that, messages featuring ISIS attacks in different countries and regions were shared repeatedly to project an image of the group as a still-relevant, all-powerful, and ubiquitous force in the world, especially in Africa and the Middle East. Considering that almost 90 percent of the messages in the channel were about ISIS attacks or activities that could be seen in any ordinary news outlet, using the intensification strategy in this way may also have contributed to the channel's success in portraying itself as a legitimate source of information – especially among members, followers, and even supporters of ISIS.

5. Conclusion

This research analysed the content of two ISIS-related Telegram channels – an interactive channel (Channel X) and a broadcasting channel (Channel Y) – to assess the similarities and differences in the strategies employed to communicate its narratives to followers. While numerous studies have been conducted on the use of various social media and messaging platforms, there was not enough literature available on assessment of the different channels or accounts used by the same group on these platforms. Assessing the content of the messages, there were clear examples of how the group could be leveraging various options and opportunities provided on Telegram to maximize their communication tactics and further establish their narratives through

[44] Toning down in political discourse falls into the category of 'mitigation strategies,' which can be considered as the opposite of 'intensification strategies.'

either more overt categorization of the in- and out- group, or subtler messages that reinforce the same divide. The qualitative analysis of the content helped us to derive the three strategies used by the channels in their messaging. Assessment of these strategies shed some light on how these groups use specific language choices to polarize the wider population and instil the given categorization among their followers. The two channels used different approaches in reinforcing their narratives through either the viewpoints and posts shared by followers (Channel X) and selective news postings that, while allowing it to establish itself as a legitimate source of information, tactically embedding ISIS-leaning discourse in seemingly generic posts (Channel Y). Finally, both channels strategically intensified the narratives quantitatively or qualitatively. Channel X users and moderators repeated similar messages in different instances to attract more attention to the issue, while also intensifying the messages separately through use of sentimental language and attached images and videos. For Channel Y, this was done through frequent reposts of the ISIS attacks around the world, implicitly intensifying the presence of a group, which in reality is viewed to have grown weaker since the fall of its physical stronghold in Iraq and Syria. Based on the findings of this research, several recommendations are summarized below:

5.1 Recommendations:

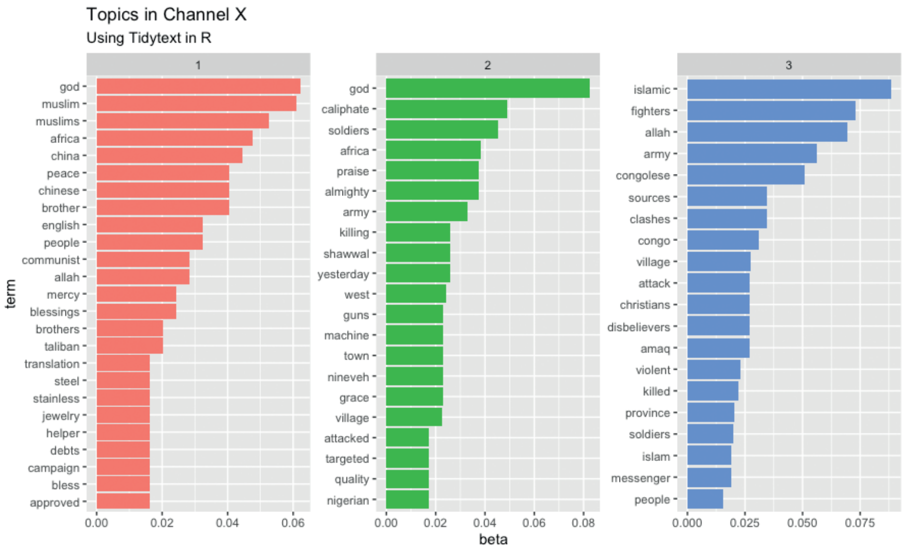
- Continue to analyse strategies employed by various terrorist groups across online platforms. Having continuous studies on how terrorists operationalize online spaces will shed light on their operations and will help inform decisions on the best ways of identifying the threat online as well as how to best approach it.
- Assess terrorists' changing online narratives and how these are used for different purposes. Leveraging frameworks such as "competitive system of meaning" will help shed light on how terrorists use facts coupled with their interpretation of situations to build their own narratives. Understanding of the narratives put forward by terrorist groups and how they are used to create a new set of "meanings" and "values" for their followers is important not only for preventative work, but also for deradicalization initiatives.
- Leverage collaborations between academics, practitioners, and policy makers to collectively assess content taken down from platforms such as Telegram to allow for a multidimensional assessment of the information. As shown through this project, such approaches will allow for a holistic analysis of information, producing well-developed recommendations for future research and policies, which in return can be used to produce responses to the use of online platforms by terrorist of different background.

Acknowledgments:

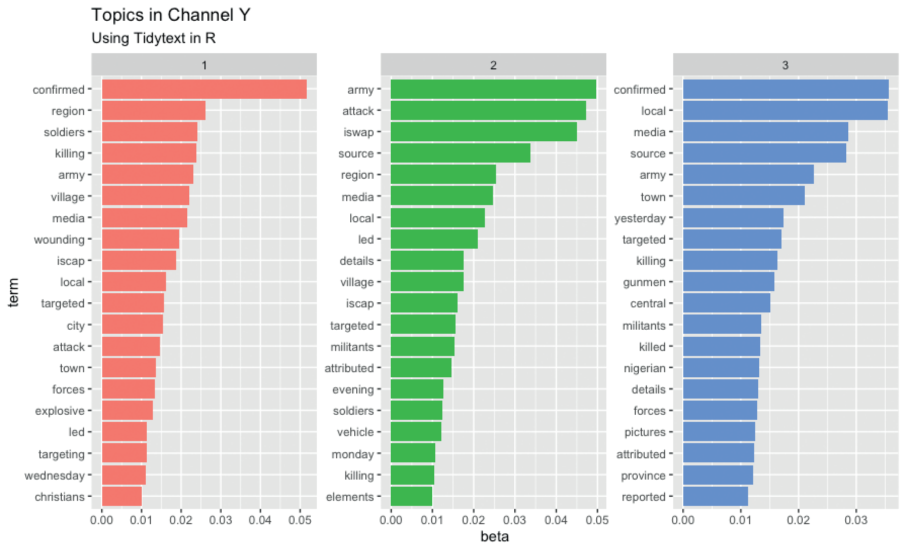
The authors gratefully acknowledge the support received for this research from HEFCW (via the Research Wales Innovation Fund) and Swansea University's Legal Innovation Lab Wales (which is part-funded by the European Regional Development Fund through the Welsh Government). The authors also appreciate the support from Tech Against Terrorism.

Appendices

Appendix 1: Topics in Channel X



Appendix 2: Topics in Channel Y



Social bots and synthetic interactions to stage digital extremist armies

Daniele Maria Barone

Daniele Maria Barone is a counter-terrorism analyst. He served as an Italian Coast Guard officer and worked as a project manager and digital communication specialist in the private sector. He graduated in Marketing & Communication at IULM University, obtained a master's degree in International Relations at ASERI Graduate School of Economics and International Relations – Catholic University of the Sacred Heart, and specialized in counter-terrorism studies earning an Executive Certificate at the International Institute for Counter-Terrorism (ICT) – Herzliya. His research interests are cyber-jihad, terrorist financing, and terrorist organizations' communication strategies.

Abstract

Artificial intelligence (AI)-made bots for social media platforms are becoming increasingly sophisticated and able to impersonate average users, developing either as valuable AI tools in the communication field or as an instrument for online deception.
As AI keeps advancing, also terrorist organizations will benefit from these technological developments to increase the efficiency of their use of social media. For instance, they could increasingly avoid being flagged by users or detected and banned by the platforms, supporting radicalization or propaganda with less risk while gaining greater resonance.
From this perspective, the analysis will firstly focus on how social bots work, their role in helping to perceive synthetic interactions as authentic interactions, and their potential contribution to social manipulation. Then, the paper will delineate how AI-bot developments intersect with terrorist or extremist communication environments.

I social media bot creati attraverso l'intelligenza artificiale (IA) diventano sempre più sofisticati e in grado di imitare con maggiore efficacia il comportamento degli utenti. Questo li ha resi sia strumenti particolarmente validi nel settore della comunicazione sia una risorsa utile per ingannare gli utenti.
Con l'avanzamento e la diffusione dell'IA, anche le organizzazioni terroristiche potranno beneficiare di questi sviluppi in campo tecnologico, migliorando la loro efficenza nell'utilizzo dei social media. Ad esempio, i social bot potrebbero aiutare le organizzazioni terroristiche a diminuire le possibilità di essere segnalati dagli utenti e sospesi dalle piattaforme social, supportando i loro processi di radicalizzazione e diffondendo la loro propaganda con un rischio inferiore ma garantendo una maggiore risonanza.
Partendo da questa prospettiva, dopo aver analizzato il funzionamento dei social bot, in quale misura questi ultimi possono favorire la percezione di interazioni sintetiche come autentiche ed il loro contributo alla manipolazione sociale, la ricerca delineerà le aree principali attraverso cui lo sviluppo tecnologico dei bot si interseca con i contesti comunicativi di gruppi terroristici o estremisti.

Keywords

Social media bot, jihad, far-right, conspiracy theories

1. Introduction

On June 16, the European Commission welcomed the strengthened Code of Practice on Disinformation, a framework to set out commitments by platforms and industry to fight disinformation.[1] The first 2018 anti-disinformation Code consisted of self-regulatory standards to fight disinformation to which tech-industry representatives agreed voluntarily.[2] The reinforcing process of the Code has been signed by 34 actors from the tech industry as online platforms, ad-tech companies, fact-checkers, and civil society organizations.[3] Amid its measures, it includes to "cut financial incentives for spreading disinformation" to "empower users with better tools to recognize, understand and flag disinformation" and to "expand fact-checking in all EU countries and all its languages." The Code also provides measures to prevent malicious actors from covering manipulative behaviors used to spread disinformation using fake accounts, deepfakes, and bot-driven amplification.[4]

In this respect, the use of artificial intelligence (AI), even at its rudimentary level, is creating a growing interest in its possible exploitation not only to spread disinformation but also for extremist or terrorist purposes.

In particular, the creation of AI-made fake accounts and bots for social media platforms are becoming increasingly sophisticated and able to impersonate average users[5] developing, on the one hand, as the most used AI tools in the communication field and, on the other hand, as an instrument for online deception.

[1] European Commission (June 16, 2022) *Disinformation: Commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3664.

[2] European Commission *2018 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

[3] European Commission (June 16, 2022) *Signatories of the 2022 Strengthened Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

[4] European Commission *The 2022 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[5] Kilcher Y. (June 3, 2022) *This is the worst AI ever*. YouTube. https://www.youtube.com/watch?v=efPrtcLdcdM.

As explained by a joint report by UNICRI and UNCCT,[6] as AI keeps advancing, also terrorist organizations will benefit from these technological developments to increase the efficiency of their use of social media. They could become more and more able to avoid being flagged by users or being detected and banned by the platforms, supporting radicalization or propaganda with less risk, while gaining greater resonance.[7]

To define in which ways AI-bot developments intersect with terrorist or extremist communication environments, the analysis will first understand how bots work, in which ways social bots could help perceive synthetic interactions as authentic interactions and their potential contribution to social manipulation.

2. A how-to guide to normalize "synthetic realness"

Even though AI is not a new technology,[8] only in the last decades it has shown its impact on businesses and people's everyday lives, making it hard to discern where it stops and humanity begins.[9] To better understand the pervasiveness of AI in the digital communication environment, it is useful to highlight some major areas in which its acceptance degree and uses are evolving.

