

ISSN 2421-4442

S T S

ICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

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



EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

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

15

ISSUE 1/2022

Milano 2022

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

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

ISSUE 1 – 15/2022

Direttore Responsabile:

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

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

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

Comitato Editoriale:

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

© 2022 **EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica**
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442

ISSN DIGITALE: 2533-0659

ISBN: 978-88-9335-956-6

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

FOCUS SUL CONFLITTO UCRAINO

MARCO LOMBARDI Russia-Ucraina: oltre la Guerra Ibrida, verso il Techno-Cognitive Warfare	7
STEFANO MARINELLI War and Crimes against Peace: Avenues to Prosecute Russia's Aggression of Ukraine	21
DANIELE MARIA BARONE Russia-Ukraine conflict: digital assets chronicles in times of war	33
FEDERICO BORGONOVO Azov Battalion: Extreme Right-Wing Militarization and Hybrid Warfare	53
MARCO ZALIANI The importance of the Cyber battleground in the Russo-Ukrainian war	61
LUCA CINCIRIPINI The hybrid response of the EU and NATO to the Russia-Ukraine conflict	69

NAVIGARE SCENARI IBRIDI: PROSPETTIVE

GIACOMO BUONCOMPAGNI L'Amore Altruistico in tempi di guerra e pandemia.....	79
DAISY MARCOLONGO Gestione dell'emergenza Covid-19: dalla teoria all'analisi. Il caso Bergamo	91

FEDERICO PRIZZI	
Il Cultural Intelligence e la Negoziazione Operativa nelle Aree di Crisi	107
RENE D. KANAYAMA	
Events in Kazakhstan’s Almaty of January 2022 – Grass-root Revolt or Terrorism Inspired Insurgency?.....	123
ALI FISHER – NICO PRUCHA	
“Working and Waiting”: The Salafi-Jihadi movement on Telegram in 2021.....	149

FOCUS SUL CONFLITTO UCRAINO

Russia-Ucraina: oltre la Guerra Ibrida, verso il Techno-Cognitive Warfare

MARCO LOMBARDI

Marco Lombardi, director of ITSTIME research center, is full professor at the Catholic University of Sacred Heart, where he teaches Crisis management and risk communication, Mass Communication theory, Sociology, Intelligence and counter terrorism, Security policies. He is the director of the Dpt. of Sociology and member of the scientific board of the School of Doctorate, the masters in Cultural Diplomacy and the School of Journalism. He managed several EU founded research projects mainly focused on terrorism, security and crisis management. He co-operates with different institutional agencies involved on security both at national and international level.

Abstract

The Russian-Ukrainian conflict unexpectedly brought war to Europe.

At present (end of March 2022) I do not consider any conclusive scenario to be foreseeable: today the most optimistic forecast is contained in the uncertainty of an evolving event, for which everything is possible. But this brief note, which introduces others that follow dedicated to the conflict between Russia and Ukraine, focuses on what so far already constitutes predictably persistent results in the medium to long term.

Now we are at the Total Hybrid War in which the dimensions of the conflict overlap, interfere, produce an escalation of effects in different contexts: no conflict had yet unfolded in this articulated form, where they are no longer needed and the predictive and interpretative drivers of the scenarios fail. This is the first Total Hybrid War that has surpassed itself, paving the way for the now present Techno-Cognitive Warfare.

The characteristics of the Ukrainian Russian confrontation can be traced back to some emerging themes: the overlapping of the dimensions of the conflict; the centrality of strategic communication; the multiplication of actors in the field.

Although the conflict is still ongoing, however, some signs of permanent change are already evident. In the paper, I discuss only a few, which concern the change in the paradigm of the now techno-cognitive war, the broad re-modeling of the meaning of cyberspace, the central role of information and communication, and, also, a consequent different mode of negotiation between the parties to accelerate the peace process.

The conclusions add to the previous reflections two hopes.

The first concerns our capacity for de-escalation: wars, this one, in particular, has clearly shown how we can risk being stuck in a symmetrical process of escalation so that every action (in every dimension of the conflict) is answered with an action of a greater degree (in every other dimension of the conflict). It is a trap, also favored by technologies, which has configured an automatism, a practice of “taken for granted”, which can only be interrupted by a conscious and responsible choice.

The second, which takes the form of advice, concerns the individual cognitive equipment that each one must assume for the governance of the flow of communication in which he is immersed. Therefore, I emphasize what I call the Principle of Maximum Protection:

- *any information is false until proven otherwise.*

and the Principle of Maximum Effectiveness:

- *every piece of information is true for its target audience.*

I expect a lasting more than ten years of the conflict that has just begun, albeit blanded and conveyed through actions that will focus on one or the other dimension (cyber, kinetic, economic, social, etc.) in an exclusive way, if those who will have to govern the confrontation will be able to avoid the simultaneous overlapping of the effects generated by the actions carried out in each dimension. In practice, we now need to learn to govern a widespread, subthreshold, and continuous global conflict: without surrendering to Cognitive Warfare as a replacement for “Peacefare”.

Il conflitto russo-ucraino ha inaspettatamente portato la guerra in Europa.

Allo stato attuale (fine marzo 2022) non reputo prevedibile alcuno scenario conclusivo: oggi la previsione più ottimista è contenuta nell’incertezza di un evento in evoluzione, per il quale tutto è possibile. Ma questa breve nota, che ne introduce altre che seguono dedicate al conflitto tra Russia e Ucraina, si concentra su quanto finora già costituisce dei risultati prevedibilmente persistenti nel medio-lungo periodo.

Ora siamo alla Guerra Ibrida totale in cui le dimensioni del conflitto si sovrappongono, interferiscono, producono una escalation di effetti in contesti diversi: ancora non si era dispiegato in questa forma articolata alcun conflitto, dove non servono più e i driver predittivi e interpretativi degli scenari falliscono. Questa è la prima Guerra Ibrida Totale che ha superato sé stessa, aprendo la via all’ormai presente Guerra Tecno-Cognitiva.

Le caratteristiche del confronto russo ucraino possono essere ricondotte ad alcuni temi emergenti: il sovrapporsi delle dimensioni del conflitto; la centralità della comunicazione strategica; la moltiplicazione degli attori sul campo.

Benché a conflitto ancora in corso, tuttavia, alcuni segni di cambiamento permanente sono già evidenti. Nel paper mi soffermo solo su alcuni, che riguardano il cambiamento del paradigma della guerra ormai tecno-cognitiva, la ri-modellazione ampia del significato di spazio cibernetic, il ruolo centrale dell’informazione e comunicazione e, anche, una conseguente diversa modalità di negoziazione tra le parti per accelerare il processo di pace.

Le conclusioni aggiungono alle riflessioni precedenti due auspici.

Il primo riguarda la nostra capacità di *de-escalation*: le guerre, questa in particolare, ha mostrato con chiarezza come si possa rischiare di restare bloccati in un processo simmetrico di *escalation*, per cui a ogni azione (in ogni dimensione del conflitto) si risponde con una azione di grado maggiore (in ogni altra dimensione del conflitto). Il secondo, che assume la forma di un consiglio, riguarda l’attrezzatura cognitiva individuale che ciascuno deve assumere rispetto al governo del flusso di comunicazione in cui è immerso secondo il Principio di Massima Tutela e il Principio di Massima Efficacia.

Keywords

Hybrid Warfare, Cognitive Warfare, Cyberspace, Ukraine, Russia

1. Premessa

Il conflitto russo-ucraino ha inaspettatamente portato la guerra in Europa.

Allo stato attuale (fine marzo 2022) non reputo prevedibile alcuno scenario conclusivo: oggi la previsione più ottimista è contenuta nell'incertezza di un evento in evoluzione, per il quale tutto è possibile.

Ma questa breve nota, che ne introduce altre dedicate al conflitto tra Russia e Ucraina in questo volume di STS, si concentra su quanto finora già costituisce dei risultati prevedibilmente persistenti nel medio-lungo periodo.

Nessuno se lo sarebbe mai aspettato, anche se la Terza Guerra Mondiale era in corso da anni e definita a “capitoli” da Papa Francesco già nel 2014: finora, tuttavia, la percezione del conflitto era tenuta distante dalle opinioni pubbliche occidentali, perché gli “eserciti” si combattevano nelle terre espropriate ai cittadini: dalla Siria all’Afghanistan, dalla Libia all’Africa profonda le cosiddette Grandi Potenze si affrontavano quotidianamente via “proxy”. Tutto questo era sufficiente a far sì che la distanza contenesse le paure delle rispettive popolazioni.

Improvvisamente, l’Ucraina è diventata la nuova terra di confronto ed essa è prossima, è di confine per l’Europa, non ci sono cuscinetti ad attutire il rombo dei cannoni. Così un drone che vola a 700 chilometri orari percorre in solitudine 1300km dall’Ucraina per schiantarsi in Croazia¹: la facile mobilità di questi anni diventa protagonista di uno spazio minaccioso senza zone di mezzo che garantiscano distanze di sicurezza: oggi non basta uno stato serve forse un continente e un oceano a dividere blocchi di vecchia memoria.

Un’opinione pubblica che ha vissuto decenni di guerre lontane, percettivamente ed emotivamente filtrate dall’apparato mediatico, si rende improvvisamente conto che la guerra non ha a che fare con la giustizia ma con la sopravvivenza di chi si trova coinvolto, indipendentemente dalle ragioni.

A chi tocca gestire il conflitto è difficile rinunciare a interrogarsi sul “perché” della guerra, ma deve capire che, assumendo la necessaria prospettiva del crisis management, determinare le cause serve solo per comprendere meglio gli effetti da contenere non per attribuire colpe. Soprattutto adesso, che la costruzione della narrativa rassicurante – quella della guerra che non c’è perché lontana – è definitivamente crollata: per la prima volta abbiamo il completo spiegamento della Guerra Ibrida, finora teorizzata da alcuni, accettata da pochi, praticata diffusamente ma sempre dispiegando con discontinuità il suo potenziale. Furono così sia l’Afghanistan che la Siria, che la più articolata guerra al terrorismo, diffuso e connesso.

¹ <https://www.ilfoglio.it/esteri/2022/03/11/video/un-vecchio-drone-militare-sovietico-si-e-schiantato-a-zagabria-in-croazia-3797541/>

La Guerra Ibrida: più volte ho commentato questa definizione del conflitto, sostenendo – non da solo! – che si trattasse di un’evoluzione del modo di fare la guerra, caratterizzata da:

- incertezza delle norme che la regolano e, dunque, grande flessibilità tattica e strategica “oltre il limite”;
- pluralità di attori (pubblici e privati) portatori di interessi specifici diversi e in conflitto tra loro per il successo, anche quando schierati dalla stessa parte;
- compresenza di asset concorrenti;
- essere una guerra delocalizzata, pervasiva e diffusa.

È proprio a partire dagli albori del conflitto Russo – Ucraino (2014) che si cominciò a definire questo scenario, spesso con grande difficoltà ad accettarlo sia a livello politico sia militare: in ogni caso esso spaventava perché, nella sua accezione, mostrava chiaramente come fosse già in corso una Terza Guerra Mondiale strisciante, cioè non riconoscibile utilizzando i canoni dei conflitti trascorsi, ma evidente negli obiettivi sottesi al confronto multidimensionale tra le potenze di questi anni.

Tutto questo era quanto avevamo definito Guerra Ibrida: senza regole, con una molteplicità di attori coinvolti e di asset impiegati. Ma oggi, le considerazioni iniziali che portarono ad elaborare questa definizione in sede NATO, non sono più sufficienti a contenere la varietà delle minacce. Finora, infatti, le diverse strategie si dispiegavano in “parallelo”, attivando cioè interventi nella dimensione cyber piuttosto che in quella militare tradizionale, o ancora in quella comunicativa piuttosto che economica, con effetti che si manifestavano all’interno della dimensione originaria, adesso non è più così.

Ora siamo alla Guerra Ibrida Totale in cui le dimensioni del conflitto si sovrappongono, interferiscono, producono una escalation di effetti in contesti diversi: ancora non si era dispiegato in questa forma articolata alcun conflitto, dove le regole che finora sono servite per identificare il nemico (che non è necessariamente chi ti spara) non servono più e i driver predittivi e interpretativi degli scenari falliscono.

I segni della guerra russo-ucraina sono evidenti:

- Il primo segno, primo perché più banale, è nella presenza di tutte le dimensioni della guerra: terra, aria, mare, spazio e cyber. Queste dimensioni sono ormai simultaneamente presenti e reciprocamente interdipendenti nell’esercitarsi sul campo.
- Gli attori si sono moltiplicati a dismisura: gli eserciti ufficiali sono una piccola componente sul terreno. A questi si aggiungono milizie su base ideologica, religiosa, economica. E poi i volontari per costituire un corpo internazionale di risposta, in un campo che è condiviso da attori “*non conflict*” quali media e NGO. Ma soprattutto un attore è sempre più presente

da protagonista: la Pubblica Opinione, che è l'audience della guerra nella dimensione cyber.

- Il privato, nella forma dei nuovi super stati globali delle *major*, si schiera su più dimensioni per sfruttare i propri *asset*: le *major* della comunicazione adeguano i palinsesti alle diverse narrative e praticano forme di propaganda e di censura; altri limitano i servizi normalmente offerti, che possono essere utilizzati da parti in causa o, al contrario, le parti in gioco trovano inaspettate *backdoor* per un utilizzo creativo dei medesimi servizi: tutti in gioco.
- L'*asset* economico si è dispiegato con le sanzioni che colpiscono la quotidianità della vita di tutti, cercando di frantumare l'opinione pubblica russa, ma con effetti boomerang sulle opinioni nazionali. L'effetto complessivo dell'attacco economico ha ormai dato avvio a un nuovo assetto economico globale che sostituirà il precedente.
- La dimensione cyber, che finora era stata descritta come la Linea Marginot di difesa statica delle infrastrutture, finalmente si riconosce per le competenze multifunzione che implicano azioni che vanno dalla inibizione e distruzione dell'hardware primario, al sabotaggio nella erogazione dei servizi dipendenti dalla rete, fino all'impiego del cyberspazio, che in questa veste deve essere garantito operativo, per l'azione più massiccia di info-war mai dispiegata, che utilizza tutte le piattaforme digitali di comunicazione possibili.

Questa è la prima Guerra Ibrida Totale che ha superato sé stessa, aprendo la via all'ormai presente Guerra Tecno-Cognitiva.

2. Verso il Cognitive Warfare

2.1 Il sovrapporsi delle dimensioni

Come ho sostenuto, il conflitto ibrido finora si era mostrato nella sua complessità generata dal moltiplicarsi delle dimensioni: per esempio, da una parte l'incremento esplosivo del tipo delle formazioni combattenti e dall'altra le numerose strategie comunicative destinate alla conquista di "cuori e menti" dei pubblici.

Invece, di questa guerra si deve sottolineare non la simultaneità ma la sovrapposizione di dimensioni e *asset*, che richiede una strategia olistica e una interdipendenza profonda delle tattiche, governata da un sistema di comando che ha la sua competenza e forza nella dimensione cognitiva².

² <https://www.itstime.it/w/guerre-future-la-nuova-centralita-dellintelligence-e-la-ridefinizione-dello-spazio-cibernetico-by-marco-lombardi/>

La differenza tra le due prospettive è enorme. Se prima era difficile che una strategia di guerra comunicativa portasse a una reazione “*boot on the field*”, adesso la sovrapposizione degli effetti (e l’aumento del rischio complessivo) è tale per cui a una narrativa può conseguire una risposta militare, in una sorta di reattività che sembra coinvolgere tutte le catene di comando e controllo. Eppure era atteso e scritto, da quando gli Stati Uniti avevano ben chiarito che un attacco a loro infrastrutture cibernetiche avrebbe potuto causare una reazione tradizionale (bombardamento) sull’origine della minaccia³. In perfetta sintonia con la Russia che, il 25 marzo 2022, ricorda con Andrei Krutskikh come “*un attacco informatico, sia esso accidentale o intenzionale, anche perpetrato sotto falsa bandiera, può facilmente portare a un’escalation, a uno scontro su vasta scala*”⁴.

Questo significa che, in questo momento, non abbiamo nessuna sicurezza di poter sostenere che una minaccia, che per sua natura appartiene agli asset comunicativi della info-war del cyber, non possa trovare una risposta rapida in una azione che riguarda un *asset*/dimensione differente, per esempio sul campo.

Si tratta di una novità a cui il sistema politico e strategico è pericolosamente esposto perché ancora non c’è una dottrina adeguata a governare la Cognitive Warfare. Probabilmente per una pluralità di ragioni, non solo legate alla rapidità (costantemente invocata come causa) del cambiamento soprattutto delle tecnologie digitali, tra cui un conflitto generazionale nella catena di comando e controllo che contrappone i caratteri anagrafici dell’esperienza analogica ai *digital born*, giovani che anche non hanno nessuna consapevolezza del significato radicale di “Guerra Fredda”, tornato ad avere senso interpretativo di questa realtà.

2.2 La comunicazione

Il paradigma della Guerra Ibrida, che aveva suggerito la persistenza di una Terza Guerra Mondiale in corso, aveva anticipato la prospettiva del *techno-cognitive confrontation* sottolineando la centralità della comunicazione nel warfare, evidenziata dalla sua autonomia rispetto alle altre armi: oggi la comunicazione non è corollario a un’azione di guerra ma è essa un’azione di guerra. Questa forma di conflitto, sperimentata oggi in Europa, arriva al “pubblico” nella sua forma mediata, cioè per gli effetti che ha sulla quotidianità prodotti

³ <https://www.itstime.it/w/guerra-ibrida-perche-avere-piu-paura-del-conflitto-russo-ucraino-by-marco-lombardi/>

⁴ <https://www.ilgiornale.it/news/mondo/mosca-lancia-lallarme-garantire-sicurezza-informatica-2020898.html>

dall'annientamento delle piattaforme di comunicazione e dalle capacità di interpretazione e comando, organizzata in una guerra di flusso (continua).

Ma questo è solo un aspetto in cui si declina la minaccia.

L'altro, a cui gli ultimi venti anni di terrorismo dovrebbero averci abituato, è lo scontro che avviene sfruttando e utilizzando il nuovo ecosistema digitale della comunicazione: in molti casi, si è già dimostrato, è controproducente attaccare l'infrastruttura che regge lo spazio cibernetico ma conviene penetrarla utilizzandola "ai limiti delle opportunità" per modificare i piani cognitivi e interpretativi sui cui si basa sia la presa di decisioni sia la produzione del consenso dell'avversario.

Questa logica è alla base della cyber war russo-ucraina che attacca infrastruttura e piattaforme, ruba identità e pone riscatti, promuove interpretazioni contro-dipendenti di realtà esclusivamente narrative: in questa guerra il ciberspazio ha cambiato forma, ampliandosi come luogo di opportunità anche per distribuire informazione "utile al nemico". Questa strategia si applica in un contesto favorevole perché come cittadini siamo più esposti, e perché come ogni situazione di incertezza richiede, ci offriamo più vulnerabili agli strumenti della comunicazione con il risultato di diventare fan e tifosi degli schieramenti, effetto cercato e voluto ovviamente dalle parti in conflitto: il mutarsi delle audience in tifoserie, per l'una o per l'altra squadra, modifica gli equilibri in campo e rende ben più difficile il negoziato.

L'obiettivo degli attori del conflitto è quello di costruire rappresentazioni nella Pubblica Opinione, che poi orienta la politica e le scelte. Russi e ucraini, pur con il medesimo scopo e con il medesimo uso strumentale della comunicazione, agiscono però in maniera diversa verso pubblici – *target audience* – diversi, ripetendo un format che ha il compito di consolidare lo zoccolo duro dei fan. Per alcuni, la maglietta militare del presidente ucraino diventa il simbolo della verità come per altri lo sono la cravatta e la maschera impassibile russa: si cade in trappola per il bisogno di avere qualcosa – qualcuno – a cui credere di fronte ad una realtà troppo complessa: vince il *brand*.

2.3 La moltiplicazione degli attori

Se la guerra ibrida è caratterizzata dalla molteplicità degli attori sul campo, lo schieramento in Ucraina supera ogni precedente storia: il combattimento, infatti, è ormai tra tanti gruppi, con la presenza di milizie straniere, tutti autonomi nel darsi le "buone ragioni" per il combattimento⁵.

⁵ <https://www.itstime.it/w/ucraina-russia-ormai-e-troppo-tardi-by-gianluca-frinchillucci-e-marco-lombardi/>

Il gruppo più conosciuto è sicuramente il Battaglione Azov, che fa parte dello schieramento ucraino, anche se le milizie di stampo neo-nazista sono varie⁶. Azov, con le sue parate e il suo stemma che ricorda Wolfsangel, ha dato il pretesto alla pubblicistica russa di definire gli ucraini nazisti. Ma non si tratta del solo gruppo con questa connotazione: per esempio sono anche emersi altri gruppi con riferimento alla divisione delle Waffen SS “Galizien”.

Con l’Ucraina combatte anche una sorta di legione straniera con volontari provenienti da tutto il mondo e la Legione Georgiana, a cui ha aderito anche l’ex ministro della Difesa Irakli Okruashvili. Ma anche due battaglioni di ceceni, “Dzhokhar Dudaev” e “Sheikh Mansour”, condividono la medesima parte dello schieramento.

Anche sul fronte russo ci si avvale di milizie che si ispirano per i simboli usati e per il linguaggio al Terzo Reich e al mondo del suprematismo bianco. Il Patriarca Kirill di Mosca e di tutte le Russie (lo scorso 6 marzo) nella Cattedrale di Cristo Salvatore nella capitale russa, ha sostenuto che: *“Siamo impegnati in una lotta che non ha un significato fisico, ma metafisico”*. È con questa legittimazione che alcune milizie si ispirano proprio alla Chiesa Ortodossa Russa e combattono la loro battaglia contro gli ucraini, che sono l’avanguardia del corrotto mondo occidentale. Ma alle milizie ortodosse si aggiungono i mussulmani ceceni, guidati dal fanatismo religioso e dalla pratica terroristica in guerra, e i gruppi ultranazionalisti russi che si ispirano al movimento Pamyat. Tra i gruppi più attivi troviamo il Movimento Imperiale Russo che ha reclutato migliaia di volontari. Ma aggiungiamo, tra i vari, il Battaglione Sparta, una formazione armata che fa parte della Repubblica Popolare di Donetsk, e il Battaglione Svarozich, gruppo pagano di adoratori del dio slavo Svarog, poi assorbito dalla Brigata Vostok, nella quale si sono arruolati anche italiani, di varia estrazione ideologica. Questo agglomerato di combattenti, convive con una sorta di legione mercenaria in cui spicca la Wagner⁷, ma a cui si aggiungono gli arruolamenti in corso in numerosi teatri di conflitto in cui la Russia è presente.

La domanda che sorge spontanea è: questa varietà reciproca di gruppi schierati sul campo in che modo risponde alla formale catena di comando e controllo? Quella stessa catena di comando che avrà il compito di “dichiarare la pace” e la fine dei combattimenti?

⁶ <https://www.itstime.it/wp-content/uploads/2022/02/Ukrainian-Right-Wing-Armies.png>

⁷ <https://wagnera.ru/>

3. La lezione appresa

A conflitto ancora in corso, tuttavia, segni di cambiamento permanente sono già evidenti. Mi soffermo solo su alcuni, sui quali si dovrà tornare, che riguardano il cambiamento del paradigma della guerra ormai tecno-cognitiva, la ri-modellazione ampia del significato di spazio cibernetico, il ruolo centrale dell'informazione e comunicazione e una conseguente diversa modalità di negoziazione tra le parti per accelerare il processo di pace.

3.1 Techno-Cognitive Confrontation

Lo scenario del conflitto emergente è ormai quello del *techno-cognitive confrontation*, che ricorda la compresenza funzionale della dimensione tecnologica e di quella tipicamente umana della conoscenza e interpretazione e che esalta il ruolo del digitale: la capacità che esso ha di far transitare e trattare enormi quantità di informazioni massimizza il rischio che, bloccando l'infrastruttura si metta in crisi la catena decisionale. Questo scenario, è caratterizzato dalla variazione di velocità dei processi, che dunque richiederanno iper-rapidità nella presa di decisioni, e dalla enorme complessità dovuta all'aumento dell'informazione, ormai costituita da frammenti di bit correlati. Un'azione di adeguamento per governare efficacemente questo conflitto deve considerare lo spazio cibernetico come lo spazio di un nuovo ecosistema, superando la sintesi contenuta nell'idea di sistema socio-tecnico, per affermare quella più recente di eco-sistema digitale. Tutto questo non ha a che fare solo con la rapidità con cui si tramettono le informazioni, piuttosto con il processo interpretativo che necessita della consapevolezza della sua attuazione, nelle premesse e nelle conclusioni, per distinguersi dalla semplice reazione automatica all'evento. La domanda è come si ottiene questa capacità di simultaneità decisionale efficiente, intesa come una super velocità cognitiva e interpretativa, laddove esplose la compresenza di oggetti significativi: meno tempo, più segni deboli "che hanno senso in relazione tra loro", più modelli interpretativi possibili.

3.2 Un ciberspazio diverso

Il cyber warfare legato all'interpretazione della difesa delle strutture all'interno di un perimetro da tutelare è ampiamente superato, al punto che questa strategia finora prioritaria potrebbe rivelarsi controproducente in contesti che preferiscano una circolazione elevata di comunicazione pubblica. In questa prospettiva, il nuovo ciberspazio non è un'area tecnologica da perimetrare per massimizzarne la sicurezza ma è anche un'area da penetrare e utilizzare in quanto campo della comunicazione strategica: il bilanciamento tra queste

due prospettive è un aspetto del governo del conflitto nuovo ed emergente. Non solo: è assolutamente verosimile che, al di là di ogni accordo per la cessazione dei combattimenti “*on the field*” la guerra continui a lungo nella dimensione digitale⁸: proprio per questa primazia della comunicazione, nel mondo reticolare e iperconnesso, è opportuno cominciare considerare la persistenza di uno stato conflittuale da governare in continuum, che si esprime nel confronto tecno-cognitivo tra attori concorrenti.

3.3 Informazione e opinione pubblica

L’impiego delle strategie di info-war porta a due conclusioni che persistiranno.

La considerazione di partenza è che nel momento in cui il pubblico è convinto di partecipare a una guerra di informazione, rinuncia alla analisi in favore dello schieramento. Infatti, nelle situazioni di incertezza, la pluralità discordante di informazioni ne acuisce il bisogno riducendo la capacità interpretativa personale, favorendo invece l’appartenenza sulla base di emotività ed affettività. Infatti, il primo obiettivo per una strategia efficace di info-war è di convincere il pubblico di essere una vittima di “*fake news*”: si tratta del primo passo per ancorarlo a rappresentazioni rassicuranti e persistenti, non necessariamente rappresentative della realtà, in cui la fiducia nel *brand* costituirà la ragione della propria appartenenza.

In questa prospettiva, dunque, la prima conclusione ci spinge ad abbandonare l’idea (fin troppo di moda in questi anni) di poter utilizzare il metodo OSInt (Open Source Intelligence) per acquisire informazioni utili in quanto tali, perché tutte le fonti risponderanno alle strategie dell’info-war. Le informazioni, in quanto dato di realtà, potranno in parte essere raccolte via HumInt e in SigInt. All’OSInt resta una diversa prospettiva: quella dell’analisi di “una pluralità di false narrative” per similitudini tra i medesimi oggetti tematizzati e per differenze tra gli oggetti delle narrative⁹, non avendo l’obiettivo di raccogliere informazione ma di comprendere il “*mood*” che si vuole promuovere nell’opinione pubblica e le strategie comunicative dei contendenti.

⁸ <https://www.cybersecurity360.it/cybersecurity-nazionale/guerra-ibrida-biden-chiede-di-rafforzare-la-cyber-security-usa-quali-scenari/>

⁹ Non è obiettivo di questo paper discutere questo aspetto dell’OSInt nel contesto dell’info-war. Per chiarire la questione si può esemplificare: a) dando per scontato che l’informazione che circola è falsa; b) che è utile capire la diversità con cui gli attori in conflitto narrano i medesimi oggetti della comunicazione; c) quali siano per ciascun attore gli oggetti esclusivi della propria comunicazione; d) etc.. Tutto ciò con l’obiettivo limitato di comprendere per differenza/similitudine lo stato d’animo che si vuole produrre nell’opinione pubblica, da parte di ciascuna fonte, e non con l’obiettivo di raccogliere informazioni descrittive della realtà dei fenomeni.

La seconda conclusione afferma con forza l'Opinione Pubblica come uno strumento centrale del conflitto tecno-cognitivo: un importante protagonista che può essere sfruttato per esercitare pressione su *audience* diverse e sulla governance del conflitto e del quale si deve tener conto nelle pratiche diplomatiche di negoziazione.

La centralità della comunicazione in queste guerre permette di sostenere che la reputazione pesa come i cadaveri dei soldati e come la mancanza del pane: nel conflitto i tre fattori sono interlacciati: un attacco comunicativo produce la risposta di un carro armato o l'assalto al forno. E viceversa.

L'effetto di questa sovrapposizione definisce la qualità della vittoria o della sconfitta, perché non tutte le vittorie o le sconfitte sono uguali nelle loro conseguenze. Si tratta di dimensioni (comunicativa, economica, militare) che oltre che determinare la vittoria o la sconfitta in una guerra, soprattutto determinano la sopravvivenza politica dei sopravvissuti nel dopo guerra. Da questo la necessità, e l'urgenza, di utilizzare la comunicazione con la stessa attenzione delle tradizionali armi di distruzione di massa.

3.4 Nuove forme di negoziato

Nei prossimi anni ci si troverà davanti alle conseguenze dovute alla sostituzione delle due forme di conflitto: quello ibrido e quello tecno-cognitivo.

La moltiplicazione degli attori sul campo (Guerra Ibrida), schierati a combattere secondo interessi molteplici e diversi, rende assolutamente incerta la loro risposta alla catena di comando e controllo istituzionale con il risultato che, molto probabilmente, la dichiarazione di cessazione dei combattimenti sarà recepita funzionalmente da ciascuno sulla base degli interessi personali. È inevitabile che un teatro "ibridato" continui a essere interessato da un perdurante livello di conflitto "tra bande" sul campo.

Il protagonismo dell'Opinione Pubblica, destinataria delle strategie comunicative della guerra tecno-cognitiva, non permette di escluderla dalle pratiche diplomatiche di negoziato: l'attore protagonista (anche le vittime sono attori protagonisti) dell'info-war richiede una partecipazione propositiva fino all'ultima sequenza perché non può più rinunciare al ruolo che si è assunto nel conflitto: questo pubblico non può andare via in silenzio. È inevitabile, dunque, trovare nuovi processi e nuove formule negoziali partecipate che ridefiniscono le pratiche di formulazione dei trattati e della loro negoziazione.

4. Conclusioni

Anche se banale è utile ripetere che la guerra tra Russia e Ucraina ha sconvolto l'assetto globale del mondo. A queste brevi note, con cui ho voluto

cominciare per “fermare” alcuni punti di riflessione che stanno emergendo a conflitto ancora in corso, in quanto aspetti che caratterizzano il prossimo periodo di turbolenza dovuta a un confronto che perdurerà modellandosi per le opportunità che saranno offerte, aggiungo due auspici.

Il primo riguarda la nostra capacità di *de-escalation*: le guerre, questa in particolare, ha mostrato con chiarezza come si possa rischiare di restare bloccati in un processo simmetrico di *escalation*, per cui a ogni azione (in ogni dimensione del conflitto) si risponde con una azione di grado maggiore (in ogni altra dimensione del conflitto). Si tratta di una trappola, favorita anche dalle tecnologie, che ha configurato un automatismo, una pratica del “dato per scontato”, che non può che essere interrotta da una scelta consapevole e responsabile.

Il secondo, che assume la forma di un consiglio, riguarda l’attrezzatura cognitiva individuale che ciascuno deve assumere rispetto al governo del flusso di comunicazione in cui è immerso. Dunque, sottolineo quello che io chiamo il Principio di Massima Tutela:

- *ogni informazione è falsa fino a prova contraria.*
e il Principio di Massima Efficacia:
- *ogni informazione è vera per la sua target-audience.*

Confido maggiormente nella responsabilità che affido a ciascuno con l’applicazione dei due principi proposti, che non in una strategia complessiva di *de-escalation*.

Piuttosto, mi aspetto un perdurare ultradecennale del conflitto da poco cominciato, seppur blandito e veicolato attraverso azioni che si concentreranno sull’una o sull’altra dimensione (cyber, cinetica, economica, sociale, etc.) in maniera esclusiva, se chi dovrà governare il confronto sarà capace di evitare la sovrapposizione simultanea degli effetti generati dalle azioni condotte in ciascuna dimensione.

In pratica, ormai abbiamo la necessità di imparare a governare un conflitto globale diffuso, sottosoglia e continuo: senza arrendersi al Cognitive Warfare in sostituzione del “Peacefare”.

References

- <https://www.ilfoglio.it/esteri/2022/03/11/video/un-vecchio-drone-militare-sovietico-si-e-schiantato-a-zagabria-in-croazia-3797541/>
- <https://www.itstime.it/w/guerre-future-la-nuova-centralita-dellintelligence-e-la-ridefinizione-dello-spazio-cibernetico-by-marco-lombardi/>
- <https://www.itstime.it/w/guerra-ibrida-perche-avere-piu-paura-del-conflitto-russo-ucraino-by-marco-lombardi/>

<https://www.ilgiornale.it/news/mondo/mosca-lancia-lallarme-garantire-sicurezza-informatica-2020898.html>

<https://www.itstime.it/w/ucraina-russia-ormai-e-troppo-tardi-by-gianluca-frinchillucci-e-marco-lombardi/>

<https://www.itstime.it/wp-content/uploads/2022/02/Ukranian-Right-Wing-Armies.png>

<https://wagnera.ru/>

<https://www.cybersecurity360.it/cybersecurity-nazionale/guerra-ibrida-biden-chiede-di-rafforzare-la-cyber-security-usa-quali-scenari/>

War and Crimes against Peace: Avenues to Prosecute Russia's Aggression of Ukraine

STEFANO MARINELLI

Stefano Marinelli, transitional justice researcher and M&E at Agency for Peacebuilding, is PhD in International Law at Middlesex University of London, and author of *The International Criminal Court and the Responsibility to Protect* (Routledge 2022, forthcoming).

Abstract

On February 24, 2022, the Russian attack on Ukraine provoked a strong international community reaction, in terms of diplomatic condemnation of Russia and support for Ukraine. There is an international consensus on the qualification of the facts that have occurred as a crime of aggression, and an unprecedented political support for Ukraine. Nevertheless, international justice does not have the possibility to prosecute those responsible for the crime.

The article presents the structural obstacles of international law in prosecuting the crime of aggression committed against Ukraine, in particular by the International Criminal Court, and illustrates possible alternatives to bring those responsible to justice. The article presents the strong and coherent reaction of the international community to the Russian military intervention, with unprecedented unity in the United Nations General Assembly, and a majority in the Security Council stopped exclusively by the Russian veto. Then, the article examines the international prohibition of the use of force, and the justifications put forward by Russia to support the legality of the operation. The Russian reasons, based on self-defense and on the purpose of protecting the populations of Donbas from genocide, prove to be unfounded. The analysis therefore concludes that the attack on Ukraine constitutes a manifest act of aggression. The study then examines the criminalization of the aggression by the International Criminal Court, presenting the jurisdictional limits that prevent the Court from prosecuting the crime in this circumstance: unlike other international crimes that the ICC is already investigating on the Ukrainian territory (crimes of war, crimes against humanity) the Court cannot exercise its jurisdiction for the crime of aggression committed by individuals of states that are not party to the Rome Statute.

Finally, alternative mechanisms for bringing justice to the Ukrainian aggression are examined: from the trial in a national court, which has the problem of immunities and of lack of expertise in prosecuting international crime, to the creation of an ad hoc or hybrid tribunal.

Il 24 febbraio 2022, l'attacco della Federazione Russa all'Ucraina ha provocato una forte reazione della comunità internazionale in termini di condanna diplomatica della Russia e di sostegno all'Ucraina. Nonostante il consenso internazionale nella qualifica dei fatti occorsi, e il sostegno politico senza precedenti, la giustizia internazionale sembra impossibilitata a perseguire i responsabili del crimine. L'articolo presenta gli ostacoli strutturali del diritto internazionale nel perseguire il crimine di aggressione commesso contro l'Ucraina, in particolare da parte della Corte Penale Internazionale, e illustra possibili alternative per fare giustizia sul

crimine. Dopo aver presentato la reazione unitaria della comunità internazionale all'intervento militare russo, con un'unità senza precedenti nell'Assemblea Generale delle Nazioni Unite, e una maggioranza nel Consiglio di Sicurezza fermata esclusivamente dal veto russo, l'articolo prende in esame il divieto internazionale di uso della forza e le giustificazioni avanzate dalla Russia per sostenere la legalità dell'operazione. Le ragioni russe, fondate sull'autodifesa e sulla finalità di proteggere le popolazioni del Donbas da un genocidio, si rivelano infondate. Si conclude quindi che l'attacco all'Ucraina costituisce un chiaro atto di aggressione. L'analisi esamina poi la criminalizzazione dell'aggressione da parte della Corte Penale Internazionale, presentando i limiti giurisdizionali che impediscono alla Corte di perseguire il crimine in questa circostanza: a differenza di altri crimini internazionali su cui ha già iniziato attività di indagine (crimini di guerra, crimini contro l'umanità) la Corte non può esercitare la propria giurisdizione per il crimine di aggressione commesso da individui di Stati che non sono parte allo Statuto di Roma. Infine, si prendono in esame meccanismi alternativi per fare giustizia sull'aggressione Ucraina: dal processo in un tribunale nazionale, che ha problemi di immunità e di specializzazione nel perseguire il crimine internazionale, fino alla creazione di un tribunale ad hoc o ibrido.

Keywords

Russia, Ukraine, International law, War crimes

1. Introduction

On 24 February 2022, the Russian Federation started a military intervention in the territory of Ukraine. The attack triggered a global «unprecedented response» (Chachko and Linos, 2022), in terms of diplomatic efforts, humanitarian aid to migrants, economic sanctions against Russia, and arms transfers to Ukraine. As a «discipline of crisis» (Charlesworth, 2002), international law is expected to play a role in the maintenance of peace and security, and in identifying and prosecuting those responsible for alleged international crimes. This study examines the structural implementation problems of international justice, which seems «largely paralyzed» (Trahan, 2022) even in a context of widespread political support and consensus on the qualifications of the events. Furthermore, this analysis presents possible avenues to hold accountable those responsible for the aggression against Ukraine.

A clear consensus developed, among scholars and states, that the invasion constitutes «one of the clearest violations of article 2(4) of the United Nations Charter since its entry into force» (Dannenbaum, 2022) and «a textbook example of the crime of aggression» (McDougall, 2022). A draft UN Security Council resolution, co-sponsored by 82 States, deplored «in the strongest terms the aggression by the Russian Federation against Ukraine in violation of Article 2 (4) of the Charter». On 25 February, the draft was voted by 11 out of 15 members of the Security Council, with 3 abstentions, but it was stopped by

the only vote against: the Russian's veto. On 2 March, an emergency session of the UN General Assembly (hereinafter, UNGA) adopted Resolution ES-11, using the same wording qualifying the Russian military operation as an act of aggression, with an overwhelming majority of 141 against 5 (UNGA, 2022). At the time of writing, the armed conflict is evolving rapidly. Negotiations are underway to find a political settlement and stop Russian's attacks, which reportedly target also «the most vulnerable» (UNICEF, UNFPA and WHO, 2022). The international community's reaction came to include the Russian expulsion from the Council of Europe (Council of Europe, 2022) and a variety of exceptional initiatives and tailored sanctions against the Russian leadership (Johns and Kotova, 2022).

In contrast with the situation on the field, efforts to bring to justice those responsible for the attack are far from evolving rapidly. Indeed, despite the general agreement on the occurrence of an illegal aggression and the widespread international support to the Ukrainian side, it is unlikely that an international tribunal will make a judicial determination of the crime of aggression, and identify and prosecute those responsible. Antonio Cassese used to affirm that «international justice has its own tempo» (Gaeta and Zappalà, 2021): the long-term nature of the international criminal law discipline, and its even longer-term objective and effects, allow drawing an analysis which transcends the current events. First, this article assesses how the invasion of Ukraine violates the prohibition of the use of force and constitutes an act of aggression. Second, it examines the criminalization of aggression in international law, and the institutional weakness of the international legal system, of the International Criminal Court *in primis*, in prosecuting those responsible. Third, it considers possible alternative avenues to grant accountability for the Ukrainian aggression.

2. The Putin Defense: Assessing the Legality of the Russian Intervention

This section examines the Russian justification for the use of force in Ukraine, to present the overall consensus on the occurrence of a crime of aggression. The use of force of the Russian Federation in the territory of Ukraine dates back to 2014, when Russia occupied Crimea and started an armed conflict in Donbas. The 2014 attacks are widely considered to constitute an act of aggression (Grant, 2015). This analysis will focus on the 2022 events.

The international law prohibiting the use of force, or *ius contra bellum* (Dinstein, 2017), is unequivocally expressed in the UN Charter, and it is consistently affirmed in the case law of the main UN judicial body: the International Court of Justice (ICJ). The Charter prohibits the use of force at

Article 2(4): «All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations». Furthermore, it sets two exceptions to the prohibition: Security Council authorization to take «action by air, sea, or land forces as may be necessary to maintain or restore international peace and security» (Article 41), and «the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations» (Article 51). The ICJ reaffirmed the prohibition in several cases. For instance, in the *Nicaragua* case, the ICJ specifically stated that the alleged purpose to protect human rights cannot constitute a legal basis to use force in violation of the UN Charter: «[t]he protection of human rights, a strictly humanitarian objective, cannot be compatible with the mining of ports, the destruction of oil installations, or again with the training, arming and equipping of armed forces» (*Nicaragua*, 1986, para. 268).

The Russian Federation justified the legality of its military intervention in a letter to the Security Council on February 24. The letter reported the speech delivered by Russian President Vladimir Putin the previous day: «The people's republics of Donbass have asked Russia for help. In this context, in accordance with Article 51 (Chapter VII) of the UN Charter ... I made a decision to carry out a special military operation. The purpose of this operation is to protect people who, for eight years now, have been facing humiliation and genocide perpetrated by the Kiev regime» (Security Council, 2022b). In so doing, the Russian Federation claimed two separate legal basis for the use of force: collective self-defense of 'the people's republics of Donbass', Donetsk and Luhansk, and protecting the same people from genocide.

Concerning collective self-defense, in accordance with article 51 of the UN Charter, this legal justification does not apply to military operations supporting non-state armed groups (see also *Nicaragua*, 1986, para. 246). Himes and Kim (2021, p. 278), examining the US justification for its military operations in Syria on the same legal ground, explain that self-defense on behalf of non-state actors is not acceptable: «by simply designating an aggrieved non-state group in any conflict in any region of the world as a “partner,” any willing state may invoke the collective self-defense of that partner to lawfully use military force against another sovereign state that poses no direct threat to its counterpart(s)». In the effort of overcoming the statehood requirement to claim self-defense, the 21 February 2022, on the eve of the attack, the Russian Federation recognized the Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR) as independent states. Yet, this unilateral act alone does not grant statehood to the entities, which remain *de iure* Ukrainian regions, called oblasts. As Weller (2022) asserted, «Russia therefore manufac-

tered the statehood necessary to invoke self-defense based on its previous invasion of parts of the two territories». Furthermore, the Russian recognition violates the principle of non-intervention and the principle of territorial integrity (Miklasová, 2022)

With reference to the protection of Donetsk and Luhans population from Ukrainian genocide, the problem is both factual and legal. First, claims that genocide is taking place in the oblasts are preposterous (Schabas, 2022). Second, genocide does not constitute an exception to the prohibition of the use of force under the UN Charter. Ukraine filed an application to the International Court of Justice, which can now make a determination on the Russian claims. The ICJ issued an order on provisional measures on March 16 (ICJ, 2022), declaring that «Ukraine has a plausible right not to be subjected to military operations by the Russian Federation for the purpose of preventing and punishing an alleged genocide in the territory of Ukraine» (para 60). The Court also considered «doubtful that the Convention, in light of its object and purpose, authorizes a Contracting Party's unilateral use of force in the territory of another State for the purpose of preventing or punishing an alleged genocide» (para 59). A further clarification on the issue at the following stages of the proceedings is desirable to clarify and reinforce the *ius contra bellum*: as Schabas (2022) maintains, «[u]nequivocal rejection of the doctrine that there are any exceptions to the use of force that are not specified in the Charter of the United Nations will make the world a safer place».

More generally, Putin's reference of the purpose of protecting people recalls the language of the doctrine of the responsibility to protect (RtoP). RtoP is a doctrine created in the early 2000s to address the international community's failure to prevent international crimes. Its definition and evolution have not been consistent, and the legal value of the doctrine is debated, as RtoP seems to have not modified existing international law norms. It has acquired an increasing relevance in the language of the UN, introducing a new jargon and a new focus on human protection in the diplomatic debate. A school of thought (e.g. Weiss, 2012; Davenport, 2016) considers RtoP as a new legal justification to use force outside the UN Charter framework. Yet, the controversy is limited to the scholarly debate, as States have consistently opposed the constitution of such an exception to the *ius contra bellum*. Indeed, all RtoP definitions adopted within the UN unequivocally mention that any measure taken pursuant to the doctrine must respect the UN Charter. The 2005 World Summit Outcome Document, adopted by consensus, specifies that all the measures invoked to protect populations must be taken «in accordance with the Charter, including Chapter VII» and «bearing in mind the principles of the Charter and international law» (UNGA, 2005). The 2009 Secretary-General's Report 'Implementing the Responsibility to Protect' af-

firms that «the responsibility to protect does not alter, indeed it reinforces, the legal obligations of Member States to refrain from the use of force except in conformity with the Charter» (UN Secretary General, 2009). As Louis Henkin (1971) observed over 50 years ago, «the fissures of the Charter are worrisome but they, too, are not as wide in international life as they loom in academic imagination».

This analysis clarifies that both Putin's claimed legal bases for the invasion of Ukraine, collective self-defense and protection of Donetsk and Luhansk population, are unfounded in international law. The following section will examine how this violation of the *ius contra bellum* constitutes a crime of aggression, thus entailing individual criminal liability, and explores the obstacles in prosecuting the crime despite the widespread international condemnation of the Russian action.

3. Crime and No Punishment: the Problems with Prosecuting Aggression

With the words of Nuremberg Prosecutor Robert Jackson, aggression «is not only an international crime; it is the supreme international crime differing only from other war crimes in that it contains within itself the accumulated evil of the whole». (*France v. Goering*, 1946, p. 172). The International Military Tribunal at Nuremberg after saw the first prosecutions for aggressive warfare in international criminal law. At Nuremberg, twelve individuals were convicted of crimes against peace. In contrast with the international law prohibiting the use of force, entailing state responsibility, the criminalization of aggression, entailing individual criminal liability, did not evolve in international law during the following decades. The crime was not included in the statutes of the ad hoc tribunals for former Yugoslavia and Rwanda. When the first permanent international criminal tribunal, the International Criminal Court was established, (with the 1998 Rome Statute, entered into force in 2002) the crime of aggression was finally included among the crimes within its jurisdiction, in addition to genocide, crimes against humanity, and war crimes. The Rome Statute defines both the crime of aggression and the act of aggression (Article 8 bis):

1. For the purpose of this Statute, 'crime of aggression' means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.
2. For the purpose of paragraph 1, 'act of aggression' means the use of armed force by a State against

the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations.

The definition implies that certain violations of the prohibition to use force are not criminalized. It establishes a threshold of ‘manifest violation’, which is both quantitative, according to gravity and scale, and qualitative, according to its character (Kress, 2018). The Elements of Crimes further detail the concept, stating for instance that the term ‘manifest’ is an objective qualification (UN Review Conference, 2010, para 3). As a manifest violation of the UN Charter, or «the most brazen illegal war waged by one sovereign state against another since World War II» (Hathaway, 2022), there is a widespread consensus that starting the invasion of Ukraine, the Russian leadership has committed a crime of aggression as defined by the ICC Statute.

While 123 countries are State Parties to the Court, the Russian Federation and Ukraine are not among them, not having ratified the ICC Statute. However, in 2015 Ukraine lodged two declarations accepting ICC jurisdiction over international crimes committed on its territory from 21 November 2013 on. As a result, the ICC can exercise jurisdiction on war crimes, crimes against humanity and genocide being committed on Ukrainian territory. Accordingly, 41 States referred the situation of Ukraine to the ICC Prosecutor, who started an investigation and commenced evidence-collection activities (International Criminal Court, 2022).

However, the crime of aggression has a separate jurisdictional regime, and the ICC cannot investigate and prosecute the crime. State Parties to the Rome Statute activated the jurisdiction on aggression in 2018, with various restrictions. Most relevantly for the present case, the Court cannot deal with the crime when committed by non-State parties nationals or on their territory, pursuant to Article 15bis of the Rome Statute. The UN Security Council would have the power to trigger the ICC jurisdiction on aggression in Ukraine, but the Russian Federation can veto any Council’s referral to the Court. In so doing, Russia can permanently avoid that its leadership is prosecuted before the International Criminal Court. Given the incapability of the ICC to investigate and prosecute aggression, the following section will explore possible alternative avenues for bringing accountability to the crime.

4. What is to be done? Alternative Avenues for Accountability

Possible solutions for prosecuting aggression in Ukraine besides the ICC include domestic prosecution before a national court, and the establishment of an ad hoc international tribunal or a hybrid tribunal.

First of all, as detailed in the previous section, the International Criminal Court cannot deal with the crime of aggression, but it is already investigating other international crimes committed in Ukraine. Thus, Einarsen and Rikhof (2022) suggest that the ICC could bypass the jurisdictional issues on the crime of aggression by prosecuting the same individuals for war crimes and crimes against humanity. This way, the Court could at least establish if a crime of aggression was perpetrated, and consider the gravity of the crime at the stage of sentencing. This creative suggestion would not constitute a proper prosecution of the crime of aggression. However, it is important to note that the ICC is likely to investigate and indict, although with different charges, the same persons who would be responsible for the crime of aggression.

Concerning opportunities for domestic prosecutions, several national systems are already investigating the crimes at stake, including Ukraine, which in 2016 convicted two Russian nationals for aggression, Alexandrov and Yerofeyev, for acts committed in Luhansk in 2015 (Sayapin, 2018), Poland and Lithuania, under the principle of universal jurisdiction (Dannebaum, 2022). Given that aggression is by definition a state crime, necessarily perpetrated by State leaders in their official capacity, the first obstacle to prosecute those responsible is immunity. Immunities have controversial limits with reference to international crimes. To sum up the prevailing views, which are not undisputed, personal immunity (*rationae personae*) concerns Heads of State, Heads of Government, diplomatic representatives and ministries of foreign affairs for any act committed while in office. Therefore, personal immunity would hinder domestic prosecutions of those responsible for aggression, which is a leadership crime, at least until they are in office. Functional immunity (*rationae materiae*) covers all state officials for acts committed in their official capacity, so including in the act of aggression, even after they leave office. Functional immunity is excluded in case of certain international crimes, but case-law and the work of the International Law Commission do not allow a definitive conclusion on the possibility to exclude functional immunity when prosecuting a crime aggression before a national court (Epik, 2021). A further problem with domestic prosecutions includes the technical expertise to conduct a trial on a complex international crime, which was already questioned in case of Ukraine with the *Alexandrov and Yerofeyev* case (Sayapin, 2018). For this reasons, the establishment of an international tribunal might be a preferable option.

On 4 March 2022, a statement titled “Calling for the Creation of a Special Tribunal for the Punishment of the Crime of Aggression Against Ukraine” was issued, signed by a number of international law academics and experts, but also politicians like Gordon Brown (who is controversially involved in the aggression against Iraq in 2003), writers like Paul Auster, Javier Cercas, Siri

Hustvedt, and Stephen Fry. An international tribunal would exclude immunity issues, given the precedent of the Special Court of Sierra Leone prosecuting a sitting Head of State (*Prosecutor v Charles Ghankay Taylor*, 2004). Furthermore, the ICC Appeals Chamber affirmed that, under customary international law, heads of state do not enjoy immunity in front of international courts, as «there is a *ius puniendi* that transcends state sovereignty and resides in the international community itself» (*Prosecutor v Al-Bashir*, 2019). Compared to a domestic prosecution, an international tribunal would also guarantee a specific expertise on the crime of aggression. An ad hoc tribunal following the model of Former Yugoslavia and Rwanda, however, should be established by the Security Council, where the Russian Federation holds the veto power. As a possible solution, some scholars (Dannebaum, 2022, Heller, 2022) may be a hybrid tribunal, on the example of the Special Court of Sierra Leone and the Extraordinary Chambers of Cambodia. This would be the result of an agreement between Ukraine and the UN, and would arguably overcome issues of immunities and lack of expertise, granting an international nature to the prosecution of the crime of aggression (Johnson, 2022).

Last but not least, all efforts to prosecute the Russian aggression against Ukraine carry a problem of selectivity. Several States supporting the current prosecution have perpetrated past aggressions which remained unpunished. The US have been consistently opposing ICC jurisdiction on the crime (Pecorella, 2021). Sander and Tallgren (2022) warn of «the longer-term expressive costs that such a tribunal would send about the selectivity of international criminal justice». These concerns require further reflection. At the present moment, they do not seem a founded reason to stop efforts to hold accountable those responsible for a blatant act of aggression. The only international trials for a crime of aggression took place in Nuremberg and Tokyo. The double-standards and biases of the Nuremberg and Tokyo trial would probably be unacceptable for the current (although flawed) standards (Sellars, 2010, Rabkin, 1999). Still, the historical legacy of these tribunals is of a positive contribution to the evolution of international justice. The character from *War and Peace* Platon Karataev affirms «Where there's law there's injustice» (Tolstoj, 1869). This recalls the necessity to acknowledge the limits of the discipline. International law, like any form of law, is inherently tied to power, is administered by human beings, and can thus only deliver partial justice. Efforts to improve fairness and equality require the adoption of other disciplines and methodologies, transcending legal concerns, and embracing social and political action.

Bibliography

Primary Sources

- Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.
- Council of Europe (2022), '1428ter meeting, 16 March 2022. Consequences of the aggression of the Russian Federation against Ukraine' 16 March. Available at https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a5d7d9 last consulted on 20 March 2022.
- International Criminal Court (2010) UN Review Conference, *Res RC/Res.6*, 11 June. Annex II.
- International Criminal Court (2019), *Prosecutor v Al-Bashir* (Judgment in the Jordan Referral re Al-Bashir Appeal), 6 May.
- International Criminal Court, *Statement of ICC Prosecutor, Karim A.A. Khan QC, on the Situation in Ukraine: Additional Referrals from Japan and North Macedonia; Contact portal launched for provision of information*, 11 March 2022.
- International Court of Justice (1986), *Nicaragua v United States of America* (Merits) ICJ Rep 134.
- International Court of Justice (2022), *Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v. Russian Federation) Request for the Indication of Provisional Measures*, 16 March.
- International Military Tribunal, *France v Goering 1946* (Judgment) [1947] 41 American Journal of International Law 172, 186.
- Special Court of Sierra Leone (2004), *Prosecutor v Charles Ghankay Taylor* (Decision on Immunity from Jurisdiction), 31 May.
- UNICEF, UNFPA and WHO (2022) *Stop attacks on health care in Ukraine, Joint statement from UNICEF, UNFPA, and WHO*, 13 March. Available at <https://www.who.int/news/item/13-03-2022-stop-attacks-on-health-care-in-ukraine> last consulted on 20 March 2022.
- United Nations General Assembly, UN Doc. A/ES-11/L.1, 1 March 2022
- United Nations Security Council (2022), *Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General*, 24 February, UN Doc. S/2022/154

Secondary Sources

- Chachko, E. and Linos, K. (2022) 'Sharing Responsibility for Ukrainian Refugees: An Unprecedented Response', *Lawfare*, 5 March. Available at <https://www.lawfareblog.com/sharing-responsibility-ukrainian-refugees-unprecedented-response> last consulted on 20 March 2022.
- Charlesworth, H. (2002). International Law: A Discipline of Crisis. *The Modern Law Review*, 65(3), 377-392.
- Dannembaum, T. (2022) 'Mechanisms for Criminal Prosecution of Russia's Aggression Against Ukraine', *Just Security*, 10 March. Available at <https://www.>

- justsecurity.org/80626/mechanisms-for-criminal-prosecution-of-russias-aggression-against-ukraine/ last consulted on 20 March 2022.
- Davenport J. (2016) 'In Defense of the Responsibility to Protect: A Response to Weissman' 35(1) *Criminal Justice Ethics* pp. 39, 67:
- Dinstein, Y. (2017) *War, Aggression and Self-Defence*, 6th ed. Cambridge: Cambridge University Press.
- Epik A. (2021), 'No Functional Immunity for Crimes under International Law before Foreign Domestic Courts An Unequivocal Message from the German Federal Court of Justice', *Journal of International Criminal Justice* 19, pp. 1263-1281.
- Einarsen T. and Rikhof J. (2022) Prosecuting the Russian Leadership for the Crime of Aggression at the International Criminal Court, Policy Brief Series No. 129 (2022), TOAEP. Available at <https://www.toaep.org/pbs-pdf/129-einarsen-rihof/> last consulted on 20 March 2022.
- Gaeta, P. and Zappalà, S. (2021) *Antonio Cassese, the Stubborn Sparrow* [Podcast] 9 December, available at <https://antonio-cassese-the-stubborn-sparrow-f3145101.simplecast.com/> last consulted on 20 March 2022.
- Hathaway O. (2022) 'International Law Goes to War in Ukraine, The Legal Pushback to Russia's Invasion' *Foreign Affairs*, 15 March, Available at <https://www.foreignaffairs.com/articles/ukraine/2022-03-15/international-law-goes-war-ukraine> last consulted on 20 March 2022.
- Heller, KJ (2022), 'The Best Option: An Extraordinary Ukrainian Chamber for Aggression', *Opinio Juris*, 16 March. Available at <https://opiniojuris.org/2022/03/16/the-best-option-an-extraordinary-ukrainian-chamber-for-aggression/> last consulted on 20 March 2022.
- Henkin L. (1971) The Reports of the Death of Article 2(4) Are Greatly Exaggerated, *The American Journal of International Law* 65(3), pp. 544-548.
- Himes A. and Kim B. (2021) 'Self-Defense on Behalf of Non-State Actors', *University of Pennsylvania Journal of International Law*, 43(1) pp. 241-279.
- Johns, F. and Kotova, A. (2022) 'Ukraine: Don't write off the international order – read and rewrite it', *The Interpreter*, 4 March. Available at <https://www.lowyinstitute.org/the-interpreter/ukraine-don-t-write-international-order-read-rewrite> last consulted on 20 March 2022.
- Johnson L. (2022), United Nations Response Options to Russia's Aggression: Opportunities and Rabbit Holes, *Just Security*, 1 March, <https://www.justsecurity.org/80395/united-nations-response-options-to-russias-aggression-opportunities-and-rabbit-holes/> last consulted on 20 March 2022.
- Kress C. (2018) 'On the Activation of ICC Jurisdiction over the Crime of Aggression' *Journal of International Criminal Justice* 16(1), pp. 1-17.
- Miklasová J. (2022) 'Russia's Recognition of the DPR and LPR as Illegal Acts under International Law', *Völkerrechtsblog*, 24 February. Available at <https://voelkerrechtsblog.org/russias-recognition-of-the-dpr-and-lpr-as-illegal-acts-under-international-law/> last consulted on 20 March 2022.
- Pecorella, G. (2021) *The United States of America and the Crime of Aggression*, New York, Routledge.

- Rabkin J. (1999) 'Nuremberg Misremembered', *SAIS Review*, The Johns Hopkins University Press, 19(2) p. 82.
- Sander B. and Tallgren I. (2022), 'On Critique and Renewal in Times of Crisis: Reflections on International Law(yers) and Putin's War on Ukraine', *Volkerrechtsblog*, 16 March. Available at <https://voelkerrechtsblog.org/on-critique-and-renewal-in-times-of-crisis/> last consulted on 20 March 2022.
- Schabas W. (2022) 'Preventing Genocide and the Ukraine/Russia case', *EJIL Talk*, 15 March. Available at <https://www.ejiltalk.org/preventing-genocide-and-the-ukraine-russia-case/> last consulted on 20 March 2022.
- Sellers K (2010) 'Imperfect Justice at Nuremberg and Tokyo', *European Journal of International Law*, 21(4) pp. 1085-1102.
- Tolstoj L. (2010, first edition 1869) *War and Peace*, Oxford University Press, p. 1043.
- Trahan J. (2022) 'Aggression and the Veto', *Just Security*, 28 February. Available at <http://opiniojuris.org/2022/02/28/aggression-and-the-veto/> last consulted on 20 March 2022.
- Weller M. (2022) 'Russia's Recognition of the 'Separatist Republics' in Ukraine was Manifestly Unlawful' *EJIL Talk*, 9 March. Available at <https://www.ejiltalk.org/russias-recognition-of-the-separatist-republics-in-ukraine-was-manifestly-unlawful/> last consulted on 20 March 2022.
- Weiss T. (2012) 'RtoP Alive and Well After Libya' 25(3) *Ethics & International Affairs* pp. 287-288

Russia-Ukraine conflict: digital assets chronicles in times of war

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. Given his experience in corporate and institutional communication, homeland security, and geopolitics, his research interests are cyber-jihad, terrorist financing, and terrorist organizations' communication strategies.

Abstract

The economic catastrophe caused by the Russian invasion of Ukraine has raised questions on the role of digital assets in this conflict. On the one hand, how crypto assets could be exploited by Moscow to circumvent international sanctions and, on the other hand, how crypto can be useful as a crowdfunding tool to finance the Ukrainian military sector.

This context turned a spotlight on the companies operating in the digital assets field, highlighting the controversies raised by the collision of the neutrality of the cryptocurrency sector with a humanitarian crisis.

With this premises, based on events and statements of the first few weeks after the Russian invasion began, this research is aimed at answering the following questions: how much can digital assets help in financing the military sector of a State? Can digital assets be a reliable alternative to international financial isolation? In which way could this conflict affect the cryptocurrency sector?

La catastrofe economica causata dall'invasione russa dell'Ucraina ha sollevato numerose domande sul ruolo che i digital asset potrebbero ricoprire in questo conflitto. Da un lato, il potenziale sfruttamento delle criptovalute da parte di Mosca per eludere le sanzioni economiche e, dall'altro, la funzione delle criptovalute nel finanziamento al settore militare ucraino attraverso il crowdfunding.

Questo contesto ha acceso un faro sulle compagnie operanti nel settore dei digital asset, facendo emergere le controversie generate dalla collisione tra la neutralità delle criptovalute con una crisi umanitaria.

Con tali premesse, basandosi su avvenimenti e dichiarazioni delle prime settimane dall'inizio dell'invasione russa, questa ricerca ha la finalità di rispondere alle seguenti domande: quanto possono aiutare le criptovalute nel finanziamento al settore militare di uno stato? Possono le criptovalute essere un'alternativa valida all'isolamento finanziario internazionale? In che modo il conflitto russo-ucraino ha un impatto nel settore delle criptovalute?

Keywords

Ukraine, hybrid warfare, cryptocurrencies, digital assets

1. Introduction

In one week the war in Ukraine has changed the global economy.¹

After invading Ukraine, Russia, the 11th largest economy in the world,² which banking assets total of more than RUB 103.8 trillion (\$1.4 trillion), has been met with an unprecedented response from the US, the UK, the EU, Canada, Japan, Australia, and other countries.³ In a week, the Russian economy, deeply ingrained in the global financial system for decades, has experienced more and more tightening⁴ international sanctions,⁵ while companies in multiple firms have bowed out of the country (e.g. Apple, Ikea, General Motors, American Express, etc).⁶

On the other hand, since Russian troops started encircling much of the country with 150.000 militaries threatening war, the Ukrainian economy has been squeezing with, among other dramatic consequences, \$12.5 billion withdrawn from accounts in the country,⁷ most of the flights canceled and commercial shipping disruption.⁸

¹ Riley C. (March 3, 2022) *How Russia's invasion of Ukraine changed the global economy in a week*. CNN Business. <https://edition.cnn.com/2022/03/03/economy/russia-invasion-global-economy/index.html>

² Elliptic (February 28, 2022) *What the Russia Sanctions Mean for Crypto Compliance*. https://www.elliptic.co/blog/what-the-russia-sanctions-mean-for-crypto-compliance?utm_content=199360335&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267

³ Black Sea Trade & Development Bank (2021) *Overview of the financial sector in Russia*. https://www.bstadb.org/Overview_of_the_fin_sector_RUSSIA.pdf

⁴ Zorthian J. (March 2, 2022) *Here's What the New, Tightened SWIFT Sanctions on Russian Banks Actually Do*. Time. <https://time.com/6153951/swift-sanctions-russia/>

⁵ Konig O., Ericsson F. (March 3, 2022) *New EU sanctions cut-off certain Russian banks from SWIFT and prohibit certain investments in Russia*. Sanctions News – A blog by Baker McKenzie. <https://sanctionsnews.bakermckenzie.com/new-eu-sanctions-cut-off-certain-russian-banks-from-swift-and-prohibit-certain-investments-in-russia/>

⁶ Isidore C. (March 3, 2022) *Why many businesses are getting tougher on Russia than sanctions require*. CNN Business. <https://edition.cnn.com/2022/03/03/business/business-go-beyond-russian-sanctions/index.html>

⁷ Hinnant L. (February 23, 2022) *Ukraine's economy is another victim of Russia's 'hybrid war'*. Associated press. <https://apnews.com/article/russia-ukraine-entertainment-business-economy-kyiv-6c93f4964cd9d26438dfd4e9c38fe76c>

⁸ Hopkins V. (February 18, 2022) *How Putin Has Already Weakened Ukraine's Economy*. The New York Times. <https://www.nytimes.com/2022/02/18/world/europe/ukraine-economy-putin.html>

Furthermore, the military capacity of these two nations is very imbalanced, with Ukraine's defense spending totaling around \$4.7 billion in 2021, which represents almost 10% of Russia's \$45.8 billion.⁹ Even though Ukrainians may be overwhelmed by the Russian military, they have still tried to resist the territorial expansion through armed resistance,¹⁰ information war,¹¹ and by receiving foreign economic and militaristic aid by state actors¹² or private donors.¹³

The economic needs that suddenly weighed on both sides of the conflict have brought out either speculations or new applications of financial technology. Indeed, since the beginning, this conflict has been also called "the world's first crypto war," as both sides have found advantages in borderless, decentralized currencies.¹⁴ In fact, on February 28, the amounts of bitcoin traded using the ruble surged to the highest point since May 2021, while bitcoin traded using the hryvnia reached the highest point since October 2021.¹⁵

In this context, digital assets have become, on the one hand, a crowdfunding tool to finance the Ukrainian military segment while, on the other hand, a potential alternative for Russia's economy to circumvent international sanctions.

With these premises, by analyzing the role covered by digital assets at the very beginning of the war, the research tries to answer the following questions: how digital assets can help finance the military sector of a State? Can digital assets subvert the economic international isolation of a State? In which way could this conflict affect the cryptocurrency sector?

⁹ Dewan A. (February 25, 2022) *Ukraine and Russia's militaries are David and Goliath. Here's how they compare*. CNN <https://edition.cnn.com/2022/02/25/europe/russia-ukraine-military-comparison-intl/index.html>

¹⁰ Raine J. (February 25, 2022) *Ukraine and the importance of resistance*. International Institute for Strategic Studies (IISS). <https://www.iiss.org/blogs/analysis/2022/02/ukraine-and-the-importance-of-resistance>

¹¹ Thompson S.A., Alba D. (March 3, 2022) *Fact and Mythmaking Blend in Ukraine's Information War*. The New York Times. <https://www.nytimes.com/2022/03/03/technology/ukraine-war-misinfo.html>

¹² Duthois T. (March 4, 2022) *Ukraine war: Which countries are sending weapons and aid to forces fighting the Russian invasion?* EuroNews <https://www.euronews.com/next/2022/03/04/ukraine-war-these-countries-are-sending-weapons-and-aid-to-forces-fighting-the-russian-inv>

¹³ Wood G.R. (February 26, 2022) *What Role for Crowdfunding Defense in Ukraine?* Small wars journal. <https://smallwarsjournal.com/jrnl/art/what-role-crowdfunding-defense-ukraine>

¹⁴ Zeitchik S., Newmyer T. (February 25, 2022) *In the world's first crypto war, uncertainty about who will benefit*. The Washington Post. <https://www.washingtonpost.com/technology/2022/02/25/cryptocurrency-ukraine-russia-war-impact/>

¹⁵ Volpicelli G.M. (March 8, 2022) *War Is Calling Crypto's 'Neutrality' Into Question*. Wired. <https://www.wired.com/story/crypto-russia-ukraine-sanctions/>

2. Crypto crowdfunding for militaristic purposes

On February 26, two days after Russia started the invasion of Ukraine, the official Twitter account of the Ukrainian government¹⁶ and Ukraine's Vice-Prime Minister, Mykhailo Fedorov,¹⁷ posted a call for cryptocurrency donations. The accounts asked users to send Bitcoin (BTC), Ethereum (ETH), and Tether (USDT), a stable coin with a value meant to mirror the value of the US dollar. In this respect, Ukraine's Vice-Prime Minister also claimed: "How will we use money? To destroy as much Russian soldiers as possible."¹⁸

To better understand this context, a brief is necessary, given that this request was not an isolated case.

Firstly, Ukraine officially legitimized Bitcoin and other cryptocurrencies last year, regulating digital financial assets and providing fraud protection for Ukrainians.¹⁹ With \$8 billion of cryptocurrency passing through the country annually, Ukraine was ranked fourth according to Chainalysis 2021 Global Crypto Adoption Index.²⁰

Moreover, the government followed the trails of the growing success of Ukrainian NGOs, volunteer groups, and hacking groups that have been crowdfunding cryptocurrencies as tensions mounted with Russia,²¹ crowdfunding funneled funds to the country's army and wider armed resistance. In this respect, the blockchain analysis provider, Elliptic, reported that donations to these groups increased by over 900% in 2021 to grow further in January, as Russia massed troops near Ukraine's border ahead of its invasion, and spike since Russia launched its invasion on February 24.

With these premises, in less than a week after the Russian invasion began, the Ukrainian call for donations broadened the types of crypto assets available

¹⁶ The official Twitter account of Ukrainian government (February 26, 2022) <https://twitter.com/Ukraine/status/1497594592438497282>.

¹⁷ Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine official Twitter account (February 26, 2022) <https://twitter.com/FedorovMykhailo/status/1497549813205848068>

¹⁸ Wilson T. (February 28, 2022) *Ukraine raises \$13 million in crypto after crowdfunding appeal*. Reuters. <https://www.reuters.com/world/china/ukraines-government-raises-crypto-worth-8-million-crowdfunding-appeal-2022-02-27/>

¹⁹ Lopatto E. (February 26, 2022) *HOW UKRAINIANS ARE FUNDRAISING IN CRYPTOCURRENCY*. The Verge. <https://www.theverge.com/2022/2/26/22952357/ukraine-bitcoin-ethereum-donation-vitalik-buterin>

²⁰ Chainalysis (October 14, 2021) *The 2021 Global Crypto Adoption Index: Worldwide Adoption Jumps Over 880% With P2P Platforms Driving Cryptocurrency Usage in Emerging Markets*. <https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/>

²¹ Elliptic (February 08, 2022) *Ukrainians Turn to Bitcoin to Crowdfund the Fight Against Russia*. <https://www.elliptic.co/blog/ukrainians-turn-to-bitcoin-to-crowdfund-the-fight-against-russia>

to crowdfund the country's military sector, adding TRON, Dogecoin, Solana,²² and Polkadot²³ (which founder, Gavin Wood, sent a \$5.8 million donation)²⁴.

Moreover, people also sent non-fungible tokens NFTs²⁵ to the Ukrainian government's²⁶ Ethereum account.²⁷ According to Elliptic, the donations included a transaction worth \$1.86 million, allegedly coming from the sale of an NFT created by Julian Assange and the digital artist, Pak, launched to help Assange's legal defense to avoid extradition from the UK to the US, and CryptoPunk NFT #5364, worth approximately \$230,000.²⁸

On March 7, ten days since the start of the Russian invasion, NGOs and the Ukrainian government raised approximately \$59.7 million through more than 120,000 crypto asset donations.²⁹ On that date, the crypto fundraising allowed the Ukrainian government to spend \$15 million of the donations it received in cryptocurrencies on military supplies, including bulletproof vests.³⁰

Nevertheless, the Ukrainian crowdfunding activity was not always easy, due to unexpected controversies and major setbacks since its very beginning.

In this regard, Come Back Alive, one of the largest organizations providing support to the Ukrainian army, established in 2014, when armed conflict broke out between Ukraine and Russian-backed separatists, began to accept crypto assets in 2018 and, at the time of writing, has already raised

²² Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine official Twitter account (March 01, 2022) <https://bit.ly/3Klbqsl>

²³ The official Twitter account of Ukrainian government (March 01, 2022) <https://twitter.com/Ukraine/status/1498547710697345027>

²⁴ Chaturvedi A. (March 3, 2022) NFTs, cryptocurrencies and now DAO join Ukraine's crowdfunding appeal. Business today. <https://www.businesstoday.in/crypto/story/nfts-cryptocurrencies-and-now-dao-join-ukraines-crowdfunding-appeal-324580-2022-03-03>

²⁵ A non-fungible token (NFT) is a digital asset that represents real-world objects (like art, music, real-estate, etc.). NFTs are unique cryptographic tokens that exist on a blockchain. They can be bought or sold but cannot be replicated.

²⁶ BBC (March 4, 2022) *Ukraine conflict: Government to sell NFTs to fund war against Russia*. <https://www.bbc.com/news/business-60613613#:~:text=Ukraine's%20government%20has%20said%20it,the%20sale%20of%20war%20bonds>

²⁷ An example: NFTU-KRAINE, Organized by Kenny Schachter & David Cash – bringing NFT artists together to raise money for Ukraine. <https://opensea.io/NFTU-KRAINE>

²⁸ DeepNFTvalue (Updated: March 5, 2022) *Cryptopunks #5364 – Price Details* <https://deepnftvalue.com/punks/5364/>

²⁹ Elliptic (Last updated: March 7th, 10:10pm UTC) *Live Updates: Ukraine Government Turns to Crypto to Crowdfund Millions of Dollars*. <https://www.elliptic.co/blog/live-updates-millions-in-crypto-crowdfunded-for-the-ukrainian-military>

³⁰ Mint (March 6, 2022) *Ukraine spends \$15 million cryptos on military gear as crypto donations pour in as humanitarian aid*. <https://www.livemint.com/market/cryptocurrency/ukraine-spends-15-million-cryptos-on-military-gear-as-crypto-donations-pour-in-as-humanitarian-aid-11646547788590.html>

several million dollars in crypto donations.³¹ The organization also created the most influential NFT issued outside the Ukrainian government through UkraineDAO,³² a decentralized autonomous organization that aims to raise ETH to be donated to Come Back Alive, auctioning an NFT of the Ukrainian flag for \$6.5 million.³³

At the beginning of the conflict, Come Back Alive didn't choose to exclusively fall back on cryptocurrencies for its crowdfunding activity. One of its primary sources of international funding was Patreon, a membership platform that connects content creators with fans and supporters, by letting users financially support and reward content creators through a monthly subscription.³⁴ The organization's Patreon page was suspended the day after the Russian invasion, because the platform "does not allow any campaigns involved in violence or purchasing of military equipment, regardless of their cause" as explained by a company spokesperson³⁵ and on a blog post on their website.³⁶

When Come Back Alive was banned from Patreon, the organization's page had already raised over \$300.000, which were refunded to contributors.

As in the case of Come Back Alive's crowdfunding campaign, digital assets can help to overlap controversies, allowing to raise funds from all over the world while circumventing either international sanctions or private digital platforms policy frameworks.

However, the unruled and not yet fully developed cryptocurrency sector, merged with a humanitarian crisis, can still raise controversies.

3. Libertarianism collided with the humanitarian crisis

Analyzing the case of Ukrainian crowdfunding via digital assets allows highlighting three main criticisms related to crypto.

- The first one regards the fact that, also for legitimate (as for illegal) donations, **cash is still king**. Cryptocurrencies still can't replace fiat money. In-

³¹ Повернись живим Facebook <https://www.facebook.com/backandalive/posts/2232521093571982>

³² <https://www.ukrainedao.love/>

³³ <https://zora.co/collections/0x715132af755D9D3d81eE0AcF11e60692719bc415/1>

³⁴ <https://www.patreon.com/it-IT>

³⁵ Nove J. (February 24, 2022) *Patreon suspends donation page for nonprofit giving body armor to Ukrainian army*. CNBC. <https://www.cnn.com/2022/02/24/patreon-suspends-come-back-alive-page-for-ukrainian-army-donations.html>

³⁶ Patreon (February 25, 2022) *In merito alla rimozione di Come Back Alive*. <https://blog.patreon.com/it-IT/in-merito-alla-rimozione-di-come-back-alive>

deed, the majority of donations for Ukraine were sent through traditional payment methods, such as bank wires and online payments services. Among these, there are many cases of cash donations to help Ukraine through money that stress the difference, in figures, between cash and digital assets.

For example, the over £85million raised by the Disasters Emergency Committee, a collective of leading UK charities.³⁷

Moreover, the initiative launched by the Ukrainian Ministry of Finance to issue military government bonds with a nominal value per bond of 1,000 hryvnias (about \$33),³⁸ to pay for its armed forces as they defend the country from a Russian invasion.³⁹ The sale came after a sharp plunge in the prices of Ukraine's existing bonds, while the finance ministry claimed that the bonds will have a yield of 11%, with a tenure of one year.⁴⁰ As reported by the Wall Street Journal, the bond sale was carried out through dealers including Citigroup, Austria's Raiffeisen Bank, and Budapest-based OTP Bank Nyrt; Ukraine's government claimed that the sale of war bonds raised about 8.14 billion Ukrainian hryvnias (\$277million).⁴¹ The government also issued bonds with a term of two months and 10% periodic interest payments, which raised \$7million.⁴²

Even though a bonds sale is not a cash donation, the different amount of money, compared to cryptocurrency donations previously explained, highlights the difference between raising money through conventional systems and crowdfunding via cryptocurrency.

³⁷ Thomas T. (March 5, 2022) *Ukraine fundraiser hits £85m as charities say money needed more than goods*. The Guardian. <https://www.theguardian.com/society/2022/mar/05/ukraine-fundraiser-hits-85m-as-charities-say-money-needed-more-than-goods>

³⁸ State sites of Ukraine – government portal Official website (March 1, 2022) *Finance Ministry: Ukraine issues military bond*. <https://www.kmu.gov.ua/en/news/minfin-1-bereznya-rozpochinayetsya-aukcion-z-prodazhu-vijskovih-obligacij>

³⁹ BBC (March 1, 2022) *Ukraine to sell 'war bonds' to fund armed forces* <https://www.bbc.com/news/business-60566776>

⁴⁰ Official account of the Ministry of Finance of Ukraine (February 28, 2022) https://twitter.com/ua_minfin/status/1498319440622104583

⁴¹ O'Brien F., Krasnolutska D., and Rocha P.A. (march 1, 2022) *Ukraine Raises Equivalent of \$277 Million From Sale of War Bonds*. Yahoo finance. [https://finance.yahoo.com/news/ukraine-raises-equivalent-277-million-154154581.html#:~:text=Ukraine%20Raises%20Equivalent%20of%20\\$24277%20Million%20From%20Sale%20of%20War%20Bonds,-Fergal%20O'Brien&text=\(Bloomberg\)%20%2D%2D%20Ukraine%20raised%208.1,its%20fight%20against%20Russia's%20invasion](https://finance.yahoo.com/news/ukraine-raises-equivalent-277-million-154154581.html#:~:text=Ukraine%20Raises%20Equivalent%20of%20$24277%20Million%20From%20Sale%20of%20War%20Bonds,-Fergal%20O'Brien&text=(Bloomberg)%20%2D%2D%20Ukraine%20raised%208.1,its%20fight%20against%20Russia's%20invasion)

⁴² Weizhen T., Wang C. (March 2, 2022) *Ukraine raises \$270 million from sale of war bonds to fund army as Russia's invasion continues*. CNBC. <https://www.cnbc.com/2022/03/02/ukraine-raises-270-million-from-sale-of-war-bonds-to-fund-army.html>

Besides the different figures, it has to be taken into account that cryptocurrency is still a reliable, fast, alternative, and emergency tool to send or receive donations, that gives total control over crowdfunding campaigns, no matter international sanctions or policies adopted by private companies.

- This lack of control over the crypto sector brings to the second main area of criticalities related to Ukrainian crowdfunding via digital assets: **the risk of attracting scammers**.⁴³

In this regard, some Ukraine-related cryptocurrency fraud schemes were launched to take advantage of people's support for Ukraine.

Some typical fraud consisted of phishing websites, forum posts, and falsified emails enticing users to help Ukraine by donating to counterfeit Bitcoin and Ethereum addresses, instead of governments wallets, that were not affiliated with the Ukrainian government.⁴⁴

There was also a scam connected to the airdrop⁴⁵ planned by the Ukrainian government⁴⁶ to reward donations⁴⁷ (canceled 29 hours after its launch).⁴⁸ Rumors said that hackers targeted Ukraine's fundraising attempts by issuing a fake token that they sent to Ukraine's Ethereum address. Allegedly, these tokens contained permission allowing the hacker to control them from whichever wallet received them.⁴⁹ So, any token sent from the

⁴³ Nicolle E. (March 3, 2022) *Ukraine's Crypto Army Is Both Inspiration and Cautionary Tale*. Bloomberg. <https://www.bloomberg.com/news/articles/2022-03-03/ukraine-s-crypto-army-is-both-inspiration-and-cautionary-tale?sref=0N1JmzAH>

⁴⁴ Sharma a. (March 1, 2022) *'Help Ukraine' crypto scams emerge as Ukraine raises over \$37 million*. Bleeping computer. <https://www.bleepingcomputer.com/news/security/help-ukraine-crypto-scams-emerge-as-ukraine-raises-over-37-million/>

⁴⁵ "An airdrop, in the cryptocurrency business, is a marketing stunt that involves sending coins or tokens to wallet addresses in order to promote awareness of a new virtual currency. Small amounts of the new virtual currency are sent to the wallets of active members of the blockchain community for free or in return for a small service, such as retweeting a post sent by the company issuing the currency." <https://www.investopedia.com/terms/a/airdrop-cryptocurrency.asp>

⁴⁶ Official Twitter account of Ukraine (March 2, 2022) <https://twitter.com/Ukraine/status/1498911922791583746?s=20&t=j4KQx4IIdj3rJgAGCxdHZA>

⁴⁷ Stentella G. (March 3, 2022) *L'Ucraina annuncia un airdrop di criptovalute, ecco tutti i dettagli*. Money.it. <https://www.money.it/Ucraina-airdrop-criptovalute-dettagli>

⁴⁸ Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine official Twitter account (March 3, 2022) <https://twitter.com/FedorovMykhailo/status/1499348177002151937?s=20&t=BJm7D5IaYQFXmcWewsFz5Q>

⁴⁹ Hake M.R. (March 4, 2022) *Dogecoin Among Major Crypto Donations to Ukraine but Watch Out for Scams!* Nasdaq. <https://www.nasdaq.com/articles/dogecoin-among-major-crypto-donations-to-ukraine-but-watch-out-for-scams>

Ukraine address would appear to have been transferred by the government, while the hacker was still in control.⁵⁰

Indeed, blockchain explorer Etherscan showed that the official Ukraine donation wallet was airdropping tokens that seemed to be controlled by an outside party,⁵¹ displaying “there are reports that this address was used in a Phishing scam. Please exercise caution when interacting with this address.”⁵²

- The third area is related to **misunderstandings between the private and public sectors** dealing with cryptocurrencies.

On the February 27, following the trend of mainstream finance aimed at squeezing the Russian economy, the Ukrainian leadership asked: “all major crypto exchanges to block addresses of Russian users.” And, in particular, claimed, “it’s crucial to freeze not only the addresses linked to Russian and Belarusian politicians but also to sabotage ordinary users.”⁵³

The answer of three of the major cryptocurrency exchanges, Coinbase Global Inc, Binance, and Kraken rejected the Ukrainian call, explaining that they couldn’t unilaterally freeze millions of innocent users’ accounts without a legal requirement to do so, because everyone should have access to basic financial services unless the law says otherwise.⁵⁴ In particular, Binance explained “crypto is meant to provide greater financial freedom for people across the globe. To unilaterally decide to ban people’s access to their crypto would fly in the face of the reason why crypto exists.”⁵⁵

Besides the fact that the Ukrainian request to freeze the accounts of exchange platforms’ Russian clients was not a legal requirement, this case highlights the changing role of crypto. Digital assets have become a mainstream industry that, put in the middle of a humanitarian crisis, loses its borderless and decentralized form to become ingrained in political issues.

⁵⁰ Trivedi V. (March 3, 2022) *This is How Ukraine’s ‘Peaceful World’ Airdrop was Exposed by Analysts*. Yahoo finance. <https://finance.yahoo.com/news/ukraine-peaceful-world-airdrop-exposed-144355689.html>

⁵¹ Wang T., Malwa S. (March 3, 2022) *‘Peaceful World’ Token Spoofs Traders Ahead of Now-Canceled Ukraine Airdrop*. CoinDesk. <https://www.coindesk.com/markets/2022/03/03/peaceful-world-token-may-be-spoofing-ukraines-airdrop/>

⁵² <https://etherscan.io/address/0xe9af51aaa1782fdc7c39048a81286505125ca303>

⁵³ Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine official Twitter account (February 27, 2022) <https://twitter.com/FedorovMykhailo/status/1497922588491792386>

⁵⁴ Nishant N. (March 4, 2022) *Coinbase, Binance resist calls to kick Russians off crypto platforms*. Reuters. <https://www.reuters.com/technology/coinbase-not-banning-russians-using-platform-ceo-says-2022-03-04/>

⁵⁵ Kharpal A. (February 28, 2022) *World’s biggest crypto exchange Binance says it will not block all Russian accounts despite Ukraine request*. CNBC. <https://www.cnbc.com/2022/02/28/binance-will-not-block-russian-accounts-after-ukraine-request.html>

In these terms, the real risk for exchange platforms is not to abide or not the law, but to change users' perception of the crypto business. Turn into centralized what was meant to be decentralized and distributed among users.

4. Russia: too big not to fail

The growing concern about how digital assets could help Russia in developing alternatives to the Western-led financial system⁵⁶ and the devalued ruble⁵⁷ are, progressively, undermining the neutrality allowed to exchange platforms.⁵⁸

In particular, among lawmakers, a few weeks after the Russian invasion of Ukraine,⁵⁹ the growing trend was to go far beyond the threat of reputational risk, assessing whether or not to force companies to choose between doing business in the US or with sanctioned Russian and Belarusian entities and individuals.⁶⁰

Following this trend, there was the launch of KleptoCapture, an interagency law enforcement task force dedicated to detecting and disrupting potential Russian sanction evasions, money laundering, and other illicit financial activity.⁶¹ The unit, created by the US Department of Justice, joins forces with France, Germany, Italy, Canada, and the European Commission, and is particularly interested in clamping down on virtual asset service providers (VASPs) which knowingly allow Russians to transact on their platforms.⁶²

⁵⁶ Suleymanova R. (March 1, 2022) *Crypto will not save Russia from sanctions, experts say*. Aljazeera. <https://www.aljazeera.com/economy/2022/3/1/crypto-will-not-save-russia-from>

⁵⁷ Fonda D. (March 18, 2022) *The Russia-Ukraine War Is Bringing Out the Good, Bad, and Ugly of Cryptocurrencies*. Barron's. https://www.barrons.com/articles/russia-ukraine-war-cryptocurrencies-51647548970?utm_content=201576331&utm_medium=social&utm_source=linkedin&hss_channel=lep-5027267

⁵⁸ Caldwell L.A. (March 8, 2022) *Warren crafts bill targeting cryptocurrency in Russia sanctions*. Nbc News. <https://www.nbcnews.com/politics/congress/warren-crafts-bill-targeting-cryptocurrency-russia-sanctions-rcna19094>

⁵⁹ Sun M. (March 7, 2022) *U.S. Warns Banks, Crypto Firms Against Potential Efforts to Evade Russian Sanctions*. The Wall Street journal. <https://www.wsj.com/articles/u-s-warns-banks-crypto-firms-against-potential-efforts-to-evade-russian-sanctions-11646696802>

⁶⁰ The United States Senate Committee on banking, housing, and urban affairs (March 17, 2022) *Understanding the Role of Digital Assets in Illicit Finance*. <https://www.banking.senate.gov/hearings/understanding-the-role-of-digital-assets-in-illicit-finance>

⁶¹ US Department of Justice – Office of Public affairs (March 2, 2022) *Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture – Task Force Will Surge Federal Law Enforcement Resources to Hold Accountable Corrupt Russian Oligarchs*. <https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture>

⁶² Elliptic (March 21, 2022) *Crypto Regulatory Affairs: Ukrainian President Signs Virtual Currency Bill into Law*. https://www.elliptic.co/blog/crypto-regulatory-affairs-ukrainian-president-signs-virtual-currency-bill-into-law?utm_campaign=Elliptic%20Essentials%20%7C%20

Also, FinCEN said a variety of actors that still retain some access to the international financial system, including crypto exchanges and administrators inside or outside Russia, could conduct evasion activities.⁶³

Moreover, to close potential sanctions loopholes, the EU issued guidance to confirm that sanctions on loans and credit to Russia include digital assets.⁶⁴

This fast-changing perception of cryptocurrency already changed the exchange platforms' approach to the ongoing conflict. For example, on March 7, the cryptocurrency exchange platform, Coinbase, declared having blocked over 25,000 addresses related to Russian individuals or entities believed to be engaging in illicit activity.⁶⁵

Nevertheless, it is a truism that, according to a simple comparison, cryptocurrency alone could not allow Russia to replace its economic environment: Russia's banking assets alone total more than RUB 103.8 trillion (\$1.4 trillion) while crypto has a total market capitalization of about \$1.7 trillion.⁶⁶

Furthermore, as reported by Al Jazeera, according to TRM labs, a blockchain intelligence company, 80% of Russia's daily foreign exchange transactions and 50% of its international trade are conducted in dollars. Thus, Moscow couldn't use crypto to replace hundreds of billions of dollars that could potentially be blocked or frozen.⁶⁷

Then, while cryptocurrency is an alternative asset, it's also neutral, decentralized, and transparent. Hence, the transparency of the blockchain facilitates transactions monitoring, while, thanks to neutrality and decentralization (with more than 400 virtual asset service providers where crypto assets can

Crypto%20Regulatory%20Affairs&utm_content=201736280&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267

⁶³ Sun M. (March 7, 2022) *U.S. Warns Banks, Crypto Firms Against Potential Efforts to Evade Russian Sanctions*. The Wall Street Journal. <https://www.wsj.com/articles/u-s-warns-banks-crypto-firms-against-potential-efforts-to-evade-russian-sanctions-11646696802>

⁶⁴ Jones H. (March 21, 2022) *Global regulators monitor crypto use in Ukraine war*. Reuters. <https://www.reuters.com/technology/global-regulators-monitor-crypto-use-ukraine-war-2022-03-21/>

⁶⁵ Grewal P. (March 7, 2022) *Using Crypto Tech to Promote Sanctions Compliance*. Coinbase blog. <https://blog.coinbase.com/using-crypto-tech-to-promote-sanctions-compliance-8a17b1dabd68>

⁶⁶ Elliptic (February 28, 2022) *What the Russia Sanctions Mean for Crypto Compliance*. https://www.elliptic.co/blog/what-the-russia-sanctions-mean-for-crypto-compliance?utm_content=199360335&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267

⁶⁷ Suleymanova R. (March 1, 2022) *Crypto will not save Russia from sanctions, experts say*. Al Jazeera. <https://www.aljazeera.com/economy/2022/3/1/crypto-will-not-save-russia-from>

be purchased with rubles)⁶⁸, sanctioned people or entities are likely to have moved their money in advance of the sanction announcements.⁶⁹

Lastly, assuming oligarchs would move billions of rubles, they would have to make many smaller transactions to avoid rousing too much suspicion. With these figures, the more an oligarch would buy a particular cryptocurrency, the more expensive it could become, creating a highly risky self-inflated bubble.⁷⁰

However, cryptocurrency could be still useful for a heavily sanctioned state like Russia to raise money, evade sanctions, and hide wealth.