2.1 A growing, promising business

The potential pervasiveness of the whole AI sector is allowing the AI market, which was valued at USD 65.48 billion in 2020, to be projected to reach USD 1,581.70 billion by 2030.[10] Indeed, AI-enabled systems will continue to support many sectors, for instance, healthcare, education, financial services,

[6] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes*. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

[7] Ciancaglini V., Gibson C., Sancho D., Amann P., Klayn A., McCarthy O., and Eira M. (November 19, 2020). *Malicious Uses and Abuses of Artificial Intelligence. Trend Micro*. EUROPOL and UNICRI. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf.

[8] Harvard special edition: *Artificial Intelligence*. https://sitn.hms.harvard.edu/special-edition-artificial-intelligence/.

[9] Forsbak Ø. (March 25, 2022) *Six AI Trends To Watch In 2022*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/03/25/six-ai-trends-to-watch-in-2022/?sh=3e1c36e62be1.

[10] PR Newswire (June 13, 2022) *Artificial Intelligence Market USD 1,581.70 Billion By 2030, Growing At A CAGR of 38.0%*. Bloomberg press release. https://www.bloomberg.com/press-releases/2022-06-13/artificial-intelligence-market-usd-1-581-70-billion-by-2030-growing-at-

engineering, security, and transport, and are already changing the way businesses understand both internal and external processes.

2.2 Big (artificial) data to kickstart the modern economy

AI is changing the foundation of the modern economy: big data.[11] AI systems work by combining large sets of data with intelligent, iterative processing algorithms to learn from patterns and features in the data that they analyze, allowing machines to learn from experience, adjust to new inputs and perform human-like tasks.

To train AI, companies used to rely exclusively on data generated by real-world events until they realized there wasn't enough data to support the algorithm's training.[12] This limit brought to provide synthetic data, which consists of a technology that enables to digitally generate the data, on demand, in whatever volume, and artificially manufactured to precise specifications.

This approach helps to bypass, for instance, confidentiality and privacy issues when gathering data to train AI for healthcare purposes, detect specific and rare patterns in credit-card frauds, and generate data required to build a safe autonomous vehicle.[13] Furthermore, synthetic data in AI systems could help remove bias in machine learning, allowing algorithmic decision-making to avoid infinitely reproducing human errors, reducing face-to-face discrimination in markets prone to implicit and explicit biases as, for example, in the context of consumer lending.[14]

2.3 Synthetic authenticity becomes the new real

With these premises, the widespread implementation of AI has brought either developments or new challenges in business, organizations, and society

a-cagr-of-38-0-valuates-reports#:~:text=Artificial%20Intelligence%20Market%20USD%201%2C581.70,38.0%25%20%2D%20Valuates%20Reports%20%2D%20Bloomberg.

[11] The Economist (May 6, 2017) *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[12] Castellanos S. (July 23, 2021) *Fake It to Make It: Companies Beef Up AI Models With Synthetic Data*. Wall Street Journal. https://www.wsj.com/articles/fake-it-to-make-it-companies-beef-up-ai-models-with-synthetic-data-11627032601.

[13] Towes R. (June 12, 2022) *Synthetic Data Is About To Transform Artificial Intelligence*. Forbes. https://www.forbes.com/sites/robtoews/2022/06/12/synthetic-data-is-about-to-transform-artificial-intelligence/?sh=5e6a76c07523.

[14] Bartlett R., Morse A., Stanton R., and Wallace N. (June 2019) *Consumer-Lending Discrimination in the FinTech Era*. National Bureau of Economic Research. https://www.nber.org/papers/w25943#:~:text=FinTech%20algorithms%20also%20discriminate%2C%20but,borrowers%20on%20low%2Dshopping%20behavior.

at large, in an ongoing process of creation of a world of synthetic realness, where AI-generated data convincingly reflect the physical world.[15] Thus, given developments and potential improvements of AI, the question, as expressed in a report by Accenture, is: "What's real, what's not and perhaps more importantly, when do we care?"[16]

In this context of blurred divergences between synthetic and real, the most evident direct interaction with AI is in the intersection between technology and communication through the use of bots in the now-familiar social media/chat services environment.

A bot is a software agent or third-party service programmed to perform certain actions on a regular or reactive basis, without having to rely, or partially relying, on human intervention. The bot analyzes the circumstances and autonomously decides what action to take. In particular, a social bot can mimic human behavior in social networks, taking part in discussions, pretending to be a real user. Social bots can post content, mostly through fake accounts, like, share, and comment. To perform efficiently a bot needs a technical infrastructure, which, in a nutshell, consists of a combination of the profile on a social media platform and the technical preconditions for partial automation of the account's behavior, through the chosen platform's Application Programming Interface (API)[17] or proprietary mechanisms[18] to interact with the website or app.[19]

Then, bots require a low level of human management: hundreds or even thousands of social bots can be managed by a single person.[20] In that regard, it has been roughly estimated that, only in 2017, there were 23 million bots

[15] Accenture (June 17, 2022) *The unreal – making synthetic, authentic*. https://www.accenture.com/th-en/insights/health/unreal-making-synthetic-authentic.

[16] Accenture (March 16, 2022) *Technology Vision 2022: "Metaverse Continuum" Redefining How the World Works, Operates and Interacts*. https://newsroom.accenture.com/subjects/metaverse/accenture-technology-vision-2022-metaverse-continuum-redefining-how-the-world-works-operates-and-interacts.htm.

[17] "An application programming interface, or API, enables companies to open up their applications' data and functionality to external third-party developers, business partners, and internal departments within their companies. This allows services and products to communicate with each other and leverage each other's data and functionality through a documented interface." IBM A*pplication Programming Interface (API)*. https://www.ibm.com/cloud/learn/api.

[18] *Bots: An introduction for developers*. Telegram. https://core.telegram.org/bots.

[19] Assenmacher D., Clever L., Frischlich L., Quandt T., Trautmann H., and Grimme C. (September 1, 2020) *Demystifying Social Bots: On the Intelligence of Automated Social Media Actors*. Social media and Society. https://journals.sagepub.com/doi/10.1177/2056305120939264.

[20] Cloudfare. *What is a social media bot? | Social media bot definition*. https://www.cloudflare.com/it-it/learning/bots/what-is-a-social-media-bot/#:~:text=Experts%20who%20have%20applied%20logarithms,designed%20to%20mimic%20human%20accounts.

on Twitter (8.5% of all accounts), 140 million bots on Facebook (5.5% of all accounts), and about 27 million bots on Instagram (8.2% of all accounts).[21]

Moreover, according to the University of California,[22] in 2020, about 13% of all Twitter users that retweeted or engaged in conspiracy theories were bots,[23] while Facebook banned 1.6 billion accounts actioned on fake accounts only in the first quarter of 2022.[24]

2.4 The manipulative side of social bot

The use of social bots to manipulate is not new but has been spreading faster over time.

For instance, social media platforms, such as Facebook and Twitter, were used to organize protests and spread awareness of updates and movements during the Arab spring.[25] Almost a decade later, those same social media platforms found and removed hundreds of bot accounts "for engaging in coordinated inauthentic behavior," as disinformation, spamming,[26] and state-backed manipulation[27] during the spring 2011 events.

Another example comes from studies claiming that the key to the success of Farage Brexit party is related to the clarity and simplicity of its messaging, compared to Change UK, the Greens, and the Liberal Democrats, and by an effective social media echo chamber of pro-Brexit bot accounts.[28] In this respect, a study in the Social Science Computer Review uncovered the deployment of a network of 13,493 Twitterbots that tweeted mainly messages

[21] Vosoughi S., Roy D., and Aral S. (March 9, 2018) *The spread of true and false news online*. Science. https://www.science.org/doi/10.1126/science.aap9559.

[22] Ferrara E., Chang H., Chen E., Muric G., and Patel J. (October 2020) *Characterizing social media manipulation in the 2020 U.S. presidential election*. First Monday, 25(11). https://firstmonday.org/ojs/index.php/fm/article/view/11431/9993.

[23] Botometer https://botometer.osome.iu.edu/.

[24] Meta, Community Standards Enforcement Report – Q1 2022 report. https://transparency.fb.com/data/community-standards-enforcement/?source=https%3A%2F%2Ftransparency.facebook.com%2Fcommunity-standards-enforcement.

[25] Roach S. (December 7, 2021) *3 TIMES BOTS HAVE IMPACTED MAJOR WORLD EVENTS*. Natacea. https://www.netacea.com/blog/3-times-bots-have-impacted-major-world-events/.

[26] Guesmi H. (January 27, 2021) *The social media myth about the Arab Spring*. AlJazeera. https://www.aljazeera.com/opinions/2021/1/27/the-social-media-myth-about-the-arab-spring.

[27] The Economic Times (November 30, 2021) *Arab Spring: The first smartphone revolution*. https://economictimes.indiatimes.com/news/international/saudi-arabia/arab-spring-the-first-smartphone-revolution/articleshow/79487524.cms.

[28] Savage M. (June 29, 2019) *How Brexit party won Euro elections on social media – simple, negative messages to older voters*. The Guardian. https://www.theguardian.com/politics/2019/jun/29/how-brexit-party-won-euro-elections-on-social-media.

supporting the Leave campaign, that were deactivated or removed by Twitter shortly after the ballot.[29]

In most recent times, a study by Carnegie Mellon University[30] on more than 200 million tweets discussing coronavirus from January to May 2020, found that about 45% of tweets on Covid were posted by accounts that behaved more like computerized robots than humans, spreading more than 100 false narratives about the virus.[31]

Nowadays, using recent developments in AI, it is possible to unleash human-like crowds of social bots, in coordinated campaigns of deception and influence[32] fueled by bots socialization with humans for attention, information, and money.[33] With advancements in natural language processing (NLP), a branch of AI that helps computers understand, interpret and manipulate human language,[34] bots can learn over time on the basis of their interactions with social media users, enabling them to respond in a manner that better resembles a human.[35]

Nevertheless, besides cutting-edge technologies or the exploitation of rudiments of AI, the manipulative use of social bots is a consequence of real people behavior and choices;[36] from programming, spreading manipulative content, and influencing communication exchanges on polarizing topics,[37] to choosing to believe those contents.

[29] Bastos M.T., Mercea D. (2017) *The Brexit Botnet and UserGenerated Hyperpartisan News*. Social Science Computer Review. https://journals.sagepub.com/doi/10.1177/0894439317734157.

[30] Allyn B. (May 20, 2020) *Researchers: Nearly Half Of Accounts Tweeting About Coronavirus Are Likely Bots*. NPR. https://www.npr.org/sections/coronavirus-live-updates/2020/05/20/859814085/researchers-nearly-half-of-accounts-tweeting-about-coronavirus-are-likely-bots?t=1655890800628.

[31] Roberts S. (June 16, 2020) *Who's a Bot? Who's Not?*. The New York Times. https://www.nytimes.com/2020/06/16/science/social-media-bots-kazemi.html.

[32] Terrence A. (June 2017) AI-Powered Social Bots. https://www.researchgate.net/publication/317650425_AI-Powered_Social_Bots.

[33] Liu X. (April 2019) A *big data approach to examining social bots on Twitter*. Journal of Services Marketing. https://www.researchgate.net/publication/332331554_A_big_data_approach_to_examining_social_bots_on_Twitter.

[34] Natural Language Processing (NLP) SAS. https://www.sas.com/it_it/insights/analytics/what-is-natural-language-processing-nlp.html.