In this respect, previous cases of financially isolated countries show potential exploitations of digital assets in case of international sanctions.

For instance, Iran, which is subject to a US-imposed total economic embargo, including a ban on all Iranian imports and sanctions on Iranian financial institutions, turned the country's surplus of oil and natural gas into electricity for state crypto-mining⁷¹ farms, consuming 500-600MW per year.⁷²

The Iranian state-sponsored crypto-mining business is so flourishing that, in August 2021, accounted for approximately 3.11% of all Bitcoin mining.⁷³ According to Elliptic,⁷⁴ this exploitation of crypto let Iran earn up to \$1 billion, while also attracting new business partners, like China, due to the competitive price of energy offered to mine cryptocurrency.⁷⁵

⁶⁸ Elliptic (February 28, 2022) *What the Russia Sanctions Mean for Crypto Compliance*. https://www.elliptic.co/blog/what-the-russia-sanctions-mean-for-crypto-compliance?utm_content=199360335&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267

⁶⁹ Levin J. (March 2, 2022) *Crypto Isn't the Sanctions Haven Its Jump Suggests*. The Washington Post. https://www.washingtonpost.com/business/crypto-isnt-the-sanctions-haven-its-jump-suggests/2022/03/01/6ee3fb7a-9987-11ec-9987-9dceee62a3f6_story.html

⁷⁰ Smith-Meyer B. (March 4, 2022) *Why crypto isn't Russia's safest haven*. Politico. <https://www.politico.eu/article/crypto-russia-safest-haven-why/>

⁷¹ Bitcoin mining is the process of creating new bitcoin by solving a computational puzzle. "Bitcoin miners run power-hungry computers, which process new transactions and add them to the blockchain. In return, the miners are rewarded with bitcoins – both from transaction fees as well as the minting of new bitcoins. The mining process effectively converts energy into cryptocurrency." Elliptic (May 21, 2022) *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*. <https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions>

⁷² Financial Tribune (January 18, 2022) *Cryptomining Suspended for 2 Weeks to Save Power*. <https://financialtribune.com/articles/business-and-markets/107075/cryptomining-suspended-for-2-weeks-to-save-power>

⁷³ Cambridge Bitcoin Electricity Consumption Index (August 2021) https://ccaf.io/cbeci/mining_map

⁷⁴ Elliptic (May 27, 2022) *Sanctions Compliance in Cryptocurrencies*. <https://www.elliptic.co/resources/elliptic-guide-to-sanctions-compliance-in-cryptocurrencies>

⁷⁵ Mine RHY YouTube channel (June 10, 2022) *RHY大型矿场 (RHY large mine Bitcoin Mining) One of the world's largest mines*. <https://www.youtube.com/watch?v=9ofEzftDFyM>

Speculations about Moscow exploiting crypto-mining to raise money are quite logical. Given the country's huge energy wealth, Putin already declared at a meeting with the government at the end of January 2022 "we ... have certain competitive advantages, especially in the so-called mining, I mean a surplus of electricity and well-trained personnel available in the country," while also instructing the government and the Bank of Russia to come to a consensus on the regulation of cryptocurrencies,⁷⁶ despite the Bank of Russia's proposal to ban mining and trading.⁷⁷

Besides crypto mining, Russia could follow the North Korean path of hacking cryptocurrency platforms.⁷⁸ Indeed, according to Chainalysis, North Korea, by launching at least seven attacks on cryptocurrency platforms, extracted nearly \$400 million worth of digital assets last year.⁷⁹

In this respect, Moscow could be backed by Russian cybercriminal groups. As the ransomware gang Conti, that declared to support Russia in its war efforts and threatened to carry out cyberattacks on enemy states,⁸⁰ and more than 15 million crypto addresses linked to criminal activity with a nexus in Russia identified by Elliptic.⁸¹

As previously explained, even though Russia would be willing to invest as much as North Korea or Iran in crypto to avoid international sanctions, is unlikely it could be able to replace the hundreds of billions of dollars blocked or frozen. Unlike North Korea or Iran, Russia has been deeply ingrained in the global financial system for decades. For instance, cryptocurrency mining

⁷⁶ Russian News Agency (January 26, 2022) *Russia has competitive advantages in cryptocurrency mining – Putin*. https://tass.com/economy/1393535?utm_source=theguardian.com&utm_medium=referral&utm_campaign=theguardian.com&utm_referrer=theguardian.com

⁷⁷ Jialiang D.P. (March 3, 2022) *Energy-Rich Russia May Turn to Bitcoin Mining to Dent Sanctions*. Bloomberg. <https://www.bloomberg.com/news/articles/2022-03-03/energy-rich-russia-may-turn-to-bitcoin-mining-to-dent-sanctions>

⁷⁸ Milmo D. (March 1, 2022) *Could Putin be exploring cryptocurrencies to bypass western sanctions?* The Guardian. <https://www.theguardian.com/business/2022/mar/01/could-putin-be-exploring-cryptocurrencies-to-bypass-western-sanctions-russia-ukraine-invasion>

⁷⁹ Chainalysis (January 13, 2022) *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*. <https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/>

⁸⁰ Dmitry Smilyanets official Twitter profile (February 25, 2022) <https://twitter.com/ddd1ms/status/1497247507474272257>

⁸¹ Elliptic (February 28, 2022) *What the Russia Sanctions Mean for Crypto Compliance*. https://www.elliptic.co/blog/what-the-russia-sanctions-mean-for-crypto-compliance?utm_content=199360335&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267

would allow Russia to monetize its energy reserves but couldn't compensate the country's crude oil and gas exports.⁸²

5. A path beyond neutrality and regulations

There are no straightforward answers on how to consider digital assets: they are perceived either as wild and unregulated asset classes or reliable financial tools.

The cryptocurrency sector has evolved in a few years, starting from a fringe technology until turning into a mainstream industry, carried out by companies backed with hundreds of millions of dollars of investment. This fast-paced market has grown around the idea of spreading borderless and neutral assets, not bound by centralized control but managed by a decentralized network, characterized by unprecedented equality among its users.

Nevertheless, amid the humanitarian crisis caused by the Russian invasion of Ukraine, the growing pressure and need for control by state actors on the cryptocurrency sector could affect the fair-minded approach that has been the hallmark of digital asset markets.

Hence, if borderless assets become subject to restrictions, how much of their anti-authority streak would still appear as a reality and not only as a marketing slogan?⁸³

The global noise of the Ukrainian tragedy has already turned a spotlight on crypto giants, that could be expanded to the whole cryptocurrency field. This sudden attention on digital assets, which seems to be the prerequisite for stricter regulation of cryptocurrencies, may follow two divergent paths.

In the worst-case scenario, it could bring to applying traditional securities market regulation to crypto. This approach, based on measures applied without understanding the technology behind cryptocurrencies, would provide an immediate sense of control over cryptocurrency businesses but turn counterproductive in the long-term, both at the security and economic level, by lowering investments, the number of users, and privacy.⁸⁴

For instance, by simplifying issues related to the cryptocurrency sector, just mirroring measures applied to banks and other financial institutions, imposing to cryptocurrency businesses to submit reports, keep records, and verify

⁸² Suleymanova R. (March 1, 2022) *Crypto will not save Russia from sanctions, experts say*. AlJazeera. <https://www.aljazeera.com/economy/2022/3/1/crypto-will-not-save-russia-from>

⁸³ Ingram D., Goggin B. (March 6, 2022) *How the Ukraine conflict became a turning point for cryptocurrency*. NBC. <https://www.nbcnews.com/news/amp/rcna18705>

⁸⁴ Barone D.M. (May 2021) *EU economic losses in the haze of jihad*. Sicurezza Terrorismo e Società. <https://www.sicurezzaeterrorismo.it/wp-content/uploads/2021/05/SicTerSoc13-EU-economic-losses-in-the-haze-of-jihad-Daniele-Maria-Barone.pdf>

the identity of customers without considering monitoring methods available thanks to the blockchain. Indeed, transactions are automatically logged on public blockchains, allowing law enforcement to view transactions, making currency transaction reports redundant and useless in this field.⁸⁵

Furthermore, as happened during the first few weeks after the Russian invasion of Ukraine, concentrate only on crypto giants, which are already adopting functional compliance programs, including AML/KYC measures, would be counterproductive, missing the focus on exchange platforms operating in high-risk jurisdictions or mixing services, which are the shadiest part in the crypto business.

Otherwise, hopefully, this renewed attention on crypto could more and more legitimize cryptocurrencies as financial assets, providing proportional measures that would help burst the bubble grown around their criminal exploitation. A renewed environment, aimed at concentrating international efforts, either from the private or the public sector, towards harmonized global regulation is vital for the crypto sector to be widely accepted.

A giant step in the evolution of digital assets, which could affect the appeal related to neutrality and anti-authoritarianism, but would encourage positive aspects that digital assets bring to the financial sector as, to mention a few, lower fees, fast transactions, borderless nature, and a decentralized network of users built around equality and trust.

References

- Barone D.M. (May 2021) *EU economic losses in the haze of jihad*. Sicurezza Terrorismo e Società. <https://www.sicurezzaerrorismosocieta.it/wp-content/uploads/2021/05/SicTerSoc13-EU-economic-losses-in-the-haze-of-jihad-Daniele-Maria-Barone.pdf>
- BBC (March 1, 2022) *Ukraine to sell 'war bonds' to fund armed forces* <https://www.bbc.com/news/business-60566776>
- BBC (March 4, 2022) *Ukraine conflict: Government to sell NFTs to fund war against Russia*. <https://www.bbc.com/news/business-60613613#:~:text=Ukraine's%20government%20has%20said%20it,the%20sale%20of%20war%20bonds>
- Black Sea Trade & Development Bank (2021) *Overview of the financial sector in Russia*. https://www.bstbd.org/Overview_of_the_fin_sector_RUSSIA.pdf
- Caldwell L.A. (March 8, 2022) *Warren crafts bill targeting cryptocurrency in Russia sanctions*. Nbc News. <https://www.nbcnews.com/politics/congress/warren-crafts-bill-targeting-cryptocurrency-russia-sanctions-rcna19094>

⁸⁵ Chainalysis (January 7, 2021) *Chainalysis' Formal Response to Treasury's Proposed Rules Regarding Unhosted Cryptocurrency Wallets*. <https://blog.chainalysis.com/reports/chainalysis-response-to-treasury-proposed-rules-unhosted-cryptocurrency-wallets>

- Cambridge Bitcoin Electricity Consumption Index (August 2021) https://ccaf.io/cbeci/mining_map
- Chainalysis (January 13, 2022) *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*. <https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/>
- Chainalysis (January 7, 2021) *Chainalysis' Formal Response to Treasury's Proposed Rules Regarding Unhosted Cryptocurrency Wallets*. <https://blog.chainalysis.com/reports/chainalysis-response-to-treasury-proposed-rules-unhosted-cryptocurrency-wallets>
- Chainalysis (October 14, 2021) *The 2021 Global Crypto Adoption Index: Worldwide Adoption Jumps Over 880% With P2P Platforms Driving Cryptocurrency Usage in Emerging Markets*. <https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/>
- Chaturvedi A. (March 3, 2022) NFTs, cryptocurrencies and now DAO join Ukraine's crowdfunding appeal. Business today. <https://www.businesstoday.in/crypto/story/nfts-cryptocurrencies-and-now-dao-join-ukraines-crowdfunding-appeal-324580-2022-03-03>
- DeepNFTvalue (Updated: March 5, 2022) *Cryptopunks #5364 – Price Details* <https://deepnftvalue.com/punks/5364/>
- Dewan A. (February 25, 2022) *Ukraine and Russia's militaries are David and Goliath. Here's how they compare*. CNN <https://edition.cnn.com/2022/02/25/europe/russia-ukraine-military-comparison-intl/index.html>
- Dmitry Smilyanets official Twitter profile (February 25, 2022) <https://twitter.com/ddd1ms/status/1497247507474272257>
- Duthois T. (March 4, 2022) *Ukraine war: Which countries are sending weapons and aid to forces fighting the Russian invasion?* EuroNews <https://www.euronews.com/next/2022/03/04/ukraine-war-these-countries-are-sending-weapons-and-aid-to-forces-fighting-the-russian-inv>
- Elliptic (May 27, 2022) *Sanctions Compliance in Cryptocurrencies*. <https://www.elliptic.co/resources/elliptic-guide-to-sanctions-compliance-in-cryptocurrencies>
- Elliptic (February 08, 2022) *Ukrainians Turn to Bitcoin to Crowdfund the Fight Against Russia*. <https://www.elliptic.co/blog/ukrainians-turn-to-bitcoin-to-crowdfund-the-fight-against-russia>
- Elliptic (February 28, 2022) *What the Russia Sanctions Mean for Crypto Compliance*. https://www.elliptic.co/blog/what-the-russia-sanctions-mean-for-crypto-compliance?utm_content=199360335&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267
- Elliptic (March 21, 2022) *Crypto Regulatory Affairs: Ukrainian President Signs Virtual Currency Bill into Law*. https://www.elliptic.co/blog/crypto-regulatory-affairs-ukrainian-president-signs-virtual-currency-bill-into-law?utm_campaign=Elliptic%20Essentials%20%7C%20Crypto%20Regulatory%20Affairs&utm_content=201736280&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267

- Elliptic (May 21, 2022) *How Iran Uses Bitcoin Mining to Evade Sanctions and “Export” Millions of Barrels of Oil*. <https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions>
- Elliptic *Live Updates: Ukraine Government Turns to Crypto to Crowdfund Millions of Dollars*. <https://www.elliptic.co/blog/live-updates-millions-in-crypto-crowdfunded-for-the-ukrainian-military>
- Financial Tribune (January 18, 2022) *Cryptomining Suspended for 2 Weeks to Save Power*. <https://financialtribune.com/articles/business-and-markets/107075/cryptomining-suspended-for-2-weeks-to-save-power>
- Fonda D. (March 18, 2022) *The Russia-Ukraine War Is Bringing Out the Good, Bad, and Ugly of Cryptocurrencies*. Barron's. https://www.barrons.com/articles/russia-ukraine-war-cryptocurrencies-51647548970?utm_content=201576331&utm_medium=social&utm_source=linkedin&hss_channel=lcp-5027267
- Grewal P. (March 7, 2022) *Using Crypto Tech to Promote Sanctions Compliance*. Coinbase blog. <https://blog.coinbase.com/using-crypto-tech-to-promote-sanctions-compliance-8a17b1dabd68>
- Hake M.R. (March 4, 2022) *Dogecoin Among Major Crypto Donations to Ukraine but Watch Out for Scams!* Nasdaq. <https://www.nasdaq.com/articles/dogecoin-among-major-crypto-donations-to-ukraine-but-watch-out-for-scams>
- Hinnant L. (February 23, 2022) *Ukraine's economy is another victim of Russia's 'hybrid war'*. Associated press. <https://apnews.com/article/russia-ukraine-entertainment-business-economy-kyiv-6c93f4964cd9d26438dfd4e9c38fe76c>
- Hopkins V. (February 18, 2022) *How Putin Has Already Weakened Ukraine's Economy*. The New York Times. <https://www.nytimes.com/2022/02/18/world/europe/ukraine-economy-putin.html>
- Ingram D., Goggin B. (March 6, 2022) *How the Ukraine conflict became a turning point for cryptocurrency*. NBC. <https://www.nbcnews.com/news/amp/rcna18705>
- Isidore C. (March 3, 2022) *Why many businesses are getting tougher on Russia than sanctions require*. CNN Business. <https://edition.cnn.com/2022/03/03/business/business-go-beyond-russian-sanctions/index.html>
- Jialiang D.P. (March 3, 2022) *Energy-Rich Russia May Turn to Bitcoin Mining to Dent Sanctions*. Bloomberg. <https://www.bloomberg.com/news/articles/2022-03-03/energy-rich-russia-may-turn-to-bitcoin-mining-to-dent-sanctions>
- Jones H. (March 21, 2022) *Global regulators monitor crypto use in Ukraine war*. Reuters. <https://www.reuters.com/technology/global-regulators-monitor-crypto-use-ukraine-war-2022-03-21/>
- Kharpal A. (February 28, 2022) *World's biggest crypto exchange Binance says it will not block all Russian accounts despite Ukraine request*. CNBC. <https://www.cnbc.com/2022/02/28/binance-will-not-block-russian-accounts-after-ukraine-request.html>
- Konig O., Ericsson F. (March 3, 2022) *New EU sanctions cut-off certain Russian banks from SWIFT and prohibit certain investments in Russia*. Sanctions News – A blog by Baker McKenzie. <https://sanctionsnews.bakermckenzie.com/new-eu-sanctions-cut-off-certain-russian-banks-from-swift-and-prohibit-certain-investments-in-russia/>

- Levin J. (March 2, 2022) *Crypto Isn't the Sanctions Haven Its Jump Suggests*. The Washington Post. https://www.washingtonpost.com/business/crypto-isnt-the-sanctions-haven-its-jump-suggests/2022/03/01/6ee3fb7a-9987-11ec-9987-9dceee62a3f6_story.html
- Lopatto E. (February 26, 2022) *HOW UKRAINIANS ARE FUNDRAISING IN CRYPTOCURRENCY*. The Verge. <https://www.theverge.com/2022/2/26/22952357/ukraine-bitcoin-ethereum-donation-vitalik-buterin>
- Milmo D. (March 1, 2022) *Could Putin be exploring cryptocurrencies to bypass western sanctions?* The Guardian. <https://www.theguardian.com/business/2022/mar/01/could-putin-be-exploring-cryptocurrencies-to-bypass-western-sanctions-russia-ukraine-invasion>
- Mine RHY YouTube channel (June 10, 2022) *RHY大型矿场 (RHY large mine Bitcoin Mining) One of the world's largest mines*. <https://www.youtube.com/watch?v=9ofEZftDFyM>
- Mint (March 6, 2022) *Ukraine spends \$15 million cryptos on military gear as crypto donations pour in as humanitarian aid*. <https://www.livemint.com/market/crypto-currency/ukraine-spends-15-million-cryptos-on-military-gear-as-crypto-donations-pour-in-as-humanitarian-aid-11646547788590.html>
- Nicolle E. (March 3, 2022) *Ukraine's Crypto Army Is Both Inspiration and Cautionary Tale*. Bloomberg. <https://www.bloomberg.com/news/articles/2022-03-03/ukraine-s-crypto-army-is-both-inspiration-and-cautionary-tale?sref=0N1JmzAH>
- Nishant N. (March 4, 2022) *Coinbase, Binance resist calls to kick Russians off crypto platforms*. Reuters. <https://www.reuters.com/technology/coinbase-not-banning-russians-using-platform-ceo-says-2022-03-04/>
- Nove J. (February 24, 2022) *Patreon suspends donation page for nonprofit giving body armor to Ukrainian army*. CNBC. <https://www.cnbc.com/2022/02/24/patreon-suspends-come-back-alive-page-for-ukrainian-army-donations.html>
- O'Brien F., Krasnolutska D., and Rocha P.A. (march 1, 2022) *Ukraine Raises Equivalent of \$277 Million From Sale of War Bonds*. Yahoo finance. [https://finance.yahoo.com/news/ukraine-raises-equivalent-277-million-154154581.html#:~:text=Ukraine%20Raises%20Equivalent%20of%20%24277%20Million%20From%20Sale%20of%20War%20Bonds,-Fergal%20O'Brien&text=\(Bloomberg\)%20%2D%2D%20Ukraine%20raised%208.1,its%20fight%20against%20Russia's%20invasion](https://finance.yahoo.com/news/ukraine-raises-equivalent-277-million-154154581.html#:~:text=Ukraine%20Raises%20Equivalent%20of%20%24277%20Million%20From%20Sale%20of%20War%20Bonds,-Fergal%20O'Brien&text=(Bloomberg)%20%2D%2D%20Ukraine%20raised%208.1,its%20fight%20against%20Russia's%20invasion)
- The official Twitter account of the Ministry of Finance of Ukraine (February 28, 2022) https://twitter.com/ua_minfin/status/1498319440622104583
- The official Twitter account of Ukraine (March 2, 2022) <https://twitter.com/Ukraine/status/1498911922791583746?s=20&t=j4KQx4IIdj3rJgAGCxdHZA>
- Patreon (February 25, 2022) *In merito alla rimozione di Come Back Alive*. <https://blog.patreon.com/it-IT/in-merito-alla-rimozione-di-come-back-alive>
- Raine J. (February 25, 2022) *Ukraine and the importance of resistance*. International Institute for Strategic Studies (IISS). <https://www.iiss.org/blogs/analysis/2022/02/ukraine-and-the-importance-of-resistance>

- Riley C. (March 3, 2022) *How Russia's invasion of Ukraine changed the global economy in a week*. CNN Business. <https://edition.cnn.com/2022/03/03/economy/russia-invasion-global-economy/index.html>
- Russian News Agency (January 26, 2022) *Russia has competitive advantages in cryptocurrency mining – Putin*. https://tass.com/economy/1393535?utm_source=theguardian.com&utm_medium=referral&utm_campaign=theguardian.com&utm_referrer=theguardian.com
- Sharma a. (March 1, 2022) *'Help Ukraine' crypto scams emerge as Ukraine raises over \$37 million*. Bleeping computer. <https://www.bleepingcomputer.com/news/security/help-ukraine-crypto-scams-emerge-as-ukraine-raises-over-37-million/>
- Smith-Meyer B. (March 4, 2022) *Why crypto isn't Russia's safest haven*. Politico. <https://www.politico.eu/article/crypto-russia-safest-haven-why/>
- State sites of Ukraine – government portal Official website (March 1, 2022) *Finance Ministry: Ukraine issues military bond*. <https://www.kmu.gov.ua/en/news/minfin-1-bereznya-rozpochinayetsya-aukcion-z-prodazhu-vijskovih-obligacij>
- Stentella G. (March 3, 2022) *L'Ucraina annuncia un airdrop di criptovalute, ecco tutti i dettagli*. Money.it. <https://www.money.it/Ucraina-airdrop-criptovalute-dettagli>
- Suleymanova R. (March 1, 2022) *Crypto will not save Russia from sanctions, experts say*. Aljazeera. <https://www.aljazeera.com/economy/2022/3/1/crypto-will-not-save-russia-from>
- Sun M. (March 7, 2022) *U.S. Warns Banks, Crypto Firms Against Potential Efforts to Evade Russian Sanctions*. The Wall Street journal. <https://www.wsj.com/articles/u-s-warns-banks-crypto-firms-against-potential-efforts-to-evade-russian-sanctions-11646696802>
- The official Twitter account of Ukrainian government (February 26, 2022) <https://twitter.com/Ukraine/status/1497594592438497282>.
- The official Twitter account of the Ministry of Finance of Ukraine (February 28, 2022) https://twitter.com/ua_minfin/status/1498319440622104583
- The official Twitter account of Ukraine (March 2, 2022) <https://twitter.com/Ukraine/status/1498911922791583746?s=20&t=j4KQx4IIdj3rJgAGCxdHZA>
- The official Twitter account of Ukrainian government (March 01, 2022) <https://twitter.com/Ukraine/status/1498547710697345027>
- The United States Senate Committee on banking, housing, and urban affairs (March 17, 2022) *Understanding the Role of Digital Assets in Illicit Finance*. <https://www.banking.senate.gov/hearings/understanding-the-role-of-digital-assets-in-illicit-finance>
- Thomas T. (March 5, 2022) *Ukraine fundraiser hits £85m as charities say money needed more than goods*. The Guardian. <https://www.theguardian.com/society/2022/mar/05/ukraine-fundraiser-hits-85m-as-charities-say-money-needed-more-than-goods>
- Thompson S.A., Alba D. (March 3, 2022) *Fact and Mythmaking Blend in Ukraine's Information War*. The New York Times. <https://www.nytimes.com/2022/03/03/technology/ukraine-war-misinfo.html>

- Trivedi V. (March 3, 2022) *This is How Ukraine's 'Peaceful World' Airdrop was Exposed by Analysts*. Yahoo finance. <https://finance.yahoo.com/news/ukraine-peaceful-world-airdrop-exposed-144355689.html>
- US Department of Justice – Office of Public affairs (March 2, 2022) *Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture – Task Force Will Surge Federal Law Enforcement Resources to Hold Accountable Corrupt Russian Oligarchs*. <https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture>
- Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine official Twitter account (February 26, 2022) <https://twitter.com/FedorovMykhailo/status/1497549813205848068>
- Volpicelli G.M. (March 8, 2022) *War Is Calling Crypto's 'Neutrality' Into Question*. Wired. <https://www.wired.com/story/crypto-russia-ukraine-sanctions/>
- Wang T., Malwa S. (March 3, 2022) *'Peaceful World' Token Spoofs Traders Ahead of Now-Canceled Ukraine Airdrop*. CoinDesk. <https://www.coindesk.com/markets/2022/03/03/peaceful-world-token-may-be-spoofing-ukraines-airdrop/>
- Weizhen T., Wang C. (March 2, 2022) *Ukraine raises \$270 million from sale of war bonds to fund army as Russia's invasion continues*. CNBC. <https://www.cnbccom/2022/03/02/ukraine-raises-270-million-from-sale-of-war-bonds-to-fund-army.html>
- Wilson T. (February 28, 2022) *Ukraine raises \$13 million in crypto after crowdfunding appeal*. Reuters. <https://www.reuters.com/world/china/ukraines-government-raises-crypto-worth-8-million-crowdfunding-appeal-2022-02-27/>
- Wood G.R. (February 26, 2022) *What Role for Crowdfunding Defense in Ukraine?* Small wars journal. <https://smallwarsjournal.com/jml/art/what-role-crowdfunding-defense-ukraine>
- Zeitchik S., Newmyer T. (February 25, 2022) *In the world's first crypto war, uncertainty about who will benefit*. The Washington Post. <https://www.washingtonpost.com/technology/2022/02/25/cryptocurrency-ukraine-russia-war-impact/>
- Zorthian J. (March 2, 2022) *Here's What the New, Tightened SWIFT Sanctions on Russian Banks Actually Do*. Time. <https://time.com/6153951/swift-sanctions-russia/>
- Повернись живим Facebook <https://www.facebook.com/backandalive/posts/2232521093571982>

Azov Battalion: Extreme Right-Wing Militarization and Hybrid Warfare

FEDERICO BORGONOVO

Federico Borgonovo is analyst and researcher at the Italian Team for Security Terroristic issues and Managing Emergencies – ITSTIME. He has a BA in Political Sciences for International Relations at Università Cattolica del Sacro Cuore (UCSC) and MA in Security Policies (PoliSi) earned as well at UCSC in Milan, with a final thesis on “Digital Ethnography on Telegram as a Counter-Terrorism Tool”. He specialized in digital ethnography, social media intelligence and social network analysis. He focused on monitoring terrorist propaganda and modelling recruitment tactics on digital environment, with particular attention on new communication technologies implemented by terrorist organizations. His research activities are oriented in particular on Islamic terrorism and right-wing extremism.

Abstract

This article analyzes the origins and features of the Azov Battalion. A hybrid weapon, which fight inside a multivariate hybrid conflict composed by a combination of urban warfare, propaganda, and politics. The Azov Battalion represent one of the clearest examples of the increasing complexity of warfare. Complexity and hybridization are due to the growing number and diversity of actors involved. The Russo-Ukrainian conflicts no longer remain local; instead, from 2014 to 2022 has increasingly attracted external actors, as right-wing extremists and extend to the Internet. This analysis, try to explain how Azov Battalion became such an effective weapon and what could be its outcome after the war. This aim was achieved by reconstructing the fundamental historical steps and then theorising the so-called Azov system. The latter is a model that synthesises Azov’s hybrid capabilities acquired through its diversification and attempts to illustrate the high degree of complexity of military systems fighting in hybrid contexts.

Keywords

Azov, Hybrid, Ideology, Ukraine, Army, War, Extremist

1. The Unit's hybrid origin

The military unit known as Azov Battalion has its roots in the Russo-Ukrainian conflict, even before it turned into open warfare. Already from its foundation, the Azov Battalion highlights a new dimension of armed mobilisation, with two distinct drivers contributing to its creation. The first driver is of an ideological nature, it is the sub-culture of the Ukrainian extreme right (also

distinguished by different sub-drivers) with anti-Russian ideology. The second is of a strategic nature and consists of the practice adopted by the Ukrainian Ministry of Defence since 2014 of organising its territorial defence through volunteer units, to fill the gaps in the regular army.¹ Both factors must then be considered within a hybrid warfare context that acts as an accelerator.

The ideological-cultural driver is the factor that contributed to the creation of a common cultural substratum on which the “**Azov subculture**” was formed. The initial cultural substratum, according to grey literature sources, seems to come from the convergence of two different extremist environments:² the ultras corner of the **Football Club Metalist Kharkiv** known as **Sect 82**, and members of the three ultranationalist parties **Patriot of Ukraine**, **Social National Assembly and Right Sector**.³ The latter is the most important component as it will transmit, to what will be a fighting unit, its future leadership as well as much of the ideological and symbolic imprinting. The element that links the two components was the presence of members of both macro-groups at the **Euromaidan** protests in 2014. Although even before the anti-Russian protests the two communities were united by a strong nationalist spirit, the guerrilla experience laid the foundations for further convergence.⁴ The neo-Nazi and supremacist component well rooted in the three mentioned parties merged with the esprit de corps and camaraderie of the *ultras* community.

The institutional driver, on the other hand, was found by analysing the operational shortcomings of the Ukrainian army and the government’s response to them. In March 2014, the first battalions of volunteers began to be formed to support the regular Ukrainian Army. On 13 April 2014, Interior Minister **Arsen Avakov** issued a decree authorising the creation of new paramilitary forces of up to 12,000 people, after which **Andriy Yevhenovych Biletsky** officially founded the Azov Battalion on 5 May. Returning to the April 2014 decree, we observe that the rationale behind this law is of fundamental importance. Indeed, at the beginning of the armed conflict in the Donbass, the Ukrainian army was suffering from several problems including demoralisation, lack of professionalism, corruption, lack of logistical support and endemic mutiny. The combination of these factors led the Ukrainian government, in particular

¹ Tetyana Malyarenko e David J. Galbreath, «Paramilitary Motivation in Ukraine: Beyond Integration and Abolition», *Southeast European and Black Sea Studies* 16, n. 1 (2 gennaio 2016): 113-138, <https://doi.org/10.1080/14683857.2016.1148414>.

² Stanford University, Stanford, e California 94305, «MMP: Azov Battalion», consultato 13 aprile 2022, <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/azov-battalion>.

³ Alexander Clapp, «The Maidan Irregulars», 2022, 9.

⁴ Rosaria Puglisi, «Heroes or Villains? Volunteer Battalions in Post-Maidan Ukraine», 2015, 20.

the Ministries of Defence and Interior, to increasingly rely on paramilitary units to conduct operations against Russian-backed rebels.

In the spring, Azov shifted its focus to eastern Ukraine, where pro-Russian protesters were beginning to seize government buildings and police stations. In May, when the pro-Russian protests turned into a full-scale Russian-backed insurgency, Azov was granted official status as a volunteer battalion and on May 6 took delivery of its first shipment of weapons. It also began to acquire foreign instructors: former soldiers from Sweden, France, Slovakia and Italy with experience in conflict zones. Azov's main target was Mariupol, a large industrial port on the Azov Sea that came under separatist control in May. On June 13, Azov stormed the rebel barricades and took control of the city centre after a six-hour battle.⁵ Since then, its main role has been to protect Mariupol and patrol the Azov coast, helping to counter arms smuggling from Russia. Between August and September 2014, the battalion takes part in the defence of Mariupol victoriously opposing the militia of the separatist forces in Donetsk. In September, Azov is formally integrated into the Ukrainian Armed Forces of the National Guard and acquires the status of a regiment regiment (*Polk Azov*, literally in Ukrainian "Regiment Azov"), increasing its numbers accordingly.⁶ Finally, it participated in several US-led exercises between 2015 and 2017, further implementing its operational capabilities.

2. The Azov System

One of the most important aspects in understanding the hybrid capabilities of the Azov unit is the close connection between symbolism, ideology, and operational activity. Starting from these three elements, we can observe how the strong hybrid connotation of Azov has materialized in a mix of military operations and socio-political activities. These aspects later laid the foundations for a real mythification.

The symbolism of Azov combines various neo-Nazi elements related to the Waffen SS, acquired from the original nucleus of the Patriot of Ukraine, with the classical symbols tied to Ukrainian nationalism.⁷ In particular, the official symbol contains the colours gold and blue, the Ukrainian Trident, the waves representing the Azov Sea, the **Wolfsangel** rune used by the "Das

⁵ Iaroslav Tynchenko, *Ukrains'ki Zbroïni Syly: Berezen' 1917 r.–Lystopad 1918 r. (Orhanizatsiia, Chysel'nist', Boïovi Diï)* (Kyïv: Tempora, 2009).

⁶ Teemu Saressalo e Aki-Mauri Huhtinen, «The Information Blitzkrieg – "Hybrid" Operations Azov Style», *The Journal of Slavic Military Studies* 31, n. 4 (2 ottobre 2018): 423-443, <https://doi.org/10.1080/13518046.2018.1521358>.

⁷ Saressalo e Huhtinen.

Reich” Waffen SS Panzer Division and finally the **Black Sun**, an icon found on the floor of Wewelsburg Castle, the ideological and spiritual centre of the SS since 1934. We note how the ideological spectrum depicted in the Azov Battalion symbol is specific but, at the same time, broad enough to reach different communicative targets. In this spectrum we find: Ukrainian nationalists, anti-Russians, neo-Nazis, neo-fascists, white supremacists, and accelerationists. In short, it is a military unit ideologically aligned with the violent extreme right that serves the Ukrainian government in the ranks of the National Guard but only formally. It is emphasised that the Ukrainian extreme right differs from most European extreme right in the fact that it is not universally hostile to the European Union and the United States. Azov’s operational history in fact confirms its close ties with US trainer partners. The extremist and veiled anti-democratic ideology, in fact, did not remain dormant for long among speeches of Azov’s founding members. In 2016 it took on greater political substance when an initial group of veterans returning from the 2015 Mariupol battles, including Andriy Biletsky himself, founded the National Corps party, initially known as Patriots of Ukraine (not to be confused with Patriot of Ukraine).⁸ The ideological core of the party revolves around neo-fascism, anti-Russian nationalism, economic nationalism, and militarism. A combination strongly reminiscent of Hitler’s National Socialism.

The indissoluble link between Azov and its political counterpart has given rise to a two-tier political-military entity capable of conducting a variety of secondary activities. We can therefore define an Azov System as consisting of a military and a political component. Both components have distinct identities and modus operandi but are part of a single system that incorporates the same subculture, the same ideological purpose and to some extent the same leadership. On one hand, the ‘**Military Azov**’ has built an impressive online propaganda apparatus that has further expanded the recruitment pool by tapping into international European far-right circuits. The network of far-right and alt-right actors in Europe, especially in France, Germany, Italy, and Sweden, thanks to music festivals such as **Asgardsrei**⁹ and mixed martial arts tournaments, including **Denis Nikitin’s White Rex**¹⁰ was linked to the recruitment apparatus of the Azov Battalion.

Among the actors in this network, we find Ouest Casual, a French group involved in both concerts and fighting tournaments, which in April 2021 reported photo-reportages of a training camp held in Ukraine by paramilitary

⁸ Clapp, «The Maidan Irregulars».

⁹ «At Ukraine’s Asgardsrei, A French Connection», *bellingcat*, 1 maggio 2020, <https://www.bellingcat.com/news/2020/05/01/at-ukraines-asgardsrei-a-french-connection/>.

¹⁰ «At Ukraine’s Asgardsrei, A French Connection».

militias close to Azov, including the **Freikorps of Ukraine**. What this informal network of supporters reveals is a **spontaneous system of European far-right militarisation**. In other words, a soft propaganda and training operation that opened the doors of Azov to the world of the European extreme right and to all those supporters willing to fight against Russia by virtue of ethnonationalist ideology. The functioning of the network was observed in the days immediately following the Russian invasion in February 2022. Following the Russian attack, the actors organised themselves as a **spontaneous infrastructure to support operations in Ukraine**. The network of groups and organisations, being already well structured, became active in a short time and immediately provided support for the recruitment, propaganda, and financing of Azov. Finally, regarding the socio-cultural sphere, despite it pertained more to the political section/side, the Military Azov as well penetrated the Ukrainian social fabric mainly through its civil/paramilitary section, the **Azov Civil Corps**¹¹ the civil/paramilitary section of Azov. This section dealt with training and education also for minors. Obviously, this section interfaced very often with the National Corps.

On the other hand, the **'Political Azov'** supported the political and ideological reasons for the anti-Russian struggle, but over time strategically distanced itself from the supremacist and neo-Nazi connotations typical of the military Azov. This was because the extremist's name was making it increasingly difficult to maintain good relations with the EU and the US. Given the fact that these alliances guaranteed the supply of funds, training, and armaments, it was vital to preserve them. The party therefore contributed to the reputation-cleansing of Azov by securing the necessary international support. National Corps' political activities include the **Intermarium project**.¹² The term originated from the idea of a security and military alliance based on the Polish-Lithuanian Commonwealth. National Corps members expanded this concept by proposing a politico-military alliance of Central and Eastern European countries located between the Black, Baltic and Adriatic Seas that would protect common foreign policy interests. The ideology underlying the Intermarium concept invokes a strong anti-Russian and alternative European spirit to the alliance with the US and EU. At the moment it is not yet at an early stage but could in the future be a force of attraction toward Ukraine and Azov.

¹¹ Saressalo e Huhtinen, «The Information Blitzkrieg — “Hybrid” Operations Azov Style».

¹² «Intermarium», Intermarium, consultato 13 aprile 2022, <https://intermarium.org.ua/en/>.

Figure 1 - *From left to right: Azov Badge, National Corps logo and Intermarium symbol*



3. Conclusions

As stated above Azov's ideology, symbolism and history have contributed to the creation of a myth. Prior to the Russo-Ukrainian War, the Azov Special Operations Regiment was certainly known for its radicalisation and anti-Russian activism but had not yet fought an open war. With the outbreak of hostilities in February 2022 and especially with the stoic defence of the city of Mariupol Azov reached a new evolutionary stage, ultimately the last one a military unit can achieve: mythologisation. The Azov special regiment is fighting in the city of Mariupol, in all probability a large part of the unit will perish in its defence, and this will contribute to a further martyrdom of the fighters. The unit's official Telegram channel itself has been renamed А3ОВ – Мариуполь, literally Azov – Mariupol. Although **mythologisation** and **martyrdom** may seem unnecessary in the short term from a military point of view, they could have serious repercussions in the long run. It is likely that Azov's wartime exploits will be imprinted in the collective imagination to such an extent that they will serve to offset the war crimes allegations made earlier and partly clear the reputation. At the same time, Azov could become a model of inspiration and emulation for other Ukrainian militias or even for other paramilitary groups in other countries. The ideological factors that have attracted far-right militiamen from all over Europe will now receive an additional emotional boost by gaining communicative power and attractiveness. Related to this is the issue of foreign fighters. It is indeed possible that the violent far right will try to use the conflict with Russia to obtain weapons and training, as well as to connect with other extremists. The members of this strand are anti-liberal, accelerationist, radical

ethnonationalists who favour the fight against the invader, be it military like Russia or migratory. They have renounced the political process as a means of influencing political change. The ideology of these extremists is centred on the claim that only through a bloody revolt can they save ‘Western civilisation’, understood through a racist and religious paradigm. The dangerousness of such ideologies is evident when one observes the almost perfect overlap with the ideological model proposed within the work “The Great Replacement” compiled by **Brenton Tarrant** and published after the attack in Christchurch in March 2019. The attack and the bomber underwent a process of mythologisation (in this specific case, the far right itself defines him as a **Saint**, consequently we talk about **Sanctification**) which led to a massive diffusion of his ideas and thought within the far-right digital ecosystem. Therefore, if the same paradigm is applied to the Azov Battalion, also because the ideological compartment is very similar to that of Brenton Tarrant, it is possible to hypothesize an impact on the extreme right-wing ecosystem (online and offline) even more pervasive and with probable effects on the terrorist-extremist threat.

Bibliography

- bellingcat. «At Ukraine’s Asgardsrei, A French Connection», 1 maggio 2020. <https://www.bellingcat.com/news/2020/05/01/at-ukraines-asgardsrei-a-french-connection/>.
- Clapp, Alexander. «The Maidan Irregulars», 2022, 9.
- Graham Macklin. «The Christchurch Attacks: Livestream Terror in the Viral Video Age», s.d., 57.
- Intermarium. «Intermarium». Consultato 13 aprile 2022. <https://intermarium.org.ua/en/>.
- Malyarenko, Tetyana, e David J. Galbreath. «Paramilitary Motivation in Ukraine: Beyond Integration and Abolition». *Southeast European and Black Sea Studies* 16, n. 1 (2 gennaio 2016): 113–38. <https://doi.org/10.1080/14683857.2016.1148414>.
- Puglisi, Rosaria. «Heroes or Villains? Volunteer Battalions in Post-Maidan Ukraine», 2015, 20.
- Saressalo, Teemu, e Aki-Mauri Huhtinen. «The Information Blitzkrieg – “Hybrid” Operations Azov Style». *The Journal of Slavic Military Studies* 31, n. 4 (2 ottobre 2018): 423–43. <https://doi.org/10.1080/13518046.2018.1521358>.
- Tynchenko, Iaroslav. *Ukraïns’ki Zbroïni Syly: Berezen’ 1917 r.–Lystopad 1918 r. (Orh-anizatsiia, Chysel’nist’, Boïovi Diï)*. (Kyïv: Tempora, 2009).
- University, © Stanford, Stanford, e California 94305. «MMP: Azov Battalion». Consultato 13 aprile 2022. <https://cisac.fsi.stanford.edu/mappingmilitants/profiles/azov-battalion>.

The importance of the Cyber battleground in the Russo-Ukrainian war

MARCO ZALIANI

Marco Zaliani is analyst and researcher at the Italian Team for Security Terroristic Issues and Managing Emergencies – ITSTIME. He has a BA in Foreign Languages for Business at Università Cattolica del Sacro Cuore (UCSC) and Master in International Relations at ASERI – Postgraduate School of Economics and International Relations (UCSC), with a final thesis titled: “Information warfare: The new frontier of international hybrid conflicts”. He specialized in Cyber Security analysis, Open Source Intelligence (OSINT) and social network analysis. He focused on monitoring terrorist propaganda and relevant threats regarding national security, with particular attention on Cyber Warfare and threats posed by terrorist and extremist organizations. His research work includes: analysis of threat trends and scenarios regarding in particular on Islamic terrorism, right-wing extremism, Cyber Warfare and national security issues in general.

Abstract

The increasingly hybrid nature of conflicts has become even more evident in the recent re-ignition of the never-dead Russian-Ukraine crisis. The new chapter of this conflict, which arose from the Russian military invasion of Ukrainian territory, was characterized by massive use of hybrid instruments of the conflict that went hand in hand with the military one. In this context, the cyber dimension of the conflict has reaffirmed its central role. As it is now an integral part of these conflicts and no longer ancillary to them. Starting from a study of the implementation of cyber-arsenals used in the Ukrainian context, we want to give a more precise image of this type of weapons which, just like conventional arsenals, are exploited to achieve specific objectives by a variety of actors. In fact, in this conflict, the “cyber-line ups” that have seen state and non-state actors intervening alongside both Russia and Ukraine are also indicative. From these considerations, one can get an idea of the current role of cyber in the context of new hybrid conflicts and specifically outline the scenarios that the Russo-Ukrainian conflict may cause in cyberspace even after hostilities are over.

Keywords

Ukraine, cyber, hybrid warfare

1. Introduction of Cyber warfare in Ukraine

The recent invasion of Ukraine conducted by Russian military forces at the end of February 2022 has sparked new fears of a conflict at Europe's door and cold war-like sentiment. Apart from the obvious military aspect of the invasion, there is one aspect that has gained increasing importance over the years which is Cyber Warfare. Since the beginning of the ongoing Russian military operation in Ukraine, it has played a central role in the conflict, and it was exploited by both sides in many ways. This is not the first time, however, that Ukraine has been at the epicenter of Russian Cyber efforts. Very much like the Baltic states, Ukraine has been over the years a sort of "testing ground" in which Russians could deploy their newest Cyber weapons. This was done both to send a message to the West regarding Russian capabilities and what to expect if a conflict breaks out in Cyber space, and at the same time to project themselves even more towards Ukraine which has a key role in the stability of the region. In 2015 and 2016 Ukrainian power-grids were subject to multiple attacks. The 2015 attack was conducted by the Russian APT (Advanced Persistent Threat) "Sandworm" using the Trojan "BlackEnergy" on energy companies in Ukraine and resulted in power outages that lasted up to six hours. Ukraine was also a major target of the malware epidemic caused by NotPetya, a destructive ransomware that targets Microsoft operating systems and encrypts everything on the hard drive. If infected by NotPetya it is technically impossible to recover the encrypted files even after the payment in BitCoin. The attack was again attributed to the Russian APT Sandworm. These major hacks were all interspersed by various less severe ones like DDoS and defacements targeting the Ukrainian government's websites. Therefore, over the years it has become evident that Cyber Warfare has been used plenty of times in Ukraine as an integral part of the war and this new phase of the conflict with Russia could not be outdone.

2. Cyber Weapons used

Much like a real battlefield, cyberspace has seen different types of weapons being used too. Their characteristics range from pure disinformation and influence to actual compromise and intrusion followed by data leaks. The following is meant to give an outline of this range of severity of the attacks that have been witnessed so far in the conflict.

- Starting from the least severe type of attacks, various **Phishing** campaigns have been recorded. Even though it must be said that Phishing can be, and oftentimes is, just a vector of more serious attacks, in Ukraine various

Phishing campaigns have been launched to force narratives on the population and influence it.

For example, at the end of February, Meta said it has seen a surge in hacking attempts against Ukrainians. It identified some from a threat actor that has been trying to hack the accounts of high-profile Ukrainians, including military officials and public figures. The threat actor typically targets people through phishing emails and then uses that to gain access to their social media accounts and post disinformation as if it is coming from the legitimate account owners. Hence, even if the attacks did not lead to major disruptions, they still tried to influence the Ukrainian population in any way possible, just like the Russian InfoWar tactics predict.

- Moving up the severity scale a different and a lot less subtle way of influence was used from both the Russian and the Ukrainian sides. That is **Defacement** of institutional and commercial websites. Website defacement is a form of “electronic vandalism” with which the visual appearance of a website or a web page is changed and/or modified with satirical or misleading content. The Hactivist group Anonymous has long been a user of such technique and it has used it also in this conflict against Russia. They have hacked into the networks of Russian state television, and they showed the reality of the atrocities that were being committed in Ukraine. This again is an example of how cyberwarfare can be used to influence the public debate also from a defensive side like Anonymous did in defense of Ukraine.¹
- The next cyber weapon used is one of relative ease of use and it has been exploited massively by both sides of the conflict. The weapon in question is a **DDoS** attack or “Distributed Denial of Service”. This kind of attack is conducted through the flooding of a target IP (a website) with thousands of requests. If there are not enough defenses against this kind of attack the requests become too many for the webserver to handle and the website becomes unreachable. This technique has been used extensively both by Russia, targeting institutions, Banks, and other commercial entities² and by Ukraine also through its IT cyber army and its cyberspace allies like Anonymous.³ In the case of Russian DDoSs, even though the scale of the attacks was moderate, and the sites recovered within hours, the clear intention was to create a sense of panic in the population that was not able to gather neither information or money.

¹ <https://fortune.com/2022/03/07/anonymous-claims-hack-of-russian-tvs-showing-putins-ukraine-invasion/>

² <https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/>

³ <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>

- The next tool in the cyber arsenals is more pervasive and bears highly destructive characteristics. During the last months, a very large use of **Wiper**-type Malwares has been detected. Wiper Malwares are a specific kind of Malware that, once it is delivered into the victim's machine, erases user data and partition information from attached drives. At least three different Wiper Malwares have been identified in Ukrainian networks. The researchers named them Isaac Wiper, Hermetic Wiper, and Caddy Wiper.⁴ Most of them required a previously established presence in the target's network, but once inside they proceeded to do the "wipe" of all the data that resulted in major problems for the entities involved. Hermetic Wiper for example has been described by researchers as remarkable for its ability to bypass Windows security features and gain write access to many low-level data-structures on the disk. In addition, the malware was set to fragment files on disk and overwrite them to make any attempt of recovery impossible.⁵
- One special mention regards the use of **Ransomware**. This kind of attack is similar to the previous one on the list, but it is normally used for financial gains since it involves a "ransom". Nevertheless, it was used by hacker groups this time to put political pressure on the enemy, making it the first use of ransomware as a hybrid warfare tool.⁶

3. Cyber line ups

The involvement of Ransomware groups in the Russo-Ukrainian conflict is another hint of the growing hybridization of conflicts. After the beginning of hostilities, several actors have picked sides and started fighting, this time however in cyberspace and not with bullets. The following are the main groups and entities, both state and non-state, that have taken part in the conflict.

Pro Ukraine groups:

- **Anonymous:** The group of hacktivists has been one of the most outspoken defiant of the Russian government. On the 24th of February they officially declared war against Russia via one of their Twitter accounts. Since then, the collective has started hitting Russian state TV networks and other governmental websites like the one of the Ministry of Defense.⁷ The latter has

⁴ <https://securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/>

⁵ <https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/>

⁶ <https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/>

⁷ <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>

not only been put offline, but its database was also compromised and then leaked online by Anonymous. Out of 100 misconfigured databases in Russia, 90 were compromised and leaked by Anonymous.⁸ The group's leaderless nature makes attribution even harder. Russia tried to link the group to some sort of American support, given the fact that most of the 17,000 IP detected and shared by the Russians were US-based.⁹ The group's dispersed nature and the relative user-friendly attacks it employs make it a tough adversary for Russia as it has been for the US when it was targeting American companies.

- **IT Cyber Army of Ukraine:** This is a prime example of the hybrid nature of the current conflict. The newly formed group has been launched by the vice-prime minister of Ukraine Mykhailo Fedorov, to fight against Russian digital intrusions and it was open to any cyber-expert would want to join. It is probably the first case in which a government openly calls for the creation of a cyber-volunteer unit from all over the world to participate in a conflict.¹⁰ In the announcement made by Fedorov, a link for a Telegram channel was also provided to coordinate attacks and to give a list of Russian entities' IP addresses to target. In the channel a series of guides and manuals were also shared, so that anyone could participate and launch DDoS attacks.
- **Belarusian Cyber Partisans:** The Belarus-based group isn't new to politically motivated attacks. It has a long story of hacks that targeted primarily Lukashenko's regime. Given Belarus' historic alliance and vicinity to Russia the group decided, both before and after the beginning of the invasion, to deploy its ransomware against targets inside Belarus.¹¹ Before the invasion the group hacked into the Belarusian Railways computer system in a bid to sabotage the deployment of Russian military units in the country and again hit the same target after the military operations started. The episode was interesting because it was one of the first cases in which ransomwares were used to pursue a political objective and not a financial one.

Pro Russia Groups:

- **Sandworm (Unit 74455):** This APT is among those actors that have intervened alongside Russia. While the Russians have always denied any link

⁸ <https://www.cnn.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results.html>

⁹ <https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/>

¹⁰ <https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/>

¹¹ <https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/>

with the group it is strongly believed that it is in fact a cyber-offensive unit of the Russian GRU, the government agency in charge of Russian Military Intelligence.¹² The group is known for the high sophistication of its hacks and has been involved in many large-scale hacks like the previously cited NotPetya. Sandworm has been reportedly targeting Ukrainian networks with a new malware dubbed by researchers “Cyclops Blink”.¹³

- **Ghostwriter (UNC1151):** This threat actor is another state-sponsored group. It has been linked with high confidence to the Belarusian government and has too been active in the Russo-Ukrainian conflict. Meta has reportedly taken down several accounts on its platforms that are linked to the group.¹⁴ These accounts were being used to target those of Ukrainian officials and military personnel. This was done to compromise them and disseminate false information regarding the conflict as if it was coming from the legitimate Ukrainian profiles.
- **Conti:** The ransomware group has, like Anonymous, officially declared that it was going to take part in the conflict alongside Russia and defend it from any outside attack. Like in the case of the Belarusian Cyber Army a ransomware group has put aside financial gains to pursue politically driven objectives. The support to Russia though backfired when a pro-Ukraine member of the group has started to leak various internal data through a twitter profile whose handle is @ContiLeaks. The leaks included the logs for the internal group chat, the entirety of Conti ransomware group’s victims’ data and even the source code of its ransomware and its decryptor. The group is one of the most successful “ransomware gangs”, and, since in the leaks were also the bitcoin wallets used to collect ransoms, it has been calculated that between 2017 and 2022 it has netted around two and a half billion dollars in BitCoin from ransom payments.

4. Consequences of Cyber Warfare in Ukraine and future scenarios

The hybridization of conflicts has become more and more evident in the recent clash between Russia and Ukraine. The weapons used, the actors involved and the dynamics that were created thanks to one or the other projected the west in a new phase of modern confrontations between states. A

¹² <https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast>

¹³ <https://www.siliconrepublic.com/enterprise/ukraine-cyberattacks-ddos-hermetic-cyclops-russia-invasion>

¹⁴ <https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers/>

phase in which, even when military clashes are over, the conflict inevitably continues in cyber-space in the form of espionage, influence, and sabotage. This (most of the times) low-intensity war in cyber-space can bring devastating consequences if states are not ready to face it. Even if, also in Ukraine, cyber-attacks have not been as devastating as they could have been, it is important that states deploy the necessary measures to respond to both direct (when networks are directly targeted) and indirect (when damages are the consequences of attacks aimed at other targets) cyber-attacks. To this sense, the hybridization of conflicts, calls to the re-definitions of potential targets. When cyber-warfare is utilized, the military and civilian targets are oftentimes blurred as important but not military targets like corporations or hospitals arise.¹⁵ The increased connectivity of the world makes the “attack surface” larger and the so called “critical infrastructures” are on the frontline. Given the fact that it is almost impossible to avoid being cyber-attacked, it is important to do everything possible to minimize potential damage if the attacker does get in.

Regarding the Russo-Ukrainian theater, it is probable that when military confrontations end, Russia will resort to the Cyber-Space to retaliate against the West for its involvement in the conflict. Before that happens, the west must be prepared to defend itself with efficacy.

Bibliography

- Carmela Chirinos, “*Anonymous claims it hacked into Russian TVs and showed the true devastation of Putin’s Ukraine invasion*”, March 7, 2022, Retrieved from: <https://fortune.com/2022/03/07/anonymous-claims-hack-of-russian-tvs-showing-putins-ukraine-invasion/>
- Steve Holland and James Pearson, “*US, UK: Russia responsible for cyberattack against Ukrainian banks*”, February 18, 2022, Retrieved from: <https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/>
- Dan Milmo, “*Anonymous: the hacker collective that has declared cyberwar on Russia*”, February 27, 2022, Retrieved from: <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>
- Cristopher Del Fierro and John Dwyer, “*CaddyWiper: Third Wiper Malware Targeting Ukrainian Organizations*”, March 15, 2022, Retrieved from: <https://securityintelligence.com/posts/caddywiper-malware-targeting-ukrainian-organizations/>
- Hasherezade, Ankur Saini and Roberto Santos, “*HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine*”, March 4, 2022, Retrieved from:

¹⁵ <https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare>

- <https://blog.malwarebytes.com/threat-intelligence/2022/03/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/>
- Peter Dickinson, “*Cyber partisans target Russian army in Belarus amid Ukraine war fears*”, January 26, 2022, Retrieved from: <https://www.atlanticcouncil.org/blogs/belarusalert/cyber-partisans-target-russian-army-in-belarus-amid-ukraine-war-fears/>
- Monica Buchanan Pitrelli, “*Anonymous declared a ‘cyber war’ against Russia. Here are the results*”, March 16, 2022, Retrieved from: <https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results.html>
- Sergiu Gatlan, “*Russia shares list of 17,000 IPs allegedly DDoSing Russian orgs*”, March 5, 2022, Retrieved from: <https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/>
- James Pearson, “*Ukraine launches ‘IT army,’ takes aim at Russian cyberspace*”, February 27, 2022, Retrieved from: <https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/>
- Andrew Marino, “*Sandworm details the group behind the worst cyberattacks in history*”, July 28, 2020, Retrieved from: <https://www.theverge.com/21344961/andy-greenberg-interview-book-sandworm-cyber-war-wired-vergecast>
- Vish Gain, “*Ukraine cyberattacks: What you need to know*”, February 24, 2022, Retrieved from: <https://www.siliconrepublic.com/enterprise/ukraine-cyberattacks-ddos-hermetic-cyclops-russia-invasion>
- Sergiu Gatlan, “*Meta: Ukrainian officials, military targeted by Ghostwriter hackers*”, February 28, 2022, Retrieved from: <https://www.bleepingcomputer.com/news/security/meta-ukrainian-officials-military-targeted-by-ghostwriter-hackers/>
- Stuart Madnick, “*What Russia’s Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare*”, March 7, 2022, Retrieved from: <https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare>

The hybrid response of the EU and NATO to the Russia-Ukraine conflict

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. Previously, 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

The ongoing conflict between Russia and Ukraine embodies the main features of hybrid warfare. Alongside the military dimension, the use of propaganda tools, disinformation campaigns and cyber-attacks has fully emerged so far, as well as the multiplicity of state and non-state actors involved. Faced with this complexity, the European Union (EU) and NATO, unable to make full use of the military instrument to contain the consequences of the conflict, have put in place a multidimensional response. Up to now, it has been articulated in the use of both hard and soft power tools that have transversally involved different sectors. On the one hand, therefore, there was the supply of military equipment to the Ukrainian front. On the other hand, lawfare instruments such as economic sanctions have been put in place, as well as trade, financial and energy measures aimed at isolating Russia from the rest of the international community. Considering the factors that have long been observed in the field of international security studies, the future context will be increasingly dominated by hybrid warfare and the need for various actors to avoid open military clashes. The response of the EU and NATO to the Russian-Ukrainian crisis could, on the one hand, highlight the difficulties of the two organizations in fully transforming themselves into global players in the framework of international security and defence. On the other hand, could be a first step toward the exercise of a potentially replicable hybrid power in the management of future crises.

Keywords

Ukraine, Russia, EU, NATO, hybrid warfare

1. Introduction

The military action undertaken by Russia with the invasion of Ukraine on February 24, 2022, represents only the final step in a conflict that began as early as 2014 at the time of the annexation of Crimea and the creation of the separatist republics of Donetsk and Luhansk. In the context of this long phase, the confrontation remained stagnant but persistent, alternating low-intensity military skirmishes with other forms of conflict performing on other levels. Precisely this multidimensionality allows us to observe what is happening in Ukraine not only under the military lens but also by appreciating the implications on the cyber, information and propaganda level. On these fronts, the conflict has never really ended or stopped in the last years, and recent military action represents only the apex of a confrontation that has progressed over time, albeit in less overt and media-relevant forms. In this context, therefore, the current conflict can be referred to as a real hybrid conflict, of which it follows the main characteristics that have been outlined by the existing literature.¹ Faced with this threat, the response of the two main European defence organizations, the European Union (EU) and NATO, involved the exercise of hybrid power, that is, a mixture of economic sanctions, military supplies, and the use of tools of soft power aimed at countering Russian action.² The complexity of the Western response, and the exercise of a power that can be defined as hybrid, follow the existing literature about the growing international economic and institutional interdependence which amplifies the use of *soft power*.³ Even if this interconnection does not eliminate conflicts, it aims at least to distance them from the military sphere. This fits in the wake of existing studies on the nature of the EU as a *civilian*⁴ or *normative power*,⁵ or as an actor more focused on the use of diplomatic and legal tools, or in shaping the conception of “normal” in international relations, rather than on the use of military force. This appeal was also favoured and promoted by the inability to fully use the classic military instrument, both because Ukraine is not a member state in either organization and to prevent further escalation of the conflict on a large scale.

¹ Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict. *Connections*, 15(2), 65-72.

² <https://www.epc.eu/en/Publications/EU-hybrid-power-to-face-the-Russian-threat~462ecc>

³ Nye, Joseph S. “Soft Power.” *Foreign Policy*, no. 80 (1990): 153-171.

⁴ Duchêne, Francois. 1973. “The European Community and the uncertainties of interdependence” in *A Nation Writ Large? Foreign Policy Problems before the European Community*. Max Kohnstamm and Wolfgang Hager, eds., pp. 1-22.

⁵ Manners, Ian. 2002. “Normative Power Europe: A Contradiction in Terms?” *Journal of Common Market Studies* 40(2): pp. 235-258.

Furthermore, to make the picture even more complex, there are numerous players, both state and non-state actors, who increase the fragmentation of the conflict, making it more difficult for Western countries and institutions to develop an articulated and coherent response strategy. This, therefore, helps to understand the premises of the choices made up to now by the EU and NATO,⁶ unable to resort to military actions against Russia and oriented towards a mosaic of measures about the *hard* and *soft power* spheres.⁷ This hybrid response may on the one hand signal the difficulty of the EU and NATO to position themselves as global actors in the field of security and defence, given the reluctance to deploy military actions even in the face of a direct attack such as the Russian one. On the other hand, it could signal a new direction in conflict management, both considering the growing proliferation of hybrid warfare and considering the difficulty, increasingly encountered in the future, of easily resorting to the military instrument.

2. The EU response

The measures taken by the EU to respond to the Russian attack have so far been multidimensional, aimed at hitting Moscow on the economic, financial, and commercial front, including for the first time the direct sale of weapons to Ukraine and therefore taking steps also on the military level. In addition to the measures launched by the EU, there are also a series of decisions taken by European companies and institutions in the cultural, artistic and sports fields aimed at punishing Russian athletes or artists to increase the country's international isolation. Although these cases do not directly concern the EU, they in any case indicate the complexity of the response implemented at the institutional level on the European continent, mixing *hard* and *soft power* tools.⁸

At the institutional level, up to now, the various member countries have managed to find a compromise between the different national sensitivities towards both Russia and the issues inherent to common defence and the so-called *strategic sovereignty* of the EU. This balance has made it possible to offer a unitary and coherent response in terms of measures taken, even if the first difficulties in coordinating a cohesive energy policy in the face of reductions in imports of gas and raw materials from Russia are already reported.⁹

What has emerged so far, in any case, is a huge recourse to the instrument of law and *lawfare* in reaction to the Russian attack. The same economic

⁶ <https://foreignpolicy.com/2022/03/23/economic-war-russia-sanctions-bailouts-west-g7-nato/>

⁷ <https://www.bbc.com/news/world-europe-60125659>

⁸ <https://www.foreignaffairs.com/articles/ukraine/2022-03-18/new-economic-containment>

⁹ <https://www.foreignaffairs.com/articles/united-states/2022-03-22/toll-economic-war>

sanctions imposed on companies and individuals are justified based on Russia's violation of international obligations. In this way, the law is used on the one hand as a foundation for the adoption of measures in response to military action, and on the other hand, as a weapon to be wielded in the context of a hybrid conflict. The impossibility for the EU to resort to military action against Russia, therefore, leaves room for various kinds of measures justified employing purely legal arguments. Up to now, they have involved various sectors in which they have operated transversally, affecting both companies linked to the Kremlin in various economic fields, and individuals deemed close to Putin's closest circle of power. The glue that makes it possible to give coherence to this plurality of decisions, at least according to the vision of Brussels, is the ability to pursue a single goal, namely that of striking Russia, weakening not only the economic and financial sphere but also the military campaign itself. Thus, once again, the multidimensionality of hybrid conflicts emerges, where the military and non-military spheres (commercial, legal, diplomatic, economic, etc.) merge, making the various facets of *hybrid warfare* indistinguishable, where everything becomes a potential tool and terrain of contention and competition.

Specifically, among the measures taken by the EU, it is possible to mention, among others, travel restrictions, freezing of assets, prohibition of commercial operations with certain companies or in the Russian energy sector. Among the various sanctions imposed, some have also taken on a strong symbolic impact, such as the ouster from the Swift system of seven Russian banks (Bank Otkritie, Novikombank, Promsvyazbank, Bank Rossiya, Sovcombank, Vnesheconombank (VEB) and VTB Bank). This measure will have the effect of disconnecting the financial institutions involved from the international financial system, compromising their ability to operate worldwide. In addition to these measures, the EU has also imposed a ban on investing and/or participating in future projects co-financed by the Russian Direct Investment Fund, as well as selling, supplying, transferring, or exporting euro banknotes to Russia or natural and legal persons in Russia.¹⁰

Russia's international isolation seems to have been undertaken also to avoid possible campaigns of influence in Western societies. This emerges from the choice to impose sanctions on media such as Russia Today and Sputnik, accused of spreading fake news and Kremlin propaganda, which are defined by the European authorities as being placed under the direct or indirect control of the authorities of the Russian Federation. These last measures are part of the strategy of countering Moscow's offensive on the widest possi-

¹⁰ <https://www.consilium.europa.eu/it/policies/sanctions/restrictive-measures-ukraine-crisis/history-restrictive-measures-ukraine-crisis/>

ble scale which, following the model of *hybrid warfare*, aims to combine the military dimension with wise use of the communication sphere. The communication plan has represented, especially following the invasion of Crimea in 2014, a crucial and successful battleground so far for Russia, which has been investing for years in actions aimed at undermining the Western liberal order. To achieve this goal, the propaganda and communication aspect is of crucial importance, to undermine the Western international order from within by corroding the bond of trust between civil society and political institutions.

3. NATO's response

NATO's reaction to Russian military action has been more confined to the military sphere, also considering the nature of the organization.¹¹ However, there was also the choice of Member States to act in favour of Ukraine on the financial and humanitarian levels, in addition to significant military supplies and logistical and intelligence support.¹² Over the weeks, both in public statements and in international meetings, there has been growing coordination in the response between the EU and NATO, in a renewed attempt to promote an effective unity of the transatlantic community after the tensions of recent years.¹³ However, NATO remains a military alliance devoted to the collective defence of its member states that in recent years has taken important steps in terms of strategic conceptualization of the hybrid threat, and the identification of possible responses. This has led to an enlargement of the military sphere which is now integrated by infrastructures destined to confront each other on the terrain of *hybrid warfare*, especially in the cyber sphere. In the specific case, the impossibility of resorting to art. 5 of the North Atlantic Treaty due to Ukraine's non-participation in NATO, prevented recourse to the deployment of the military instrument directly in the ongoing conflict. This was offset by the huge increase in military force deployed along the eastern flank of the Alliance,¹⁴ or in countries such as Poland, Hungary, Romania, and the Baltic Republics.¹⁵ Although equipped with a lower range of tools than the EU has, given the structural and purpose diversity of the two organizations, NATO has also offered a hybrid response aimed at integrating with the various packages of measures and sanctions already imposed by the EU.

¹¹ <https://www.theguardian.com/world/2022/mar/23/nato-countries-to-give-ukraine-kit-to-protect-against-chemical-and-nuclear-attacks>

¹² https://www.nato.int/cps/en/natohq/news_192476.htm?utm_source=linkedin&utm_medium=sme&utm_id=220227%2Bukraine%2Bnato%2Bsupport

¹³ https://www.nato.int/cps/en/natohq/official_texts_193719.htm

¹⁴ <https://foreignpolicy.com/2022/03/24/nato-russia-war-deploy-new-battle-groups-eastern-europe/>

¹⁵ <https://www.nytimes.com/2022/03/02/world/europe/nato-weapons-ukraine-russia.html>

The supply of military equipment to Ukraine,¹⁶ in fact, makes it possible to avoid a formal entry into the ongoing conflict, an event that would have no basis in the Treaties or support from public opinion but allows for the pursuit of strategic objectives in a less blatant but equally substantial form.

4. Future developments

The ongoing conflict in Ukraine is one of the new forms of conflict defined as hybrid in the light of the multidimensionality through which it is developing. As previously stated, it does not consist only of a military component, the most evident external form of the conflict, but also of a communicative and cybersphere that has been supporting Russian military actions, or the Moscow proxies, in Ukraine since 2014. Against this background, the response put in place by the main Western defence organizations, namely NATO and the EU, consisted of the exercise of a sort of hybrid power, a mixture of measures operating on several levels (economic, commercial, financial, legal, military as well as soft power tools) aimed at countering Russian military action and forcing Putin to change his initial objectives. The implementation of these actions is due both to formal reasons (i.e. the non-participation of Ukraine in both organizations), as well as political and strategic, due to the growing reluctance of Western societies to resort to war for the huge costs and fear of possible escalation. The path taken may indicate, in a future perspective, two antithetical yet relevant elements.

On the one hand, it may indicate, once again, the inability of the two organizations to rethink themselves in the changed European threat framework and to project themselves as global players in the international security scenario. These difficulties would confirm the troubling restructuring of the European security architecture, whose governance has been limited for years by the difficulty of identifying a division of responsibilities between the EU and NATO. This is both considering the basic misunderstanding about the role that the EU and European countries should play about the United States (and therefore NATO) and for the different national preferences within the EU between Atlanticist countries and those who push in the direction of greater European strategic sovereignty.¹⁷ Following this interpretation, therefore, the implementation of sanctioning measures such as those adopted so far would be yet another proof of the obstacles that hinder the definitive

¹⁶ <https://www.euronews.com/my-europe/2022/03/24/chemical-weapons-nato-to-provide-ukraine-with-equipment-to-counter-russian-threat>

¹⁷ <https://foreignpolicy.com/2022/03/24/war-ukraine-russia-eu-defense-military-nato-europe/>

projection of the EU and NATO on the stage of international security and defence, through a coherent and punctual division of tasks.

On the other hand, on the contrary, the work carried out so far by the two institutions could signal a model that could potentially be replicated in the future in the event of new conflicts. As indicated by a substantial part of the academic and political debate in the field of security studies, the future scenario will be that of a gradual and constant increase in the hybridization of the conflict. This will imply, over time, that the military instrument will be significantly less used due to its economic and social costs to favour hidden and covert forms of conducting hostilities. Considering this process, the countries of the transatlantic community will be increasingly pushed to identify new tools to respond to the actions coming from hostile actors and the crises arising in its neighbourhood, whose destabilization seems destined to increase. The developments of the current conflict will therefore be of extreme importance to evaluate the effectiveness of these tools as well as to evaluate their possible replicability in any future theatres of conflict.

Bibliography

- Duchêne, Francois. 1973. "The European Community and the uncertainties of interdependence" in *A Nation Writ Large? Foreign Policy Problems before the European Community*. Max Kohnstamm and Wolfgang Hager, eds., pp.1-22. London: Macmillan.
- Giegerich, B. (2016). "Hybrid Warfare and the Changing Character of Conflict". *Connections*, 15(2), 65-72.
- Manners, Ian. 2002. "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 40(2): pp. 235-258.
- Nye, Joseph S. "Soft Power." *Foreign Policy*, no. 80 (1990): 153-171.

Sitography

- BBC. 2022. "What sanctions are being imposed on Russia over Ukraine invasion?". Retrieved from: <https://www.bbc.com/news/world-europe-60125659>. Accessed 28 March 2022.
- Balfour, R. 2022. "What Russia's war in Ukraine means for Europe". Retrieved from: <https://carnegieeurope.eu/strategieurope/86587>. Accessed 9 March 2022.
- Borges De Castro, R. EU 'hybrid power' to face the Russian threat. Retrieved from: <https://www.epc.eu/en/Publications/EU-hybrid-power-to-face-the-Russian-threat~462ecc>. Accessed 20 March 2022.
- Consilium. 2022. Retrieved from: <https://www.consilium.europa.eu/it/policies/sanctions/restrictive-measures-ukraine-crisis/history-restrictive-measures-ukraine-crisis/>. Accessed 31 March 2022.

- Erlanger, S. 2022. The New York Times. “NATO Countries Pour Weapons Into Ukraine, Risking Conflict With Russia”. Retrieved from: <https://www.nytimes.com/2022/03/02/world/europe/nato-weapons-ukraine-russia.html>. Accessed 9 March 2022.
- Euronews. 2022. “Chemical weapons: NATO to provide Ukraine with equipment to counter Russian threat”. Retrieved from: <https://www.euronews.com/my-europe/2022/03/24/chemical-weapons-nato-to-provide-ukraine-with-equipment-to-counter-russian-threat>. Accessed 26 March 2022.
- Gramer, R., 2022. Foreign Policy. “NATO to deploy four new battle groups to Eastern flank”. Retrieved from: <https://foreignpolicy.com/2022/03/24/nato-russia-war-deploy-new-battle-groups-eastern-europe/>. Accessed 28 March 2022.
- Kleln, M., Schnelder, J., Talbot, D. 2022. Foreign Policy. “Only a financial NATO can win the economic war”. Retrieved from: <https://foreignpolicy.com/2022/03/23/economic-war-russia-sanctions-bailouts-west-g7-nato/>. Accessed 25 March 2022.
- Mulder, N. 2022. Foreign Affairs. “The toll of economic war”. Retrieved from: <https://www.foreignaffairs.com/articles/united-states/2022-03-22/toll-economic-war>. Accessed 26 March 2022.
- NATO. 2022. “NATO allies boost support to Ukraine”. Retrieved from: https://www.nato.int/cps/en/natohq/news_192476.htm?utm_source=linkedin&utm_medium=smc&utm_id=220227%2Bukraine%2Bnato%2Bsupport. Accessed 9 March 2022.
- NATO. 2022. “Statement by NATO Heads of State and Government”. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_193719.htm. Accessed 25 March 2022.
- Norrlof, C. 2022. Foreign Affairs. “The new economic containment”. Retrieved from: <https://www.foreignaffairs.com/articles/ukraine/2022-03-18/new-economic-containment>. Accessed 22 March 2022.
- Sabbagh, D., Roth, A. 2022. The Guardian. “NATO countries set to give Ukraine kit to protect against nuclear and chemical attacks”. Retrieved from: <https://www.theguardian.com/world/2022/mar/23/nato-countries-to-give-ukraine-kit-to-protect-against-chemical-and-nuclear-attacks>. Accessed 27 March 2022.

NAVIGARE SCENARI IBRIDI: PROSPETTIVE

L'Amore Altruistico in tempi di guerra e pandemia

GIACOMO BUONCOMPAGNI

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

Abstract

Pitirim A. Sorokin, a Russian sociologist naturalised in the United States and a leading figure in 20th century sociology, stated that historical and techno-cultural changes have not always produced positive results within societies, but at times even negative (or more precisely, 'destructive') ones: individualism, antagonism, an excess of technology and rationality, and in particular the fall of the bonds of solidarity towards the different and the loss of the feeling of belonging (Mangone 2015; Cimagalli 2010; Marletti 2018; Perrotta 2016).

Altruism can also be one of the indispensable ingredients of social life, useful for preventing crises and conflicts.

No society can exist without an "altruistic and creative love" that has as its aim the "altruisation" of individuals and social institutions: a complex process/project capable of encompassing the emotional, supra-rational and spiritual aspects of human relations (including online), starting from the idea that all men can recognise themselves in certain moral principles, eternal and universal.

Considering the current pandemic and war scenarios, the aim of the paper is to illustrate the main theoretical lines of Sorokin's scientific thought, which made sociology a "science at the service of humanity" useful also for the study of disasters, i.e. all those events involving conjunctions of physical conditions and definitions of human damage and social disorders (e.g. natural disasters, wars and cyber attacks).

Pitirim A. Sorokin, sociologo russo naturalizzato statunitense, figura di spicco della sociologia del XX secolo, affermava che i mutamenti storici e tecno-culturali non sempre hanno prodotto risultati positivi all'interno delle società, ma a tratti anche negativi (o più precisamente "distruttivi"): individualismo, antagonismo, eccesso di tecnica e di razionalità, ed in particolare la caduta dei vincoli di solidarietà nei confronti del diverso e della perdita del sentimento di appartenenza (Mangone 2015; Cimagalli 2010; Marletti 2018; Perrotta 2016).

L'altruismo può essere uno degli ingredienti indispensabili alla vita sociale, utile per prevenire crisi e conflitti.

Nessuna società può esistere, infatti, senza un "amore altruistico e creativo" che abbia come fine "l'altruizzazione" degli individui e delle istituzioni sociali: un processo/progetto complesso in grado di comprendere gli aspetti emotivi, sovra-razionali e spirituali delle relazioni uma-

ne (anche online), partendo dall'idea che tutti gli uomini possono riconoscersi in determinati principi morali, eterni ed universali.

Considerando gli attuali scenari di pandemia e di guerra, lo scopo del paper è quello di illustrare le principali linee teoriche del pensiero scientifico di Sorokin, che ha fatto della sociologia una "scienza al servizio dell'umanità" utile anche per lo studio dei disastri, cioè di tutti quegli eventi che coinvolgono congiunzioni di condizioni fisiche e definizioni di danno umano e disturbi sociali (ad esempio, calamità naturali, guerre e cyberattacchi).

Keywords

Sorokin, altruism, media, digital, crisis, covid19, war

1. Introduzione

Dopo due anni di pandemia, le società di tutto il mondo sembravano ormai pronte ad affrontare un periodo di "rinascita", ricostruire le proprie economie, risollevarne la credibilità delle proprie istituzioni e rafforzare quelle relazioni sospese ormai da troppo tempo e da mesi "congelate" all'interno delle piattaforme digitali.

Ma in quanto entropiche, le nostre società creano costantemente i fattori delle loro stesse crisi globali, i cui effetti danneggiano pesantemente prima di tutto la dimensione locale e quotidiana delle nostre esistenze.

E il nuovo conflitto tra Russia e Ucraina è un esempio di questa entropia, di una nuova crisi umanitaria che si intreccia con quella sanitaria ed economica ancora in corso.

Del resto, la vita di ogni società è una fluttuazione incessante tra periodi di benessere e calamità, affermava Sorokin, la cui figura è oggi più che mai attuale.

La sua sociologia è in qualche modo immersa in un'ampia visione del mondo, capace di coniugare analisi scientifica e bisogni profondi del mondo contemporaneo.

Per questo motivo alcuni autori (Burawoy 2004; Jeffries 2005; Cimagalli, 2010; Mangone 2015) riconoscono lo studioso russo come esponente di spicco di una scienza capace di parlare alla società e svolgere un ruolo pubblico significativo, superando quell'idea di sociologia come "industria di ricerche", incapace di raffigurare scenari e costruire solide teorie per dare risposte ai problemi globali.

E solo attraverso una prospettiva integralista di conoscenza, secondo cui ogni società può essere compresa a partire dalla cultura, cioè da un sistema di significati, norme e valori che emergono dalla natura bio-sociale dell'individuo, è possibile garantire l'interdipendenza alle scienze sociali e rendere

possibile le comprensioni delle crisi in atto, fornendo gli elementi corretti per superarla (Ponomareva 2011, Sofritti, 2018).

Quella di Pitrim A. Sorokin è una delle figure più complesse, poliedriche, rintracciabili nella riflessione sociologica della prima metà del Novecento, grazie al suo essere uno “studioso integrale”, impegnato a descrivere da un lato, la società nelle sue articolazioni e dinamiche, dall’altro, a esplorare l’uomo nella sua interezza, comprese le dimensioni culturali e spirituali.

La sociologia come “sistema integrato” si fonda perciò sull’interdipendenza di cultura, società e personalità e ha il compito di analizzare sia gli aspetti socioculturali, sia quelli psicologici e di “altre energie”, come quelle biologiche, razionali e spirituali (Perrotta 2016; Maretti 2018).

Ciò che rende attuale il pensiero di Sorokin e utilizzabile poi come strumento e metodo per leggere la contemporaneità, è connesso alla forza delle sue idee, alla grande importanza che viene riservata ai fattori mentali e culturali nello studio dei processi di cambiamento storico-sociale, alla sua capacità di trovare il posto, anche all’interno di una massa di dati quantitativi, a tutte le componenti delle produzioni umane, artistiche, affettive ed emozionali *in primis*.

Sorokin critica, infatti, una visione esclusivamente razionale dell’uomo inteso come essere umano, e non come un robot. L’individuo, composto secondo il sociologo, di mente, corpo e spirito, è creatore di quella realtà socioculturale che comprende, oltre agli aspetti logico-empirici, anche quelli sovra-razionali.

Come “sociologo della modernità” (Gambescia 2002; Cimagalli 2010) descrive un mondo in via di estinzione, a causa del progresso incontrollato e di un “sensismo attivo”, innovatore e propulsivo, che va isterilendosi nel materialismo passivo dell’edonismo, del profitto, dell’interesse egoistico. A partire dal XX secolo, in particolare, la creatività è andata diminuendo, l’economica sensista non è stata più in grado di garantire quello che prometteva. Ricchezza e benessere hanno così subito un importante arresto.

2. Crisi della modernità

Le guerre, le rivoluzioni, i conflitti, i suicidi nella società industrializzata che hanno caratterizzato il Novecento sono la dimostrazione di come la transizione dalla morente cultura sensista alla nascente cultura ideazionale sia stato un periodo particolarmente tormentato e drammatico per la storia dell’uomo.

Nella società moderna occidentale ogni aspetto della vita, dell’organizzazione sociale e della cultura si trova in uno stato di seria crisi: educazione socio-morale, scienza, filosofia, religione, politica, economia e ogni forma di relazione umana positiva, di senso (famiglia, matrimonio.) vivono una fase di

grave sgretolamento e si vengono così a generare aspri conflitti e altre conseguenze sociali particolarmente negative (Sorokin, 1957).

La decadenza della modernità sensista, visibile in tutti i settori della vita sociale e culturale, porta alla rovina delle politiche contrattualistiche e delle istituzioni economiche fondate sul principio della libertà individuali, e, allo stesso tempo, favorisce il passaggio dalla democrazia ai nuovi governi totalitari comunisti e fascisti, supportati da un uso intenzionalmente manipolatorio e ingannevole dei media elettronici (Gorman, McLean 2011; Merlo 2011).

Il progressivo sfaldamento dei legami e delle appartenenze comunitarie hanno favorito la nascita di nuove relazioni fondate sempre più sulla vicinanza e la comune appartenenza; l'individuo che subisce sempre di più le conseguenze del progresso tecnologico e dei veloci mutamenti socio-economici, appare sempre più erratico, libero, isolato, mobile, affrancato da legami personali vincolanti e autonomo rispetto alle idee, mutevoli e largamente indipendenti, apparentemente capace di costruire la propria identità attraverso lo scambio sociale con l'Altro (Simmel 1995; Bauman 2001; Cimagalli 2010, Elliot, Urry 2005).

Termini come "individualizzazione", "identità riflessiva", "vita liquida" sono stati utilizzati proprio per evidenziare il carattere mobile, fluido e dispersivo del mondo contemporaneo e parallelamente l'emergere di un "nuovo individualismo" come insieme di processi istituzionali e nuovi modelli di formazione dell'identità (Bauman 2001; Elliot, Urry 2005; Moores 2017).

È interessante notare come la visione di Sorokin si intrecci, in modo complementare, con altri studiosi di scienze sociali che, anche se in momenti storici differenti, riconoscono i tratti principali riguardanti la crisi della modernità e dell'individuo da un lato, e dall'altro analizzano il nuovo contesto urbano "mercattizzato" (la società come "terra straniera"), la scomparsa dell'intimità fiduciosa e della solidarietà tradizionale che caratterizzavano i rapporti comunitari tra persone "altre", ormai distanti, sempre più simili alle macchine.

Ad esempio, nel 1965 l'antropologo Ashley Montagu in *The Human Revolution* (p. 24) sottolineava come l'uomo progredito nella civiltà fosse diventato «sempre più, e non meno, aggressivo e guerriero» e come nella società moderna la maggior parte degli individui fosse ormai abituato a badare a sé in modo autonomo a tal punto da risultare difficile capire oggi come, in ogni fase della storia, l'uomo abbia vissuto *per necessità* una vita di coinvolgimento nel benessere dei propri simili.

In *A War and Peace in the Global Village* Marshall McLuhan (1968) esprimeva preoccupazione circa la nascita del "villaggio globale" nell'era dei computer e delle reti, in quanto la condivisione di un unico spazio (pubblico) da parte di milioni di individui e di culture differenti avrebbe generato una "grande tribalizzazione elettronica", rendendoci solo apparentemente

tutti “fratelli” e impedendo solidarietà e amore tra gli individui. Secondo lo studioso il solo modo di affrontare questo problema era “dosare” lo spazio e i media¹.

Lo stesso Barber (1992) descriveva uno spazio inedito da abitare in seguito alla globalizzazione, pronto a collegarsi in un'unica rete guidata dalla tecnologia e dall'ecologia della comunicazione, ma in queste stesse forze riconosceva la causa dell'emergere di nuove forme di conflitto tra culture e tribù in un mondo che si stava contemporaneamente allontanando e avvicinando².

Nel suo saggio *Communication in a global village* Dean Barnlund (1998), analizzando l'idea proposta da McLuhan, in merito al concetto di estraneità e ai cambiamenti comunicativi e mediali in corso, si chiedeva se e in che modo i nuovi “residenti” avrebbero compreso, rispettato e valorizzato le differenze dei loro “vicini di casa” oppure, al contrario, se gli “abitanti del villaggio” si fossero di lì a poco trasformati in un agglomerato di estranei, residenti nei ghetti, accomunati solo dalle reciproche antipatie, interrogandosi inoltre su come la politica e le istituzioni avessero agito per alleviare i conflitti all'interno delle comunità.

È come se la modernità accompagnata dal progresso tecnico e tecnologico avesse rivelato il proprio lato inquieto, irrazionale e violento, creando fratture culturali, spersonalizzazioni, odio e conflitto, eliminando ogni forma umana di collaborazione e di altruismo.

3. Breve storia (sociologica) dell'altruismo

Il termine “altruismo”, innanzitutto, è un neologismo comtiano che nasce insieme alla sociologia (Merlo, 2011), impiegato dal sociologo Augusto Comte per definire sia la naturale inclinazione umana alla socialità (insieme all'egoismo) sia per indicare l'imperativo morale della nuova religione positiva (*vivre pour autrui*). Per Comte come per Durkheim, “altruismo” è amore per la società, rappresenta la fusione dell'io individuale nell'io collettivo nella società tradizionale (solidarietà meccanica) e la spinta alla cooperazione nella società moderna (solidarietà organica).

Lo studio dell'altruismo, dopo un periodo di assenza nella sociologia del Novecento, torna ad interessare le scienze sociali. Max Scheler e Jacques Martin sottolineano come il “vivere per gli altri” sia importante per sentirsi parte del genere umano, ma un “altruismo sentimentale” non produce automaticamente gesti concreti di benevolenza verso gli Altri (Merlo, 2011).

¹ de Kerchove D. (1996), *Marshall McLuhan secondo Derrick de Kerckhove*, disponibile al sito: <https://www.youtube.com/watch?v=jBflrcEilao>.

² Barber B. (1992), *Jihad vs. McWorld*, Corgi, London.

È con Sorokin che l'altruismo si fa poi sociologia, o meglio, Scienza per l'Altro.

L'Altruismo in questo caso, così come l'amore e la collaborazione, sono descritte come forze positive che agiscono nella vita sociale, forme di relazione significative fra due o più persone, nella quale le aspirazioni o gli scopi di una persona sono condivisi e assecondati nella loro realizzazione da altre persone (Perrotta 2016; Cimagalli 2020; Mangone 2019; 2020). L'Amore altruistico è la più alta forma di energia, intesa come capacità dell'individuo di agire e produrre un effetto positivo, benefico e creativo, capace di arginare gli effetti distruttivi dell'egoismo, dei conflitti, delle sopraffazioni, delle politiche predatorie.

L'Altruismo, inoltre, è sì atto d'amore, ma che deve essere coltivato e/o riscoperto non soltanto dall'individuo. È necessario che anche i gruppi sociali, la cultura e le istituzioni riescano a convertirsi alla religione positiva dell'altruismo.