[35] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes*. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

[36] CITS *How is Fake News Spread? Bots, People like You, Trolls, and Microtargeting*. https://www.cits.ucsb.edu/fake-news/spread.

[37] Chen W., Pacheco D., Yang K., Menczer F. (September 22, 2021) Neutral bots probe political bias on social media. Nature. https://www.nature.com/articles/s41467-021-25738-6.

Then, the malicious use of social bots needs to be contextualized in the ideology of terrorist or extremist groups. Thus, the next step of the analysis will be to outline how these actors have already and could further empower the consolidated acceptance of human-bot interaction through their ideology.

3. Social bots and jihad: different uses serving different purposes

Jihadist groups' ability to build and maintain a large online community through social media is well known, as well as their capacity, growing out of a state of necessity or creativity, to be early adopters of new technologies. In this respect, the nexus between AI and jihadist communication strategies is no exception: over time, jihadist groups have proven they can get out the most even with basic notions of AI or lack of financial resources.

Every day, bots are being used by jihadis, especially on Telegram,[38] for a wide variety of purposes.

The evolution of jihadists' exploitation of social bots can be analyzed by relating some topic cases with the objectives bots were meant to fulfill in the jihadist landscape.

3.1 Exploit users to expand the organization's influence

In 2014, long before the stricter policy adoption on terrorist propaganda by social media platforms, Daesh spread its official app "Dawn of the Glad Tidings" also known as "Dawn." It was an Arabic-language Twitter app, advertised by its top users as a way to keep up on the latest news about the jihadist group.[39] As a result, thousands of their Twitter followers installed the app on the web or their Android phones through the Google Play store and, after releasing a fair amount of personal data and signing up, they allowed the app to post tweets from their accounts.[40] Thus, Daesh was able to share, through thousands of accounts, simultaneously, content decided by its social-

[38] ISIS watch on Telegram claims that, only on June 22, 2022, 685 terrorist bots and channels has been banned and, since the beginning of June 2022, a total of 11387 terrorist bots and channels has been banned. https://t.me/ISISwatch/1049.

[39] Berger J.M. (June 16, 2014) *How ISIS Games Twitter*. The Atlantic. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[40] Kingsley P. (June 23, 2014) *Who is behind Isis's terrifying online propaganda operation?* The Guardian. https://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq.

media operation branches, gaining a far larger online reach than only top users would otherwise allow.

Dawn allowed to spread news of Daesh advances, trending hashtags, and propaganda videos, interrupting ongoing conversations and letting IS content seeps into popular discourse while contributing to create the organization's image of a violent and unstoppable force.[41]

3.2 Instruct and inform a digital community

The "Bot Mujahideen" Telegram Channel[42] worked as a centralized online interface meant to provide information on a wide range of topics related to jihad fighters in Syria.[43] It was launched in 2016 and, even though it stated it was "not affiliated with any organization and adheres to the path of the Sunnah and jihad," the correspondence published on the channel indicated its support for Jabhat Fateh al-Sham (formerly Al-Nusra Front, which was identified with Al-Qaeda) and other jihad factions tied to the group.[44]

The operative functions of the Bot Mujahideen declined through the management of several other Telegram channels, called "rooms"; each room was dedicated to a different issue and had over 1,000 members. As reported in a research by the ICT, among other rooms, the bot controlled: the "Military Sciences room" ('Ulum 'Askariyya) focused on military topics (e.g. study and operation of various weapons, defense against aircraft shootings, the study and assembly of explosive devices, etc.); "The Public Market of the Brothers," a virtual market for the sale and purchase of weapons; "Network Mujahideen Newsletter" a bot aimed to keep supporters updated on events about the jihad in Syria.

[41] Garfield L. (December 14, 2015) *ISIS has created thousands of political bots – and hacktivists want you to destroy them*. Business insider. https://www.businessinsider.com/anonymous-battles-isis-political-bots-2015-12?r=US&IR=T.

[42] Antinori A. (April 10, 2017) *The "Jihadi Wolf" Threat*. Europol. https://www.europol.europa.eu/sites/default/files/documents/antinoria_thejihadiwolfthreat.pdf.

[43] "On the profile of the channel it states that the channel expressed a "unique military jihadist collective program on the Telegram social network, as it is not affiliated with any organization and adheres to the path of the Sunnah and jihad". In addition, it states that "the Bot is a complete jihadist library. Its membership is composed of unique groups that are supervised by mujahideen and experts in their fields". @bot_mojahed2016_bot" ICT Cyber Desk (December 2016) *Cyber-Terrorism Activities Report No. 19*. International Institute for Counter-Terrorism (ICT).

[44] Barak M. (February 12, 2017) *The "Bot Mujahideen" Telegram Channel*. International Institute for Counter-Terrorism (ICT). https://ict.org.il/the-bot-mujahideen-telegram-channel/.

3.3 Secure and enlarge the recruitment process

As reported by MEMRI, the pro-Al-Qaeda Jaysh Al-Malahim Al-Electronic Telegram channel, in July 2020, announced the beginning of a recruiting process for supporters with expertise in programming, "media raids," film montage, hacking, translation, and graphic design. Those interested were directed to contact two Telegram bots.[45]

Meanwhile, the pro-ISIS Basa'ir Da'wah Foundation, on Telegram, urged supporters specialized in graphic design, poetry, and religious studies, to join the foundation's team by contacting its bot (Ghiras11bot) on the platform.[46]

Another example regards Bahrun Naim, one of former Daesh's top Indonesian propaganda distributors and mastermind of several terrorist attacks,[47] who also established a bot on Telegram to communicate with potential Indonesian recruits. The bot was also used as a propaganda vector, greeting users with an automated message in Bahasa Indonesian and subsequently sharing messages and videos, such as interviews with militants or guides for the fabrication of homemade explosives.[48]

Regarding the recruitment, same as for propaganda, these clusters of bots were employed so that if one account were suspended, other bots from the same cluster could continue its activities.[49]

3.4 Maintain the presence of digital archives widespread and permanent

Jihadist groups are also able to deploy bots designed to ensure access to digital archives of jihadi content produced by groups and media organizations.

[45] MEMRI Cyber terrorism and jihad lab (July 20, 2020) *Pro-Al-Qaeda Media Group Directs Supporters With Expertise In Programming, Hacking, And 'Media Raids' To Contact Telegram Bots*. https://www.memri.org/cjlab/pro-al-qaeda-media-group-directs-supporters-expertise-programming-hacking-and-media-raids.

[46] Stalinsky S., Sosnow R. (August 5, 2020) *Jihadi Use Of Bots On The Encrypted Messaging Platform Telegram*. MEMRI. https://www.memri.org/reports/jihadi-use-bots-encrypted-messaging-platform-telegram#_ednref13.

[47] Gunaratna R. (October 2018) *Mastermind of Terror: The Life and Death of Bahrun Naim*. Counter Terrorist Trends and Analyses Vol. 10, No. 10. https://www.jstor.org/stable/26501459?seq=1.

[48] Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet*. HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

[49] Garfield L. (14 December 2014) *ISIS has Created Thousands of Political Bots – and Hacktivistas Want You to Destroy Them*. Business Insider. https://www.businessinsider.com/anonymous-battles-isispolitical-bots-2015-12.

In this context, in 2017, Al-Shabaab's news agency, Shahada, used a bot on Telegram to share with supporters links to the group's most recent channel,[50] to keep a constant connection with its followers, even if their channel would have been suspended.[51] This strategy is used by many jihadist groups to maintain a constant information flow with their audience and quickly spread and keep track, for instance, of their latest magazine issues.

Another topical example regards Daesh's largest digital archives, nicknamed by CTC and ISD the "Cloud Caliphate,"[52] which held 97,706 folders and files, with more than 90,000 items in more than seven different languages.

This digital repository, which counted almost 10,000 unique visitors a month, curated a shared history of the movement while providing a way to continually replenish extremist content on the net.[53]

One of the ways to reach this huge library on the history and present of Daesh was thorough a cluster of pro-IS accounts that led to the discovery of the "Cloud Caliphate" aided by the 'TweetItBot' on Telegram, which also allowed users to share links directly from Telegram to Twitter. Furthermore, researchers believe the cache was tied to a digital support group named Sarh al-Khilafah, which allegedly operated a Telegram bot tasked with disseminating portions of the cache, folder-by-folder, to assure its constant presence online.

3.5 Keep in touch with supporters to encourage and improve terrorist attacks

Following the terrorist attack perpetrated with axes by two Palestinians in the Israeli city of Elad,[54] a Telegram channel, that supports Iran-backed militias, published a statement promising free weapons to residents of the

[50] MEMRI (June 30, 2017) *Al-Shabab Al-Mujahideen's Shahada News Agency Launches Bot to Connect with Users on Telegram.* https://www.memri.org/jttm/al-shabab-al-mujahideens-shahada-news-agency-launches-%E2%80%8Ebot-connect-users-telegram-%E2%80%8E.

[51] Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet.* HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

[52] Ayad M., Amarasingam A., Alexander A. (May 2021) *The Cloud Caliphate: Archiving the Islamic State in Real-Time.* Institute for Strategic Dialogue and Combating Terrorism Center at West Point. https://www.isdglobal.org/isd-publications/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/.

[53] Silva S. (September 4, 2020) *Islamic State: Giant library of group's online propaganda discovered.* BBC News. https://www.bbc.com/news/technology-54011034.

[54] BBC (May 5, 2022) *Elad attack: Three dead in central Israeli city.* https://www.bbc.com/news/world-middle-east-61339751.

West Bank willing to perpetrate terrorist attacks against Israel. The statement reads, "Do you live in the West Bank and want a rifle or a pistol? Please note, the weapons are free of charge. Contact us via the bot. We speak Arabic and English."[55] In this case, even though the statement did not include the address of the bot, there already were several known bots associated with the channel.

3.6 From AI basics to more complex jihadist social bots

The common denominator of the above-mentioned cases is the use of bots aimed to prevent setbacks[56] by facilitating recruitment and propaganda, displaying jihadist groups' defensive posture towards potential counter-terrorism measures.

But social bots have also the potential to help terrorist groups perpetrate active actions.

In this field, DoS or DDoS attacks,[57] already appealing to cybercriminals and other malicious actors, can be launched with very little effort and their performance has a relatively considerable impact. AI is likely to be exploited to make DoS or DDoS simpler, thanks to automating processes. For instance, machine learning algorithms[58] can be used to control the botnets behind the attack or enable them to identify vulnerable systems through sophisticated network reconnaissance.

In this respect, in 2016-2017, Daesh launched a series of DDoS attacks using a DDoS tool named "Caliphate Cannon." These attacks were quite successful and targeted military, economic, and education infrastructures, displaying the seriousness of this threat and encouraging its hacking division to perpetrate similar attacks against online services.[59]

[55] MEMRI (May 8, 2022) Telegram Channel That Supports Iran-Backed Militias Offers Free Weapons To West Bank Residents To Perpetrate Terrorist Attacks. https://www.memri.org/jttm/telegram-channel-supports-iran-backed-militias-offers-free-weapons-west-bank-residents.

[56] Cox K., Marcellino W., Bellasio J., Ward A., Galai K., Meranto S., Persi Paoli G. (November 2018) *Social Media in Africa – A Double-Edged Sword for Security and Development.* United Nations Development Programme (UNDP) Regional Centre for Africa. https://www.rand.org/pubs/external_publications/EP67728.html.