4. L'Amore Altruistico

La diversità ha sempre rappresentato una fonte potenziale di frizione e d'incomprensione nella storia umana.

Difficilmente nei secoli si è potuto evitare il contatto con la differenza, così, la maggior parte delle volte, le risposte iniziali, anche di carattere politico, sono state quelle di evitare o cambiare culturalmente i diversi da noi, o ancora, nei casi più estremi, eliminarli: gli esempi di genocidio o i casi individuali di crimini commessi per odio sono episodi piuttosto recenti che riguardano principalmente il riemergere di atteggiamenti di razzismo e xenofobia.

Lo strumento adottato per creare una maggiore coesione e collaborazione all'interno di un gruppo composto da membri di una stessa cultura, dove si scambiano significati e si riconoscono alcuni comportamenti come appropriati, è quello della comunicazione monoculturale. Questo tipo di comunicazione si basa sulla "similarità" e favorisce una conoscenza condivisa della realtà, «permette generalmente ai membri della stessa cultura di prevedere le risposte degli altri basandosi su quella che sarebbe la propria reazione in simili circostanze» (Bennet 2015, p. 24).

In situazioni cross-culturali il processo comunicativo non può però basarsi sulla somiglianza, i significati devono essere creati intenzionalmente e la comunicazione deve mostrarsi più consapevole ed efficace affinché non si creino situazioni di conflitto e atteggiamenti etnocentrici; in questo caso lo strumento che prevede il superamento della somiglianza e la considerazione della differenza è quello della comunicazione interculturale fondata sul principio di diversità e orientata all'empatia, dunque capace di accettare e riconoscere le differenze.

Solo sviluppando la capacità di comunicare a livello globale, aprendosi all'Altro, non rinunciando necessariamente alla propria storia e cultura, i "diversi" possono relazionarsi in modo efficace e produttivo nella società e per far questo è fondamentale coinvolgere aspetti cognitivi, affettivi e comportamentali in relazione alle quattro dimensioni che definiscono la comunicazione interculturale: mentalità globale, sviluppo del sé, mappatura della cultura e allineamento dell'interazione (Chen, 2005).

Le differenze somatiche, di etnia, di sesso, di politica, di religione, di per sé non rappresentano, secondo la sua visione, un ostacolo alla solidarietà tra popoli e gruppi sociali, non impediscono l'amore tra due persone. Il vero ostacolo da superare è rappresentato invece dal "veleno dell'egoismo tribale" (Sorokin 1941; Merlo 2011), che i meccanismi della comunicazione elettronica-digitale e le logiche algoritmiche tendono oggi a rafforzare causando sempre più angoscia, autodistruzione e l'espulsione sociale dell'Altro.

Per Sorokin però la chiave per interpretare la complessità dell'oggi non risiede tanto nel progresso, responsabile di aver prodotto risultati non sempre positivi, ma nella concezione del sistema integrato socioculturale, che tiene insieme il piano materiale e quello ideologico-simbolico. Inoltre, rispetto al pensiero degli studiosi sopra citati e a ciò che attualmente emerge nel discorso pubblico, il sociologo russo conferma ancora l'attualità del suo pensiero nella società multiculturale interconnessa, quando sottolinea come sia errato ritenere che l'unica causa dei conflitti sociali e delle guerre sia la diversità esistente tra le persone, le culture e le società.

5. La dimensione "cyber" dell'amore altruistico

Superando inoltre ogni forma di determinismo tecnologico, è evidente come sottolinea in parte anche il sociologo russo, che gli attori principali, in grado di risolvere le crisi, siano gli individui stessi e il loro operato, il cui scopo dovrebbe essere allontanare lo spettro di una nuova catastrofe e "l'estensione universale dell'altruismo", anche sfruttando le opportunità offerte dai mezzi di comunicazione sociali e digitali.

Quest'ultimi da intendersi oggi come "psico-tecnologie": media che modificano i nostri cervelli, o quegli ambienti sociali in cui stabiliamo contatti (Sorokin, 1957, de Kerchove 2014; Couldry 2015, Cerretti, Padula 2016).

Concentrandosi sull'idea di "uomo mediale" e sugli usi sociali-solidali-altruistici delle tecnologie si cercherà di ricostruire il concetto di "amore altruistico" nell'era digitale, estendendo a livello teorico, il tentativo di Sorokin di fare della sociologia (e della tecnologia, in questo caso) una "scienza dell'altruismo", contribuendo al rinnovamento sociale alla ri-generazione dell'umanità.

Ciò che manca nel pensiero di Sorokin è un'idea di tecnologia come proiezione dell'essere umano, e non di un dispositivo pericoloso separato da esso o di uno strumento ormai fuori controllo (Marletti, 2018). L'individuo non usa i media, ma è media, gli spazi di rete non sono ambienti in cui l'uomo comunica, ma sono la riflessione della sua stessa qualità etica.

L'individuo è connesso con il mondo, aperto alla relazione e sempre meno disposto a diventare schiavo delle logiche medialità ed economiche (Lo Presti 1990; Silverstone 2009; Giaccardi 2012; Codeluppi 2017).

Intesa in questo senso la tecnologia non è solo profitto o strumento di violenza, ma medium sociale-digitale diviene quel "luogo" in grado di "curare" e ospitare forme originarie di energia creativa, definizione che Sorokin dà di altruismo, dove "persone comuni" e "persone eccezionali", non tendono a tribalizzarsi a causa della loro diversità, ma a comportarsi da "buoni vicini", a intrattenere relazioni sociali positive, testimoniando valori solidi e costruttivi (Silverstone 2009; Cimagalli 2010, 2020).

Le scienze sociali, in particolare la sociologia culturale e dei media, negli ultimi anni hanno concentrato l'attenzione principalmente sugli aspetti negativi che riguardavano l'alterità, l'immigrazione e il ruolo dei mezzi di comunicazione (pregiudizi, disinformazione, discorsi d'odio.), senza considerare troppo l'altro lato della tecnologia in rapporto a questi temi. Ad esempio, la possibilità che possano esistere forme di altruismo e solidarietà di natura digitale, oltre ai numerosi rischi tecnologici e casi di cyber-violenza. Parafrasando Sorokin, a volte è più utile concentrarsi su "ciò che brilla", piuttosto che sugli aspetti problematici, e da qui ripartire per lo studio dei problemi della società sensista.

A questo punto cercare di creare un ponte tra il pensiero del sociologo russo, il concetto di altruismo (digitale) e la rivoluzione tecnologica diventa non solo scientificamente interessante, ma necessario.

La nuova sfida contemporanea è comprendere come la responsabilità dell'individuo e del suo operato da un lato, e la potenza dell'interconnessione dei nuovi media dall'altro, siano in grado di creare le basi per un'amicizia digitale, superando/limitando egocentrismi e tribalismi alimentati dalla disgregazione sensista e dall'utilizzo scorretto e manipolatorio delle tecnologie (già evidenziato anche da Sorokin nella prima metà del Novecento) che potrebbero invece essere utilizzate anche con finalità sociali e di integrazione.

Nessuna società può esistere senza un "amore altruistico e creativo" che abbia come fine "l'altruizzazione" degli individui e delle istituzioni sociali: un processo/progetto complesso in grado di comprendere gli aspetti emotivi, sovra-razionali e spirituali delle relazioni umane (anche online), partendo dall'idea che tutti gli uomini possono riconoscersi in determinati principi morali, eterni ed universali.

E tale condizione potrebbe essere ri-creata anche attraverso gli strumenti digitali ed esistere negli ambienti online, provando in questo modo ad estendere, a livello teorico, il tentativo di Sorokin di fare della sociologia (anche digitale, in questo caso) una “scienza dell’altruismo” nell’era dell’interconnessione globale.

6. Conclusioni

Per concludere, riprendendo come riferimento il linguaggio di Sorokin, quanto descritto e analizzato rappresenta un esempio di “amore creativo altruistico” applicato al mondo digitale, forme più elevate di energia umana, supportate da elementi tecnici e tecnologici, rintracciabili sottoforma sia di narrazioni positive aperte all’Altro, sia di strumenti operativi (solidali) come siti, app, blog e social network (tecnologie solidali) all’interno degli spazi virtuali e della cultura digitale, che, per come vengono ancora oggi descritti e percepiti, sembrano presentarsi come il prolungamento di quella cultura sensista, responsabile del prevalere di egoismi e delle ingiustizie.

Negli ambienti online le logiche della condivisione e della vetrinizzazione non solo possono mettere in risalto l’esistenza di personalità altruistiche, ma più lo stesso spazio digitale si mostra aperto a valori altruistici e a pratiche mediali creative in grado di “contagiare” tecnicamente e culturalmente forme di solidarietà ordinarie, maggiori sono le possibilità che ogni soggetto connesso conosca e applichi l’amore altruistico anche digitalmente, contro ogni forma di ingiustizia sociale e di discriminazione.

Istituzioni, i mezzi tradizionali di informazione e le principali agenzie di socializzazione dovrebbero investire sull’educazione altruistica, suggerisce lo stesso Sorokin, ma soprattutto sulla ricerca di tecniche educative e formative, facendo appello non solo alla ragione, ma toccando l’affettività e l’emotività dell’individuo.

Le persone sono in grado di provare simpatia e comprensione umana, sostiene Edgar Morin (2015, p. 89), soprattutto quando la sofferenza e l’ingiustizia ci appare all’improvviso tramite un’immagine o su qualsiasi altro supporto mediale. Anche attraverso la rappresentazione sociale e strumenti mediali, Comprensione dell’Altro e Altruismo possono essere generati.

Ciò accade perché si attua un processo di identificazione e di simpatia che “permette di vedere la complessità degli aspetti di una persona”.

L’eliminazione delle forme di violenza e delle crisi sociali, non può dunque essere affidata solo ed esclusivamente a specifici “settori” della società (diritto, educazione, religione, cultura, tecnologia).

Il futuro dell’umanità e il suo sviluppo è nelle mani della stessa umanità che deve impegnarsi a costruire un noi collettivo, solide reti di collaborazio-

ne e strumenti (tecnologie) a misura d'uomo per contrastare i disastri e ogni forma di egoismo che mettono a rischio la convivenza civile all'interno di una società (Sorokin, 1948, p. 57):

Una società pacifica, armoniosa e creativa può esistere solo quando i suoi membri hanno almeno un minimo di amore, simpatia e compassione che assicurano aiuto reciproco, cooperazione e trattamento equo. In questa condizione (...) le gioie e i dolori di un membro sono condivisi dagli altri.

Bibliografia

- Appadurai A. (2005), *Sicuri da morire*, Meltemi, Roma.
- Barber B. (1992), *Jihad vs. McWorld*, Corgi, London.
- Bartholini I. (2015), *Violenza di prossimità*, Franco Angeli, Milano.
- Bauder, H. (2011), *Immigration dialectic: Imagining community, economy and nation*, University of Toronto Press, Toronto.
- Bauman Z. (1996), *Le sfide dell'etica*, Feltrinelli, Milano.
- Bauman Z. (2001), *Modernità liquida*, Laterza, Roma-Bari.
- Bennett J. (2015), *Principi di comunicazione interculturale. Paradigmi e pratiche*, Franco Angeli, Milano.
- Boccia Artieri G. (2012), *Stati di connessione*, Franco Angeli, Milano
- Brunwasser M. (2015), "A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone", testo disponibile al sito: <https://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html>.
- Buoncompagni G. (2019) Per una sociologia dell'ospitalità: L'Altro nella società postmoderna tra paradossi, diritti umani, narrazione mediale e crimini di pace, in Federici M.C., (a cura di), *L'Arte femminile della Mediazioni. Risultanze di una ricerca su donne immigrate, rifugiate e del loro percorso formativo di Mediatrici*, Armando Editore, pp. 73-102.
- Buoncompagni G., D'Ambrosi L. (2020), Hate Speech Towards Migrants, in La Rocca G. Torvisco J.M., (a cura di), *Technological and Digital Risk: Research Issues*, Peter Lang Publishing, pp. 177-190.
- Buoncompagni G. (2021), *Cybermigration. La dimensione digitale dell'immigrazione*, PM edizioni.
- Burawoy M (2004), Manifesto for Public Sociology, *Social Problem*, 5.
- Cesareo V. (2001), *Per un dialogo interculturale*, Vita&Pensiero, Milano.
- Chen Guo-M. (2005), A model of global communication competence, *China Media Research*, 1, pp. 3-11.
- Cimagalli F. (2010), *Sorokin. Attualità di un classico della sociologia*, Aracne, Roma.
- Cimagalli, F. (2020), Is There a Place for Altruism in Sociological Thought? *Human Arenas* 3, pp. 52-66.
- Couldry N. (2015), *Sociologia dei nuovi media. Teoria sociale e pratiche mediali digitali*, Pearson, Milano.

- de Kerchove D. (1996), *Marshall McLuhan secondo Derrick de Kerckhove*, text available at link: <https://www.youtube.com/watch?v=jBflrcEilao>.
- de Kerchove D. (2014), *Psicotecnologie connettive*, Egea, Milano.
- Elliot A., Urry J., (2005), *Vite mobili*, il Mulino, Bologna.
- Gambescia C. (2002), *Invito alla letteratura di Sorokin*, Ed. Settimo Sigillo, Roma.
- Garcea E. (1996), *La comunicazione interculturale*, Armando, Roma.
- Giaccardi C. (2012), *La comunicazione interculturale nell'era digitale*, il Mulino, Bologna.
- Gorman L., McLean D. (2011), *Media e società nel mondo contemporaneo*, Il Mulino, Bologna.
- IOM (2018), *World Migration Report*, IOM, Geneva.
- Jenkins H. (2007), *Cultura convergente*, Apogeo, Milano.
- Jeffries V. (2005), Integralism and Public Social Science, *The Catholic Social Science Review*, 10.
- Jo Cox Committee (2017). *Relazione finale Camera dei Deputati XVII Legislatura*, testo disponibile al sito: https://www.camera.it/application/xmanager/projects/leg17/attachments/commissione_intolleranza_resoconti/resocontos/000/000/012/resoconto_2017_03_09_def.pdf.
- Mangone E. (2015), *Salle "calamità" di Sorokin alla "rinascita". La sociologia integrale per lo studio dei disastri*, Franco Angeli, Milano.
- Mangone, E. (2019), Gratitude and the Relational Theory of Society, *Human Arenas. An Interdisciplinary Journal of Psychology, Culture, and Meaning*, vol. 2, issue 1, pp. 34-44.
- Mangone E. (2020), Towards a New Configuration of the Ego / Alter Relationship: The Rediscovery of Altruism, *Revista Latinoamericana de Estudios sobre Cuerpos, Emociones y Sociedad – RELACES*, N°34. Año 12.
- Merlo V. (2011), *Il miracolo dell'altruismo umano. La sociologia dell'amore di P.A. Sorokin*, Armando ed., Roma.
- Marci T. (2017), *La società degli altri. Ripensare l'ospitalità*, Le Lettere, Firenze.
- Marletti C.A. (2018), Pitirim A. Sorokin: contributo alla rivisitazione di un classico della sociologia, *Quaderni di Sociologia*, 76, pp. 107-126.
- McLuhan M. (1968), *War and Peace in the Global Village*, Touchstone S&S, New York.
- Morin E. (2015), *Etica e identità umana*, Egea, Milano.
- Perrotta A. (2016), *Sorokin e i sentimenti dimenticati*, in D'Amato M., a cura di, *Ragioni e sentimenti*, Roma Tre Press, Roma.
- Ponomareva I. (2011), Pitirim A. Sorokin: the Interconnection between his Life and Scientific World, *International Sociology*, XXVI, 6, pp. 878-904.
- Pred A., Watts M. (1992), *Reworking Modernity: Capitalism and Symbolic Discontent*, Rutgers University Press, New Brunswick.
- Schiesaro G. (2018), *I migranti con lo smartphone*, VIS, Roma.
- Sennett R. (2012), *Lo straniero: due saggi sull'esilio*, Feltrinelli, Milano.
- Silverstone R. (2009), *Mediapolis, La responsabilità dei media nella civiltà globale*, Vita&Pensiero, Milano.
- Simmel G. (1996), *Le metropoli e la vita dello spirito*, Armando editore, Roma.

- Sofritti F. (2018), Pitirim Aleksandrovich Sorokin. Ascesa, declino e ritorno di un maestro del pensiero sociologico, *The Lab's Quarterly*, 1, pp. 7-30.
- Sorokin P.A. (1941), *Crisis of Our Age*, New York, E.P. Dutton & Co.
- SWG (2017), *Hate speech e fake news tra cittadini, lavoratori e dirigenti*, Trieste.
- Tech Against Trafficking (TAT) (2021), *Accelerating the Use of Technology to Combat Human Trafficking*, text available at link: <https://techagainstrafficking.org/accelerating-the-use-of-technology-to-combat-human-trafficking/>.
- Urry J. (2000), *Sociology beyond Societies: Mobilities for the Twenty-first century*, Routledge, London.
- Vox-Osservatorio Italiano sui diritti (2018). La Mappa dell'Intolleranza. Milano. Accessed May 03, 2019. <http://www.voxdiritti.it/la-mappa-dellintolleranzaanno-3-la-nuova-radiografia-dellitalia-che-odia-online/>.
- Ziccardi, G. (2016), *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina Editore, Milano.

Gestione dell'emergenza Covid-19: dalla teoria all'analisi. Il caso Bergamo

DAISY MARCOLONGO

Daisy Marcolongo, 24 anni, laurea magistrale in Politiche Pubbliche, indirizzo Politiche per la sicurezza presso l'Università Cattolica di Milano. Attualmente lavora in ambito cybersecurity presso una società di consulenza a Milano. Dal 2017 ricopre la carica di Assessore Comunale presso il comune di Brembate di Sopra in provincia di Bergamo e si occupa principalmente di commercio e attività produttive.

Abstract

L'intento dell'elaborato è quello di analizzare, dal punto di vista organizzativo e comunicativo, la gestione dell'emergenza Covid-19 in Italia, rivolgendo un'attenzione particolare alla provincia di Bergamo. Al fine di raggiungere tale intento sono stati utilizzati due strumenti di ricerca: l'intervista semi-strutturata ad amministratori locali, Protezione civile e volontari e il questionario strutturato alla popolazione. Dallo studio in profondità è emersa l'incredibile capacità degli enti locali e dei volontari di organizzarsi per fronteggiare l'emergenza senza indicazioni precise e in assenza di dispositivi di protezione, utilizzando conoscenze pregresse e piani di prevenzione non aggiornati. La gestione dell'emergenza in Italia è stata caratterizzata da un susseguirsi di DPCM e ordinanze regionali che hanno regolato il comportamento dei cittadini e l'apertura o chiusura di esercizi commerciali, luoghi di ritrovo e centri sportivi. Inizialmente le misure sono state accolte in modo favorevole dalla popolazione, tuttavia, sono emerse serie difficoltà di gestione della comunicazione; infatti, si evidenzia un uso scorretto dei canali social ufficiali del governo utilizzati per diffondere, anticipatamente e senza un'adeguata analisi comunicativa, notizie contenute in documenti ufficiali, aumentando incertezza tra popolazione e amministratori locali.

Keywords

Covid-19, crisis management, Bergamo

1. Emergenza Covid-19: questioni generali

Definire il concetto di emergenza non è cosa semplice, il dibattito attorno a questo termine è tuttora in corso e nel colloquio informale è spesso asso-

ciato ai termini disastro e crisi¹; tuttavia, gli studiosi europei prediligono identificare l'emergenza con un input stressante in un sistema, che lo costringe a reagire per ritornare allo stato iniziale di equilibrio (De Vincentiis 2010). La probabilità che un evento, spesso definito come pericolo², produca un'emergenza è definita rischio, ossia il potenziale danno causato dalla minaccia (Michael J. Fagel e Jennifer Hesterman 2017). Un altro elemento fondamentale da considerare durante la gestione di un'emergenza è il rapporto tra le istituzioni e la popolazione: è essenziale per le istituzioni mantenere solida la fiducia con la popolazione durante la gestione dell'emergenza, affinché la crisi emergenziale non si traduca in disordine sociale³. Inoltre l'impatto della crisi e l'esito del disastro potrebbero stravolgere le relazioni sociali e il contesto politico, economico e sociale (Lucini 2014). Tuttavia, gli effetti di una crisi sono già contenuti nel sistema che viene colpito, per questo motivo la prevenzione rappresenta l'attività adatta per ridurre i rischi connessi agli eventi generatori di crisi (Lombardi 2005). I diversi tipi di attività definiti per rispondere a una crisi sono determinati in relazione ad uno specifico modello di organizzazione e interpretazione, devono essere adatti a ridurre la vulnerabilità⁴ del sistema e aumentare la conoscenza della comunità. L'emergenza è parte integrante della società attuale, quasi da essere considerata normalità (Beck 2000), ed è per questo motivo che gli strumenti del diritto si adattano a questa concezione di società del rischio in cui l'emergenza non è un evento patologico ma diviene elemento fisiologico. Negli ultimi anni abbiamo assistito ad una proliferazione di norme che cercano di prevenire i pericoli insiti nella società e che individuano il rischio non più come una concezione individuale ma come una concezione sociale (Fioritto 2008).

L'epidemia Covid-19 è dichiarata emergenza di sanità pubblica di rilevanza internazionale il 30 gennaio 2020 dall'Organizzazione mondiale della sanità. A seguito di questa dichiarazione e del diffondersi dell'epidemia anche in Italia, il 31 gennaio 2020 il Consiglio dei Ministri delibera lo stato di emergenza per la durata di sei mesi, fino al 31 luglio 2020, instaurando il peculiare regime derogatorio contenuto nel codice di Protezione civile del 2018 (Trombetta 2020). L'ordinamento italiano è caratterizzato da un fenomeno detto "dilatazione dell'emergenza" secondo cui gli stati di emergenza vengo-

¹ Il concetto di crisi è caratterizzato da tre condizioni: una sorpresa per i responsabili delle decisioni, una minaccia per gli obiettivi ad alta priorità e un tempo limitato a disposizione per la risposta (Hermann 1972).

² Il pericolo è definito come una caratteristica di un sistema che è in grado di produrre un danno all'interno di quel sistema (De Vincentiis 2010).

³ Fase durante la quale le istituzioni consolidate perdono la loro influenza (Almond, Flanagan, e Mundt 1973).

⁴ Predisposizione ad essere colpiti da un evento.

no continuamente prorogati al fine di mantenere la dilatazione dei poteri del governo, ed è proprio a causa di questa sua natura fortemente derogatoria che il diritto di emergenza si pone spesso in contrasto con i principi costituzionali (Bartolomei 1979).

Il primo caso di Covid-19 in Italia è stato confermato nella tarda notte del 20 febbraio 2020 in Regione Lombardia, il paziente denominato “paziente zero” era un uomo di 38 anni, ricoverato all’Ospedale di Codogno, con una lieve polmonite resistente alle terapie, la particolarità di questo paziente era che non aveva intrapreso nessun viaggio in Cina e che non aveva avuto nessun apparente contatto con persone contagiate. Tra il 20 e il 21 febbraio il Ministro della Salute emana due ordinanze. La prima ordinanza disponeva la sospensione di tutte le attività lavorative, sociali e ludiche nei comuni colpiti dal contagio, mentre la seconda disponeva di applicare la misura della quarantena per quattordici giorni a tutti coloro che avessero avuto contatti con persone infette e imponeva a tutti gli individui che avessero fatto rientro in Italia da una delle zone della Cina colpite dall’epidemia, di segnalare il rientro alle autorità sanitarie competenti. Il Governo costruisce un nuovo percorso normativo basato su una logica di accentramento e speditezza (Cavino 2020) e l’asse della legislazione si sposta su una logica di decreti d’urgenza (Trombetta 2020). La Protezione civile è materia concorrente Stato-Regioni, ma durante un’emergenza si tende ad un accentramento istituzionale e normativo e una verticalizzazione dei rapporti tra gli organi costituzionali (Boggero 2020). Durante l’emergenza Covid-19 questo aspetto è confermato dalla scelta di agire tramite DPCM, i quali rendono illegittime tutte le ordinanze emanate da autorità diverse dal Presidente del Consiglio dei Ministri e adottate dopo l’entrata in vigore del DPCM. Laddove la norma regionale non sia contrastante con quella del DPCM, ma sia soltanto più restrittiva, trova applicazione il principio di specialità (Boggero 2020), secondo cui la legge speciale deroga quella generale, anche se successiva.

2. La risposta organizzativa

La risposta organizzativa inizia dalla conoscenza del territorio e delle soglie di pericolo stabilite in relazione ai vari rischi che insistono su quest’ultimo. La conoscenza è alla base delle attività di previsione necessarie per definire gli stati di attivazione per i rischi prevedibili, che comprendono le attività di attenzione, preallarme e allarme. Ad ognuna di queste attività corrispondono determinate procedure nella pianificazione di emergenza. Attraverso due documenti denominati “COVID-19 strategic preparedness and response

⁵ Il primo paziente individuato nel campione della popolazione di un’indagine epidemiologica.

plan operational planning guidelines to support country preparedness and response” (SPRP) pubblicato a febbraio 2020 e “2019 Novel coronavirus (2019 nCoV): strategic preparedness and response plan” aggiornato ad aprile 2020, l’OMS identifica gli 8 pilastri strategici che costituiscono la strategia chiave nella risposta alla pandemia Covid-19. L’Italia nell’organizzazione della propria risposta all’epidemia ha seguito le indicazioni contenute negli 8 pilastri definiti dall’OMS, dimostrando un elevato livello di preparedness (Ministero della Salute 2020). Per quanto concerne il primo pilastro, denominato “Coordinamento nazionale, pianificazione, e monitoraggio”, durante il periodo di transizione epidemica in Italia rimangono attivi tutti i meccanismi di coordinamento e di interfaccia multisettoriale e interistituzionale necessari per la promulgazione di atti di programmazione nazionale, nonché la redazione di documenti di policy riguardanti organizzazione, pianificazione e indirizzo tecnico-scientifico. Il coordinamento tra il livello nazionale e il livello regionale è oggetto di continui monitoraggi. Inoltre, l’ISS⁶, in coordinamento con il Ministero della Salute, ha implementato un sistema di monitoraggio settimanale per la classificazione quantitativa del rischio e della resilienza dei sistemi assistenziali e territoriali a livello regionale.

Per quanto concerne il pilastro 3 relativo a “sorveglianza, team di risposta rapida, indagine sui casi” si fa riferimento all’ordinanza n. 640 della Presidenza del Consiglio dei Ministri Dipartimento della Protezione civile del 27 febbraio 2020 che istituisce l’attività del sistema di sorveglianza integrata epidemiologica e microbiologica Covid-19 coordinata dall’ISS. Queste attività di identificazione e gestione dei contatti dei casi probabili o confermati di Covid-19 sono fondamentali al fine di interrompere le catene di trasmissione del virus, intervenendo tramite quarantena e sorveglianza attiva. L’identificazione e la gestione dei contatti stretti è stata svolta a livello locale dalle autorità sanitarie territoriali. Prevalentemente sono state svolte tre tipologie di attività: richiesta delle liste dei passeggeri di aerei, navi, pullman e treni, con identificazione dei contatti stretti dei passeggeri e la comunicazione delle loro informazioni personali, segnalazione di individui positivi al virus alle autorità sanitarie regionali per l’attivazione della sorveglianza sanitaria ed infine scambi di messaggi selettivi tra i Paesi europei ed extraeuropei.

Il pilastro numero 6 denominato “Infection prevention and control (IPC)” comprende tutte le attività di aggiornamento dei documenti tecnici a supporto delle attività di prevenzione e di controllo delle infezioni. L’aggiornamento riguarda principalmente i riferimenti normativi e le informazioni sulle conoscenze scientifiche disponibili in quel settore. Gli strumenti maggiormente utilizzati sono stati le circolari del Ministero della Salute, i rapporti

⁶ Istituto Superiore di Sanità.

ISS Covid-19, i documenti tecnici INAIL ed infine i documenti del CTS e Regionali. Le indicazioni sulla gestione della quarantena e dell'isolamento domiciliare, l'uso dei dispositivi di protezione nelle attività assistenziali, la gestione degli ambienti indoor e delle attività socioassistenziali e la sanificazione degli ambienti sono state aggiornate continuamente (Cicchetti, Basile, e Di Brino 2020). Uno dei capisaldi della strategia di contenimento della circolazione del virus nella popolazione generale è stato l'obbligo di utilizzo di mascherine per la protezione delle vie respiratorie in tutti gli ambienti chiusi e anche all'aperto quando non sia possibile mantenere la distanza di un metro fra le persone. Attività compresa nel pilastro numero 6 a supporto della prevenzione e del controllo delle infezioni è stata la formazione continua degli operatori sanitari attraverso corsi FAD e materiali formativi.

In riferimento al pilastro 8, denominato "Supporto operativo e logistica", sono state potenziate le strutture di terapia intensiva e sub-intensiva attraverso le disposizioni contenute nel Decreto Rilancio. Per poter attuare questo potenziamento sono stati effettuati lavori infrastrutturali di adeguamento dei presidi ospedalieri e un aggiornamento delle apparecchiature necessarie ad attrezzare i posti letto. Per quanto riguarda l'approvvigionamento di dispositivi di protezione, il Commissario ne assicura quotidianamente a titolo gratuito alle Regioni e alle Province autonome la fornitura, secondo i fabbisogni indicati bisettimanalmente dalle amministrazioni. Per quanto riguarda il potenziamento del personale nel settore sanitario, il governo ha introdotto procedure semplificate di reclutamento, aprendo bandi per profili specifici e consentendo alle ASL regionali e locali di aprire propri bandi di reclutamento in relazione alle proprie esigenze.

3. La comunicazione nella gestione dell'emergenza

La gestione della comunicazione in emergenza è cruciale, sia in termini di informazione che formazione. Nel primo caso si tratta dell'informazione veicolata dai media, la quale viene catalogata come risposta alla crisi in corso. Questa tipologia di comunicazione è fondamentale sia per quanto concerne la ricerca, sia per quanto concerne le strategie operative a livello istituzionale. D'altro canto, quando si fa riferimento alla formazione si intende l'azione pro-attiva e preventiva, ossia la strategia da mettere in atto per sviluppare una sub-cultura del rischio e ridurre la vulnerabilità sistemica (Lombardi 2005). Nelle situazioni di crisi l'opinione pubblica è creata dai media, i quali spostano le tendenze e mutano le opinioni dei cittadini (Mauro Wolf 1992) tramite la pubblicazione e la non pubblicazione delle notizie. La selezione delle notizie avviene tramite la funzione di agenda setting, ossia la definizione di una gerarchia di informazioni che devono

essere pubblicate e la conseguente strategia di comunicazione (Lombardi 2005). Una funzione fondamentale è svolta dagli opinion leaders (Dawkins 2004), coloro che possiedono potere di influenza e rilanciando messaggi da loro interpretati, influenzano interi gruppi sociali, svolgendo il ruolo di mediatori tra i media e i cittadini. Per questo motivo le campagne informative devono essere formulate in relazione alla popolazione, non esiste una campagna informativa universale e adattabile a tutti gli scenari (Axjonow, Ernstberger, e Pott 2018).

L'attività di pianificazione è presente anche nell'ambito della comunicazione, permette di normalizzare la gestione e il controllo della crisi tramite un approccio proattivo. Nel momento in cui avviene un evento critico non è possibile pianificare ed organizzare per mancanza di tempo, per questo motivo è fondamentale avere un piano di comunicazione già predisposto in caso di emergenza. Il piano di comunicazione ha l'obiettivo di creare fiducia e credibilità nella popolazione, bisogna dimostrare empatia nei confronti della popolazione, competenza, esperienza, prontezza e dedizione (Reynolds e Seeger 2005). Il pilastro strategico OMS che fa riferimento al tema della comunicazione è il pilastro numero 2, definito "Comunicazione del rischio e coinvolgimento della popolazione". Le attività di comunicazione sviluppate durante la fase di transizione, perseguono l'obiettivo di promuovere azioni volte al contenimento dell'epidemia. Nella prima fase emergenziale viene attivato il meccanismo di coordinamento RCCE⁷, il quale rimarrà attivo anche nelle fasi successive dell'emergenza, e il Gruppo di comunicazione composto dall'Ufficio Stampa, il Servizio Comunicazione scientifica e alcuni esperti di riferimento. Nella fase autunnale, le istituzioni, attraverso una comunicazione organizzata, continuano a garantire la produzione costante di contenuti finalizzati ad accrescere la consapevolezza della popolazione, soprattutto in contrasto alla diffusione di fake news⁸ attraverso i principali canali istituzionali, comunicati stampa, social, infografiche e con la creazione di un'apposita sezione sul sito del Ministero della Salute⁹. Le istituzioni si impegnano inoltre a fornire i dati della sorveglianza e i dati sulla situazione epidemiologica attraverso i canali social e il web.

Per poter meglio organizzare la comunicazione in emergenza è necessario che le istituzioni definiscano un portavoce istituzionale, nel caso dell'emergenza Covid-19 è individuato all'interno del CTS¹⁰, con ordinanza n. 663 del

⁷ Risk Communication and Community Engagement.

⁸ Notizie false che creano disinformazione.

⁹ <https://www.salute.gov.it/portale/nuovocoronavirus/archivioFakeNewsNuovoCoronavirus.jsp>

¹⁰ Comitato Tecnico Scientifico.

18 aprile 2020¹¹, il prof. Silvio Brusaferrò, presidente dell'Istituto superiore di sanità. Il responsabile della comunicazione si assume la responsabilità di dimostrare serietà nelle proprie comunicazioni e riconoscere il problema senza nasconderselo. Inoltre deve essere in grado di assumersi la responsabilità delle cattive notizie, senza attendere la fine della crisi per poter comunicare e dare risposte certe (Lagadec 1994). È difficile ottenere una comunicazione efficace durante emergenze sanitarie di questo tipo, si evidenziano infatti due profonde carenze nella gestione della comunicazione durante la crisi. La prima carenza relativa alla differenza temporale tra la divulgazione del messaggio istituzionale e del messaggio a mezzo stampa, la seconda relativa alla scelta di utilizzare social media come mezzo di comunicazione per trasmettere i discorsi ufficiali del Presidente del Consiglio.

4. Caso Studio: Bergamo

La data chiave dello scoppio dell'epidemia nella provincia di Bergamo è il 23 febbraio 2020, giorno nel quale vengono diagnosticati i primi due casi di Covid-19 della Bergamasca: due pazienti dell'ospedale Pesenti Fenaroli di Alzano Lombardo (Valseriana News 2020b). Dal momento in cui emerge la positività di un paziente nell'ospedale di Alzano vengono effettuati tamponi sul personale sanitario entrato in contatto con i pazienti positivi, molti di loro risultano affetti da Covid-19, anche se asintomatici. Nei giorni successivi le disposizioni cambiano e vengono sottoposti a tampone solo le persone con sintomi. Inizialmente nessuno dei pazienti ricoverati all'ospedale di Alzano Lombardo e affetti da polmoniti interstiziali, viene sottoposto a tampone molecolare perché non sussistono le condizioni per la definizione di "caso sospetto"¹² (Valseriana News 2020a). La mancata diagnosi di positività tra i pazienti di Alzano causa il propagarsi dell'infezione tra pazienti e operatori sanitari. Un primo errore di gestione emerge dalle indicazioni date ai dipendenti dell'ospedale di Alzano la sera del 23 febbraio: gli operatori sanitari e i pazienti transitati nell'ospedale sono ritornati dalle loro famiglie senza precauzioni e senza aver effettuato tamponi, con il rischio di trasmettere l'infezione ai famigliari. Il pronto soccorso dell'ospedale di Alzano viene chiuso domenica 23 febbraio su ordine del direttore medico Giuseppe Marzulli, tut-

¹¹ Ordinanza n. 633, 18 aprile 2020, Ulteriori interventi urgenti di Protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili.

¹² La circolare del Ministero della Salute del 27 gennaio 2020 definisce caso sospetto colui che è stato in Cina nei 14 giorni precedenti l'insorgenza di sintomi o è stato a contatto con pazienti Covid.

tavia la chiusura ha una durata di poche ore e il pronto soccorso viene riaperto senza effettuare le giuste attività di sanificazione. Emerge la mancata applicazione dei protocolli base per la gestione di casi Covid-19 accertati, come isolare il paziente positivo, testare i contatti stretti e tracciare i futuri contatti. Inoltre, a seguito della decisione di riaprire l'ospedale di Alzano, non vengono predefiniti dei percorsi differenziati di sicurezza per distinguere i pazienti con sintomatologia Covid-19 dai pazienti con altre malattie. Inoltre, sono stati utilizzati dispositivi di protezione individuale incompleti e inadeguati, non garantendo la giusta protezione al personale sanitario a contatto con i pazienti positivi. Nell'ospedale di Alzano viene dato l'ordine di utilizzare i dispositivi di protezione contenuti nelle colonnine antincendio (Nava 2020) data la carenza di mascherine chirurgiche. Le tute di bio-contenimento erano scarse e nonostante fossero monouso venivano sanificate all'interno delle ambulanze per essere riutilizzate più volte.

Con il DPCM del primo marzo l'Italia viene divisa in tre zone, la zona rossa, nella quale si applicano misure di massimo contenimento, la zona arancione, in cui si applicano misure di contenimento minori, ed infine la zona gialla nazionale dove si applicano misure di informazione e prevenzione. Il 2 marzo l'Istituto Superiore di Sanità invia una nota riservata al governo per richiedere la chiusura dei comuni di Alzano e Nembro includendoli nella zona rossa, a causa dell'alta incidenza di casi e per la vicinanza alla città di Bergamo. La richiesta non viene accolta, tuttavia il 4 marzo viene adottato un DPCM che introduce ulteriori misure per contrastare la diffusione del virus a livello nazionale: vengono sospese tutte le attività didattiche nelle scuole e nelle università. Il 5 marzo presso l'Hotel Continental di Osio Sotto si trovano i militari del III Battaglione Lombardia dell'Arma dei Carabinieri che attendono indicazioni per la creazione della zona rossa nei comuni di Alzano e Nembro. Tuttavia, alle 21:30 ricevono l'ordine di rientrare, di non istituire la zona rossa, ma di rimanere pronti per la mattina successiva. Il giorno dopo altri quattrocento uomini raggiungono Bergamo ma rimangono inattivi fino al 9 marzo, giorno in cui viene creata la zona arancione in tutta Lombardia. L'11 marzo tutta l'Italia è in quarantena, inizia il primo lockdown nazionale e gli ospedali della provincia di Bergamo si trovano in grave sofferenza. La maggior parte dei cittadini che chiedono soccorso vengono trasportati con le ambulanze all'Ospedale Papa Giovanni XXIII di Bergamo. L'unità di malattie infettive dell'ospedale viene riconfigurata per trattare solo i pazienti con Covid-19, e gli altri pazienti vengono ridistribuiti in tutto l'ospedale o, quando possibile, vengono dimessi. Il 28 marzo l'unità di terapia intensiva decide di bloccare gli ingressi ai pazienti di età superiore ai 70 anni (Walker e Maremont 2020). Vengono organizzati corsi di formazione per il personale sanitario che viene ricollocato in reparti Covid-19: in una settimana vengo-

no formati più di 1500 operatori. Tutti gli interventi chirurgici non urgenti, compresi quasi tutti i trapianti, vengono sospesi mentre rimangono aperti gli ambulatori per le urgenze e le prestazioni ambulatoriali non differibili. Il 18 marzo i morti sono così tanti che il crematorio di Bergamo non riesce a sostenere i ritmi, per cremare un uomo ci vogliono circa 10 giorni e le scorte di urne funerarie sono terminate. Le bare rimangono nelle case e negli ospedali per giorni e nei cimiteri vengono accatastate in attesa delle funzioni. In un mese e mezzo a Bergamo muoiono 6 mila persone a causa del Covid-19 e in alcuni paesi il tasso di mortalità incrementa del duemila per cento rispetto all'anno precedente. È sempre il 18 marzo la data che segna la città di Bergamo, con l'immagine dei trenta camion militari che trasportano 65 bare fuori regione, perché a Bergamo non possono essere smaltite. Il 25 marzo 2020 l'Associazione Nazionale Alpini inizia la costruzione dell'Ospedale da campo in Fiera a Bergamo, 1.127 volontari tra alpini, artigiani e imprenditori bergamaschi lavorarono ininterrottamente riuscendo a rendere attivo l'ospedale il 6 aprile, con 40 posti letto. Alla data dell'8 aprile, pur avendo attivato nuovi posti letto in terapia intensiva, la Lombardia si trova in una situazione di saturazione delle terapie intensive, dovendo ricorrere al trasferimento dei pazienti in altre Regioni o all'estero. Solo a partire dal mese di maggio 2020 gli ospedali di Bergamo riescono a gestire i pazienti positivi in entrata, le ambulanze riescono a trasportare tutti e nessun sospetto Covid-19 viene lasciato a casa o nelle RSA (Bianco 2020). Con l'arrivo della stagione autunnale il numero di positivi torna a salire, costringendo, il 2 novembre 2020, la riapertura dell'ospedale da campo in Fiera a Bergamo (Ufficio Comunicazione ASST Papa Giovanni XXIII 2020) non solo per ospitare pazienti bergamaschi ma pazienti provenienti da tutta la Lombardia.

Al fine di esplorare in profondità i sentimenti, i pensieri e le osservazioni di chi ha vissuto in prima persona la gestione dell'emergenza Covid-19 nella provincia di Bergamo, viene effettuata una ricerca tramite due strumenti: l'intervista semi-strutturata, che permette di effettuare un'analisi in profondità modificando le domande in relazione alle esigenze che emergono nel corso dell'intervista e il questionario ai cittadini, lo strumento più adatto per analizzare la percezione dell'organizzazione e della comunicazione durante l'emergenza Covid-19. I soggetti coinvolti nell'intervista ricoprono ruoli chiave nella gestione dell'emergenza, si tratta di volontari della Protezione civile, volontari della Croce Rossa italiana, operatori sanitari, tecnici di laboratorio e amministratori locali e regionali. Per questa analisi sono state intervistate 25 persone, tra cui 15 amministratori di enti locali (4 donne, 11 uomini) due dei quali volontari in Protezione civile, 7 operatori sanitari (5 donne e 2 uomini), uno dei quali volontario in Croce Rossa e 3 volontari della Protezione civile (3 uomini). Il questionario anonimo si compone di quattro sezioni,

la prima dedicata ad alcune domande generali relative alla demografia dei soggetti che hanno aderito all'analisi, la seconda relativa al concetto generale di emergenza Covid-19 e le modalità di prevenzione del contagio e la terza dedicata alla comunicazione durante l'emergenza. Infine, l'ultima sezione è relativa alle esperienze personali, con domande aperte che lasciano spazio a racconti di esperienze di vita. Sono 80 i cittadini bergamaschi che hanno aderito all'analisi, il campione ha un'età media di 37 anni, con un'età minima di 16 anni e un'età massima di 66 anni.

Dallo studio in profondità emerge una buona conoscenza, da parte della maggioranza del campione, del concetto di emergenza. I sentimenti scaturiti a seguito dell'insorgere della crisi pandemica hanno permesso di associare il termine emergenza alla rottura della routine quotidiana, anche De Vincenziis (2010) lo aveva definito in questo modo. Per meglio gestire e contenere la crisi, alcuni amministratori locali e volontari di Protezione civile sottolineano la necessità di conoscere a fondo il territorio, restando in linea con le direttive di Protezione civile e Regione Lombardia. Tuttavia, la tecnica che ha fatto da padrona è stata l'improvvisazione, tanto che la maggior parte degli amministratori, operatori sanitari e volontari dichiarano di non aver ricevuto indicazioni chiare, ma di aver improvvisato per poter dare una risposta il più rapida possibile. Per rispondere ad una crisi possono essere utilizzate procedure previste o improvvisate: a Bergamo le procedure improvvisate sono state la maggioranza, a partire da chi ha deciso di procurarsi tamponi autonomamente per le proprie RSA, a chi ha consegnato spesa, pasti e bombole di ossigeno ad ogni cittadino. A Bergamo si è creata una subcultura dell'emergenza, la popolazione, le amministrazioni locali, i volontari di Protezione civile e gli operatori sanitari hanno risposto all'emergenza facendo fede alla propria conoscenza e preparazione, affrontando un evento raro senza precedenti e indefinibile dal punto di vista cognitivo. Il bisogno informativo è stato colmato da conoscenze già in possesso da volontari ed amministratori, le risposte non sono arrivate dagli organi competenti. Tuttavia, gli amministratori locali sottolineano come da Regione Lombardia e dal Governo siano arrivate risorse specifiche per questa emergenza, per aiutare la popolazione in difficoltà attraverso la distribuzione di buoni pasto all'inizio, e sostegno economico per la ripresa delle attività in seguito. La maggior parte del campione intervistato afferma che, con il senno del poi, a Bergamo si è fatto il possibile per fronteggiare la crisi, utilizzando tutte le risorse a disposizione e impiegando ogni mezzo disponibile. Il pericolo è individuato dagli intervistati nell'assenza di prevenzione e organizzazione, che si traduce sul lato pratico nella mancanza di un piano pandemico aggiornato. Anche all'interno degli ospedali, i piani di emergenza applicati non sono stati del tutto funzionali: si evidenziano mancanze nell'organizzazione dei percorsi di accesso agli ambulatori, con

percorsi “puliti” e percorsi “sporchi” che si sovrappongono. L'assenza di dispositivi di protezione sufficienti anche all'interno delle ambulanze ha impedito agli operatori di lavorare in sicurezza, portandoli a rischiare la vita ad ogni turno. Dall'analisi emerge che la fiducia nelle istituzioni durante l'emergenza Covid-19 è pressoché rimasta invariata, il campione ritiene che le istituzioni abbiano fatto tutto il possibile per sostenere le amministrazioni locali e i volontari durante l'emergenza, anche con risorse limitate. Tuttavia, l'impatto della crisi ha interferito nella fiducia nella politica, la quale non ha saputo dare risposte univoche e chiare a chi le richiedeva. La popolazione non ha ritenuto adeguate alcune scelte, legate ad influenze politiche ed effettuate solo con lo scopo di mantenere uno status quo all'interno del sistema geopolitico internazionale. Gli effetti della crisi sono già contenuti nel sistema che viene colpito; infatti, molti degli intervistati che affermano di non avere fiducia nelle istituzioni sottolineano di non averla mai avuta, evidenziando un sentimento già diffuso all'interno della popolazione.