[57] Denial-of-service (DoS) attack is a denial of service attack. Distributed denial-of-service (DDoS) attack is where multiple systems target a single system with a DoS attack.

[58] Machine learning is a branch of AI and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy. IBM https://www.ibm.com/cloud/learn/machine-learning.

[59] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes.* https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

Soon, jihadist groups could also rely on more sophisticated, open-source, language AI tools to generate new content and engage with users. As some studies highlighted, among others, open-source tools like GPT-2[60] could be used to post auto-generated commentary on current events, promote likeminded posts, overwhelm conversations on social media, or re-direct conversations online to match with jihadist ideological views. Using GPT-2, with existing auto-detection technology, is not always possible to distinguish human-generated extremist content from AI-generated extremist content.

Finally, AI could be used to expand one of the major aspects that allow terrorist groups, and their various support arms, to evolve online: supporter-to-supporter learning.[61] As jihadist supporters learn from each other's methods or mistakes, the spread and development of social bots could exponentially increase, in numbers and efficiency, this emulation process from supporter-to-supporter to bot-to-supporter/supporter-to-bot learning.

4. Bots exploitation to arm digital crowds

According to a report by GNET, while Daesh (and jihadist groups in general) relied heavily on bot technology, racially and ethnically motivated violent extremist networks have so far refrained from widespread bot usage, mostly because of their different objectives and the more permissive online environment in which they operate.[62]

Nevertheless, far-right or conspiracy groups' use of social bots, deriving from different purposes and environments than jihadist groups, can highlight further communication branches in which AI can be exploited.

However, this part of the analysis is not detached from the previous one dedicated to jihadist groups.

[60] "GPT-2, an open-source unsupervised language model developed by Open AI that generates coherent paragraphs of text, performs reading comprehension, machine translation, question answering, and summarization without task-specific training." Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet*. HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

[61] Ayad M., Amarasingam A., Alexander A. (May 2021) *The Cloud Caliphate: Archiving the Islamic State in Real-Time*. Institute for Strategic Dialogue and Combating Terrorism Center at West Point. https://www.isdglobal.org/isd-publications/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/.

[62] Veilleux-Lepage Y., Daymon C., and Archambault E. (June 7, 2022) *Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies*. Global Network on Extremism & Technology. https://gnet-research.org/2022/06/07/learning-from-foes-how-racially-and-ethnically-motivated-violent-extremists-embrace-and-mimic-islamic-states-use-of-emerging-technologies/.

The following focus on the relation between extremist or conspiracy narratives and social bots is aimed to outline additional macro-areas of communication in which social bots can be exploited to reach malicious goals. Moreover, it doesn't exclude that also other religious, ethnically, politically motivated extremist or terrorist groups could use these declinations of social bots to fulfill their purposes.

4.1 Programmed defamation campaigns

According to the US Department of Homeland Security, social media bots can be used to harass users, overwhelming them to the point of deactivation.[63]

Harassment campaigns have long been an issue in online spaces[64] and can bring a twofold implication when perpetrated by extremist groups: reinforce their community and narratives while depriving their targets of the use of communication to defend themselves.

For instance, as reported by MEMRI, the neo-Nazi National Socialist Club's Telegram channel posted an invitation to its supporters, called "the white nationalist community" to "come together and Harass" companies whose employees "risk losing their employment" if their white supremacist and antisemitic views become known. The post suggested to act by creating bots able to "call and email these companies constantly to the point it disrupts their business and hurts their revenue."[65]

Harassing campaigns can also have the purpose of defaming targets, directly undermining their credibility or social influence. In these cases, bots can be deployed to amplify vitriolic attacks at scale.[66]

In 2017 U.S. far-right activists helped amplify a leak of hacked emails belonging to Emmanuel Macron, during its campaign for the French presi-

[63] US Department of Homeland Security (May 2018) *NATIONAL PROTECTION AND PROGRAMS DIRECTORATE – Office of Cyber and Infrastructure Analysis*. https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf.

[64] Geiger S.R. (2016) *Bot-based collective blocklists in Twitter: The counterpublic moderation of harassment in a networked public space*. Information, Communication, and Society 19(6). https://stuartgeiger.com/blockbots-ics.pdf.

[65] Stalinsky S. (April 13, 2022) *Neo-Nazis And White Supremacists Are Using Telegram Bots To Recruit Members, Disseminate Content, Maintain Supporter Anonymity, Promote Events, And Obtain Information About Individuals To Be Targeted For Attack*. MEMRI. https://www.memri.org/cjlab/neo-nazis-and-white-supremacists-are-using-telegram-bots-recruit-members-disseminate-content.

[66] Nyst N., Monaco N. (2018) *STATE-SPONSORED TROLLING How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Institute for the Future. https://www.iftf.org/statesponsoredtrolling/.

dential election, with a disinformation campaign consisting of rumors, fake news, and forged documents. An analysis by the Atlantic Council found that, on Twitter, the hashtag #MacronLeaks reached 47,000 tweets in three and a half hours and appeared in almost half a million tweets in twenty-four hours.[67] The hashtag was first used by Jack Posobiec, an internet performer and writer for the far-right news organization The Rebel, who declared to have shared a post he saw on 4chan.[68] Researchers found that the #MacronLeaks hashtag, due to the immediate, frequent, and concentrated engagement,[69] clearly indicated the use of social bots,[70] which also helped move the hashtag from the United States to France.[71]

4.2 Support and spread polarized views and fake news

Research from the University of California analyzed the use of social bots on left-leaning tweets and right-leaning tweets during the 2020 US elections.[72] From both macro-groups, the study highlighted six major types of Twitter bots: "Astroturf: manually labeled political bots that systematically delete content; Fake follower: bots purchased to increase follower counts; Financial: bots that post using "cashtags"; Self declared: bots from botwiki.org; Spammer: accounts labeled as spambots from several datasets; Other: miscellaneous other bots obtained from manual annotation, user feedback, etc."

In particular, in the macro-group of bots that tweeted right-leaning content, researchers found also clusters of bots posting highly structured conspiracy theory-related tweets with links and references to conspiracy theories

[67] Jeangène Vilmer J. (June 2019) *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/.

[68] Volz D. (May 7, 2017) *U.S. far-right activists, WikiLeaks and bots help amplify Macron leaks: researchers. Reuters.* https://www.reuters.com/article/us-france-election-cyber-idUSKBN1820QO.

[69] Hayden M.E. (January 29, 2021) *Twitter personality Jack Posobiec worked alongside other American far-right extremists in amplifying the fruits of an apparent Russian military intelligence (GRU) hack intended to disrupt the outcome of the French elections in May 2017*. Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2021/01/29/jack-posobiec-central-spreading-russian-intelligence-led-macronleaks-hack.

[70] Ferrara E. (August 2017) *Disinformation and social bot operations in the run up to the 2017 French presidential election*. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/8005.

[71] Southern Poverty Law Center. Jack Posobiec. https://www.splcenter.org/fighting-hate/extremist-files/individual/jack-posobiec.

[72] Ferrara E., Chang H., Chen E., Muric G., and Patel J. (October 2020) *Characterizing social media manipulation in the 2020 U.S. presidential election*. First Monday, 25(11). https://firstmonday.org/ojs/index.php/fm/article/view/11431/9993.

(i.e. Qanon,[73] "gate" conspiracies as #obamagate,[74] Covid conspiracies)[75] and links to conspiracy news organizations and web sites.

These kind of bot networks are established on bots designed to post content based on the major topics discussed inside the communities they try to blend into. Once they have gained a credible profile, they can disseminate disinformation or conspiracy theories as efficiently as users' accounts.[76] This mechanism leverages the increasing tendency for users on social media to interact prevalently with like-minded groups of people. This approach tends to make fake content more and more realistic, with the risk of blurring the line between legitimate political views and extremist narratives, while attracting broader support.[77]

Furthermore, the next generation of bots will threaten to move beyond text generation to audio and video manipulation.[78] Indeed, over time, disinformation campaigns on social media are likely to be aided by deepfakes,[79] a type of fake audio or visual content that has been manipulated or generated using Generative adversarial networks[80] (GANs).[81] Deepfake has been used, for instance, to produce the fake video, entirely fabricated using AI and wi-

[73] Roose K. (September 3, 2021) *What Is QAnon, the Viral Pro-Trump Conspiracy Theory?* The New York Times. https://www.nytimes.com/article/what-is-qanon.html.

[74] Wolfe J. (May 14, 2020) *Explainer: Trump keeps raising 'Obamagate.' What's that*? Reuters. https://www.reuters.com/article/us-usa-trump-obamagate-explainer-idUSKBN22Q1JL.

[75] Pertwee E., Simas C., and Larson H.J. (March 10, 2022) *An epidemic of uncertainty: rumors, conspiracy theories and vaccine hesitancy*. Nature. https://www.nature.com/articles/s41591-022-01728-z.

[76] Bontridder N., Poullet Y. (November 25, 2021) The role of artificial intelligence in disinformation. Cambridge University Press. https://www.cambridge.org/core/journals/data-and-policy/article/role-of-artificial-intelligence-in-disinformation/7C4BF6CA35184F149143DE968FC4C3B6#r1.

[77] Rovny J. (February 29, 2012) *Where do radical right parties stand? Position blurring in multidimensional competition*. Cambridge University Press. https://www.cambridge.org/core/journals/european-political-science-review/article/abs/where-do-radical-right-parties-stand-position-blurring-in-multidimensional-competition/69358EA1E09F6AD5B302631306AA4B16.

[78] Marcellino W., Magnuson M., Stickels A., Boudreax B., Helmus T.C., Geist E., and Winkelman Z. (2020) *Counter-Radicalization Bot Research – Using Social Bots to Fight Violent Extremism*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2705.html.

[79] CNN Business. *When seeing is no longer believing*. https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

[80] Generative adversarial networks (GANs) are algorithmic architectures that use two neural networks, pitting one against the other (thus the "adversarial") in order to generate new, synthetic instances of data that can pass for real data. They are used widely in image generation, video generation and voice generation. Pathmind. *Generative Adversarial Network Definition*. https://wiki.pathmind.com/generative-adversarial-network-gan.

[81] United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The*

dely shared on social media,[82] showing Ukrainian President, Volodymyr Zelenskyy, calling on Ukrainian citizens to stop fighting Russian soldiers and surrender their weapons, also claiming he had already fled Kyiv.[83]

4.3 Promote events

Neo-Nazis and white supremacists use bots to announce and promote events, such as marches and conferences.

In June 2021 a post forwarded by a French neo-nazi channel belonging to the "Cercle des Amis d'Adolf Hitler" announced an event titled "Adolf Hitler: Une Vie, Des Valeurs" to be held in Paris. It added that those interested could use the @Cercle_Hitler_Bot to register for the event.[84]

Furthermore, extremist events can also be exploited by state-sponsored botnets to spread extremist narratives and discord.

In the aftermath of the events of the white supremacist rally in Charlottesville, Virginia, researchers found that a large number of automated bots generating Twitter posts helped make right-wing conspiracy theories, and rallying cries about Charlottesville, go viral. The analyzed social bots sample included pro-Russian accounts that were pushing content from state-controlled outlets Russia Today and Sputnik.[85] One year later, Republican Rep. Tom Garrett also claimed, in an interview with CNN,[86] that FBI officials told him that Russian-sponsored social bots were attempting to sow discord around far-right circles before the event took place.

Malicious Use Of Artificial Intelligence For Terrorist Purposes. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

[82] Atlantic Council Digital Forensic Lab (March 16, 2022) *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/.

[83] Cote J. (April 1, 2022) *DEEPFAKES AND FAKE NEWS POSE A GROWING THREAT TO DEMOCRACY, EXPERTS WARN*. Northeastern. https://news.northeastern.edu/2022/04/01/deepfakes-fake-news-threat-democracy/.

[84] Stalinsky S. (April 13, 2022) *Neo-Nazis And White Supremacists Are Using Telegram Bots To Recruit Members, Disseminate Content, Maintain Supporter Anonymity, Promote Events, And Obtain Information About Individuals To Be Targeted For Attack*. MEMRI. https://www.memri.org/cjlab/neo-nazis-and-white-supremacists-are-using-telegram-bots-recruit-members-disseminate-content.

[85] Arnsdorf I. (August 23, 2017) *Pro-Russian Bots Take Up the Right-Wing Cause After Charlottesville*. ProPublica. https://www.propublica.org/article/pro-russian-bots-take-up-the-right-wing-cause-after-charlottesville.

[86] Nobles R. (August 13, 2018) *GOP lawmaker: FBI has evidence Russian bots were fanning flames before Charlottesville violence*. CNN. https://edition.cnn.com/2018/08/13/politics/tom-garrett-russian-bots-charlottesville-violence/index.html.

5. Coordinated waves of a digital crowd

Theoretically, crowd behavior can be compared to fluid dynamics. Its density doesn't let people move forward continuously, so they need to stop and wait for another opportunity to advance, generating "stop-and-go waves."[87] In these terms, digital crowds' behavior should also be better analyzed and understood because, even though they are physically dispersed, they can be considered as a collectively intelligent complex system, with unlimited growth.[88]

Uncontrolled exposure to extremist narratives or disinformation can have an impact on collective behavior and "when perturbed, complex systems tend to exhibit finite resilience followed by catastrophic, sudden, and often irreversible changes,"[89] similarly to stop-and-go waves.

Social bots can help coordinate the extent of these waves but is still not clear how much the manipulation of digital crowds can reverberate in real life or policymaking.[90] Indeed, existing research extensively studied bot detection, but bot coordination is still emerging and still requires more in-depth analysis.[91]

Even though who is running social bots is not always detectable, as bots can be exploited either for provocative campaigns or as part of an information war[92] while conspiracies or extremist contents tend to follow current events even when there aren't coordinated campaigns,[93] recurring patterns on the to-

[87] Lamb E. (January 17, 2017) *How Fluid Dynamics Can Help You Navigate Crowds*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/what-fluid-dynamics-can-teach-us-about-navigating-crowds-180961823/#:~:text=As%20a%20crowd%20gets%20denser,move%20forward%20into%20any%20gaps.

[88] Aradu C., Blank T. (2014) *The Politics of digital crowds*. Lo s uaderno Q, vol. 33. https://www.academia.edu/9989238/The_Politics_of_digital_crowds.

[89] Holtz J. (June 14, 2021) *Communication technology, study of collective behavior must be 'crisis discipline,' researchers argue*. University of Washington. https://www.washington.edu/news/2021/06/14/communication-technology-study-of-collective-behavior-must-be-crisis-discipline-researchers-argue/.

[90] Schreiber M. (March 4, 2022) *'Bot holiday': Covid disinformation down as social media pivot to Ukraine*. The Guardian. https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

[91] Khaund T., Kirdemir B., Agarwal N., Liu H., Morstatter F. (August 19, 2021) Social Bots and Their Coordination During Online Campaigns: A Survey. IEEE Transactions on Computational Social Systems. https://ieeexplore.ieee.org/document/9518390.

[92] Cantini R., Marozzo F., Talia D., and Trunfio P. (January 4, 2022) *Analyzing Political Polarization on Social Media by Deleting Bot Spamming*. Special Issue – Big Data and Cognitive Computing: 5th Anniversary Feature Papers. https://www.mdpi.com/2504-2289/6/1/3.

[93] Schreiber M. (March 4, 2022) *'Bot holiday': Covid disinformation down as social media pivot to Ukraine*. The Guardian. https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

pics and languages used by botnets coordinated activities can still be detected and should be better analyzed.

For instance, some cases represent a coordinated shift of social bots to different stories; coordinated attempts to expand and actualize disinformation or extremist narratives to follow an agenda, pushing new topics, new terms, and hashtags in the social media environment.

In this respect, a study on bots and misinformation on Covid analyzed social bot tweets from January 2020 to August 2020. Some of these bots, identified between 2011 and 2019, were discovered before the pandemic and were originally designed for non-COVID-19 purposes, such as promoting product hashtags, retweeting political candidates, and spreading links to malicious content.[94]

Other researchers found that, in the wake of Russia's invasion of Ukraine, online activity on Twitter surged by nearly 20%. The analysis highlighted that ethnically motivated extremist accounts, such as those posting content on New World Order (NWO) conspiracy,[95] shifted from topics related to Covid, a secret group controlling the global economy, and speculations about the end times,[96] almost entirely into Ukraine and Putin themes.[97]

Understanding the exploitation of botnets could help increase public awareness and avoid users, and public figures, from involuntarily becoming echo chambers for malicious social bots clusters. This could be a valuable tool to prevent either state or non-state malicious actors from generating unpredictable waves of digital crowds at their advantage.

These are not marginal aspects, because, as explained by the above-mentioned theory on crowd behavior and fluid dynamics: even though waves do not always portend a collapse, the stop-and-go wave can also be a warning signal for the situation in the crowd to become critical.[98]

[94] McKenzie H., Giorgi S., Devoto A., Rahman M., Ungar L., Schwartz H.A., EpsteinD.H., Leggio L., and Curtis B. (May 20, 2021) *Bots and Misinformation Spread on Social Media: Implications for COVID-19*. Journal of Medical Internet Research. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8139392/.

[95] Flores M. (May 30, 2022) *The New World Order: The Historical Origins of a Dangerous Modern Conspiracy Theory*. Middlebury Institute of International Studies at Monterey. https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/new-world-order-historical-origins-dangerous.

[96] Barkun M. (May 2012) *Culture of Conspiracy: Apocalyptic Visions in Contemporary America*. California Scholarship Online.

[97] NCRI insight report (March 1, 2022) *New World Order Conspiracy Theories and Anti-Nato Rhetoric Surging on Twitter Amid Russian Invasion of Ukraine*. https://networkcontagion.us/wp-content/uploads/NCRI-Insights-SitRep-March-2022.pdf.

[98] Lamb E. (January 17, 2017) *How Fluid Dynamics Can Help You Navigate Crowds*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/what-fluid-dynamics-can-teach-us-

References

Accenture (June 17, 2022) *The unreal – making synthetic, authentic*. https://www.accenture.com/th-en/insights/health/unreal-making-synthetic-authentic.

Accenture (March 16, 2022) *Technology Vision 2022: "Metaverse Continuum" Redefining How the World Works, Operates and Interacts*. https://newsroom.accenture.com/subjects/metaverse/accenture-technology-vision-2022-metaverse-continuum-redefining-how-the-world-works-operates-and-interacts.htm.

Allyn B. (May 20, 2020) *Researchers: Nearly Half Of Accounts Tweeting About Coronavirus Are Likely Bots*. NPR. https://www.npr.org/sections/coronavirus-live-updates/2020/05/20/859814085/researchers-nearly-half-of-accounts-tweeting-about-coronavirus-are-likely-bots?t=1655890800628.

Antinori A. (April 10, 2017) *The "Jihadi Wolf" Threat*. Europol. https://www.europol.europa.eu/sites/default/files/documents/antinoria_thejihadiwolfthreat.pdf.

Aradu C., Blank T. (2014) *The Politics of digital crowds*. Lo s uaderno Q, vol. 33. https://www.academia.edu/9989238/The_Politics_of_digital_crowds.

Arnsdorf I. (August 23, 2017) *Pro-Russian Bots Take Up the Right-Wing Cause After Charlottesville*. ProPublica. https://www.propublica.org/article/pro-russian-bots-take-up-the-right-wing-cause-after-charlottesville.

Assenmacher D., Clever L., Frischlich L., Quandt T., Trautmann H., and Grimme C. (September 1, 2020) *Demystifying Social Bots: On the Intelligence of Automated Social Media Actors*. Social media and Society. https://journals.sagepub.com/doi/10.1177/2056305120939264.

Atlantic Council Digital Forensic Lab (March 16, 2022) *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/.

Ayad M., Amarasingam A., Alexander A. (May 2021) *The Cloud Caliphate: Archiving the Islamic State in Real-Time*. Institute for Strategic Dialogue and Combating Terrorism Center at West Point. https://www.isdglobal.org/isd-publications/the-cloud-caliphate-archiving-the-islamic-state-in-real-time/.

Barak M. (February 12, 2017) *The "Bot Mujahideen" Telegram Channel*. International Institute for Counter-Terrorism (ICT). https://ict.org.il/the-bot-mujahideen-telegram-channel/.

Barkun M. (May 2012) *Culture of Conspiracy: Apocalyptic Visions in Contemporary America*. California Scholarship Online.

Bartlett R., Morse A., Stanton R., and Wallace N. (June 2019) *Consumer-Lending Discrimination in the FinTech Era*. National Bureau of Economic Research. https://www.nber.org/papers/w25943#:~:text=FinTech%20algorithms%20also%20discriminate%2C%20but,borrowers%20on%20low%2Dshopping%20behavior.

about-navigating-crowds-180961823/#:~:text=As%20a%20crowd%20gets%20denser,move%20forward%20into%20any%20gaps.

Bastos M.T., Mercea D. (2017) *The Brexit Botnet and UserGenerated Hyperpartisan News*. Social Science Computer Review. https://journals.sagepub.com/doi/10.1177/0894439317734157.

BBC (May 5, 2022) *Elad attack: Three dead in central Israeli city*. https://www.bbc.com/news/world-middle-east-61339751.

Berger J.M. (June 16, 2014) *How ISIS Games Twitter*. The Atlantic. https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

Bontridder N., Poullet Y. (November 25, 2021) The role of artificial intelligence in disinformation. Cambridge University Press. https://www.cambridge.org/core/journals/data-and-policy/article/role-of-artificial-intelligence-in-disinformation/7C4BF6CA35184F149143DE968FC4C3B6#r1.

Botometer https://botometer.osome.iu.edu/.

Cantini R., Marozzo F., Talia D., and Trunfio P. (January 4, 2022) *Analyzing Political Polarization on Social Media by Deleting Bot Spamming*. Special Issue – Big Data and Cognitive Computing: 5th Anniversary Feature Papers. https://www.mdpi.com/2504-2289/6/1/3.

Castellanos S. (July 23, 2021) *Fake It to Make It: Companies Beef Up AI Models With Synthetic Data*. Wall Street Journal. https://www.wsj.com/articles/fake-it-to-make-it-companies-beef-up-ai-models-with-synthetic-data-11627032601.

Chen W., Pacheco D., Yang K., Menczer F. (September 22, 2021) *Neutral bots probe political bias on social media*. Nature. https://www.nature.com/articles/s41467-021-25738-6.

Ciancaglini V., Gibson C., Sancho D., Amann P., Klayn A., McCarthy O., and Eira M. (November 19, 2020). *Malicious Uses and Abuses of Artificial Intelligence. Trend Micro*. EUROPOL and UNICRI. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf.

CITS *How is Fake News Spread? Bots, People like You, Trolls, and Microtargeting*. https://www.cits.ucsb.edu/fake-news/spread.