Per quanto riguarda la comunicazione, volontari, amministratori locali e operatori sanitari hanno individuato autonomamente un portavoce di fiducia che rispondeva alle domande e comunicasse le informazioni utili per attuare le giuste azioni durante l'emergenza. Le informazioni fornite dal governo e dall'OMS erano spesso contrastanti, se non assenti, e i volontari e amministratori locali attivi sul territorio hanno preferito affidarsi a persone fidate per ottenere le giuste informazioni. La comunicazione da parte dei media, secondo il campione, ha rappresentato la realtà dei fatti: a Bergamo il terrorismo attuato dai media non è stata un'interpretazione esagerata della realtà, ma una rappresentazione di quello che gli operatori sanitari vivevano stando in corsia. Tuttavia, i media hanno interferito con la comunicazione istituzionale, anticipando informazioni e rendendo difficoltoso il lavoro degli amministratori locali, diventati punto di riferimento per i cittadini. Le informazioni dovevano provenire da un'unica fonte, piuttosto che da diverse e dovevano utilizzare codici linguistici e narrativi precisi, piuttosto che una semplice riproduzione dell'informazione.

Se da un lato i volontari, gli operatori sanitari e gli amministratori locali hanno ritenuto corrette le misure di restrizione della circolazione delle persone adottate, la maggioranza dei cittadini compresi nel campione le ha ritenute adeguate solo in parte. Emerge la discordanza tra chi ha vissuto l'emergenza dal punto di vista dell'azione e chi ha subito le decisioni prese, senza comprendere fino in fondo la realtà dei fatti. I cittadini mostrano una percezione positiva riguardo all'applicazione delle misure di prevenzione della trasmissione del virus, come lavarsi le mani ed indossare dispositivi di protezione, i fattori sociali potrebbero influenzare la percezione del rischio e

i comportamenti adottati durante le emergenze, infatti, una percezione più elevata del rischio è stata riscontrata in coloro che hanno contratto il virus.

5. Un nuovo modello di Crisis management

Dal momento in cui le crisi seppur attese sono imprevedibili (Borell e Eriksson 2013), è difficile individuare uno specifico modello di crisis management per una futura crisi pandemica, non conoscendo le caratteristiche del virus le azioni di prevenzione e gestione dell'emergenza possono solo essere ipotizzate. Le azioni di prevenzione devono essere svolte prima del "momento zero"; ad esempio, l'attuazione di corsi di aggiornamento al personale sanitario, l'individuazione di un team per la gestione della comunicazione in fase di emergenza e la creazione di corretti canali di informazione al fine di istruire la popolazione sui comportamenti da attuare in caso di positività. La popolazione non è stata correttamente istruita sull'isolamento domiciliare, spesso le persone in quarantena condividevano stanze con altri componenti della famiglia rischiando di trasmettere il virus. In mancanza di ospedali da campo dove poter isolare i soggetti positivi, l'isolamento domiciliare è stata l'unica soluzione, ma non è sempre stata attuata nel modo corretto. Il tasso di propagazione del virus è molto elevato all'interno delle abitazioni e gli operatori sanitari sono stati il veicolo di contagio maggiore all'interno delle famiglie (Bianco 2020). Dal punto di vista organizzativo, è necessario dotare gli ospedali di tamponi, al fine di eseguire uno screening rapido su pazienti e personale sanitario e isolare la malattia all'interno delle strutture, evitando il trasferimento all'esterno. A tal fine, sarebbe opportuno costruire degli ospedali da campo dove trasferire i pazienti positivi, per garantire il giusto isolamento. Inoltre, l'assenza di materiale e dispositivi di protezione non è stata gestita fin da subito, dovevano essere predisposti bandi per l'acquisizione di materiale. Diversi fattori hanno influenzato la diffusione dell'epidemia nella provincia di Bergamo, come l'età media della popolazione superiore alla media nazionale e l'alto tasso di industrializzazione della provincia, motivo per cui in ottica di prevenzione è necessario analizzare il territorio e strutturare un piano di emergenza in relazione alle caratteristiche della popolazione.

Per le attività di soccorso, l'isolamento è fondamentale, allestire un'area di quarantena intorno all'epicentro del focolaio svolge un ruolo essenziale nel controllo dell'infezione. Mettendo a confronto la velocità di risposta dell'Italia e della Cina dopo la scoperta del cinquantesimo caso di Covid-19, emerge che l'Italia ha applicato le misure di chiusura delle attività e di isolamento della popolazione due settimane dopo rispetto al paese asiatico. Da alcuni studi emerge che imporre un blocco nel nord Italia con due settimane di anticipo probabilmente avrebbe garantito una minore diffusione dell'epide-

mia. Partendo dall'analisi delle criticità del territorio si evidenzia una carenza di personale medico all'interno delle strutture, una carenza di dispositivi di protezione e tamponi per l'individuazione dell'infezione. È necessario intervenire su questi aspetti, migliorando le forniture negli ospedali e nelle RSA, rivedendo i piani di emergenza all'interno delle strutture, prevedendo percorsi separati per l'isolamento dei pazienti risultati positivi al virus. Infine, introdurre l'utilizzo della telemedicina e del telefono (Senni 2020) per velocizzare le pratiche non urgenti.

Di seguito si ha l'attività di recupero, nella quale emerge la capacità di resilienza del territorio. Dopo una crisi pandemica è necessario ristabilire la routine all'interno delle strutture ospedaliere, rimuovendo la distinzione fra reparti "puliti" e "sporchi". Se necessario, introdurre percorsi di sostegno agli operatori sanitari che hanno lavorato durante l'emergenza e hanno sofferto sia fisicamente sia psicologicamente. Dal punto di vista della popolazione, il governo deve erogare sussidi a coloro che non hanno potuto svolgere il proprio lavoro e sostenere le famiglie in difficoltà economica, oltre che riorganizzare il rientro nelle scuole per bambini e ragazzi a seguito di un periodo di didattica a distanza. Ritornare alle proprie abitudini pre-emergenza non è immediato e ogni cittadino trascorrerà un periodo di transizione durante il quale ripercorrerà cognitivamente le fasi appena vissute, prima di interiorizzarle e superarle. Questa fase può anche essere definita decompressione emotiva (De Vincentiis 2010) ed ha l'obiettivo di legittimare e normalizzare gli stati interni personali.

6. Conclusioni

L'emergenza Covid-19 ha colpito ogni paese e ogni parte del mondo, per questo motivo affrontare il rischio di future pandemie richiede uno sforzo globale (Daszak, Olival, e Li 2020), non è possibile immaginare un piano di emergenza pandemica ridotto ad un singolo Stato. Oggi viviamo in un mondo globalizzato, dove persone e merci si spostano continuamente tenendo in continua connessione ogni parte del pianeta. Il focolaio Covid-19 originario della Cina era significativamente collegato al mercato di fauna selvatica nel paese: un primo obiettivo globale è quello di attivare dei programmi di controllo e prevenzione nei mercati animali per future epidemie e pandemie. È importante sottolineare che il driver della malattia tra gli Stati è stato lo spostamento di persone, che espandendo le proprie attività su scala globale hanno la necessità di spostarsi nel mondo (Casti e Adobati 2020).

Sul piano della legislazione, occorre riorganizzare il sistema statale, stabilendo una forma di governo stabile che sia in grado di gestire una crisi pandemica senza innescare crisi parlamentari e politiche. L'emergenza Co-

vid-19 ha fatto emergere una leadership non continuativa e non focalizzata sui principi di crisis management. È necessario riflettere sul modello parlamentare tradizionale e sulla sua praticabilità in situazioni di emergenza (Louvin 2020), il principio di tutela della salute ha legittimato provvedimenti contingibili e urgenti, tuttavia la legge non definisce precisamente i contorni di questi provvedimenti stabilendo debbano essere adottati con nesso di congruità e in proporzione fra le misure adottate e la qualità e natura degli eventi. Lo stato di emergenza non può avere una durata indefinita e non deve ledere i diritti dei cittadini, occorre una riflessione sulle previsioni costituzionali e una possibile rivisitazione della norma (Nicotra 2020).

Dal punto di vista sanitario, legge regionale del 14 dicembre 2021, n. 22¹³ ha apportato alcune modifiche al sistema, potenziando la medicina territoriale, la prevenzione e l'Assistenza Domiciliare Integrata (ADI). Anche a livello nazionale devono essere ridefinite le dimensioni delle ASST, al fine di renderle maggiormente funzionali ed efficienti nell'erogazione dei servizi. Per quanto riguarda il sistema di Protezione civile e i piani di emergenza, sono già state messe in atto alcune modifiche riguardanti la predisposizione dei piani ai diversi livelli territoriali tramite la direttiva del Presidente del Consiglio dei Ministri del 30 aprile 2021¹⁴. La direttiva suggerisce l'individuazione di ambiti composti da un insieme di Comuni limitrofi che cooperano tra loro e nei quali le attività di riduzione del rischio possono essere esercitate in modo unitario.

Durante l'emergenza bisogna agire, l'attività di preparazione deve avvenire necessariamente prima dello scoppio della crisi: in Italia è stato il virus Covid-19 a dominare l'emergenza. Volontari, amministratori locali e operatori sanitari sono stati travolti dagli eventi, comandati da un agente sconosciuto, e hanno dovuto rispondere all'emergenza improvvisando, organizzandosi al meglio con le risorse a disposizione e seguendo le direttive di piani di prevenzione non aggiornati.

Bibliografia

- Almond, Gabriel A, Scott C Flanagan, e Robert J Mundt. 1973. *Crisis, Choice, and Change; Historical Studies of Political Development*. Boston: Little, Brown.
- Axjonow, Anastasia, Jürgen Ernstberger, e Christiane Pott. 2018. «The Impact of Corporate Social Responsibility Disclosure on Corporate Reputation: A Non-

¹³ Legge regionale 14 dicembre 2021, n. 22 “Modifiche al Titolo I e al Titolo VII della legge regionale 30 dicembre 2009, n. 33 (Testo unico delle leggi regionali in materia di sanità)”

¹⁴ Direttiva del Presidente del Consiglio dei Ministri, 30 aprile 2021, Indirizzi per la predisposizione dei piani di protezione civile ai diversi livelli territoriali.

- Professional Stakeholder Perspective». *Journal of Business Ethics* 151 (2): 429-450. <https://doi.org/10.1007/s10551-016-3225-4>.
- Bartolomei, Franco. 1979. *Potere di ordinanza e ordinanze di necessità*. Milano: Giuffrè. <http://www.libreriantiquaria.com/it>.
- Beck, Ulrich. 2000. *La società del rischio. Verso una seconda modernità*. Roma: Carocci.
- Bianco, Simone. 2020. «Coronavirus Bergamo, il primario Marco Rizzi: “Fase 2, serve cautela, evitiamo il ritorno delle folle in Città Alta”». *Corriere della Sera*. 1 maggio 2020. https://bergamo.corriere.it/notizie/cronaca/20_maggio_01/coronavirus-bergamo-primario-marco-rizzi-fase-2-serve-cautela-evitiamo-ritorno-folle-citta-alta-02b834a4-8b7c-11ea-b0cd-a1732823ac8b.shtml.
- Boggero, Giovanni. 2020. «Le “more” dell’adozione dei DPCM sono “ghiotte” per le Regioni. Prime osservazioni sull’intreccio di poteri normativi tra Stato e Regioni in tema di Covid-19». *Diritti regionali. Rivista di diritto delle autonomie territoriali* n. 1/2020.
- Borell, Jonas, e Kerstin Eriksson. 2013. «Learning Effectiveness of Discussion-Based Crisis Management Exercises». *International Journal of Disaster Risk Reduction* 5 (settembre): 28–37. <https://doi.org/10.1016/j.ijdr.2013.05.001>.
- Casti, Emanuela, e Fulvio Adobati. 2020. «Mapping riflessivo sul contagio Covid-19. Dalla localizzazione del fenomeno all’importanza della sua dimensione territoriale. 1° Rapporto di ricerca: Perché proprio a Bergamo?» Università degli studi di Bergamo.
- Cavino, Massimo. 2020. «Covid-19. Una prima lettura dei provvedimenti adottati dal Governo». 18 marzo 2020. <https://www.federalismi.it/AppOpenFilePDF.cfm>.
- Cicchetti, Americo, Michele Basile, e Eugenio Di Brino. 2020. «Analisi dei modelli organizzativi di risposta al Covid-19 Instant REPORT #23: 08 Ottobre 2020». *Altems*.
- Daszak, Peter, Kevin J. Olival, e Hongying Li. 2020. «A Strategy to Prevent Future Epidemics Similar to the 2019-NCov Outbreak». *Biosafety and Health* 2 (1): 6-8. <https://doi.org/10.1016/j.bsheal.2020.01.003>.
- Dawkins, Jenny. 2004. «Corporate responsibility: The communication challenge». *Journal of Communication Management* 9 (2): 108–19. <https://doi.org/10.1108/13632540510621362>.
- De Vincentiis, Mauro. 2010. *Comunicare l'emergenza. Crisis management: la gestione delle notizie che non si vorrebbero mai dare*. Roma: Centro di documentazione giornalistica.
- Fioritto, Alfredo. 2008. *L'amministrazione dell'emergenza tra autorità e garanzie*. Il Mulino. <https://www.mulino.it/isbn>.
- Hermann, Charles F. 1972. *International Crises; Insights from Behavioral Research*. New York: Free Press.
- Lagadec, Patrick. 1994. *Crisis management. Come affrontare e gestire emergenze e imprevisti*. Franco Angeli.
- Lombardi, Marco. 2005. *Comunicare nell'emergenza*. Vita e Pensiero.
- Louvin, Roberto. 2020. «Una prorogatio infinita: permanenza, reviviscenza e confusione dei poteri regionali in situazioni di emergenza istituzionale». *Consulta Online*.

- Lucini, Barbara. 2014. *Disaster Resilience from a Sociological Perspective: Exploring Three Italian Earthquakes as Models for Disaster Resilience Planning*. Humanitarian Solutions in the 21st Century. Springer International Publishing. <https://doi.org/10.1007/978-3-319-04738-6>.
- Mauro Wolf. 1992. *Gli effetti sociali dei media*. Bompiani. <https://www.libreriauniversitaria.it/effetti-sociali-media-wolf-mauro/libro/9788845218712>.
- Michael J. Fagel e Jennifer Hesterman. 2017. *Soft Targets and Crisis Management. What Emergency Planners and Security Professionals Need to Know*. Prima edizione. Boca Raton: CRC Press. Taylor & Francis Group.
- Ministero della Salute. 2020. «Prevenzione e risposta a Covid-19: evoluzione della strategia e pianificazione nella fase di transizione per il periodo autunno-invernale.»
- Nava, Francesca. 2020. *Il focolaio. Da Bergamo al contagio nazionale*. Prima. Editori Laterza.
- Nicotra, Ida Angela. 2020. «L'epidemia da Covid-19 e il tempo della responsabilità». *Diritti regionali. Rivista di diritto delle autonomie territoriali*, n. 1 (marzo): 28.
- Reynolds, Barbara, e Matthew w. Seeger. 2005. «Crisis and Emergency Risk Communication as an Integrative Model». *Journal of Health Communication* 10 (1): 43–55. <https://doi.org/10.1080/10810730590904571>.
- Senni, Michele. 2020. «Covid-19 experience in Bergamo, Italy». ESC. European Society of Cardiology.
- Trombetta, Gabriele. 2020. «Emergenza COVID-19: Un Tentativo Di Inquadramento – Amministrazione in Cammino». 27 maggio 2020. <https://www.amministrazioneincammino.luiss.it/2020/05/27/emergenza-covid-19-un-tentativo-di-inquadramento/>.
- Ufficio Comunicazione ASST Papa Giovanni XXIII. 2020. «Riattivato l'ospedale alla Fiera di Bergamo | ASST Papa Giovanni XXIII». 4 novembre 2020. <https://www.asst-pg23.it/2020/11/riattivato-lospedale-alla-fiera-bergamo>.
- Valseriana News. 2020a. «Quella notte all'ospedale di Alzano, l'incertezza del Coronavirus e il tampone non fatto». *Valseriana News* (blog). 22 marzo 2020. <https://www.valseriananews.it/2020/03/22/quella-notte-allospedale-di-alzano-lincertezza-del-coronavirus-e-il-tampone-non-fatto/>.
- . 2020b. «Quella domenica di febbraio, i 4 casi di Coronavirus all'ospedale di Alzano Lombardo». *Valseriana News* (blog). 23 aprile 2020. <https://www.valseriananews.it/2020/04/23/quella-domenica-di-febbraio-i-4-casi-di-coronavirus-allospedale-di-alzano-lombardo/>.
- Walker, Marcus, e Mark Maremont. 2020. «Lessons From Italy's Hospital Meltdown. 'Every Day You Lose, the Contagion Gets Worse.'». *Wall Street Journal*, 17 marzo 2020, par. World. <https://www.wsj.com/articles/every-day-you-lose-the-contagion-gets-worse-lessons-from-italys-hospital-meltdown-11584455470>.

Il Cultural Intelligence e la Negoziazione Operativa nelle Aree di Crisi¹

FEDERICO PRIZZI

Federico Prizzi è un Antropologo, Polemologo e Storico Militare presso il Punt-Institute dell'Università Addoun di Galkaio in Puntland. Inoltre, è membro della *European Association of Social Anthropologists* (EASA). In qualità di esperto di *Cultural Intelligence* militare ha effettuato numerose ricerche sul campo in Asia Centrale, Sud-Est asiatico, Medio Oriente e nei Balcani, con analisi dedicate ai movimenti insorgenti, ai conflitti asimmetrici e alla condotta di guerre non convenzionali. È *Subject Matter Expert* di Cooperazione Civile-Militare (CI-MIC) e di Negoziazione Operativa. È autore di numerosi libri e saggi pubblicati con diverse case editrici.

Abstract

La Negoziazione Operativa è una delle attività più importanti che possono essere richieste a un etnografo di guerra. Essa consiste in tutte quelle trattative svolte in supporto alle operazioni militari, sia in tempo di pace che di guerra, con le autorità locali (formali e informali), con personale militare e paramilitare, con i rappresentanti di organizzazioni internazionali così come con comuni cittadini. In particolare, la negoziazione consiste in una necessità che due o più parti hanno di trovare un accordo accettato da tutti i contendenti. Accordo che deve essere vantaggioso per gli interessi di ciascuna delle parti coinvolte. Differisce, pertanto, dalla mediazione poiché quest'ultima necessita della presenza di un terzo attore percepito, dai due o più contendenti, come neutrale e imparziale. Infine, differisce, dalla negoziazione operativa condotta dalle forze di polizia, perché quest'ultima è strettamente legata alla liberazione di ostaggi.

Keywords

Cultural intelligence, cultural diplomacy, negoziazione operativa, aree di crisi

1. Il Team di Negoziazione

La negoziazione operativa è sempre il risultato di un lavoro di squadra non dell'attività di un singolo che si muove sul terreno in modo isolato e autonomo. Il team di negoziazione è composto da cinque elementi:

¹ **Avvertimento:** i contenuti di questo capitolo possono trovare una loro completa spiegazione solo attraverso un addestramento continuo e differenziato svolto sotto la supervisione di personale qualificato.

1. il Negoziatore;
2. il *Note Taker*;
3. l'Interprete;
4. il *Guardian Angel*;
5. il Conduttore.

In caso di specifiche esigenze operative può essere ridotto a tre elementi: il negoziatore, il *Note Taker* e l'interprete. In ogni caso, il team di negoziazione deve essere affiancato almeno da un altro team che possa rimpiazzarlo in caso di necessità.

Ogni elemento del team ha un ruolo preciso:

1.1 Il Negoziatore

È il team leader, colui che materialmente conduce la negoziazione con la controparte in un luogo prescelto. Fondamentale per il successo della negoziazione è selezionare il negoziatore adatto per una determinata negoziazione. Infatti, l'essere un negoziatore esperto non è un'automatica garanzia di successo, poiché ogni negoziato necessita un determinato tipo di negoziatore.

Il negoziatore è comunque un professionista con vasta e diversificata esperienza professionale alle proprie spalle. Un'esperienza che deve essere maturata sul campo in aree geografiche e in contesti operativi diversi. Deve avere uno specifico percorso di studi, ad esempio, nel campo dell'antropologia, della sociologia, della psicologia o anche delle scienze politiche. Deve inoltre avere una profonda conoscenza culturale del teatro operativo e possibilmente della lingua locale. Notoriamente deve avere una forte autonomia decisionale, altrimenti non è un reale negoziatore, ma un semplice intermediario.

1.2 Il *Note Taker*

È il vice del negoziatore nell'ambito del team. È colui il quale prende nota di quanto viene detto durante la negoziazione. Previo consenso della controparte, si può anche registrare o videoregistrare l'incontro. Tuttavia, si consiglia di prendere sempre nota per iscritto di quanto accade durante la negoziazione. In particolare, il *Note Taker* deve prestare particolare attenzione a quella che è l'atmosfera durante l'incontro, carpendone i dettagli. Deve osservare la coerenza tra il linguaggio verbale, paraverbale e non verbale degli astanti, soprattutto di quelli più vicini alla controparte. Deve guardare attentamente come la controparte reagisca a certe tematiche, se ha reale capacità decisionale o se questa dipenda, ad esempio, da un attore informale presente al *meeting*.

Proprio l'osservazione dell'ambiente permette al *Note Taker* di essere di supporto al negoziatore, il quale, essendo concentrato nel convincere la controparte non riuscirà a prestare anche la dovuta attenzione a tutti gli aspetti che stanno caratterizzando l'incontro. Per questo motivo all'interno del team, in fase di pianificazione, devono essere decisi dei segnali precisi, dei gesti non verbali, che permettano al team di comunicare tra tutti gli elementi durante la negoziazione. Ciò, senza però generare il sospetto da parte della controparte.

In caso di impossibilità ad avere un *Guardian Angel* nella *meeting room*, il *Note Taker* sarà anche il responsabile della *close protection* del negoziatore occupandosi anche degli aspetti relativi la sicurezza dell'intero team.

1.3 L'Interprete

È una figura fondamentale all'interno del team poiché, se il negoziatore non è autonomo dal punto di vista linguistico, permette di rendere i contenuti del negoziato pienamente comprensibili a entrambe le parti. Nella gran parte dei casi è un nativo proveniente dal paese dove si sta svolgendo l'operazione militare. A questo proposito, è fondamentale avere una persona che sia qualificata nella funzione di traduzione, un professionista appositamente formato in questo settore poiché un semplice assistente linguistico spesso non basta. Intendendo per assistente linguistico un conoscitore di una lingua franca, ad esempio l'inglese, che faciliti la comunicazione tra il negoziatore e la sua controparte. Controparte che potrebbe parlare solo la propria lingua nativa. La necessità di inserire nel team un interprete professionista è dettata, infatti, dall'esigenza di fornire in tempo reale al negoziatore l'effettivo peso dato alle parole durante l'interazione. Cogliendone perciò anche le sfumature concettuali, non solamente linguistiche.

Come facilmente immaginabile, la negoziazione è incentrata sulla scelta delle parole adatte da pronunciare nel momento voluto. Le parole, come i gesti, nell'arte della persuasione, non possono essere improvvisati, ma devono essere il risultato di una attenta scelta fatta in fase di pianificazione.

La negoziazione, inoltre, serve non solamente a raggiungere un accordo nel breve-medio termine, ma anche a veicolare specifici messaggi a determinati destinatari, cioè a persuaderli. Messaggi che dovranno inserire la negoziazione stessa in un contesto operativo più ampio al fine di massimizzarne gli effetti nel lungo tempo.

Nell'impiego dell'interprete bisogna anche tenere in considerazione che, nella gran parte delle circostanze, egli è un civile *embedded* nel team di negoziatori militari. Questo comporta che l'interprete dovrà essere sottoposto a uno specifico addestramento prima del suo impiego. Ad esempio, dove posizionarsi durante il negoziato quando esso è svolto in piedi o da seduto, così

come sulla base della tipologia della stanza o di tavolo. Come tradurre la conversazione al negoziatore e come evitare di cadere nelle provocazioni o nelle pressioni psicologiche della controparte. Quali gesti usare per comunicare con il negoziatore senza essere scoperto. Come reagire in caso di imboscata o di *Insider Threat*. Come sottoporsi a un briefing pre-negoziazione e come contribuire all'*After Action Review* al termine del negoziato.

Ne consegue, che la selezione del giusto interprete sia una attività che richieda tempo e accuratezza. Una selezione che non tenga solamente in considerazione l'essere stimato persona affidabile nella gestione delle informazioni (con relativo nulla osta di sicurezza), ma soprattutto del contesto nel quale dovrà operare. Infatti, il vissuto personale, gli aspetti della vita privata, l'appartenenza etnico-religiosa, il profilo culturale, l'età, lo stato psicofisico, sono tutti aspetti che dovranno essere valutati durante la selezione e l'impiego dell'interprete. Allo stesso modo, dovrà essere deciso dal negoziatore quale tipologia di vestiario l'interprete dovrà adottare (uniforme militare o vestiti civili), sulla base del suo sesso e della sua età, sempre rapportato al contesto del negoziato. Analogamente, dovrà essere deciso dal negoziatore se trasportare l'interprete con mezzi militari o con quelli civili.

Infine, fondamentale sarà decidere il numero di interpreti necessari alla negoziazione sulla base della durata della stessa, poiché essa è notoriamente un'attività che richiede un elevato dispendio di energie fisiche e psichiche.

1.4 Il *Guardian Angel*

È il principale responsabile della *close protection* del negoziatore e del resto del team. È l'iniziale tassello di un sistema di sicurezza ad anelli concentrici che ruota intorno al team di negoziazione. Il *Guardian Angel* è un militare armato che, nelle migliori delle ipotesi, si trova dentro la stanza dove avviene la negoziazione. Il suo compito è quello di reagire prontamente in caso di minaccia interna o esterna al team. Fondamentale, pertanto, è la sua conoscenza del luogo d'incontro. Per fare qualche esempio: la tipologia di edificio/piano/stanza, le possibili vie di uscita, lo spessore delle pareti e la tipologia di porte e finestre presenti, così come sul dove posizionarsi all'interno della stanza per evitare di influenzare negativamente l'andamento del negoziato. Inoltre, deve sapere come comunicare con il team in caso di pericolo e come evacuarlo in area sicura. Fondamentale, pertanto, è il coordinamento con il conduttore del mezzo che si troverà all'esterno del luogo dove si svolge il negoziato.

1.5 Il Conduttore

Il conduttore non abbandonerà mai il proprio veicolo al fine di garantirne la sicurezza dello stesso il più possibile, anche se da solo. Ovviamente, il numero di personale impiegato nella sicurezza del team di negoziazione dipenderà dal contesto operativo nel quale si svolgerà il negoziato e dalle reali capacità in termini di personale disponibile.

2. La Negoziazione

L'80% del successo di una negoziazione dipende dalla sua pianificazione che, insieme alla condotta e all'*After Action Review*, rappresentano le tre fasi principali che caratterizzano una negoziazione. Pertanto, qui di seguito, si analizzerà ciascuna delle tre fasi sulla base degli elementi che le contraddistinguono.

3. La Pianificazione

La pianificazione di una negoziazione deve necessariamente passare per le seguenti fasi:

1. Analisi degli obiettivi che si intendono raggiungere con la negoziazione;
2. Raccolta informativa sulla controparte;
3. Studio dell'ambiente dove si svolgerà il negoziato da un punto di vista geografico e topografico;
4. Studio dell'ambiente da un punto di vista delle procedure di sicurezza da adottare;
5. Studio dell'ambiente dal punto di vista culturale;
6. Individuazione delle possibili strategie negoziali;
7. Selezione delle tecniche per contrastare le strategie avversarie;
8. *Dress Code* e *Weapon Code*;
9. Addestramento e importanza dei giochi di ruolo;
10. Elaborazione della reportistica a seguito del negoziato.

3.1 Analisi degli obiettivi che si intendono raggiungere con la negoziazione

In questa fase iniziale bisogna avere chiaro cosa vogliamo ottenere dal negoziato e che tipo di risultati ci aspettiamo a corto, medio e lungo termine. Non avere fin da subito le idee chiare comporterà un inevitabile spreco di tempo e di risorse che sarebbero potute essere destinate ad altre attività più premianti. È consigliabile, comunque, non cercare di conseguire troppi obiettivi in una singola negoziazione. Infatti, sebbene le caratteristiche del

contesto operativo determineranno le tempistiche e cosa si intenda realizzare, in ogni incontro bisognerebbe cercare di raggiungere non più di due punti ritenuti importanti. Ciò al fine di muoversi a piccoli passi verso il consolidamento di un rapporto di fiducia tra le due parti coinvolte. Fiducia che, grazie anche a una costruita empatia tra il negoziatore e la sua controparte, possa portare entrambe le parti a mantenere gli impegni presi in fase di negoziazione poiché convintamente creduti come unica possibilità per risolvere una situazione altrimenti difficile da gestire.

3.2 Raccolta informativa sulla controparte

Consiste nel raccogliere il maggior numero di informazioni possibili sulla controparte, informazioni di natura diversa quali: profilo psicologico e personalità, formazione culturale e professionale, orientamento politico, gruppo etnico e religioso, relazioni affettive e interessi personali. Nonché, l'esperienza nel campo della negoziazione e l'atteggiamento nei negoziati precedenti avuti con personale militare. Quali strategie sono state precedentemente messe in campo dai nostri negoziatori e quali strategie ha invece adottato la controparte. Informazioni quest'ultime ricavabili, ad esempio, dalle *Post Meeting Minutes*. Centrale, pertanto, per ogni team di negoziazione è l'aver un proprio database dal quale ricavare le informazioni necessarie per creare un dossier sulla controparte, così come il poter accedere alle informazioni contenute in altri database non gestiti direttamente dal team.

A titolo di esempio, basti pensare all'importanza di raccogliere fotografie sulla controparte tramite i *social media* e internet. Oltre a nomi, volti, date, luoghi ed eventi, dalle fotografie si possono cogliere dettagli che magari non appaiono a un primo *screening online*, come: tipo di vestiario che la nostra controparte è solita portare (tipologia, colore, loghi, oggetti personali, tipologia di oggetti, ecc.), prossemica ed espressioni facciali nelle interazioni sociali, persone che ricorrono nelle sue vicinanze in diverse occasioni, ecc.

3.3 Studio dell'ambiente dove si svolgerà il negoziato da un punto di vista geografico e topografico

Studiare il luogo dove avverrà il negoziato da un punto di vista geografico e topografico è funzionale alla comprensione del contesto fisico nel quale il negoziato sarà svolto. Fotografie aeree, immagini satellitari, carte topografiche, ricostruzioni in 3D, video, immagini di varia natura, *sketch map*, tutto può essere utile a questo scopo. Tuttavia, l'esigenza di questo tipo di analisi non è solamente relativa alla sicurezza dei movimenti e dei luoghi e a come pianificare il contrasto a una minaccia. Ma anche alla comprensione delle ca-

ratteristiche del luogo scelto per il negoziato dal punto di vista della geografia umana e di quella del paesaggio. Ovvero come, da un punto di vista spaziale, gli uomini siano distribuiti in un'area specifica e come quell'area sia abitata. Come la distanza o la vicinanza da altri centri antropizzati influenzino le attività economiche e politiche, culturali e sociali di quel contesto particolare.

Notorio è, ad esempio, che le posizioni centrali favoriscano i contatti e le relazioni, mentre la periferia presenta prevalentemente un interesse per le risorse di cui dispone. Pertanto, si dovrà studiare il luogo del negoziato sulla base del rapporto che i locali hanno con i propri ecosistemi, cercando di analizzare su quali logiche si basa un certo ordinamento spaziale. Infine, bisognerà capire come i locali concepiscano il mondo e quale senso gli attribuiscono attraverso lo studio degli edifici di culto (religiosi o laici), dei monumenti, delle statue, della toponomastica, ecc., vicini al luogo dove si svolgerà il negoziato.

3.4 Studio dell'ambiente da un punto di vista delle procedure di sicurezza da adottare

Le procedure relative la sicurezza riguardano tre momenti principali: il movimento dal campo base al luogo ove avverrà la negoziazione, la sicurezza da porre in essere sul luogo della negoziazione e, infine, il movimento di rientro al campo base. Al fine di effettuare un'analisi efficace, dopo aver studiato la morfologia del terreno e i rischi associati, bisogna tenere in considerazione i vari fattori che potrebbero mettere a rischio il movimento e la condotta del negoziato. Quando si parla di sicurezza non bisogna però immaginare necessariamente imboscate o attacchi con ordigni improvvisati (IED) o l'essere sottoposti al tiro di un cecchino. Malattie, foratura di una ruota di un mezzo, incidente stradale, cambio improvviso del luogo di negoziazione o del negoziatore della controparte, sono tutti aspetti che devono essere sempre tenuti in considerazione in fase di pianificazione. Aspetti che, comunque, sono strettamente correlati al concetto di sicurezza *tout court*.

A questo proposito ci sono quattro tipologie di luoghi ove avviene la negoziazione:

- a. Il luogo d'incontro scelto da noi;
- b. Il luogo d'incontro scelto dalla controparte;
- c. Un luogo d'incontro neutrale;
- d. Il luogo d'incontro virtuale.

a. *Il luogo d'incontro scelto da noi*

Se è il team di negoziazione che deve scegliere il luogo d'incontro dovranno essere tenute in considerazione due possibilità:

1. Svolgere l'incontro all'interno dell'edificio dove generalmente lavora il team;

2. Scegliere un luogo lontano dal proprio edificio, ma comunque in una zona sotto il controllo del proprio contingente militare.

Nel primo caso, dovranno essere poste in essere tutte le regole tipiche della *Operations Security* (OPSEC). Ovvero, tutte quelle misure volte a negare ai potenziali avversari l'accesso a informazioni sul team di negoziazione identificando, controllando e proteggendo preventivamente anche quelle informazioni considerate non classificate e comunque apparentemente non significative. Generalmente, l'OPSEC si basa su cinque fasi: identificazione delle informazioni critiche, analisi delle minacce, analisi delle vulnerabilità, valutazione dei rischi e applicazione di adeguate contromisure. Ciò vuol dire, che non dovranno essere presenti nel luogo scelto per il meeting mappe, fotografie, organigrammi, documenti, equipaggiamenti, ecc. Particolare attenzione, inoltre, dovrà essere prestata a tutto quello che si trova nel luogo del negoziato e nelle immediate vicinanze, anche in ciò che è stato lasciato nella spazzatura.

Idealmente (secondo caso), si dovrebbe avere una stanza completamente dedicata ai meeting in un edificio lontano dagli uffici dove generalmente si lavora. Questa stanza dovrà essere arredata secondo le logiche della semiotica culturale. Questo perché la tipologia della stanza, il colore delle pareti, la forma del tavolo, la tipologia di arredi, la scelta di dove collocare gli ospiti, la tipologia di sedute per i negoziatori e per la controparte, sono tutti aspetti che devono essere scelti in fase di pianificazione per creare un ambiente che favorisca un certo tipo di comunicazione diretta e subliminale nei destinatari. A ciò si tenga poi in considerazione la convenienza o meno di far accedere la controparte con armi e dispositivi elettronici (cellulari, laptop, tablet, ecc.) all'interno del luogo della riunione.

b. Il luogo d'incontro scelto dalla controparte

In questa ipotesi, è particolarmente utile quanto precedentemente studiato dal punto di vista geografico e topografico. Infatti, le prime domande alle quali il team dovrà rispondere sono: “perché è stato proposto questo luogo?”, “in quale piano/edificio/quartiere/città/regione si trova?”, “quale significato culturale e ideologico ha questo posto per la controparte e per la comunità locale?”, “quale significato ha avuto questo luogo nel passato?”, “quanto sono lontani i centri del potere? (potere politico, religioso, economico, culturale, ecc.) del gruppo di appartenenza della nostra controparte?”. Bisogna, pertanto, capire in quale contesto fisico la controparte intenda svolgere la negoziazione. Ciò, infatti, aiuterà anche a comprendere il tipo di pressione psicologica alla quale il team sarà sottoposto. Poiché il tutto potrebbe essere stato organizzato in maniera tale da mettere, fin dalle prime fasi, in soggezione psicologica il team di negoziazione al fine di massimizzare il profitto durante le trattative. Come

in una partita di calcio, il ruolo della tifoseria della squadra che gioca in casa (tipo di stadio, coreografie, luci, cori, slogan, striscioni, suoni, fischi, applausi) è a volte determinante per far conseguire la vittoria alla propria squadra, così avviene anche nelle negoziazioni. Trovare lungo il nostro itinerario persone armate, autovetture incendiate, blocchi stradali, ammassamento di persone che protestano, spari in aria, esplosioni, ecc. prima, durante e dopo la negoziazione, sono spesso strategie volute per intimidire il team di negoziatori. Intimidazione creata ad arte, per avanzare richieste che, in condizioni normali, troverebbero maggiore resistenza da parte dei negoziatori stessi.

A queste considerazioni andranno ovviamente aggiunte quelle relative alla sicurezza, le quali però devono essere sempre inserite in un preciso contesto socio-culturale.

c. Un luogo d'incontro neutrale

Un luogo neutrale è tale perché proposto da una o più persone che sono considerate neutrali dalle parti contrapposte. Parti che hanno richiesto la mediazione di una terza figura ritenuta appunto imparziale, cioè, non legata alle logiche del conflitto. Ovviamente, il luogo ove si svolgerà il negoziato deve essere un luogo prima di tutto sicuro e collocato in un'area che, dal punto di vista geografico e soprattutto simbolico, rappresenti una forma di garanzia. Tuttavia, il team di negoziazione dovrà sempre assicurarsi che il luogo neutrale proposto, anche in buona fede, lo sia veramente. Bisognerà cioè verificare che quel luogo non sia stato utilizzato nel passato per altri incontri o che non abbia assunto un qualche legame ideologico per una realtà specifica. Ciò al fine di evitare eventuali strumentalizzazioni propagandistiche dell'incontro stesso.

d. Il luogo d'incontro virtuale

Pur non essendo uno strumento ottimale per raggiungere un accordo, poiché la negoziazione necessita sempre di un'interazione umana reale, di tipo fisico, per essere considerata credibile da tutti gli attori coinvolti, ci possono essere delle esigenze operative che possono limitare la mobilità dei negoziatori. Pertanto, la negoziazione virtuale diviene importante non tanto per raggiungere risultati duraturi, quanto per mantenere il dialogo aperto tra i vari soggetti. Uno strumento, di conseguenza, temporaneo, che può anche aiutare a preparare il terreno in vista del successivo incontro in un determinato luogo fisico.

A questo proposito, quattro sono i modi per negoziare virtualmente:

1. Via telefono;
2. Videoconferenze;
3. Social Media;
4. Via email.

3.5 Studio dell'ambiente dal punto di vista culturale

Nel corso di questo capitolo si è fatto più volte accenno all'importanza dello studio della dimensione culturale per effettuare una negoziazione, ma come si studia una cultura diversa? Quali passaggi vanno fatti e in che ordine?

Il *Cultural Intelligence* è il metodo per studiare una cultura diversa in un determinato ambiente operativo. In estrema sintesi, bisognerà mettere in pratica la seguente metodologia che parte da come si presenta fisicamente il singolo individuo, fino ad ampliare l'osservazione al contesto socio-culturale nel quale è inserito:

1. Osservare come gli appartenenti di una determinata cultura militare/paramilitare/criminale si presentino: tatuaggi, scarnificazioni, piercing, gioielli, ecc.;
2. Analisi della tipologia di abbigliamento, equipaggiamento ed armamento utilizzato;
3. Funzioni e ruoli sociali nell'organizzazione in base al genere (ad esempio: le "vedove nere" nell'ambito jihadista o le "madrine" e le "supplenti" in quello mafioso);
4. Concetto di vita e di morte e simbolismo ad esso associato (ad esempio: la "Santa Muerte" e il "Jesùs Malverde" dei narcos messicani o il martirio nella logica della jihad);
5. Matrimoni e rapporti di parentela nell'ambito dell'organizzazione oggetto di studio (ad esempio: la famiglia quale perno della struttura ndranghetista o i matrimoni combinati tra i leader jihadisti e le donne di comunità locali in Africa e in Medio Oriente);
6. La funzione sociale dei bambini, degli anziani e dei malati;
7. Il rapporto tra religione ufficiale, clero e luoghi di culto e organizzazione, nonché gli adattamenti religiosi alla cultura del gruppo armato;
8. Il concetto di tempo (studio dei calendari, delle festività, com'è cadenzata una giornata tipo);
9. Tipologia di scrittura (codici, murales, striscioni, bandiere, slogan, motti);
10. Tradizione orale (canzoni, miti, leggende, proverbi, modi di dire, slang);
11. Utilizzo della lingua nelle conversazioni e sua connessione con il linguaggio non verbale e paraverbale anche sulla base di quanto già evidenziato dagli studi di Etnopragmatica, ma applicato a specifiche culture e sottoculture armate (ad esempio: i neologismi e la gestualità coverbale della cultura rap);
12. Sistema economico (ad esempio: i sistemi di pagamento, le modalità di trasferimento del denaro ("hawala"), la funzione sociale del baratto, dei regali, cosa è considerato localmente il benessere, ecc.);

13. La funzione dell'arte, della musica, dei balli negli eventi collettivi e familiari;
14. Il rapporto tra cibo e cultura locale, quali sono i tabù, i periodi di astinenza, di digiuno o di festa.

Un campo di ricerca vasto e diversificato che, necessariamente, ha bisogno di antropologi e sociologi ad esso dedicati.

3.6 Individuazione delle possibili strategie negoziali

Quando si parla di strategie negoziali bisogna pensare a come se stessi giocando in una partita di scacchi, immaginando in anticipo le mosse dell'avversario e come contrastarle. Tuttavia, la negoziazione, a differenza di una partita di scacchi, non deve vedere alla fine un vincitore unico, ma entrambi devono lasciare il tavolo delle trattative con la convinzione di aver conseguito comunque un risultato positivo. Non si deve pertanto umiliare l'avversario, anche quando la situazione operativa ce lo permetterebbe. Infatti, è molto meglio salvare la faccia del proprio avversario che stringerlo in un angolo da dove poi non avrà più nulla da perdere. Le strategie, di conseguenza, devono essere necessariamente molteplici in modo non solamente di prevedere i vari sviluppi che la trattativa potrebbe assumere, ma anche per permettere al negoziatore una certa flessibilità nella negoziazione. Ciò, al fine di massimizzare comunque il profitto se la situazione contingente lo permette.

3.7 Selezione delle tecniche per contrastare le strategie avversarie

In questa sede non si intende svelare i trucchi del mestiere, basterà dire che non sempre le teorie tipiche della negoziazione economica sono applicabili alla negoziazione operativa. Termini quali *Best Alternative to a Negotiated Agreement* (BATNA) o *Worst Alternative to a Negotiated Agreement* (WATNA), o strategie quali *win-win* o *win-lose*, sebbene abbiano una loro fondatezza in ogni logica negoziale, la filosofia che vi è però a monte non lo è per ogni contesto. Infatti, ciò che può essere valido per un businessman o per un avvocato, in una negoziazione con gruppi armati le modalità negoziali possono far leva anche su aspetti diversi.