Cloudfare. *What is a social media bot? | Social media bot definition*. https://www.cloudflare.com/it-it/learning/bots/what-is-a-social-media-bot/#:~:text=Experts%20who%20have%20applied%20logarithms,designed%20to%20mimic%20human%20accounts.

CNN Business. *When seeing is no longer believing*. https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

Cote J. (April 1, 2022) *DEEPFAKES AND FAKE NEWS POSE A GROWING THREAT TO DEMOCRACY, EXPERTS WARN*. Northeastern. https://news.northeastern.edu/2022/04/01/deepfakes-fake-news-threat-democracy/.

Cox K., Marcellino W., Bellasio J., Ward A., Galai K., Meranto S., Persi Paoli G. (November 2018) *Social Media in Africa – A Double-Edged Sword for Security and Development*. United Nations Development Programme (UNDP) Regional Centre for Africa. https://www.rand.org/pubs/external_publications/EP67728.html.

European Commission (June 16, 2022) *Disinformation: Commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3664.

European Commission (June 16, 2022) *Signatories of the 2022 Strengthened Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

European Commission *2018 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

European Commission *The 2022 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

Ferrara E. (August 2017) *Disinformation and social bot operations in the run up to the 2017 French presidential election*. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/8005.

Ferrara E., Chang H., Chen E., Muric G., and Patel J. (October 2020) *Characterizing social media manipulation in the 2020 U.S. presidential election*. First Monday, 25(11). https://firstmonday.org/ojs/index.php/fm/article/view/11431/9993.

Flores M. (May 30, 2022) *The New World Order: The Historical Origins of a Dangerous Modern Conspiracy Theory*. Middlebury Institute of International Studies at Monterey. https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/new-world-order-historical-origins-dangerous.

Forsbak Ø. (March 25, 2022) *Six AI Trends To Watch In 2022*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/03/25/six-ai-trends-to-watch-in-2022/?sh=3e1c36e62be1.

Garfield L. (14 December 2014) *ISIS has Created Thousands of Political Bots – and Hacktivistas Want You to Destroy Them*. Business Insider. https://www.businessinsider.com/anonymous-battles-isispolitical-bots-2015-12.

Geiger S.R. (2016) *Bot-based collective blocklists in Twitter: The counterpublic moderation of harassment in a networked public space*. Information, Communication, and Society 19(6). https://stuartgeiger.com/blockbots-ics.pdf.

Guesmi H. (January 27, 2021) *The social media myth about the Arab Spring*. AlJazeera. https://www.aljazeera.com/opinions/2021/1/27/the-social-media-myth-about-the-arab-spring.

Gunaratna R. (October 2018) *Mastermind of Terror: The Life and Death of Bahrun Naim*. Counter Terrorist Trends and Analyses Vol. 10, No. 10. https://www.jstor.org/stable/26501459?seq=1.

Harvard special edition: *Artificial Intelligence*. https://sitn.hms.harvard.edu/special-edition-artificial-intelligence/.

Hayden M.E. (January 29, 2021) *Twitter personality Jack Posobiec worked alongside other American far-right extremists in amplifying the fruits of an apparent Russian military intelligence (GRU) hack intended to disrupt the outcome of the French elections in May 2017*. Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2021/01/29/jack-posobiec-central-spreading-russian-intelligence-led-macronleaks-hack.

Holtz J. (June 14, 2021) *Communication technology, study of collective behavior must be 'crisis discipline,' researchers argue*. University of Washington. https://www.washington.edu/news/2021/06/14/communication-technology-study-of-collective-behavior-must-be-crisis-discipline-researchers-argue/.

IBM *Application Programming Interface (API)*. https://www.ibm.com/cloud/learn/api.

IBM *Machine learning*. https://www.ibm.com/cloud/learn/machine-learning.

ICT Cyber Desk (December 2016) *Cyber-Terrorism Activities Report No. 19*. International Institute for Counter-Terrorism (ICT).

ISIS watch on Telegram https://t.me/ISISwatch/1049.

Jeangène Vilmer J. (June 2019) *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/.

Khaund T., Kirdemir B., Agarwal N., Liu H., Morstatter F. (August 19, 2021) Social Bots and Their Coordination During Online Campaigns: A Survey. IEEE Transactions on Computational Social Systems. https://ieeexplore.ieee.org/document/9518390.

Kilcher Y. (June 3, 2022) *This is the worst AI ever*. YouTube. https://www.youtube.com/watch?v=efPrtcLdcdM.

Kingsley P. (June 23, 2014) *Who is behind Isis's terrifying online propaganda operation?* The Guardian. https://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq.

Lamb E. (January 17, 2017) *How Fluid Dynamics Can Help You Navigate Crowds*. Smithsonian Magazine. https://www.smithsonianmag.com/science-nature/what-fluid-dynamics-can-teach-us-about-navigating-crowds-180961823/#:~:text=As%20a%20crowd%20gets%20denser,move%20forward%20into%20any%20gaps.

Liu X. (April 2019) *A big data approach to examining social bots on Twitter*. Journal of Services Marketing. https://www.researchgate.net/publication/332331554_A_big_data_approach_to_examining_social_bots_on_Twitter.

Marcellino W., Magnuson M., Stickels A., Boudreax B., Helmus T.C., Geist E., and Winkelman Z. (2020) *Counter-Radicalization Bot Research – Using Social Bots to Fight Violent Extremism*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2705.html.

McKenzie H., Giorgi S., Devoto A., Rahman M., Ungar L., Schwartz H.A., EpsteinD.H., Leggio L., and Curtis B. (May 20, 2021) *Bots and Misinformation Spread on Social Media: Implications for COVID-19*. Journal of Medical Internet Research. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8139392/.

MEMRI (June 30, 2017) *Al-Shabab Al-Mujahideen's Shahada News Agency Launches Bot to Connect with Users on Telegram*. https://www.memri.org/jttm/al-shabab-al-mujahideens-shahada-news-agency-launches-%E2%80%8Ebot-connect-users-telegram-%E2%80%8E.

MEMRI (May 8, 2022) Telegram Channel That Supports Iran-Backed Militias Offers Free Weapons To West Bank Residents To Perpetrate Terrorist Attacks. https://

www.memri.org/jttm/telegram-channel-supports-iran-backed-militias-offers-free-weapons-west-bank-residents.

MEMRI Cyber terrorism and jihad lab (July 20, 2020) *Pro-Al-Qaeda Media Group Directs Supporters With Expertise In Programming, Hacking, And 'Media Raids' To Contact Telegram Bots*. https://www.memri.org/cjlab/pro-al-qaeda-media-group-directs-supporters-expertise-programming-hacking-and-media-raids.

Meta, Community Standards Enforcement Report – Q1 2022 report. https://transparency.fb.com/data/community-standards-enforcement/?source=https%3A%2F%2Ftransparency.facebook.com%2Fcommunity-standards-enforcement.

Natural Language Processing (NLP) SAS. https://www.sas.com/it_it/insights/analytics/what-is-natural-language-processing-nlp.html.

NCRI insight report (March 1, 2022) *New World Order Conspiracy Theories and Anti-Nato Rhetoric Surging on Twitter Amid Russian Invasion of Ukraine*. https://networkcontagion.us/wp-content/uploads/NCRI-Insights-SitRep-March-2022.pdf.

Nobles R. (August 13, 2018) *GOP lawmaker: FBI has evidence Russian bots were fanning flames before Charlottesville violence*. CNN. https://edition.cnn.com/2018/08/13/politics/tom-garrett-russian-bots-charlottesville-violence/index.html.

Nyst N., Monaco N. (2018) *STATE-SPONSORED TROLLING How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Institute for the Future. https://www.iftf.org/statesponsoredtrolling/.

Pathmind. *Generative Adversarial Network Definition*. https://wiki.pathmind.com/generative-adversarial-network-gan.

Pertwee E., Simas C., and Larson H.J. (March 10, 2022) *An epidemic of uncertainty: rumors, conspiracy theories and vaccine hesitancy*. Nature. https://www.nature.com/articles/s41591-022-01728-z.

PR Newswire (June 13, 2022) *Artificial Intelligence Market USD 1,581.70 Billion By 2030, Growing At A CAGR of 38.0%*. Bloomberg press release. https://www.bloomberg.com/press-releases/2022-06-13/artificial-intelligence-market-usd-1-581-70-billion-by-2030-growing-at-a-cagr-of-38-0-valuates-reports#:~:text=Artificial%20Intelligence%20Market%20USD%201%2C581.70,38.0%25%20%2D%20Valuates%20Reports%20%2D%20Bloomberg.

Roach S. (December 7, 2021) *3 TIMES BOTS HAVE IMPACTED MAJOR WORLD EVENTS*. Natacea. https://www.netacea.com/blog/3-times-bots-have-impacted-major-world-events/.

Roberts S. (June 16, 2020) *Who's a Bot? Who's Not?*. The New York Times. https://www.nytimes.com/2020/06/16/science/social-media-bots-kazemi.html.

Roose K. (September 3, 2021) *What Is QAnon, the Viral Pro-Trump Conspiracy Theory?* The New York Times. https://www.nytimes.com/article/what-is-qanon.html.

Rovny J. (February 29, 2012) *Where do radical right parties stand? Position blurring in multidimensional competition*. Cambridge University Press. https://www.cambridge.org/core/journals/european-political-science-review/article/abs/where-do-radical-right-parties-stand-position-blurring-in-multidimensional-competition/69358EA1E09F6AD5B302631306AA4B16.

Savage M. (June 29, 2019) *How Brexit party won Euro elections on social media – simple, negative messages to older voters*. The Guardian. https://www.theguardian.com/politics/2019/jun/29/how-brexit-party-won-euro-elections-on-social-media.

Schreiber M. (March 4, 2022) *'Bot holiday': Covid disinformation down as social media pivot to Ukraine*. The Guardian. https://www.theguardian.com/media/2022/mar/04/bot-holiday-covid-misinformation-ukraine-social-media.

Silva S. (September 4, 2020) *Islamic State: Giant library of group's online propaganda discovered*. BBC News. https://www.bbc.com/news/technology-54011034.

Southern Poverty Law Center. Jack Posobiec. https://www.splcenter.org/fighting-hate/extremist-files/individual/jack-posobiec.

Stalinsky S. (April 13, 2022) *Neo-Nazis And White Supremacists Are Using Telegram Bots To Recruit Members, Disseminate Content, Maintain Supporter Anonymity, Promote Events, And Obtain Information About Individuals To Be Targeted For Attack*. MEMRI. https://www.memri.org/cjlab/neo-nazis-and-white-supremacists-are-using-telegram-bots-recruit-members-disseminate-content.

Stalinsky S., Sosnow R. (August 5, 2020) *Jihadi Use Of Bots On The Encrypted Messaging Platform Telegram*. MEMRI. https://www.memri.org/reports/jihadi-use-bots-encrypted-messaging-platform-telegram#_ednref13.

Terrence A. (June 2017) AI-Powered Social Bots. https://www.researchgate.net/publication/317650425_AI-Powered_Social_Bots.

The Economic Times (November 30, 2021) *Arab Spring: The first smartphone revolution*. https://economictimes.indiatimes.com/news/international/saudi-arabia/arab-spring-the-first-smartphone-revolution/articleshow/79487524.cms.

The Economist (May 6, 2017) *The world's most valuable resource is no longer oil, but data*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Towes R. (June 12, 2022) *Synthetic Data Is About To Transform Artificial Intelligence*. Forbes. https://www.forbes.com/sites/robtoews/2022/06/12/synthetic-data-is-about-to-transform-artificial-intelligence/?sh=5e6a76c07523.

United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Office of Counter-Terrorism (UNCCT) (2022) *Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes*. https://unicri.it/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes.

US Department of Homeland Security (May 2018) *NATIONAL PROTECTION AND PROGRAMS DIRECTORATE – Office of Cyber and Infrastructure Analysis*. https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf.

Veilleux-Lepage Y., Daymon C., and Archambault E. (June 7, 2022) *Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State's Use of Emerging Technologies*. Global Network on Extremism & Technology. https://gnet-research.org/2022/06/07/learning-from-foes-how-racially-and-ethnically-motivated-violent-extremists-embrace-and-mimic-islamic-states-use-of-emerging-technologies/.

Volz D. (May 7, 2017) *U.S. far-right activists, WikiLeaks and bots help amplify Macron leaks: researchers. Reuters.* https://www.reuters.com/article/us-france-election-cyber-idUSKBN1820QO.

Vosoughi S., Roy D., and Aral S. (March 9, 2018) *The spread of true and false news online*. Science. https://www.science.org/doi/10.1126/science.aap9559.

Wolfe J. (May 14, 2020) *Explainer: Trump keeps raising 'Obamagate.' What's that?* Reuters. https://www.reuters.com/article/us-usa-trump-obamagate-explainer-idUSKBN22Q1JL.

Zeiger S., Gyte J. (November 2020) *Prevention of Radicalization on Social Media and the Internet.* HANDBOOK OF TERRORISM PREVENTION – Chapter 12. https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/.

Crisis management vs. cyber threats

Mirosław Karpiuk

Mirosław Karpiuk, PhD., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ORCID: 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl.

Abstract

An effective response to cyber crises is determined not only by having forces and resources adequate to such a threat, but having appropriate regulations in this regard are also important. The European Union has not yet developed common standards to deal with the threats that cause such crises, instead leaving crisis management in the event of such crises situations caused by cyber-attacks firmly to national legislation.

Commission Recommendation (EU) 2021/1086 of 23 June 2021 on the Establishment of a Common Cyberspace Unit (OJ EU L 237, p. 1) states that Member States and relevant EU institutions, bodies and agencies should ensure a coordinated EU response to, and recovery from, large-scale cyber incidents and crises. In this situation, it is necessary to swiftly and effectively mobilise operational resources for mutual assistance. In order to provide an effective coordinated response to cyber crises, relevant actors should be able to share best practices and ensure necessary preparedness. Their operation should take into account existing processes and the expertise of the different cybersecurity communities.

In turn, according to Commission Recommendation (EU) 2017/1584 of 13 September 2017 on the Coordinated Response to Large-Scale Cybersecurity Incidents and Crises (OJ EU L 239, p. 36), Member States and EU institutions should establish an EU Cybersecurity Crisis Response Framework integrating the objectives and modalities of cooperation. The EU Cybersecurity Crisis Response Framework should, in particular, identify the relevant actors, EU institutions and Member State authorities, at all necessary levels – technical, operational, strategic – and develop standard operating procedures that define the way in which these cooperate within the context of EU crisis management mechanisms. Emphasis should be placed on enabling the exchange of information without undue delay and coordinating the response during large-scale cybersecurity incidents and crises.

Keywords

Crisis management, cybersecurity, critical infrastructure, essential service

1. Introduction

Cyber threats can lead to all sorts of adverse phenomena, including crises, especially if cyber-attacks target communication and information systems designed to achieve the state's strategic objectives, including those related to ensuring the continuity of critical infrastructure. Threats in cyberspace can lead to crisis situations, especially since public institutions and private entities are largely digitised and the communication and information systems they use are not always properly secured.

The Polish legislators in Article 2 of the Act of 26 April 2007 on Crisis Management (consolidated text: Journal of Laws of 2022, item 261, as amended – hereinafter: the ACM) defines crisis management as the activities of public administration authorities which are part of State security management, and which consist in the prevention of crisis situations, the preparation to control such crisis situations as part of planned activities, response in the event of the occurrence of a crisis situation, the elimination of their consequences, and the restoration of resources and critical infrastructure. Based on the legal definition of crisis management, it is possible to distinguish four phases of crisis management: prevention, preparation, response and recovery (Czuryk, Dunaj, Karpiuk, Prokop 2016, p. 21). The term comprises the activities of public administration authorities that involve responding to a threat resulting in the emergence of a crisis situation (or the possibility thereof). The preventive aspects of such activities are extremely important, allowing the prevention of the emergence of such situations.

A crisis situation, as defined in Article 3(1) of the ACM, is a situation that has a negative impact on the level of security of the population, can cause significant damages to property or the natural environment, and results in substantial limitations of the activities performed by public administration authorities due to inadequate forces and resources. The legislators do not list the prerequisites that can lead to such a situation, so it should be assumed that it can be triggered by any threat that significantly affects the level of security. Such situations can therefore also emerge due to cyber threats. Accordingly, the role of the authorities responsible for crisis management is also to act to ensure cybersecurity, to the extent that threats in cyberspace may result in the emergence of a crisis situation.

As defined in Article 2(4) of the Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws of 2020, item 1369, as amended – hereinafter: the NCSA) cybersecurity means the resilience of information systems to any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems. And an information system is a communication and information system and the electronic data processed in it. A communication and information system is defined in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (Journal of Laws of 2021, item 2070 as amended) as a set of cooperating IT hardware and software, providing the possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type. The concept of cybersecurity involves the protection of resources (data, information, i.e. digital content), the protection of communication and information systems and networks, devices, as well as the protection of content transmission over the network (Chałubinska-Jentkiewicz 2019, p. 20)

The managing authorities are also part of the National Cybersecurity System, the objective of which, pursuant to Article 3 of the NCSA, is to ensure cybersecurity at a national level, including the uninterrupted provision of essential services and digital services by achieving an appropriate level of security of the information systems used to provide these services and ensuring the handling of incidents.

According to Commission Recommendation (EU) 2021/1086 of 23 June 2021 on the Establishment of a Common Cyberspace Unit (OJ EU L 237, p. 1), faced with the cross-border nature of cybersecurity threats and the continuous surge of more complex, pervasive and targeted attacks, relevant cybersecurity institutions and actors should increase their ability to respond to such threats and attacks by harnessing existing resources and better coordinating efforts. All relevant actors in the EU need to be prepared to respond collectively and exchange information in such scope. The purpose of this Recommendation is to identify the actions necessary to coordinate EU efforts to prevent, detect, discourage, deter, mitigate and respond to large-scale cyber incidents and crises. Member States and relevant EU institutions, bodies and agencies should ensure that, in cases of large-scale cybersecurity incidents and crises, they coordinate their efforts through a Joint Cyber Unit which enables mutual assistance through expertise from Member State authorities and relevant EU institutions, bodies and agencies.

2. Critical infrastructure protection against cybersecurity threats

The objective of the crisis management system is to protect critical infrastructures from the threats that have an impact on their operation. The operation of critical infrastructures can be disrupted by threats occurring in cyberspace, so the protection must take into account the principles of cybersecurity allowing them to operate properly, and so not only the anticipation and elimination of obstacles, but also the elimination of any damage caused by unwanted incidents.

(National) critical infrastructure should be construed as systems and their functionally related facilities, including civil structures, equipment, installations, services essential to the security of the state and its citizens required to ensure the smooth functioning of public administration authorities, as well as institutions and entrepreneurs. This definition is given in Article 3(2) of the ACM, also indicating that it includes the following systems: 1) the supply of energy, energy-producing raw materials and fuels; 2) communications systems; 3) ICT networks; 4) financial systems; 5) food supply; 6) water supply; 7) health care systems; 8) transport systems; 9) rescue systems; 10) systems ensuring the continuity of public administration; 11) manufacturing, warehousing, storage and the use of chemical and radioactive substances, including pipelines for dangerous substances. A critical infrastructure will have a European dimension if its disruption or destruction would have a significant impact on at least two European Union member states.

In Article 3(3) of the ACM the legislators also defined critical infrastructure protection, defined as all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter threats, risks or vulnerabilities, as well as to limit and neutralise their effects and to ensure their rapid restoration in case of breakdowns, attacks or other events which disrupt their proper functioning. Therefore, critical infrastructure protection comprises a preventive aspect (anticipating threats and providing protection against them), a current aspect (combating threats), and a follow-up aspect (removing the effects of threats). All these stages of critical infrastructure protection are very important from the perspective of effective crisis management, including cases of threats occurring in cyberspace.

An important planning document covering critical infrastructure protection is the National Critical Infrastructure Protection Programme established by the Council of Ministers in the form of a resolution. It clearly provides that the critical infrastructure protection system should apply to all types of identified threats – natural, intentional or technical – and be prepared to restore the functions performed by the infrastructure as quickly as possible. In addition, the system should be comprehensive and flexible, as well as easy for those responsible for protecting critical infrastructure to apply and to understand its mechanisms. Critical infrastructure protection is carried out, among other things, through the provision of ICT security, which is seen as a set of organisational and technical measures aimed at minimising the risk of disrupting the functioning of this infrastructure following any unauthorised impact on communication and information systems. Pursuant to § 7 of the Regulation of the Council of Ministers of 30 April 2010 on the National Critical Infrastructure Protection Programme (Journal of Laws of 2010 No. 83, item 541), the conditions for improving critical infrastructure security are created through: 1) the implementation of the designated priorities and objectives of the programme; 2) ensuring conditions for improving the protection and continuity of critical infrastructure; 3) preparation for crisis situations that may result from or adversely affect the disruption of critical infrastructure; 4) the preparation for responding in situations of the destruction or disruption of critical infrastructure; 5) ensuring conditions for critical infrastructure reconstruction; 6) compliance with the standards and requirements of the programme; 7) cooperation in implementing the programme.

The National Critical Infrastructure Protection Programme is an element of planned activities performed by public administration in the area of security, which also involves cyber threats. Public administration authorities are required to draw up various types of plans, strategies, or programmes. Furthermore, in their planning documents they sometimes have to take into account cybersecurity as an important element to ensure efficient performance of the public tasks that need to be protected against cyber threats. Planning, including planning for cyberspace, makes it possible to take coordinated action allowing for the proper, timely and harmonious implementation of the objectives set for public administration in an organised and continuous manner, especially with the involvement of many entities (Karpiuk 2021, p. 47).

In Article 6(1) of the ACM, the legislators generally define critical infrastructure protection tasks, indicating that they include: 1) the collection and processing of information concerning threats to critical infrastructure; 2) the development and implementation of procedures in the event of threats to critical infrastructure; 4) the reconstruction of critical infrastructure; 5) collaboration between public administration and owners, owner-like possessors and lessees of critical infrastructure facilities, installations or devices in respect of their protection. Threats to critical infrastructure can vary in nature and affect it in different ways. Particularly dangerous are attacks on communication and information systems, including those used for fundamental tasks, whether in terms of the stability of the economy or the normal operation of the state, especially since the critical infrastructure serving these purposes is largely automated and thus vulnerable to cyber-attacks.

Owners, autonomous possessors and dependent possessors of critical infrastructure facilities, installations or equipment are obliged to protect them, in particular by preparing and implementing, adequately to the foreseen threats, critical infrastructure protection plans and by maintaining their own backup systems ensuring security and sustaining the functioning of this infrastructure until its complete restoration. If at the same time they are operators of essential services, they include in their critical infrastructure protection plans documentation concerning cybersecurity of the information systems used to provide essential services. This obligation is imposed by Article 6 (5-5a) of the ACM. Therefore, in this instance, the cybersecurity elements must be mandatorily taken into account when drawing up critical infrastructure protection plans.