3.8 Dress Code e Weapon Code

Il codice di abbigliamento (*dress code*) è una serie di regole, spesso non scritte, su quale sia il capo di vestiario da utilizzare in determinati contesti. Generalmente, si distinguono due macrocategorie: abbigliamento formale e informale. In entrambi i casi, l'abbigliamento deve essere considerato formale o informale sulla base della cultura locale e non di quella del team di nego-

ziatori. Senza addentrarci in esempi antropologici estremi, tratti dal rapporto tra abbigliamento e cultura materiale, basti semplicemente pensare a come il concetto di abbigliamento informale possa essere recepito diversamente da un italiano e da un nordamericano. Inoltre, bisognerà prestare molta attenzione al rapporto tra *dress code* e genere. Ad esempio, se nel team c'è una donna, giovane o anziana, o un ragazzo/a o se la donna o il ragazzo sono presenti nel gruppo della controparte. Se il team di negoziatori è tutto composto da personale militare bisognerà prendere in considerazione, coerentemente con le regole imposte dal Diritto Internazionale e dalle Regole d'Ingaggio, se indossare o meno l'uniforme. Lo stesso principio verrà adottato anche per l'interprete. Da non dimenticare, inoltre, l'aver o meno l'armamento (in evidenza o nascosto) o il giubbotto antiproiettile (esposto o un sottocamicia antiproiettile). Infine, bisognerà prestare molta cura a un aspetto fondamentale a prescindere se si è in abbigliamento formale o informale: la coerenza del proprio *body language* con la parte verbale della negoziazione. Infatti, se la tipologia di vestiario mette a disagio il negoziatore, la sua capacità di trattare ne sarà fortemente influenzata. Basti qui l'esempio di una negoziazione a bordo di una piscina mentre tutti gli astanti sono in costume da bagno. Il clima informale potrebbe mettere a disagio quel negoziatore che soffre, ad esempio, di un lieve dismorfismo corporeo. Questo esempio estremo evidenzia non solamente l'importanza di capire il contesto, ma anche a ricordare l'importanza che ha l'individuare il negoziatore adatto a portare a termine un certo tipo di negoziato.

3.9 Addestramento e importanza dei giochi di ruolo

L'addestramento deve essere assolutamente realistico e fatto a "partiti contrapposti" nella tradizionale metodologia militare che vuole simulare il combattimento sul campo di battaglia. Qui, tuttavia, ciò che conta è avere tre gruppi distinti:

- a. Il team di negoziatori (Team A);
- b. I giocatori di ruolo;
- c. Il team di riserva (Team B).

L'addestramento è volto a mettere in discussione quanto pianificato dal team di negoziazione. In particolare i giocatori di ruolo (*role players*) dovranno identificarsi con la controparte cercando di mettere in atto una controstrategia che possa evidenziare le carenze metodologiche e di coordinamento interno del team prima del suo impiego. Il tutto dovrà essere videoregistrato con più telecamere da angolazioni diverse. Naturalmente, oltre alla fase di negoziazione vera e propria dovranno anche essere simulate una serie di si-

tuazioni che minaccino la sicurezza del team, dalla semplice colluttazione all'*insider threat*.

A questo addestramento dovrà presenziare e prepararsi anche il team di riserva (Team B) che, in caso di necessità, potrebbe sostituire il Team A. Avere, infine, anche l'opportunità di un Team C da inserire in questa attività è fortemente auspicabile.

3.10 Elaborazione della reportistica a seguito del negoziato

Come anticipato inizialmente, il *Note Taker* ha il compito di prendere nota dei contenuti, dei risultati e dell'atmosfera che ha caratterizzato il negoziato. Il tutto dovrà poi essere trascritto nelle cosiddette *Post Meeting Minutes*, ovvero un rapporto che fornisca una descrizione precisa di tutto l'andamento del negoziato evidenziando i lati positivi e gli errori, cosa si è osservato e cosa non è stato possibile osservare, come si sono comportati gli appartenenti del team e quelli della controparte, così come i problemi logistici e di sicurezza incontrati nello svolgimento dell'attività. L'importanza di questa tipologia di report sta nella sua condivisione all'interno dello staff militare, poiché vi potrebbero essere informazione e dettagli utili anche per altri uffici che non necessariamente sono coinvolti direttamente nel supportare la negoziazione. Inoltre, questa tipologia di report, sono estremamente utili nel breve-medio termine per tutti i successivi team di negoziatori che dovessero incontrare la stessa controparte od operare nella stessa zona.

4. La Condotta

La condotta si articola su tre fasi principali:

1. *L'Ice Breaker*;
2. La condotta vera e propria;
3. Come concludere un negoziato.

4.1 *L'Ice Breaker*

Saper rompere il ghiaccio è il primo passaggio fondamentale per iniziare una negoziazione. Ciò serve prima di tutto a ridurre la tensione tra le parti e a stabilire un rapporto di fiducia necessario per il conseguimento degli obiettivi prefissati dalla trattativa. Inoltre, evitare di andare direttamente all'oggetto della negoziazione prendendosi il tempo di conversare di argomenti generali (tempo, sport, vacanze, cibo, arte) intrattenendosi con la controparte è un'occasione importante per studiare ulteriormente chi abbiamo di fronte. Per questo motivo non bisogna avere fretta di iniziare la negoziazione, ma

bisogna far decantare il momento fino a cogliere l'occasione ideale per iniziare. Chiaramente, ciò sarà più facile da gestire quando si è i padroni di casa e siamo noi che abbiamo scelto il luogo del negoziato. Tuttavia, anche nel caso in cui fossimo noi gli ospiti, è consigliabile adattarsi senza fretta alle regole dell'ospitalità locali. Regole che, necessariamente, dovranno essere conosciute a priori dal team.

4.2 La Condotta

Prima di tutto, una negoziazione deve essere necessariamente inserita in modo coerente con il generale contesto socio-politico che sta caratterizzando in quel momento l'ambito operativo dove avviene la trattativa. Non avrebbe appunto significato svolgere una negoziazione che si prefigga obiettivi che non tengano in considerazione gli sviluppi operativi generali.

Ad esempio, se a livello politico c'è uno scontro tra i rappresentanti del governo ufficiale e quelli della milizia che controlla una porzione di territorio in funzione antigovernativa in merito al controllo di alcune fonti d'acqua utili anche all'irrigazione dei campi, sarebbe assurdo negoziare la possibilità di avere dei pivot mobili a irrigazione circolare in una zona governativa, dipendente da queste stesse fonti, senza conoscere le richieste avanzate a livello politico dagli appartenenti alla milizia stessa.

Pertanto, in una concomitante negoziazione a livello locale con i miliziani, questi aspetti a livello nazionale avranno certamente una certa ricaduta. Aspetti, che influenzeranno sicuramente l'Agenda del negoziato stesso.

Con il termine Agenda si deve, in particolare, intendere la struttura portante dell'impalcatura negoziale. Infatti, essa è costituita dagli argomenti che verranno trattati durante il meeting. Argomenti che sono il risultato della pianificazione negoziale e di un precedente accordo con la controparte. Tanto è vero che, di cosa parlare e di quanto tempo dedicare ai punti presenti nell'Agenda, è il risultato degli accordi preparatori al negoziato stesso. Ciò serve a chiarire in maniera trasparente a tutti gli astanti il perché ci si incontra e quali saranno gli argomenti trattati. È fondamentale, di conseguenza, che quanto inserito nell'Agenda sia condiviso e voluto da tutti, che non vi siano sorprese e che durante la negoziazione non vengano inseriti argomenti non precedentemente concordati. Compito del negoziatore, pertanto, sarà anche quello di evitare che qualcuno dei presenti inserisca tematiche nuove durante la fase negoziale. Tematiche che, eventualmente, potranno poi essere inserite in una negoziazione successiva.

Inoltre, seguire l'Agenda permetterà di mettere in atto quelle strategie pianificate in fase di preparazione. Ovviamente, non bisogna però considerare la negoziazione come un'attività rigida, che non si possa adattare alle circo-

stanze. Essa è invece uno strumento che permette di instaurare un dialogo aperto, chiaro e trasparente senza porre la controparte di fronte a situazioni/ richieste impreviste che potrebbero indispettire chi ci è di fronte, vanificando così l'intera negoziazione e potenzialmente la credibilità del team. Fondamentale, perciò, sarà dimostrare sempre da parte del negoziatore empatia non solamente verso la controparte, ma anche per gli argomenti trattati durante la negoziazione.

4.3 Come concludere un negoziato

Saper concludere una negoziazione nel modo migliore a volte può essere più importante di come si è condotta la negoziazione stessa, poiché essa è l'ultima immagine che lasciamo di noi nella controparte. Quella che gli rimarrà maggiormente impressa e che conserverà anche quando gli proponeremo un nuovo incontro. È pertanto un momento fondamentale. Per questo motivo bisogna sempre cercare di chiudere una negoziazione in maniera positiva, soprattutto dal punto di vista interpersonale, se non è possibile per i contenuti affrontati.

Se un minimo risultato è stato comunque raggiunto è bene ribadirlo e metterlo per iscritto prima di lasciare il luogo della negoziazione, condividendolo con la nostra controparte.

In questa fase, idealmente, dovrebbe anche essere pattuita una data per la continuazione della negoziazione.

Infine, se si è i padroni di casa, è assolutamente consigliabile garantirsi che, al termine dell'incontro, tutti gli astanti lascino il luogo della negoziazione allo stesso tempo. Ciò al fine di fugare eventuali sospetti, mantenendo un'immagine di credibilità e trasparenza.

5. L'*After Action Review*

L'*After Action Review* è una attività obbligatoria da fare "a caldo". Cioè, immediatamente dopo essere rientrati al campo base. Tutto il team vi deve partecipare al fine di analizzare ciò che è stato fatto anche in termini di errori individuali e collettivi, quali strategie abbiano funzionato e quali no, cosa sia stato osservato nei movimenti logistici e nella negoziazione. Tutte le osservazioni andranno poi inserite nelle *Post Meeting Minutes* e nel database del team. Infine, sotto la supervisione di personale medico specializzato, il team dovrà essere sottoposto a controlli che mirino a verificare lo stress subito dai vari componenti. Ciò poiché la negoziazione operativa, per sua natura, è condotta in aree ad elevato rischio fisico e la sindrome post-traumatica da

stress (PTSD) è un male che spesso, in modo carsico, emerge quando l'individuo meno se lo aspetta.

6. Conclusioni

La Negoziazione Operativa è un'attività che richiede un lavoro di squadra condotto in maniera intensa e professionale. Essa è il risultato di un addestramento specifico e di una formazione culturale ampia e diversificata. La scelta del personale idoneo da impiegare in aree di crisi non è facile e richiede un costante lavoro di selezione e formazione².

References

F. Prizzi e P. Micholou, *La Negoziazione Operativa nelle Aree di Crisi*, pubblicazione prevista nel 2023.

² Per un approfondimento della Negoziazione Operativa e delle tematiche affrontate in questo capitolo, si rimanda il lettore al libro di Federico Prizzi e Paraskevi Micholou intitolato *La Negoziazione Operativa nelle Aree di Crisi* di prevista pubblicazione nel 2023.

Events in Kazakhstan's Almaty of January 2022 – Grass-root Revolt or Terrorism Inspired Insurgency?

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

While the world in March 2022 is immersed in yet another military conflict on the territory of ex-Soviet Union, the Year of the Tiger started to show from its very beginning that solving various disputes is fastest through means of violence, and its subsequent suppression by means of power. This time it was on the territory of Kazakhstan, and the cause for outbreak of violence in Almaty and elsewhere between January 5 and 7, unseen in this magnitude so far in Kazakhstan, may have been benign in its nature – ever growing prices of fuel, exponentiated by ever expanding poverty gap in Kazakh society.

However, the instantaneous and extremely tough measures taken by the country's leadership – coupled with immediate involvement of military forces of the Collective Security Treaty Organization – indicated that much more than a mere overruling of popular dissent was at stake, and in order to attain its objective to silence the opposition, a clear and robust message had to be sent across.

Kazakhstan, in its 30 years of independence, has probably not been utterly immune to various types of disputes stemming from uneven distribution of wealth – certainly a long-term rule by one and only Nursultan Nazarbaev brought some “guarantees” of stability – but the extend of chaos, public disruption and the amount of blood spilled during the countermanding of rebellion indicates that the relatively peaceful period of country's post-Soviet development may be over and the oil and uranium rich nation needs to contend with both foreign interference as well as internal changes.

The events classified by some as insurgency, by some as a terrorist attempt to overthrow the local or perhaps even national government, and by some as a trivial fight between the tribal clans aiming at control of the nation's riches and the future, may have lasted not long – everything happened almost as unexpectedly and swiftly as a squall coming out of nowhere – but were a testimony to the fact that the political and economic status quo in any of the post-Soviet republics is not a long-term matter, and instead it can change at a whim of those having an access to both means and desires to alter the established ways. This article examines the vari-

ous viewpoints of both the possible causes of Almaty events of January 2022, as well as future ramifications for security status in the region, and perhaps also beyond.

Mentre il mondo nel marzo 2022 è immerso nell'ennesimo conflitto militare sul territorio dell'ex Unione Sovietica, l'Anno della Tigre ha iniziato a mostrare fin dall'inizio che la soluzione di varie controversie è più veloce attraverso la violenza, e la sua successiva soppressione per mezzo del potere. Questa volta si trovava nel territorio del Kazakistan, e la causa delle proteste ad Almaty il 5 gennaio potrebbe essere stata di natura benigna – prezzi sempre crescenti del carburante, a causa del divario di povertà sempre crescente nella società kazaka.

Tuttavia, le misure istantanee ed estremamente dure prese dalla leadership del Paese – insieme al coinvolgimento immediato delle forze militari dell'Organizzazione del Trattato di sicurezza collettiva – ha indicato che era in gioco molto più di un semplice annullamento del dissenso popolare, e per raggiungere il suo obiettivo di mettere a tacere l'opposizione, doveva essere inviato un messaggio chiaro e forte.

Non si può dire che il Kazakistan, nei suoi 30 anni di indipendenza, sia stato immune da vari tipi di contenziosi derivanti dalla distribuzione diseguale della ricchezza – certamente un governo a lungo termine di un solo e solo Nursultan Nazarbaev ha portato “garanzie” di stabilità – ma indica l'estensione del caos, il disordine pubblico e la quantità di sangue versato durante la revoca della ribellione che il periodo relativamente pacifico dello sviluppo post-sovietico del Paese potrebbe essere terminato e la nazione ricca di petrolio e uranio deve fare i conti sia con l'interferenza straniera che con i cambiamenti interni.

Gli eventi classificati da alcuni come ribellione, da alcuni come tentativo terroristico di rovesciare il governo locale o forse anche nazionale, e da alcuni come una banale lotta tra i clan tribali che mirano al controllo del futuro della nazione, potrebbe essere durato non a lungo – tutto accadde quasi inaspettatamente e rapidamente come una burrasca proveniente dal nulla – ma erano una testimonianza del fatto che lo status quo politico ed economico in una qualsiasi delle repubbliche post-sovietiche non è una questione a lungo termine, e invece può cambiare per un capriccio di coloro che hanno accesso sia ai mezzi che ai desideri di alterare i modi stabiliti. Questo articolo esamina i vari punti di vista di entrambe le possibili cause degli eventi di Almaty del gennaio 2022, così come le future ramificazioni per lo stato di sicurezza nella regione, e forse anche oltre.

Keywords

Kazakhstan, Central Asia, Terrorism, Insurgency, Regional Security, Coup d'état

1. Introduction – Mixed Signals as to the Underlining Causes of the Countrywide Revolt

Although the majority of Kazakhstan's population (being constitutionally a secular state) follows a non-denominational Islam (over 70%), the country has a considerable Slavic populace, and hence more than a quarter of the nations' inhabitants following Eastern Orthodox Christianity usually remains in a festive mode well into mid-January (Orthodox Christmas and the New Year falling onto January 7 and January 14, respectively). It was therefore with a rude awakening for many to witness utter disorder followed by a lack of securi-

ty forces' response to apparent attack on both administrative and general city's buildings and properties in the morning of January 5 in Almaty, Kazakhstan's largest city and, until 1997, the nation's capital. And it was even more appalling to consequently witness the crashing of the dissent with brute military force including the troops brought in from abroad. The city and most other parts of Kazakhstan came to watch events unprecedented in the country to date, and dubbed "Bloody January", the affair faded away little less than two weeks later, following a swift CSTO military intervention and uncompromising re-taking of control of Almaty before any noticeable shockwaves reached the capital Nursultan.

For most of the international observers, the news about street protests unrolling into armed attacks on city's municipality office as well as widespread marauding and attacks on property, did not have a point of reference – why Almaty, why Kazakhstan, and why so early into the new year – these were the questions asked. While it was definitely too early to understand what was happening, roughly four possible directions (each being beneficial to some as a theory, or detrimental to some in narrative) were being presented across international social media and news platforms:

1.1 Theory of direct Russian involvement, including orchestrating the revolt and subsequent sending in the CSTO troops

The immediate call of Kazakhstan's president Kassym-Jomart Tokayev to turn to military forces of the Collective Security Treaty Organization was essentially interpreted (amid already heightened tension around building up of Russian armed forces close to Ukrainian borders) as Russians most likely rehearsing the entry of its troops into Ukraine, with Almaty being an easy and useful "training material". Therefore the attention seemed to have shifted towards the actual entry of CSTO troops onto the territory of Kazakhstan, rather than the revolt and public chaos themselves.

1.2 Theory of Western interference as a prelude to new episode of Great Power conflict

Another theme that immediately found a number of grateful followers (resonating with the distant topic of Great Game played by Western powers in the region of Central Asia for centuries), that is was Western intelligence operation trying to destabilize the Russian Eastern front. In some of the early announcements of president Tokayev, it even seemed that he was referring to interfering Western elements as those causing the havoc in his homeland – which also was a useful narrative for Tokayev already becoming, by necessity, closer to Russia.

1.3 Theory of internal power struggle, visible only to those within the system

Mindful of the country's tribal past, where each "khan" or "bey" had its place and all "games" had to be played according to their wealth and power distribution, many immediately seized on the notion that it could well be the former president Nursultan Nazarbaev himself bankrolling and orchestrating the revolt. Several factors seemed to have been in favor of this theory – as Nazarbaev is frail and sick, he understands once he is dead his eldest daughter will not only not become the president (claimed as an original agreement between Nazarbaev and Tokaev at time of "temporary" handing over the country's rule to Tokaev in 2019) – and therefore he needed to "speed up" the handover back to original "first family's" hands. A number of analyses appeared online, articulating all Nazarbaev's foreign properties (amassed wealth during his 30-year-reign, that is), as well as domestic resources and assets that will be in the interest of Nazarbaev clan to "protect".

1.4 Terrorism inspired insurgency and outright attempt of coup d'état

Quite from the onset of the Almaty events, president Tokaev made sure to divert all attention to both foreign elements inciting the insurgency accompanied by looting as well as domestic "terrorists" that were promptly taken off the streets and detained in unpublicized locations. The government officials made certain references to Islamic radicals playing a role, as well as the role of citizens of neighboring Kyrgyzstan and Uzbekistan (some sources mentioning as many as 20,000 foreign "fighters" taking part in the events), but solid empirical evidence is yet to be obtained – although anyone familiar with the Central Asian region realities will understand that likelihood of rogue fundamentalists' participation, wanting to take advantage of a possible power, is real.¹

¹ Author attempted to corroborate allegations of involvement on part of Kyrgyz and Uzbek nationals – as some news outlets reported Kazakhstan's government stance that "thousands" of armed foreign terrorists were behind the Almaty insurgency. In the wording of some of these assertions, a certain attempt to accuse respective governments in sanctioning the riots in Almaty, although Kyrgyzstan in question is itself a member of CSTO and subsequently took actions supporting the incumbent Kazakh government in suppressing the violent dissent. Involvement of a state actor Uzbekistan in clandestine support of insurgents is also unlikely – given both the political neutrality of Uzbekistan that seems to play an integral part in its current government's approach to international issues, as well as clear support of Uzbekistan's leadership to president Tokaev. Nevertheless, on part of Kyrgyzstan, a former presidential adviser was consulted – who not only refuted claims that "thousands of Kyrgyz citizens may have been involved" – for one,

As with most of the geopolitical and socioeconomic issues distinctive to Central Asian region, it is probably a mix of all above – only the time will tell, but no conflict in this region goes unutilized by the multitude of players and stakeholders. Author will not be touching upon the issue of influence of Turkey in this essay, but it can be imagined that as part of Turkey's Pan-Turkism movement – at times bordering at vividly expressed desires to revive the Ottoman Empire – Turkey does have her own position and intentions, and it would only be a matter of time when the country's aspirations would crystallize in a form of direct involvement.

Let us examine some of these theses as both to their likelihood as well as consequent impact on further development of Kazakhstan's geopolitical vectors – and what lessons can be drawn not only for Kazakhstan's elites and grass-root population, but also for the country's neighbors.

2. Precursory Occurrences of Popular Dissent in Kazakhstan's History

In the 30 years of country's independence, Kazakhstan managed to stay away from mainstream political violence, in stark contrast from its neighbors Kyrgyzstan (regular mass protests and uprising claiming a heavy toll on both human lives and property) and to some extent Uzbekistan (with occurrences of violence close to ethnic cleansing towards the fall of the Soviet Union in Fergana Valley, and the notorious 2005 Andijan massacre). Kazakhstan's post-Soviet period of development does not also compare to that of Tajikistan, engulfed in a full-fledged civil war that dragged for 5 years between 1992 and 1997. The country's composition and interaction with the internation-

citing the ongoing border closure measures related to COVID restrictions (and therefore a physical inability of Kyrgyz citizens to enter Kazakhstan for the purpose of either orchestrating or participating in the insurgency); for two, the actual individuals who may have been arrested in Almaty carrying Kyrgyz identification were proven to be bystanders “being in a wrong place at a wrong time” (Ministry of Foreign Affairs of Kyrgyzstan even asked for these individuals to be located in detention and released immediately); and for three, Kyrgyz nationals being already too busy with complaints against their own government and incumbent president Sadyr Japarov's inability to take the country out of an economic impasse. On part of Uzbekistan, a former long-term ambassador of its Foreign Ministry, active in the region of post-Soviet Union, commented that currently the Uzbek authorities control strictly involvement of its citizens abroad in unsanctioned or outright illegal activities (referring to practice of curtailing of any Uzbek citizen, suspected in general radicalism, in his travel abroad), and if there were any Uzbek nationals involved in Almaty riots as deliberately deployed insurgents, they would have absolutely nowhere to go or return. Besides, any publicly available information on the identities of those killed in action or detained was limited, and in general not sought after by the international community.

al community based on abundance of natural resources does not also come close to the political, economic and social anatomy of Turkmenistan, deeply lingering in a North Korea-style of isolationism and utter disregard for most concepts of civil society.

While the regular suppression of opposition figures and human rights activists in Kazakhstan is not rare, the only major violent incident that had roots in deepening social divide caused by rising inequalities among the populace is so-called Zhanaozen massacre of December 2011, when anywhere from 15 people upwards were killed by riot police with orders to shoot to kill during unrest on the country Independence Day. The protests came about as a direct consequence of Zhanaozen strike among oilfield workers earlier in May and consequent dismissal of about 1,000 employees of Ozenmunaigas oil field, and in January 2022 it was again Zhanaozen in Mangystau region along the Caspian shore where the inhabitants took to the streets protesting increasing prices of essential products and fuel, corruption and human rights abuses. Although in 2022 the demonstrations in Zhanaozen and nearby Aktau proceeded without masses resorting to violence, the rest of the country took a different path and as a result of direct deployment of domestic military and CSTO special forces, hundreds of Kazakh citizens lost their lives.

While the objective of this discourse is not to dwell into issues of Islamic radicalism, uncertainties created by unstable Afghanistan in Taliban hands, as well as long history of various extremist elements making their way into every aspect of life in Central Asian region do make Islamic factor the one that needs to be reckoned with. As Baizakova and McDermott note:

Kazakhstan, being the most stable and safe country in the region, witnessed a series of alleged extremist terrorist acts since 2011. The number of Islamic activists has grown, particularly in rural areas. As an official response to that, Kazakhstan continues to improve its legislation on combating terrorism and extremism. However, since this experience of domestic “political violence” in 2011-12, the country has suffered no major incidents.²

3. Recapitulation of January 5 Events in Almaty

We refer to the events in Almaty as of “January 5 Events” because this was the day when the relatively peaceful protests already taking place for 2-3 days, suddenly became gravely violent, and in striking contrast to local masses calling for betterment of their livelihoods new groupings appeared almost out of nowhere and started pillaging the city. While most of the city’s population was

² Baizakova Z. and McDermott R.N. (2015), *Reassessing the Barriers to Islamic Radicalization in Kazakhstan*, pp. xi-xii.

not able to either comprehend the timing or grasp the full extent of sudden riots and armed looting, the subsequent numerous reports by international journalists entering Almaty through Nursultan (operations at Almaty airport were suspended on January 5, amidst the destruction of its facilities such as ATMs and duty free shops) within the next 3-4 weeks indicate, that not all inhabitants of the city had knowledge of violent disturbance being planned or being in the stage of execution. Initial protests originating on January 2 in the city of Zhanaozen, which witnessed oil sector workers' strike in 2011, quickly spread not only to Almaty, but most of regional administrative centers around Kazakhstan. While the earliest displays of dissent did try to draw attention to steep increases in prices of essential goods, with a particular attention to liquefied gas used as a fuel, very soon the protests grew into political outcry, and then loud slogans disappeared and instead a full-fledge armed violence took to the streets. In the major address to the nation by the president Tokaev on January 7 (primarily in Russian language), he was quick to call the perpetrators "terrorists, armed bandits and criminals", referring to "20,000 individuals armed, highly specialized and prepared in terrorism and urban warfare", arising from both foreign and domestic ranks. The insurgents' "preparedness" apparently displayed itself also in prompt dissemination of fake news and media manipulation (the country-wide landline internet access was disconnected immediately in the aftermath of January 5 tolls on the streets of Almaty, but reinstated by January 7). The president, while agreeing to placing a price cap on liquefied gas for next 6 months, dismissed any notion of "negotiating" with the insurgents, and instead ordered to shoot to kill anyone resembling an armed protester, with the need to "utterly destroy" the enemies. Referring to CSTO troops, including 3,000 Russian paratroopers already deployed on January 6, he elaborately thanked leaders of Armenia (currently holding chairmanship of CSTO), Belarus, Kyrgyzstan and Tajikistan – all participating in "restoring law and order in Kazakhstan", and then went on expressing exceptional gratitude to Russian president Putin, for adhering to principles of collective security. He also mentioned leaders of China, Uzbekistan and Turkey, as well as United Nations, as being thankful for their support of legitimate Kazakhstan government.

I believe Tokaev's mention of China and Uzbekistan warrants some elaboration – by January 6, when the CSTO military intervention was already imminent, signals were received that prior to consulting CSTO leadership and Putin himself, Tokaev spent time speaking with both Chinese leader Xi Jinping and Uzbek president Shavkat Mirziyoyev, apparently voicing a request to consider to send in their respective armed forces to quell the growing armed dissent. Reportedly, both foreign leaders politely declined the request – China ostensibly wary of the fact that a Chinese military intervention cracking down

on nominally Muslim Kazakhs may not go down well with the West, already regularly criticizing China's approach to their domestic "Uighur problem". President of Uzbekistan, well aware of the fact that his tenure from 2016 to date has been marked with international success in attracting foreign investments into Uzbekistan, gradual full opening of the country to the world as opposed to years of his predecessor's seclusion, and gaining a reputation of being neutral enough not to encroach upon his neighbors' affairs, also rejected the idea of his country's forces getting involved in clearly Kazakhstan's internal strife – and perhaps did even remember the international uproar caused by Uzbek special security forces gaining notoriety for effectiveness for their "take no hostage" approach in liquidating a 2005 revolt in Andijan.³

It was by January 3, when some of the regular inhabitants of Almaty (who may have been joined by people from neighboring villages) took to the streets in solidarity with their Zhanaozen compatriots, criticizing mainly the current economic course of the country's leadership reflected in decreasing standards of life. While about 20 protesters were arrested on January 3, another 100 of local inhabitants participating in the mass dissent were detained on January 4. It should be noted that most of the social media calls to gather publicly up to that time were encouraging explicitly peaceful protests, without reference to any violent outburst of emotions. The several thousands of predominantly young people that took to the streets were mostly shouting economic slogans, with understandably underlining tones that the current government needs to take steps for improvement. By January 4 night, however, the masses of people essentially paralyzed the main road arteries of the city, and clashes with law enforcement started to take place. Through the multitude of footages that made it onto internet before the landline connections were severed indicate that the leaders heading the groupings in the crowds are heard to call for "resolution of issues through discussions" and explicitly instructing "not to touch each other" and "not to damage any cars in the way", as well as "not to burn anything". Obviously wary of the possible methods of police and law enforcement forces, many protesters also caution not to engage in violence because "tomorrow they [the government] will accuse us [the protesters] of inciting violence and destruction". At the same time, with the largest crowd gathering on the square in front of the city's municipality administration, nobody from the city's administration even attempted to come forward and start a dialogue, although the crowd was heard calling for the region's governor to come out (which shortly changed into calls for the governor to be sacked). The law enforcement did start to apply smoke grenades and tear gas and the

³ The fact of President Tokaev's approach to China and Uzbekistan at the onset of the crisis being provided by an intelligence source.

crowds started to disperse. The presence of youngsters on the streets of Almaty continued into morning of January 5, when apparently the police in riot gear, many of them positioned on the roofs of police stations, tried in vain to diffuse accumulated mass of people, with possible application of fire arms resulting in injuries and deaths among the demonstrators. The mob then started to move onto critical government buildings, such as Almaty office of National Security Committee or local police academy – and by that time, the law enforcement personnel started to withdraw, or outright run away. Sometimes before the noon of January 5 the most violent attacks started to take place, and some of the footages clearly shows the change in groups' objectives as well as behavior.

In early hours of January 5, president Tokaev, having declared emergency situation in Almaty (in addition to Mangystau Region on the Caspian Shore), spoke in a televised address, noting no preparedness to compromise on public order. He dismissed the Cabinet, and swiftly took over as the Chairman of the Security Council replacing Nursultan Nazarbaev. One of the most notable additional moves was a dismissal and subsequent arrest of several prominent commanders of the feared National Security Committee (KNB), including its chairman Karim Massimov, an ethnic Uyghur and long-time staunch supporter of Nursultan Nazarbaev, having served also as his Prime Minister. Massimov, who was outright accused of preparing the coup d'état, and is apparently awaiting trial for high treason, was during Nazarbaev rule often mentioned as a possible successor in country's presidency.

By accounts of Almaty inhabitants – who initially shared the events as they saw it either on the streets or from their windows with their relatives living abroad, who in turn were able to shed some light on what was happening (those living inside Almaty, even mainly economic if contacted from abroad, would simply not talk to strangers – the extent of arbitrary arrests and risk of being killed was just too big) – the strangest phenomenon during early afternoon hours of January 5 (after the initial clashes of protesters with local police) was a sudden utter absence of law enforcement tackling the riots as well as fire brigades needed to extinguish burning cars and other property. Riots in their commencing stages in early morning grew violent, with an attack on Almaty municipal office and presidential residence, and there have been numerous accounts of police officers' corpses lying on the pavements – decapitated. The mass of protesters, by now indistinguishable whether locals or “foreign” then went about the city almost systematically, looting shops, banks, local press offices and trading centers, also making their way into many of the office buildings and TV station, simply destroying or burning everything in their path – the locals brave enough to film the scenes of marauding themselves were starting to question whether the looting has anything in common

with initial protests. It was only in the morning of January 6 when police together with Kazakh military already receiving support from CSTO troops went onto sweeping operation through the city, indeed firing into crowds and more or less attaining the order. By January 7, as a result of systematic “counter-terrorism operation” however, the “20,000 foreign and domestic terrorists” disappeared from the sight and the city, and the toll of over 200 dead⁴, 500 gravely injured, 2,000 detained without their relatives knowing where, and roughly USD 100 million in property damages loomed over the country as a stark contrast vis-à-vis the country’s 30 years of relative quietness and stability.⁵

By morning of January 6, the Almaty residents took to the Republican Square of the city again, this time appealing to the authorities with their assertion that those who looted and pillaged the properties the day before were never present in the initial protests highlighting the economic inequities impacting most of ordinary citizens of the country, and that those calling for improvement of living standards did not participate in widespread stealing and vandalizing of the city assets. They also pleaded with the president Tokaev to withdraw the army (presumably referring also to CSTO forces), but by some accounts, special forces opened fire into these crowds towards that evening. Some of the footages confirming these claims made it to the international social media, and on the morning of January 7, blood was splattered over the square, with people realizing that some of their relatives lost their lives. On the same day, during the televised speech, president Tokaev confirmed that he had ordered to “shoot to kill without warning shots”, and that the military operation launched in the city the day before was in fact a “counter-terrorist operation”. In fact, most of the Kazakh human rights activists that have been voicing their criticism of both Nazarbaev and Tokaev regimes for some time, agree that the largest human toll came about as the result of January 6 and 7 suppression of peaceful protests (that came out to the streets to negate their involvement in January 5 pogroms), and that the “terrorism” charges were brought up in order to justify live firing at 30,000 plus of Almaty residents on those two days.

Although the images of “Almaty burning” were the primary ones making it to the world press, most of Kazakhstan’s regional centers fell to chaos and violence during January 4-6 period. In contrast to city of Almaty, the adminis-

⁴ Most of them civilian population of the city (also including two decapitated law enforcement recruits), although human rights activists claim the toll is higher – they have tried so far in vain to gain access to the full list of dead citizens, pressing the authorities to publish their names. The activists also suspect that in this metropole, some of the people who lost their lives did not even purposefully participated in demonstrations.

⁵ Summary of footages with commentaries, as well as immediate estimates by both local and foreign press corps in the immediate aftermath of January 5-7 events.

trative center of Almaty Region, Taldykorgan (some 270 km to the north-east of Almaty), saw more rudimentary display of protests by the local population during January 4-5, whereby the local statue of Nursultan Nazarbaev was not only demolished, but the upper part of the statue hanged by its head in front of municipality office. The local detention center was attacked as well as there was an attempt to break into National Security Committee's office, and the course of events took more violent form right from the onset of demonstrations. In the city of Talas in the south, on the border with Kyrgyzstan, a local mob stormed a police station, pillaging the station's supply of firearms. The events in this administrative center of Jambyl Region were described more as pogroms rather than demonstrations, leaving at least 15 dead by January 5. In the third most populous city of Shymkent, itself one of the main industrial centers of Kazakhshtan on the border with Uzbekistan (some 700 km west of Almaty and mere 120 km north of Tashkent), the violence started to be demonstrated at night between January 5 and 6, after the local protesters resorted to setting few police cars on fire. On the morning of January 6, the city woke to burnt down exhibition center, looted Turkistan Palace as well as a shopping center – all this in the midst of blood and spent cartridges on the streets. The rice production center of Kyzylorda city and pre-Second World War capital of Kazakh Autonomous Socialist Soviet Republic (more than 1,000 km to the west of Almaty), saw more of anti-Nazarbaev display of both protests and violence (both the city's court house and headquarters of Nur Otan, Kazakhstan's ruling political party⁶ were set on fire), and the active shooting lasted for several hours on January 5, amidst relatively early retreat of local police forces unable to hold off the masses. The city of Aktobe, the largest conglomerate in western Kazakhstan near Russian border, city of Uralsk on the western (i.e. European) side of the Ural river, Caspian harbor and petrochemical city of Atyrau, north-eastern conclave of Semey that has served prior to 1989 as a nuclear testing site (and until 2007 known as Semipalatinsk), mining and metallurgical center of Ust-Kamenogorsk in Eastern Kazakhstan, have all witnessed similar events, mostly starting off as protests in support of Zhanaozen citizens, and eventually escalating into clashes with local police. Interestingly enough, the city of Zhanaozen where the initial Kazakh protests started on January 2 and one-time nuclear power plant location city Aktau on the Caspian shore, were the only one where the protesters did not resort to violence, with their primary demand being return to pre-1993 Constitution and resignation of the incumbent president Tokaev, and by January 8, when most other Kazakh megalopolises were literally on fire, the

⁶ As a ruling political party led by president Tokaev, renamed to Amanat at the end of January 2022, after replacing Nursultan Nazarbaev as its chairman.

dissent has faded away. Explicitly peaceful protests in Zhanaozen and Aktau, without local police resorting to any restrictive measures, did however notice the attempts of agent-provocateurs to stir up commotion, which apparently did not succeed.⁷

4. Plausibility of Deliberate Involvement by Russia, Covered by “Mandate of CSTO”

By “involvement”, separate issues should be understood – either complicity in stirring up the initial events themselves that inevitably lead to CSTO intervention, or seizing upon an opportunity to showcase the CSTO and Russian military muscle in crushing a local rebellion. There are three main factors contributing to this theory, each remaining as a fact, rather than hypothesis:

- a. The speed with which president Tokaev turned to Russian president Vladimir Putin with a request to engage the articles of collective security to swiftly quell the “terrorist insurgency designed as coup d’état”.
- b. The speed with which Putin and CSTO agreed to “assist” Kazakhstan in countering the insurgency and the composition of “peacekeeping forces” of CSTO itself.⁸

For points a. and b., it should be noted that Articles of collective security stipulate deployment of CSTO forces on its member’s territory in the case of foreign invasion, not to suppress domestic protests, however violent they may have been. The insurgency also did not pose a threat to territorial integrity of Kazakhstan – all forms of protests were either aimed at changing the current economic status quo or to potentially cause a disruption within the governing circles in order to bring about a drastic change.⁹ It is rather clear, that in order

⁷ By a number of accounts of Kazakh diaspora living in Russia and United Arab Emirates, referring to their interaction with relatives in Kazakhstan.

⁸ CSTO, having been established 30 years ago as a “collective security instrument” and after 2002 functioning as explicitly military alliance, currently counts Russia, Belarus, Armenia, Kazakhstan, Kyrgyzstan and Tajikistan as members, but during its history Georgia, Azerbaijan and Uzbekistan were also temporarily attached to the body. There are 3,600 active military troops ready for peacekeeping operations, in addition to over 20,000 of so-called Collective Rapid Reaction Force ready to be deployed upon request of a member state, and it is understood that up to 85% of this military body consists of members of Russian armed forces. It is also understood that depending on the magnitude of needed deployment, additional numbers from respective regular armed forces can be drawn.

⁹ By such standards, Kyrgyzstan would need to be inviting CSTO troops to counter its regular domestic turmoil, which almost every time borders on open insurgency and by end-result they always resemble a full-fledged coup d’état – the country’s president almost always gives in and resigns. In fact, during the so-called Second Kyrgyz Revolution of April 2010, then interim president Roza Otunbayeva did voice a need to call in CSTO forces (the mass protests, with

to invoke the article for immediate deployment of CSTO troops into Kazakhstan, president Tokaev resorted to emphasizing involvement of “foreign fighters” in particular in Almaty insurgency, and there was little time for anyone to analyze who these “foreign fighters” may be, and nobody was questioning the plausibility of territorial integrity threat.¹⁰

Broader approach can also be taken in analysis of an almost immediate reaction by Putin to send in the CSTO troops led by Russian armed forces – Kazakhstan during Nazarbaev rule did not represent a model vassal nation that would be nodding to Moscow’s directives – and given its vast natural resources that could be well traded internationally in all directions, the country took often independent, at times even pro-Western positions. In other words, whoever planned, orchestrated and executed the Almaty insurgency knew that Russia will take notice, or perhaps even Russia will seize the opportunity to ingratiate Kazakhstan’s incumbent leadership into tighter economic and political bond.

c. Appointment of Russian Armed Forces Colonel General Andrey Serdyukov as the head of CSTO peacekeeping forces in Kazakhstan in January 2022.

For those following carefully involvement of Russian Armed Forces in the region of post-Soviet Union, as well as other “hot spots”, notably in the Middle East, the mere mention of General Serdyukov should ring a distinct bell – he fought in the First Chechen War of 1994 – 1996, and he was a deputy brigade commander of Russian forces in Kosovo, participating also in the standoff between Russian and NATO forces at Pristina airport in June 1999. But more importantly, this is the individual who led Russian armed forces in March 2014 in Crimea and commanded Russian troops in breakaway part of Ukrainian Donbass in August 2015. Furthermore, Syria conflict observers would remember him as the Commander of Russian troops deployed to Syria, for the period of April to September 2019. The apparent career of this 60-year-old Russian army star so far culminated in leading the CSTO troops entering Kazakhstan this January, and it may not be far from the possible

elements of nationalist clashes with local Uzbek diaspora, resulted in internal displacement of several hundreds of inhabitants, and result-wise had graver repercussions than January 2022 events in Kazakhstan). Vladimir Putin, during that time fulfilling the role of Prime Minister, declined CSTO intervention, referring to the lack of foreign involvement in the Kyrgyz uprising. It can be safely said that Kyrgyzstan in the eyes of Russia does not represent a nation whose position would endanger Russia’s geopolitical objectives in the region, and therefore whatever internal turbulence persistently prevails, it can be left up to the Kyrgyz citizens to handle.

¹⁰ By the same token, Prime Minister of Armenia, currently holding the chairmanship of CSTO, was directly criticized for not “inviting” the CSTO forces to subdue Azerbaijan’s troops entering the Nagorno-Karabakh – although technically Nagorno-Karabakh is not an Armenian enclave, but internationally unrecognized independent Republic of Artsakh.

truth that a military cadre of this caliber and experience would be left out of ongoing Russian army operations in Ukraine. In every case, quelling of Kazakhstan dissent was important enough to Vladimir Putin to deploy the best of his best, and conclusions can be drawn from this consideration.

Therefore, in retrospect of Russian military incursion into Ukraine on February 24, we may want to extrapolate, that Russia's involvement in rapid reaction to Almaty events may have meant involvement in both preparation of the insurgency overwhelming the many of Kazakhstan's cities, as well as subsequent "attentive" response to artificially created crisis.

5. Theory on Terrorism Inspired Insurgency and Outright Attempt of Coup d'état

As outlined in the previous paragraphs, the speed with which president Tokaev came to conclusions that "terrorists originating in foreign land" are the major element of January insurgency designed to both "destabilize the country and depose the legitimate leadership", as well as the speed with which Russian president Putin reacted in dispatching CSTO troops, do partially answer whether the whole affair was of recognized terrorists' making. Perhaps the recent trend of blaming any nefarious circumstance first to terrorism, and then trying to explain what the specific empirical evidence is, was applied this time as well. In every case, hastily accepted presumption even before the full events unfolded made way for drastic curbing of the popular rebellion, and the major take away for all players involved will most likely be that regime of president Tokaev will hold onto control of the country's affairs without compromise.

6. Internal Power Struggle(s) as the Most Probable Cause

One of the indications that the riots developing into armed insurgency could have been prepared and executed by Nazarbaev supporters with former president's tacit (or perhaps even explicit) agreement, was that many of the protesting were shouting anti-Tokaev and anti-current government slogans – although any political observer would have known by now that any discord and dissatisfaction in economic status quo is more of a result of Nazarbaev's 30-year rule, rather than president Tokaev's 2-year period of presidential administration. Some of the cities involved in mass protests did seem to direct their anger at Nazarbaev (attacking his statues, tearing down the name plates, calling his name out) – but this was perhaps because Tokaev did not manage to install his personality cult (yet), and the city streets are not named after To-

kaev nor there are multiple statues of the incumbent president. As evidence of Tokaev seizing on the notion of possible Nazarbaev-instigated insurgency are the facts that the incumbent himself replaced Nazarbaev in the post of Head of National Security Council (initially awarded to Nazarbaev as a position for life) and immediately not only sacked but also arrested Karim Massimov – the head of Kazakh intelligence until January 2022 and long term loyal prime minister under Nazarbaev (Massimov himself an ethnic Uighur). Some observers also note the fact, that given the several hundreds of billions (anywhere between 300 and 600) that Nazarbaev managed to amass for his family during his 30-year tenure, Tokaev may feel he has not grasped the true potential as “commander-in-chief” as yet, and considers it is time for Nazarbaev clan to be disconnected from the socio-economic life in Kazakhstan. If the message of the rebellion, on the other hand, was to show to Tokaev that Nazarbaev clan is not ready to leave the cushy posts within both constitutional bodies as well as state business conglomerates, then Tokaev had to point to himself as “new sheriff in town”. In every case, Tokaev is obviously not ready to leave.¹¹

President Tokaev came out of the January conflict, potentially disastrous not only to him but also to the stability of the whole Central Asian region, as an experienced crisis manager, who stood his ground and quickly restored “law and order”. Faithful to the centuries-long notion that most conflicting situations in Central Asia need to end with parties at least “saving a face”, Nazarbaev, who did not make a public appearance until almost end of January, in a televised speech confirmed that during all this tumultuous month he was in the capital Nursultan, did not leave the country and since 2019 has been “enjoying his well-deserved retirement”. He also did not forget to remind the public, that at time when he left the post of the first president of Kazakhstan, he handed over all powers to Kassym-Jomart Tokaev, the only legitimate president and nation’s leader today. Most likely echoing the not-so-secret rumors around the world that the January events were a result of bloody stand-off between Tokaev and Nazarbaev clans, he even volunteered to validate that “there is no conflict in this country” and “that any rumors

¹¹ The back-room discussions with most of the political analysts engaged in Central Asian region will reveal, that absolutely everybody understands that Nursultan Nazarbaev was not ready to leave in 2019 would it not be for his declining health. While in the cultures of the “East”, a male successor is prepared, all of Nazarbaev’s children are females, and with immediate propelling of his eldest daughter Daryga, the nation could have an uneasy time to absorb the choice. Therefore it is more or less accepted as the reality that Nazarbaev handed over the rule to Tokaev with explicit understanding of both parties that Nazarbaev clan’s political and business interests would be untouched, and perhaps they would even grow in scope. What is more, there may have been an agreement between the two gentlemen that after some time, Daryga would “ascend to the throne”, which apparently did not happen.

regarding this conflict are baseless”. He did not go onto explaining, however, why his closest family members till January holding either high constitutional offices or influential economic positions, are nowhere to be seen or heard.¹²

The question of whether all family business around Nursultan Nazarbaev, including the political and economic influence the first president’s close family members yielded until January 2022, would be liquidated by Tokaev as a possible scenario in the near future may be another topic for discourse. The unilateral dismissal of Nazarbaev from the posts of both Security Council and ruling political party Nur Otan chairmanships by Tokaev is a powerful message to Tokaev’s opponents and allies alike, and at the end of the whole January affair, it is Tokaev who undoubtedly strengthened his position at home and abroad.