A critical infrastructure protection plan drawn up by its operator, pursuant to § 2 of the Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans (Journal of Laws of 2010 No. 83, item 542), should include: 1) general data: a) including the name and location of any critical infrastructure, b) allowing the identification of the operators of critical infrastructure, including names, addresses and registered offices, c) allowing the identification of the entities that manage the company on behalf of the operator of critical infrastructures, including names, addresses and registered offices, d) including, to the extent necessary for the implementation of crisis management tasks, the business data of the owners, autonomous possessors and dependent possessors of facilities, installations or equipment of critical infrastructure responsible for maintaining contacts with entities competent for the protection of critical infrastructure, e) including the name of the person drawing up the plan; 2) critical infrastructure data including: (a) characteristics and basic technical parameters, (b) a plan (map) showing the location of facilities, installations or the system, (c) functional connections to other facilities, installations, equipment or services; 3) characteristics of: (a) threats to critical infrastructure and an assessment of the risk of their occurrence, together with anticipated scenarios for the development of events, (b) the dependence of critical infrastructure on other critical infrastructure systems and the possibility of disruption as a result of disruptions in other critical infrastructure systems, (c) their own resources that can be used to protect critical infrastructure, (d) resources of territorially competent authorities that can be used to protect critical infrastructure; 4) essential options: (a) to act in a situation of threat or disruption to the operation of critical infrastructure, (b) to ensure continued operation of critical infrastructure, (c) to reconstruct critical infrastructure; 5) principles of cooperation with locally competent: (a) crisis management centres, (b) public administration authorities.

3. Essential services vs. cyber threats

Essential services are of major importance for crisis management. The NCSA imposes a number of cybersecurity protection obligations on owners, autonomous possessors and dependent possessors of critical infrastructure facilities, installations or equipment that are operators of essential services.

They are provided in the energy, transportation, banking, health care, water supply, or digital infrastructure sectors.

An essential service is defined in Article 2(16) of the NCSA as a service that is essential for the maintenance of critical societal and/or economic activities, as included in the list of essential services.

The authority competent for cybersecurity shall issue a decision recognising the entity as an operator of essential services if: 1) the entity provides an essential service; 2) the provision of this service depends on information systems; 3) an incident would have significant disruptive effects on the provision of essential services by that operator. The above-mentioned prerequisites, which make it possible to decide whether a given entity should be recognised as an operator of essential services, are set forth in Article 5(2) of the NCSA. The above-mentioned prerequisites must be met together, which means that the absence of any one of them prevents a public administration authority from issuing an identification decision. The legislators do not specify whether the authority initiates the procedure for recognising an entity as an operator of essential service ex officio or upon the request of the party, so it should be assumed that both forms are permissible.

For the entity that no longer meets the requirements for recognising it as an operator of an essential service, the competent authority for cybersecurity, pursuant to Article 5(6) of the NCSA, shall issue a decision declaring an expiration of the decision under which it was recognised as an operator of essential services. Derogation from legal circulation of such a defective decision is the duty of the relevant authority.

The legislators impose on operators of essential services additional obligations connected with ensuring cybersecurity. They are required, under Article 8 of the NCSA, to implement a security management system in the information system used in the provision of essential services. The system aims to ensure: 1) regular incident-risk assessment and risk management, 2) the implementation of the appropriate technical and organisational measures proportionate to the assessed risk, taking into account the latest state of the art measures, including (a) the maintenance and safe operation of the information system, (b) security and the continued provision of the services on which the provision of the essential service is dependent, (c) the deployment, record-keeping, and maintenance of action plans which allow the continuous and uninterrupted provision of the essential service, and ensure the confidentiality, integrity, availability, and authenticity of information, (d) the implementation of a continuous monitoring system to supervise the information system used to provide the essential service, 3) the collecting of information on cybersecurity threats and the vulnerabilities of the information system used to provide the essential service, 4) incident management, 5) the applying of measures to minimise the impact of incidents on the security of the information system used to provide the essential service. In this regard it is necessary to keep the software up to date, apply security measures against unauthorised modification in the information system and take immediate action upon identifying a vulnerability or a cybersecurity threat, 6) using the means of communication which facilitate accurate and safe communication within the national cybersecurity system. Security of the information systems used to provide essential services is an important aspect of crisis management, the purpose of which is to neutralise phenomena that adversely affects the level of security, causes significant restrictions in the operation of specific public administration authorities or events that have, or may have, an adverse impact on cybersecurity.

Article 9 of the NCSA imposes an obligation to: 1) designate a person responsible for communicating with entities in the National Cybersecurity System, 2) provides essential-service users with access to knowledge which allows them to understand cybersecurity threats and to employ effective precautions against such threats as required in relation to the essential services provided, in particular by publishing relevant information on an operator's website, 3) inform the authority competent for cybersecurity about which EU member states the entity has been recognised as an operator of essential services in, and the date of termination of the provision of the essential service, no later than within three months of changing the data. This obligation is imposed on operators of essential services.

If an operator of essential services is at the same time the owner, autonomous possessor or dependent possessor of facilities, installation, equipment or services being part of a critical infrastructure, which has an approved critical infrastructure protection plan that includes cybersecurity documentation of the information system used to provide the essential service, he is not required to develop it once again. He is released from this obligation under Article 10(4) of the NCSA. However, he is required to apply it and keep it up to date, as well as establish supervision over it.

As provided for in Article 11 of the NCSA, operators of essential services are also obliged to: 1) ensure incident handling, 2) provide access to information on recorded incidents to the relevant Computer Security Incident Response Team CSIRT MON, CSIRT NASK, or CSIRT GOV, insofar as necessary for the performance of its tasks, 3) classify a given incident as serious based on the thresholds for considering a given incident as serious (these thresholds are set out in the Regulation of the Council of Ministers of 31 October 2018 on Serious Incidents Thresholds, Journal of Laws of 2018, item 2180), 4) promptly report any serious incident, not later than within 24 hours from its detection, to the relevant CSIRT MON, CSIRT NASK, or

CSIRT GOV, 5) cooperate with the relevant CSIRT MON, CSIRT NASK, or CSIRT GOV during the handling of a serious and critical incident by providing the required data, including personal data, 6) remedy vulnerabilities that have led, or could have led, to a serious incident, a significant incident or a critical incident, and inform the authority competent for cybersecurity of their remediation.

Operators of essential services are required to ensure that a security audit of the information system used for the purpose of the provision of essential services is conducted at least once every two years. This obligation is provided for in Article 15(1) of the NCSA. The role of the audit is to evaluate the examined areas and inform about the effectiveness of the processes taking place, which were designed to help a specific entity achieve its planned strategic goals (Romaniuk 2022, p. 200). Neither the entire activity of operators of essential services, nor the facilities, installations, or equipment of critical infrastructure, but the information system used to provide essential services, are subject to auditing.

4. Conclusions

Cybersecurity is a specialised security department that aims to protect information systems against threats (Czuryk 2019, p. 42). Information systems are widely used not only by private actors (including entrepreneurs), but also by public authorities, and serve not only for faster communication (including over long distances), but also for the performance of tasks, including those of fundamental importance to the state and its institutions. They are therefore important to the normal operation of the state, and consequently must be protected to eliminate cyber-attacks that disrupt their functioning. This normal operation of the state also ensures the proper operation of critical infrastructures which are vulnerable to cyber-attacks.

Cybersecurity threats may lead to a crisis situation, so it will be necessary to initiate actions appropriate to crisis management, which may, among others, result in restrictions on civil liberties.

Disruptions to information and communications systems and networks are highlighted in the National Crisis Management Plan, by indicating that they are caused by, among others, cyber threats that includes both intentional actions (attacks, sabotage) with the use of and against information systems, as well as unintentional actions (failures, errors). They are among the most disruptive (in terms of damage) incidents hitting modern society, critical infrastructures and essential services. Cybersecurity incidents are becoming more common because: 1) generally available tools and devices are sufficient enough to carry out an attack in cyberspace; 2) cyberspace does not have specific control barriers; 3) the probability of finding vulnerabilities is relatively high; the targets of intentional actions are very diverse – computer networks are at risk, as well as government computers, banking and private enterprise systems, and home users; 4) due to the widespread use of information systems and their diversity, failures and errors become more and more likely. According to the National Crisis Management Plan, communication and information systems and networks are disrupted due to: 1) human factors, where we are dealing with ignorance or the disregard of regulations and procedures; 2) computer sabotage, organisational error, human error, a lack of supervision; 3) the modification of systems and data; 4) technical or programming errors (application vulnerability); 5) failure, sabotage, damage or the theft of transmission elements; 6) a lack of control of the hardware and software supply chain; 7) a lack of developed, implemented and applied security policies and procedures; 8) a lack of implemented and tested safeguards adequate to identify threats; 9) a lack of regularity in updating security systems; 10) a lack of regularly conducted security tests of IT infrastructure; 11) IT staff shortages; 12) a lack of, or a low level of, training on cyber threats and information security. These disruptions can occur in government institutions and offices, in government administration, or in local government. Disruptions to communication and information systems and networks also occurs amongst entrepreneurs, including those that are operators of critical infrastructure or essential services.

Ensuring cybersecurity requires international cooperation for the protection of cyberspace. Developing a unified security system should guarantee a high level of protection in all cooperating states (Chałubinska-Jentkiewicz, Karpiuk, Kostrubiec 2021, p. 72). This international cooperation should also take into account the protection of critical infrastructure, when this infrastructure also serves for the provision of essential services that depend on information systems.

According to Commission Recommendation (EU) 2017/1584 of 13 September 2017 on the Coordinated Response to Large-Scale Cyber Incidents and Crises (OJEU L 239, p. 36), the use of, and dependence on, information and communication technologies have become fundamental aspects in all sectors of economic activity as companies and citizens are more interconnected and interdependent across more sectors and borders than ever before. A cybersecurity incident affecting organisations in more than one Member State, or even the entire Union, with potential serious disruptions to the internal market or more broadly to the network and information systems on which the Union economy, democracy and society rely is a scenario that Member States and EU institutions have to be well-prepared for. A cybersecurity incident may be considered a crisis at Union level when the disruption caused by the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at the Union political level. Cybersecurity incidents can trigger a broader crisis, impacting sectors of activity beyond network and information systems and communication networks. Any appropriate response must rely upon both cyber and non-cyber mitigation activities.

Bibliography

Chałubińska-Jentkiewicz, K. (2019) Cyberbezpieczeństwo – zagadnienia definicyjne, *Cybersecurity and Law*, 2, pp. 7-23.

Chałubińska-Jentkiewicz, K., Karpiuk, M., Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* Maribor.

Czuryk M. (2019) Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity *Cybersecurity and Law* no. 2, pp. 39-50.

Czuryk, M., Dunaj, K., Karpiuk, M., Prokop, K. (2016) *Prawo zarządzania kryzysowego. Zarys systemu* Olsztyn.

Karpiuk, M. (2021) Cybersecurity as an element in the planning activities of public administration *Cybersecurity and Law* no. 1, pp. 45-52.

Romaniuk, P. (2022) Administrative and legal obligations of the auditee in connection with the performance of an audit task in local government units *Cybersecurity and Law* no. 1, pp. 191-201.

Questo volume è stato stampato
nel mese di dicembre 2022
su materiali e con tecnologie ecocompatibili
presso la LITOGRAFIA SOLARI
Peschiera Borromeo (MI)

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: 978-88-9335-041-9

9 788893 350419

Euro 20,00