7. Deliberations as for Western Interference as a Prelude to New Episode of Great Power Conflict

Central Asian region itself was the place that gave the world the notion of Great Game – essentially referring to centuries-long antagonism between the Russian Tsar and British Empire, so the continuous involvement by Western powers in many of the happenings of Central Asia holding some significance for their geopolitical control is understandable. Ariel Cohen, in his treatise on Kazakhstan’s development in post-Soviet era, outlines the notion of “New Great Game”, gaining new vectors to contend with for Kazakhstan’s leaders:

Competition among the global actors in the Caspian and Central Asian regions has prompted many analysts to compare the situation with the “Great Game” – a confrontation between the Russian and British empires for influence in Central Asia in the 19th century. In the 21st century, however, more players are competing for presence in the region. In order to maintain

¹² His eldest daughter Daryga, member of the Kazakh Mazhilis (parliament), and at time of her father’s retirement rumored to take over as the nation’s president, does not attend parliamentary sessions anymore. Daryga’s second husband Kairat Sharipbaev (although the official marriage has never been confirmed) holding until January 15, 2022 the post of a chief executive at natural gas pipeline operator QazaqGas has resigned. Another Nazarbaev’s son-in-law, married to the former president’s second daughter Dinara, Timur Kulibaev, resigned as chairman of Atameken, Kazakhstan’s National Chamber of Entrepreneurs and the main business lobby group, on January 17. Samat Abish, Nazarbaev’s nephew and second in command of the all-powerful intelligence agency – National Security Committee – was also dismissed on January 17. Nazarbaev’s another son-in-law, husband of his youngest daughter Aliya, Dimash Dosanov, resigned as a chief executive of state oil pipeline conglomerate KazTransOil, on January 15. As of end of January 2022, all of Nazarbaev’s daughters, with their respective families, are reported to be either in the United Arab Emirates or Turkey.

a balance of external interests, Kazakhstan has chosen a path of transparency concerning the country's foreign policy. Over the years Nazarbayev, regardless of the geopolitical climate at the time, has undertaken Eurasian integration initiatives, as well as consulting with the political leadership in Moscow, Washington and Beijing on all important projects in the oil and gas sector. This multi-vector policy course has thus far prevented a single global political player from achieving complete hegemony over Central Asia.¹³

Should we examine the actual geopolitical vectors taken by Nazarbaev in his 30 years in power, indeed as a wise "clansman" he had to court both those in the West (mainly USA and EU), as well as the power centers of the East (Russia and China). Economically, given the vast natural resources mainly in oil and uranium (but not limited to), it was the Western world that benefited from the utilization of this wealth. At one time, Japanese companies controlled 30% of all uranium mining aimed at supplying Japan's multiple nuclear power plants with sustainable source of fuel. In oil sector, from as early as 1993, Chevron Texaco and ExxonMobil held 75% of the Tengiz oil field in Caspian Sea, developing it jointly with Kazakh and Russian counterparts. Another major breakthrough for Western interests came when between 1996 and 2003 Chevron, Mobil, Shell and BP joined the Caspian Pipeline Consortium, transporting oil from Kashagan oil field to world markets. Nazarbaev was clearly important to the West, and as with many similar individuals controlling vast resources, the West not only did not comment on periodic human rights abuses and persecution of political opposition within Kazakhstan, but often lent a willing hand to quell dissent within Nazarbaev surroundings.¹⁴

Although the Panama Papers in 2018 revealed a multitude of offshore wealth related to Nazarbaev clan, during January 2022 events in Kazakhstan when whereabouts of Nazarbaev himself as well as his extended family were unknown, the Western media limited themselves to highlighting some real estate held by Nazarbaev family overseas, without particular deliberations on his stance towards the country-wide uprising.

¹³ Cohen A. (2008), *Kazakhstan: The Road to Independence – Energy Policy and the Birth of a Nation*, p. 84.

¹⁴ One of the many telling examples would be the story of Nazarbaev's eldest daughter Daryga's first husband Rakhat Aliyev (himself a one-time heavyweight of Kazakh intelligence and political elite) who concluded his career by ambassadorship to Austria, but after criticism of his father-in-law, he suddenly found himself accused and convicted of various crimes in absentia, and subsequently died "by suicide" in an Austrian detention jail in 2015.

8. Scarecrow of Terrorism in the Region during the Weeks that Followed

The “Siege of Almaty”, if the roughly two-week long events can be called – referring to the initial insurgency and subsequent swift response from both restructured Kazakh internal security forces and CSTO troops, seemed to have left the people’s minds very quickly in its aftermath. Just as unexpectedly the incident occurred at the beginning of the year, by the end of January 2022 most of the region and the world was focused on other issues, mainly on the build-up of Russian armed forces along the Ukrainian borders. The Almaty events were in fact more reminiscent of Kazakhstan’s politically volatile neighbor – Kyrgyzstan – where as recently as in October 2020 (dubbed “Third Kyrgyz Revolution”) the mass violent protests in the capital Bishkek aimed at alleged parliamentary election votes rigging resulted in subsequent resignation of then president Sooronbay Jeenbekov. The Kyrgyz nation has grown accustomed to regular popular revolt, by many seen as legitimate display of democracy in action, so the January insurgency in Almaty was not seen as something extraordinary – although it surprised those who viewed Kazakhstan as a politically stable Central Asian state.

However, it perhaps benefits mentioning two issues, both occurring in Kyrgyzstan in the coming weeks of January, where the explanation was in part attributed to possible terrorism, although in extend and implications for the country and the region did not have such wide ranging effect as the Almaty events.

8.1 Issue 1 – Widespread unexpected blackout affecting Kyrgyzstan, Kazakhstan and Uzbekistan on January 25

On Tuesday January 25, southern Kazakhstan (including its largest city Almaty), northern Kyrgyzstan (including the capital Bishkek) and most of Uzbekistan (including the capital Tashkent) reported power outages that affected not only the electricity networks, but also all other utilities such as gas and water supply, in addition to most of the critical infrastructure (in particular in Uzbekistan). While most of the media outlets reported “emergency imbalances” and outlined some of the technicalities of the current electricity grid system in Central Asia¹⁵, it was faster and more telling to actually ask some of the affected cities’ residents on their notion of what happened. While Almaty and Bishkek experienced black-outs lasting not more than 4-5 hours, Tashkent for example was affected for almost 24 hours, and because of non-functioning gas and water supplies in addition to electricity, inhabitants

¹⁵ <https://thediomat.com/2022/01/blackouts-strike-kazakhstan-kyrgyzstan-and-uzbekistan>.

quickly rushed to empty the local supermarkets of most essential goods, mainly bottled water. The first hurried conclusion, given the scale of power outage across three major countries of Central Asia, was “terrorism”, although very quickly the most plausible technological causes were being discussed over the media.¹⁶

8.2 Issue 2 – Mass protests in Bishkek aimed at freeing the recently detained public activists

Between January 25 and 27, masses took to the streets of Bishkek in protest of a journalist Bolot Temirov and Kyrgyz traditional bard singer Bolot Nazarov being detained – who were subsequently under the public pressure released. Both Temirov and Nazarov were initially arrested on charges related to alleged illegal narcotics possession, but the protesters quickly deduced that the recent Temirov’s broadcast about Kyrgyz President Sadyr Japarov and the head of the country’s State Committee for National Security, Kamchybek Tashiev, (accusing both of high profile corruption) were the real reasons for detention. The protests, although this time they did not grow into storming into official administrative buildings as in October 2020, were loud enough to be heard across the region, but somehow got lost in international press coverage. Since the State Committee for National Security’s (de facto both an intelligence and counter-intelligence KGB-style apparatus) main activities focus on countering narcotics trade across the region and terrorism (very often two areas intricately linked as one financing the other), to many it was clear that by accusations related to drug charges the government wants to subconsciously invoke another perception of “terrorism threat”. Instead, the protesters in support of detainees, actively voiced a need to immediately dis-

¹⁶ The author’s long-time government contact in Bishkek commented the temporary energy loss to four possible causes:

- An act of terrorism on the territory of Kazakhstan within a critical infrastructure point (presumably in electricity supply grid) lead not only to instant black-out locally, but also affected the networks across three countries
- A technological fire at an unidentified power station in Uzbekistan lead to wide-spread blackout (this theory apparently explaining why Tashkent was affected for prolonged period of time) – this possible cause was even coupled by a short video circulating social media allegedly showing the fire – although as usually is the case, the video does not specify the exact location, time or even the fact that it is a power station
- A deliberate act of switching off the electricity supply on part of Turkmenistan lead to wide-spread blackout. One of the reasons as to why Bishkek was able to limit the power outage to several hours the contact mentioned the proper functioning of both Kemin hydro power plant and Datka-Kemin electricity power line launched in 2015, effectively making sure that the local power is restored quickly.

miss Kamchybek Tashiev, as well as Minister of Interior Ulan Niyazbekov, and the protests' vigor allegedly even made the president Japarov consider the pros and cons of such high-level dismissals. At the end, however, the officials remained in place and Japarov was later seen travelling to Beijing Olympics instead. It is beyond doubt though, that Almaty events of January made the incumbent Kyrgyz leader think twice about possible launching of power mechanisms to suppress the dissent, and resolved to free the detainees and thus even indirectly admit that the charges were fabricated. It also shows the region's sensitivity to mass displays of dissent, and in Kyrgyz case, not wanting to repeat the scale of disapproval – similar to that which brought the current president to power.

9. Conclusions

One conclusion that can be drawn with certainty is that the chain of events in Almaty and country-wide Kazakhstan between January 2 and 5 quickly got out of general population's hands and the whole affair grew from a household dissent into violent armed insurgency, being suppressed likewise with arms and violence. If the initial meetings were organized and brought about by the general population protesting steep rise in fuel prices and other essentials, the country's power elites speedily classified the uprising as “terrorist insurgency leading to coup d'état” and dealt with it accordingly. As far as city of Almaty, as the center of CSTO intervention, is concerned, it is understood that many participants in the violent riots were brought in from neighboring villages immersed in poverty (possibly paid for their participation), and some elements of foreign involvement was confirmed. One of the questions asked by many is that why Almaty was chosen as the main stage of these events – in relation to other parts of the country (apart from artificially constructed capital city Nursultan) – as Almaty has always been prospering by any Central Asian standards, and perhaps that is one of the reasons why the city's residents faced difficulties in understanding the scope of both dissent as well as government's reaction.

Another common observation is – if the aim of the “foreign terrorists” was indeed the a coup d'état – then why the capital Nursultan was left out of the “action” and the protests concentrated mainly on industrial and commercial centers around the country.

As part of the “New Great Game” discourse, many of the lessons from January events in Kazakhstan can be drawn regarding the new West-East standoff today, bordering at the commencement of full-fledged World War III. Giving some weight to the plausibility of active Russian involvement from the onset of country-wide attempt for uprising in Kazakhstan, it may perhaps merit to mention that this time it was the “Russian Empire” which launched the

preemptive “strike”, in order to keep the West at bay. The Western powers, it seems, took notice, but were again caught off guard less than two months later, this time much closer to their geopolitical domain.

Combined with situation in Ukraine in February 2022, and with yet again emerging military clashes amidst stand-off in Nagorno-Karabakh between Armenia and Azerbaijan, there seems to be a growing pattern for solving the accumulated political and economic issues in the area of post-Soviet Union – use of brute force from the very beginning of a conflict, with little regard for ordinary citizens who are always caught in the middle, and who are reduced to solving existential problems, rather than those played in high geopolitics.

In retrospect of the very beginning of this year, and the world having lived through March that continuously brings a graphic reminder of the surrounding universe, the events in Almaty were nothing but a mild awakening into the new geo-political realities of 21st century. Power methods prevail over diplomacy as a solving medium. Violence is applied from the outbreak of any conflict as the means to subdue challenges to status quo. Blood needs to be spilled in order to remember what is at stake and what values the humankind gradually leaves behind in its quest for imaginary control.

References

- Abazov R. (1998), *Practice of Foreign Policy Making: Formation of Post-Soviet Politics of Kazakhstan, Kyrgyzstan, and Uzbekistan*, NATO Research Fellowship supported Paper.
- Abdrakhmanov T. (2013), *L'islam au Kazakhstan: les rapports Etats-religion (XVI-Ilème – Xxème siècles)*, a Doctorate Thesis, Université Michelde Montaigne, Bordeaux, France.
- Akhpanov A., Skakov A., Sembekova B., Madiyeva A. and Amirgaliyev A. (2019), *About Counteraction To Extremism And Terrorism In Kazakhstan*, *Revista de Ciencias Humanas y Sociales Año 35, N° 88*, Oficina de Publicaciones Científicas de la Facultad Experimental de Ciencias, Universidad del Zulia, Maracaibo – Venezuela.
- Almen D. (2013), *Turkey's Foreign Policy towards Kazakhstan in the Post-Soviet Period*, a Master's Thesis, the Graduate School of Social Sciences, Middle East Technical University, Ankara, Turkey.
- Anti-Corruption Reforms in Kazakhstan – Round 3 Monitoring of the Istanbul Anti-Corruption Action Plan (2014)*, Report adopted at the Istanbul Anti-Corruption Action Plan plenary meeting on 10 October 2014, Organisation for Economic Co-Operation and Development, Paris, France.
- Akiner S. (2005), *Violence in Andijan, 13 May 2005: An Independent Assessment*, Central Asia-Caucasus Institute & Silk Road Studies Program, USA & Sweden.

- Akylbayeva I., Malgarayeva Z., Abdigaliyeva G. and Kochshigulova K. (2014), Potentiality of Religious Conflict in Kazakhstan, *European Scientific Journal* June 2014 /SPECIAL/ edition vol. 1.
- Azizian R. (2006), Countering Islamic Radicalism in Central Asia, Article in *Quarterly Journal*, Winter Supplement 2006.
- Baisagatova D.B., Kemelbekov S.T., Smagulova D.A. and Kozhamberdiyeva A.S. (2016), Correlation of Concepts “Extremism” and “Terrorism” in Countering the Financing of Terrorism and Extremism, Article in *International Journal of Environmental & Science Education*, Vol. 11, No. 13.
- Baizakova Z. and McDermott R.N. (2015), Reassessing the Barriers to Islamic Radicalization in Kazakhstan, Strategic Studies Institute, US Army War College.
- Baran Z., Starr S.F. and Cornell S.E. (2006), Islamic Radicalism in Central Asia and the Caucasus: Implications for the EU, Central Asia-Caucasus Institute & Silk Road Studies Program, USA & Sweden.
- Biard A. (2019), “We Pray for Our President”: Saudi-Inspired Loyalist Salafism and the Business Sector in Kazakhstan, Working Paper, Berkley Center for Religion, Peace and World Affairs, Georgetown University.
- Becker C.M., Marchenko G.A., Khakimzhanov S., Seitenova A.S. and Ivliev V. (2009), *Social Security Reform in Transition Economies – Lessons from Kazakhstan*, Palgrave Macmillan, New York, USA.
- Beissembayev S. (2016), Religious Extremism in Kazakhstan: From Criminal Networks to Jihad, *The Central Asia Fellowship Papers* No. 15.
- Bertelsmann Stiftung’s Transformation Index (BTI) Country Report – Kazakhstan (2018), Bertelsmann Stiftung, Germany.
- 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.
- Chen A. (2017), Kazakhstan’s Geo-economic Quest for Power in a Multipolar World, a Master’s Thesis, Naval Postgraduate School, Monterey, USA.
- Chufrin G. (ed.) (2001), *The Security of the Caspian Sea Region*, Stockholm International Peace Research Institute, Oxford University Press.
- Cohen A. (2008), *Kazakhstan: The Road to Independence – Energy Policy and the Birth of a Nation*, Central Asia-Caucasus Institute & Silk Road Studies Program, USA & Sweden.
- Cornell S.E., Starr S.F. and Tucker J. (2018), *Religion and the Secular State in Kazakhstan*, Central Asia-Caucasus Institute & Silk Road Studies Program, USA & Sweden.
- Country Flyer – Kazakhstan (2021), *The NATO Science for Peace and Security Programme*.
- Cummings S.N. (2005), *Kazakhstan – Power and the Elite*, I.B. Tauris, London and New York.

- 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.
- Derichs C. and Fleschenberg A. (eds.) (2010), *Religious Fundamentalisms and Their Gendered Impacts in Asia*, Friedrich-Ebert-Stiftung, Berlin, Germany.
- Dildabekova D. and Robertson O. (eds.) (2013), *Counter-terrorism in Kazakhstan – Why the Death Penalty Is No Solution*, Penal Reform International, London, United Kingdom.
- Esposito J.L., Voll J.O. and Bakar O. (eds) (2008), *Asian Islam in the 21st Century*, Oxford University Press, New York, USA.
- Evers F., Klötzer J., Seifert A.C. and Somfalvy E. (2018), *Civilian Prevention of Radicalization in Central Asia*, Working Paper 30, Centre for OSCE Research, Institute for Peace and Security Policy (IFSH), University of Hamburg, Germany.
- Evron Y. (2007), *China's Anti-Terrorism Policy*, Article in Strategic Assessment, Volume 10, No. 3, December 2007.
- Gabriel M.A. (2015), *Islam and Terrorism – The Truth about ISIS, the Middle East, and Islamic Jihad*, FrontLine Charisma Media, Lake Mary, USA.
- Global Terrorism Index (2020), *Measuring the Impact of Terrorism*, Institute for Economics & Peace, Sydney, Australia.
- Gussarova A. (ed.) (2016), *Current Challenges to Central Asia and Afghanistan: Towards a Better World in 2040*, Central Asia Institute for Strategic Studies, Friedrich-Ebert-Stiftung.
- 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.
- Kangas R. (2018), *Redefining Extremism in Central Asia*, Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW) Strategy Series: Focus on Defense and International Security, Berlin, Germany.
- Karin E. (2017), *Central Asia: Facing Radical Islam* (Russie.Nei.Visions No. 98), Institut français des relations internationales (IFRI) Russia/NIS Center, Paris, France.
- Kazakhstan – Tier 2 (2018), United States Commission on International Religious Freedom (USCIRF) Annual Report.
- Khalid A. (2007), *Islam after Communism – Religion and Politics in Central Asia*, University of California Press, Berkeley, USA.
- Kurmashev A., Akhmedyanova D., Zholdasbekova A. and Sadri H. (2018), *Kazakhstan's Middle Power Response to Terrorism*, Article in Insight Turkey Vol. 20 / No. 4.
- Law of the Republic of Kazakhstan – On Combating Legalization (Laundering) of Illegally Gained Income and Financing of Terrorism.
- Lenz-Raymann K. (2014), *Securitization of Islam: A Vicious Circle (Counter-Terrorism and Freedom of Religion in Central Asia)*, Swiss National Science Foundation.
- Lemon E. (2018), *Talking Up Terrorism in Central Asia* (Kennan Cable No. 38), Woodrow Wilson International Center for Scholars, USA.

- Lynch III T.F., Bouffard M., King K. and Vickowski G. (2016), *The Return of Foreign Fighters to Central Asia: Implications for U.S. Counterterrorism Policy* (Strategic Perspectives, No. 21), Center for Strategic Research, Institute for National Strategic Studies, National Defense University, USA.
- Mankoff J. (2009), *Russian Foreign Policy – The Return of Great Power Politics*, A Council on Foreign Relations Book, Rowman & Littlefield Publishers, Inc., USA.
- McDermott R.N. (2012), *Kazakhstan – Russia – Enduring Eurasian Defence Partners*, Danish Institute for International Studies, Copenhagen, Denmark.
- Migacheva K. and Frederick B. (eds.) (2018), *Religion, Conflict, and Stability in the Former Soviet Union*, RAND Corporation, Santa Monica, USA.
- Mori S. and Taccetti L. (2016), *Rising Extremism in Central Asia? – Stability in the Heartland for a Secure Eurasia*, European Institute for Asian Studies, Brussels, Belgium.
- Mohammadov A.H. and Ashrafi M. (2017), *Investigating the Challenges of Religious Extremism in Central Asia and Its Impact on the National Security of the Surrounding Nations*, *QUID 2017*, pp. 2789-2796, Special Issue N°1, Institución Universitaria Salazar y Herrera, Medellín – Colombia.
- Nazpary J. (2002), *Post-Soviet Chaos – Violence and Dispossession in Kazakhstan*, Pluto Press, London and Sterling.
- Nurgaliyeva L. (2016), *Kazakhstan's Economic Soft Balancing Policy vis-à-vis Russia: From the Eurasian Union to the Economic Cooperation with Turkey*, *Journal of Eurasian Studies* 7 (2016) 92–105.
- Olcott M.B. (2007), *The Roots of Radical Islam in Central Asia*, Carnegie Endowment for International Peace, USA.
- Omelicheva M.Y. (2011), *Counterterrorism Policies in Central Asia*, Routledge Central Asian Studies, New York, USA.
- 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.
- Omelicheva M.Y. (2013), *Terrorism in Central Asia – Dynamics, Dimensions and Sources* (Article retrieved from *Education about Asia* Volume 18, Number 3, Winter 2013), Association for Asian Studies, USA, <https://www.asianstudies.org/publications/ea/archives/terrorism-in-central-asia-dynamics-dimensions-and-sources/>.
- Rashid A. (2000), *Taliban – Islam, Oil and the New Great Game in Central Asia*, I.B. Tauris, London and New York.
- Rashid A. (2001), *Taliban – Militant Islam, Oil and Fundamentalism in Central Asia*, Yale University Press, New Haven and London.
- Reljić D. (2008), *Political Extremism, Terrorism, and Media in Central Asia – The Examples of Kazakhstan and Kyrgyzstan*, International Media Support, Copenhagen, Denmark.
- Rittmann M. (2012), *Striking Oil, Striking Workers – Violations of Labor Rights in Kazakhstan's Oil Sector*, Human Rights Watch, USA.
- Russell M. (2022), *Chaos and crackdown in Kazakhstan: What next?*, Members' Research Service, European Parliamentary Research Service.

- Rysbekova S., Kurmanaliyeva A. and Borbassova K. (2018), Educating for Tolerance in Kazakhstan, *Comparative Literature and Culture* Volume 20, Issue 2, Article 10, Purdue University Press.
- Satre J. (2022), Demonstrations in Kazakhstan: From Energy Price Hike to Political Crisis, Article in *Armed Conflict Location & Event Data Project (ACLED)*.
- Sorbello P. (2015), The Role of Energy in Russian Foreign Policy towards Kazakhstan, *Energy Brains*.
- Todoroki E., Celik K. and Kholmatov M. (2011), Alternative Remittance Systems in Kazakhstan, *Financial Market Integrity Financial and Private Sector Development*, The World Bank.
- Tukhvatulin S.T., Zhotabayev Z.R., Azarov V.A. and Silayev M.E. (1998), National Nuclear Center of the Republic of Kazakhstan in the System of Nuclear Terrorism Counteractions at Kazakhstan Territory, *International Atomic Energy Agency Paper IAEA-CN-98/4/03*.
- Tuyakbayev S. (2003), Security Issues in Central Asia and Foreign Security Policies of Kazakhstan and Uzbekistan, *UNISCI Discussion Papers No. 3*, Madrid, Spain.
- Warikoo K (ed.) (2011), *Religion and Security in South and Central Asia*, Central Asia Research Forum Series, Routledge, London and New York.
- Wolters A. (2014), *The State and Islam in Central Asia: Administering the Religious Threat or Engaging Muslim Communities?*, PFH Forschungspapiere/Research Papers, No. 2014/03, Göttingen, Germany.
- Yemelianova G. (ed.) (2010), *Radical Islam in the Former Soviet Union*, Routledge Contemporary Russia and Eastern Europe Series, London and New York.
- Yilamu W. (2018), *Neoliberalism and Post-Soviet Transition – Kazakhstan and Uzbekistan*, Palgrave Macmillan, Cham, Switzerland.
- Zenn J. and Kuehnast K. (2014), *Preventing Violent Extremism in Kyrgyzstan*, United States Institute of Peace Special Report 355, Washington D.C., USA.

Websites

- <https://cabar.asia/>
<https://eurasianet.org/>
<https://fergana.ru/>
<https://www.longwarjournal.org/>
<https://www.voanews.com/>

“Working and Waiting”: The Salafi-Jihadi movement on Telegram in 2021

ALI FISHER – NICO PRUCHA

Ali Fisher has a dual specialism in Strategic Communication and Data Science. Ali worked at the University of Exeter as a Lecturer in International Relations and as Director of Counterpoint, the think tank of the British Council in London. He subsequently worked as Associate Director of Digital Media Research at InterMedia, and Director of Mappa Mundi Consulting. In recent years he was Principal Data Scientist at the Vienna Observatory for Applied Research into Terrorism and Extremism, (VORTEX) at the University of Vienna, a Research Fellow at the University of Southern California, and now is Director of Human Cognition Ltd. based on London. In additions to his academic work, he has worked on Strategic Communication projects and Counter Terrorism projects for European and US Government Departments. He has used Big Data techniques and Network Analysis to support efforts to disrupt extremist networks of influence as well as the interrupt the distribution of images of child sexual abuse. Ali has a PhD from University of Birmingham.

Nico Prucha is Chief Content Curator at Human Cognition and Head of the Extremism Desk at T3K. He is a fluent Arabic speaking specialist in Jihadist theology and strategy. His work has covered the use of the internet by Jihadist groups from the mid-2000s to the present and documented shifts in strategy from Forum to Twitter to Telegram. Focused on al-Qa”ida and Islamic State he has written numerous evidence-based research articles on the lingual and theological aspects of their da”wa and media strategies. His blog is available at www.onlinejihad.net. Nico has a PhD from University of Vienna.

Abstract

Salafi-Jihadi groups adopted the Telegram messaging platform around 2016. Since then, it has been a mainstay of the information ecosystem for groups such as al-Dawlat al-Islamiyah (IS) and al-Qaeda (AQ) and other foreign terrorist organisations (FTO). While the Salafi-Jihadi movement has been using Telegram, the general userbase of the platform has grown rapidly, it was 5th most downloaded mobile app worldwide in 2021 and 13th most used social platform globally.¹ This paper uses examines how the Salafi-Jihadi movement operates on Telegram as a network of interconnected hubs where traffic and influence flow in multiple directions creating a vast dynamic ecosystem. This research offers the most comprehensive analysis, to date, of the information ecosystem of Salafi-Jihadi groups on Telegram. It is based on observation during 2021 of over 7,000

¹ Simon Kemp, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 <https://blog.hootsuite.com/simon-kemp-social-media/>; <https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Mobile-App-Rankings-Downloads.png>; <https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Worlds-Most-Used-Social-Platforms.png>

channels belonging to elements of the Salafi-Jihadi movement including IS, AQ, Taliban, the Muslim Brotherhood, and Hamas, along with Salafi channels of importance to the movement. It finds that just under 90% of the channels connect into a single giant network (including channels from IS, AQ, Taliban, the Muslim Brotherhood, and Hamas). This means they are part of an interconnected ecosystem which comprise sub-clusters that have varying degrees of shared meaning. They often share common sources of content, frequently those channels on the Salafi side of the Salafi-Jihadi nexus. Such channels create a permissive environment in which Salafi-Jihadi groups can target their intended audience, and share material to bolster their theological position to craft a specific religious identity. Furthermore, the most important Salafi channels are much more likely than other channels to be sharing join links to other channels. Despite the volume of data available via Telegram, with some notable exceptions, much of the analysis and commentary of the Salafi-Jihad movement on Telegram has been anecdotal or superficial, resulting in the image of very insular Jihadi communities just talking to themselves.² In 2021, far from being driven off Telegram (or the internet) by EUROPOL led disruption efforts, the Salafi-Jihadi movement and the FTO elements within it, have reconfigured just as a flock of birds adjusts in flight to the attack of a predator. In 2022 they continue to exploit the platform.

Keywords

Salafi-Jihadi movement, Telegram, strategic communication

1. Introduction

Salafi-Jihadi groups adopted The Telegram messaging platform around 2016. Since then, it has been a mainstay of the Salafi-Jihadi information ecosystem for groups such as al-Dawlat al-Islamiyya (IS) and al-Qaeda (AQ) and other foreign terrorist organisations (FTO). While the Salafi-Jihadi movement has been using Telegram, the userbase of the platform has grown rapidly. It was 5th most downloaded mobile app worldwide and 13th most used social platform in 2021.³ In contrast, Twitter once hailed as the platform on which IS achieved mass reach is now ranked 15th by user numbers and has approximately 100 million fewer users than Telegram and didn't feature in the top mobile downloads.⁴

² For a lengthy analysis see, Spagna, Nicolo' Giuseppe, *Ethnographizing Islamic State's Digital Community on Telegram Platform; Socio-Organizational Anatomy and New Models of Threat*, BTT, (November 2021).

³ Simon Kemp, *TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats)*, October 21, 2021 <https://blog.hootsuite.com/simon-kemp-social-media/>; <https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Mobile-App-Rankings-Downloads.png>; <https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Worlds-Most-Used-Social-Platforms.png>

⁴ Simon Kemp, *TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats)*, October 21, 2021 <https://blog.hootsuite.com/simon-kemp-social-media/>; <https://blog.hootsuite.com/simon-kemp-social-media/>

There have been numerous attempts over the years to ‘deplatform’ Salafi-Jihadi groups. Much has been made in the press and by ‘embedded academics’ from the transatlantic orthodoxy of Terrorism Studies, about the attempt by EUROPOL to prevent Jihadi groups from using Telegram.⁵ The imminent removal of Jihadi groups from Telegram was trailed in advance by some researchers, whom have advisory connections to EUROPOL, and later the effort was hailed as having “resolutely trashed the Islamic State’s presence on Telegram”.⁶ This follows a familiar pattern where many researchers and ‘embedded academics’ in the transatlantic orthodoxy of Terrorism Studies, have perpetuated a ‘success narrative’ about the online efforts against Salafi-Jihadi groups, while the Media Mujahidin have been forging ahead, exploiting new technologies and approaches.⁷

Despite the volume of data available via Telegram, with some notable exceptions, much of the analysis and commentary of the Salafi-Jihad movement on Telegram has been anecdotal, superficial, or focused on a single group resulting in the image of very insular Jihadi communities just talking to themselves.⁸ Most work focuses on the use of Telegram by IS, with comparatively little attention paid to AQ or Taliban activity.⁹

com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Mobile-App-Rankings-Downloads.png; <https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Worlds-Most-Used-Social-Platforms.png>

⁵ The role of ‘embedded academics’ in the transatlantic orthodoxy of Terrorism Studies, Jackson, RDW, ‘The Case for a Critical Terrorism Studies’ (2007) <http://hdl.handle.net/2160/1945>; <https://pure.aber.ac.uk/portal/files/99753/APSA-2007-Paper-final2.pdf>

⁶ <https://www.wired.co.uk/article/isis-telegram-security>

⁷ The role of ‘embedded academics’ in the transatlantic orthodoxy of Terrorism Studies, Jackson, RDW, ‘The Case for a Critical Terrorism Studies’ (2007) <http://hdl.handle.net/2160/1945>; <https://pure.aber.ac.uk/portal/files/99753/APSA-2007-Paper-final2.pdf>

⁸ For a lengthy analysis see, Spagna, Nicolo’ Giuseppe, *Ethnographizing Islamic State’s Digital Community on Telegram Platform; Socio-Organizational Anatomy and New Models of Threat*, BTT, (November 2021); Yayla, Ahmet S., and Anne Speckhard. “Telegram: The mighty application that ISIS loves.” *International Center for the Study of Violent Extremism* 9 (2017); Bloom, Mia, Hicham Tiflati, and John Horgan. “Navigating ISIS’s preferred platform: Telegram1.” *Terrorism and Political Violence* 31.6 (2019): 1242-1254; Shehabat, Ahmad, Teodor Mitew, and Yahia Alzoubi. “Encrypted jihad: Investigating the role of Telegram App in lone wolf attacks in the West.” *Journal of strategic security* 10.3 (2017): 27-53; Bloom, Mia, and Chelsea Daymon. “Assessing the future threat: ISIS’s virtual caliphate.” *Orbis* 62.3 (2018): 372-388; Criezis, Meili. “Online Deceptions.” *Perspectives on Terrorism* 14.1 (2020): 67-73; Amarasingham, Amarnath, Shiraz Maher, and Charlie Winter. “How Telegram disruption impacts jihadist platform migration.” *Centre for Research and Evidence on Security Threats* (2021).

⁹ Prucha, Nico. “Is and the jihadist information highway—projecting influence and religious identity via telegram.” *Perspectives on Terrorism* 10.6 (2016): 48-58.

Using a progressive evidence-based approach, the collaboration between data science and domain expertise, is fundamental for this research. This approach enables researchers to develop a strategic level ‘bird’s eye view’ of the way Salafi-Jihadi use the Telegram platform, how the groups related to each other and how designated Foreign Terrorist Organisations relate to other groups who coordinate around interpretations of Salafi theology and employ the rich and long-standing textual traditions to further their cause.

The paper offers the most comprehensive analysis, to date of the information ecosystem of Salafi-Jihadi groups on Telegram. Based on Telegram messages observed during 2021 of over 7,000 channels belonging to elements of the Salafi-Jihadi movement including IS, AQ, Taliban, the Muslim Brotherhood, and Hamas, along with Salafi channels of importance to the movement.

It finds around 90% of the channels connect into a single giant network. They are not insular, as some would believe, but part of an interconnected ecosystem which comprise sub-clusters that have varying degrees of shared meaning. This does not necessarily mean that FTO channels directly share content from each other, they instead share common sources of content, frequently those on the Salafi side of the Salafi-Jihadi nexus. Common sources of content are, for example, a range of historical Salafi writings by scholar such as Ibn Taymiyya, Muhammad ibn ‘Abd al-Wahhab, or Ibn al-Qayyim. Such channels create a permissive environment in which Salafi-Jihadi groups can target their intended audience, and from which theologically aligned material to bolster the credibility of their theological position is shared.

In 2021, far from being driven off Telegram (or the internet) the Salafi-Jihadi movement and the FTO elements within it, have reconfigured just as a flock of birds adjusts in flight to the attack of a predator. In 2022 they have continued to exploit the platform.

2. What is Telegram

The Media Mujahidin have used Telegram to communicate since 2016.¹⁰ According to Telegram developers, Telegram is a cloud-based instant messaging service, providing optional end-to-end encrypted messaging. Telegram lets users access their chats from multiple devices with messages that are heavily encrypted and can self-destruct. Telegram has no limits on the size of your

¹⁰ Prucha, Nico. “Is and the jihadist information highway—projecting influence and religious identity via telegram.” *Perspectives on Terrorism* 10.6 (2016): 48-58; Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. *The New Netwar: Countering extremism online*. Policy Exchange, 2017.

media and chats, and groups can hold up to 200,000 members.¹¹ It is free and open, having an open API and protocol free for everyone, which has allowed users to build their own bots, and even their own clients to access Telegram.

Over the last five years Telegram has been the most important social media platform for jihadist media operatives, to project influence, disseminate videos, text documents, pictures, audio and torrent files. Since its adoption, Telegram has customarily been the first point where Salafi-Jihadi content is released into the information ecosystem.

Much of the ‘success narrative’ produced by the Transatlantic orthodoxy of Terrorism Studies has presented the adoption of Telegram as the result of disruption on Twitter forcing IS and AQ to use smaller platforms on the margins of the internet. From the perspective of the Media Mujahidin Telegram has had much greater utility for their efforts to communicate with supporters. Telegram created the opportunity for the Media Mujahidin to use one app to have encrypted conversations, share large files, broadcast content to thousands of users, large group text chat, now with the option to allow millions of users to chat live¹² along with one-to-one video, and automated features including bots¹³ to moderate groups or interact with users to share content.

It is important to note, while the move to Telegram by the Media Mujahidin has been mythologized within the transatlantic orthodoxy of terrorism studies as the result of a ‘successful’ effort to drive them from Twitter, there is another perspective. First, the tech landscape has shifted dramatically. Telegram now has both a larger userbase than Twitter and a greater number of mobile downloads. Second, even when Salafi-Jihadi groups such as the Taliban are able to use Twitter openly and maintain classical websites, they have Telegram groups with tens of thousands of users. Third, Telegram enables users to engage with the full range of groups and content across both sides of the Salafi-Jihadi nexus, not just Foreign Terrorist Organisations.¹⁴ Fourth, on Telegram large Salafi networks are well established. This is the primary target audience for Salafi-Jihadi groups to garner sympathizers and recruits, with the Media Mujahidin linking to Salafi-only channels and resharing Salafi content within Salafi-Jihadi channels to demonstrate the application of theology at the center of Salafi scholarship in the Salafi-Jihadi ambition of why and for what they fight. For example, the Islamic States uses anti-Shiite theology to dehumanize Iraqi Shiites and as an ultimate justification to execute captured Iraqis, accused of working for the army and being Shiite. For this pur-

¹¹ <https://telegram.org/>

¹² <https://telegram.org/blog/voice-chats-on-steroids#limitless-voice-chats>

¹³ <https://core.telegram.org/bots>

¹⁴ For detail on Salafi-Jihadi Nexus see: Fisher, Prucha, ‘Understanding the Global Jihadist Movement 20 years after 9/11’, EICTP Expert Paper, October 2021.

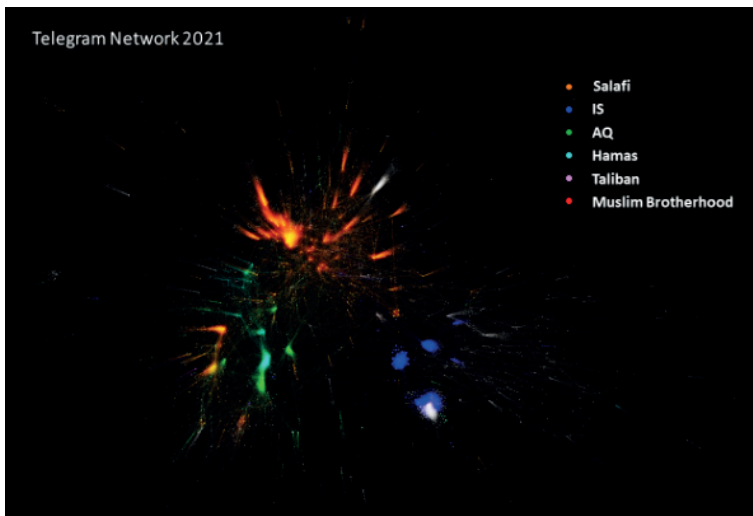
pose, Salafi scholar positions are embedded into IS videos showing the killing and filming inside Shia mosques in Iraq as further ‘proof’ of the ‘heresy’ that makes the fight against all Shia Muslims an ultimate obligation.¹⁵

3. Telegram Data

The full range of material of mainstream Salafi and Salafi-Jihad material is available on Telegram. Channels¹⁶ were identified by fluent Arabic speaking subject matter experts, joining both open channels and channels requiring prior interaction with group admins to gain access. The channels which were joined were associated with well-known Salafi-Jihadi groups and aligned organisations or Salafi channels shared by Salafi-Jihadi groups. Data is collected in near real-time via the Telegram API.¹⁷ All messages forwarded in 2021 were aggregated to build the dataset for the network graph.

The network of content sharing (one channel/group resharing messages from another channel/group) within the core of the movement shows a network of over 7,200 channels. The network of content sharing during 2021 shows that despite the orthodox narrative about “trashed” networks and driving IS from Telegram, the movement is still well established and active on the platform.

Figure 1 - *Telegram Network 2021*



¹⁵ Out of the many possible examples, the IS videos Salil al-Sawarim, part 4 and ‘ala Minhaj al-Nubuwa demonstrate this mindset based on theology very clearly.

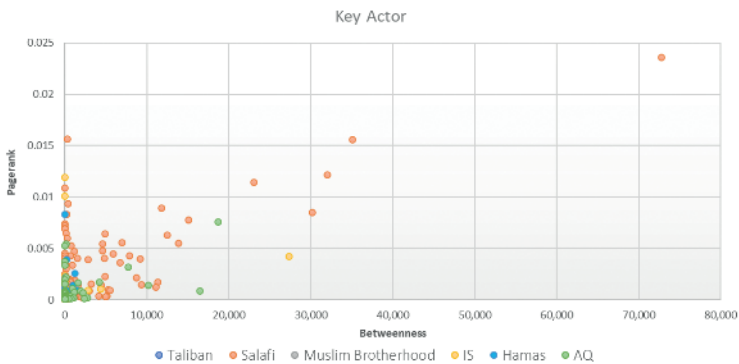
¹⁶ Channels is used to describe the range of broadcast channels, and group chats.

¹⁷ Data was collected by BlackLight, a product of Human Cognition ltd. BlackLight has been used to deliver data to Governmental agencies and Social Media companies in Europe and the United States.

There are 11,553 connections between the channels. While this creates a large network, this is only 0.04% of the potential connections. This is a sparse network but one which still has an underlying structure. Examining the graph in detail finds almost 90% (89.3% – 6,466 of 7,241 total) of channels are connected in a single giant component. This network has a diameter of 14 and comprises 36 communities or particularly interconnected network sub-clusters.¹⁸

The existence of the giant component emphasises the ability for the network to remain connected despite efforts at disruption. This ‘giant’ component comprises channels associated with groups including IS, AQ, Taliban, Hamas, and the Muslim Brotherhood, along with many Salafi channels. It shows that while Salafi-Jihadi groups rarely share content directly from each other’s channels, they are still connected via primarily Salafi groups. This means that while IS, AQ, Hamas, Taliban and the Muslim Brotherhood may not connect directly, they are all connected to the same network, and draw on the same ecosystem of content and theological material, which, at its heart, is comprised of thousands and thousands of pages mainly in Arabic, penned by historical and contemporary Salafi scholars.

Figure 2 - Key Actor graph based on betweenness and PageRank



A Key Actor graph shows the important nodes within a network based on betweenness and PageRank.¹⁹ Betweenness shows how important a node is

¹⁸ Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, Etienne Lefebvre, Fast unfolding of communities in large networks, in *Journal of Statistical Mechanics: Theory and Experiment* 2008 (10), P1000; R. Lambiotte, J.-C. Delvenne, M. Barahona Laplacian Dynamics and Multiscale Modular Structure in Networks 2009

¹⁹ Fisher, A., et al. “Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability.” Policy Brief, Royal United Services Institute, London (2019). (p.16); Willis, Alistair, Ali Fisher, and Ilia Lvov. “Mapping networks of influence: tracking Twitter conversations through time and space.” *Participations: Journal of Audience & Reception Studies* 12.1 (2015): 494-530; Marie Gillespie et al., “Understanding the Changing Cultural Value

Elements of IS content are easy to find within these channels. Here two clips from IS videos appear between pictures of a cat and a picture of roses. One clip features an IS-suicide bomber, with his smiling portrait blended into the explosion with the IS-logo in the top right replaced with a crying emoji. Beneath the video the context is made clear in the comment: “The messenger of god, peace and blessings be upon him, said: “who fears setting out at nightfall and does so nevertheless will reach a house, for god’s rewards are plentiful, for god’s reward is nothing but paradise.”²⁰ The part of this hadith (saying by prophet Muhammad) “for god’s rewards are plentiful” is used as a hashtag that easily allows users to find the same or similar content within subscribed Telegram groups. The passage of the above stated hadith “for god’s rewards are plentiful” is used in texts produced by AQ, as a reference for those killed in the 1980s in Afghanistan, as well as in addresses by senior leaders, including Osama bin Laden.

Figure 4 - Screenshot from Telegram



Other images depict the suffering of IS-women in Syrian/Iraqi prison camps. Emphasising the importance of the Salafi-Jihadi nexus, in addition to IS material the channel shares links to other Salafi channels.

Other channels feature a mixture of Salafi and jihadi content, including the imagery of horse and rider flying a black banner in the background, while an armed man – seen here as a mujahid – tends to his white horse. The most dedicated hearts are often those who are silent. The imagery presents to the initiated audience the Mujahideen being on the frontlines (ribat), observant,

²⁰ Narrated by Abu Hurayra, one of the prophet’s companions, relayed via the hadith collections by al-Bukhari, Muslim, Tirmidhi and Abu Dawud. For an explanation of the hadith and the sources: Ibn Taymiyya, al-Tuhfat al-Iraqiyya.

ready for action, while first and foremost serving God and the Islamic community they claim to represent.

Figure 5 - Screenshots from Telegram



The channels also link to each other, note the image of the cat in the channel profile. In classical Islam cats were pure animals and the complete opposite to dogs. This may also call to mind the example of Omar who on finding a cat was sleeping on his sleeve, decided that instead of waking the cat he would cut off his sleeve.

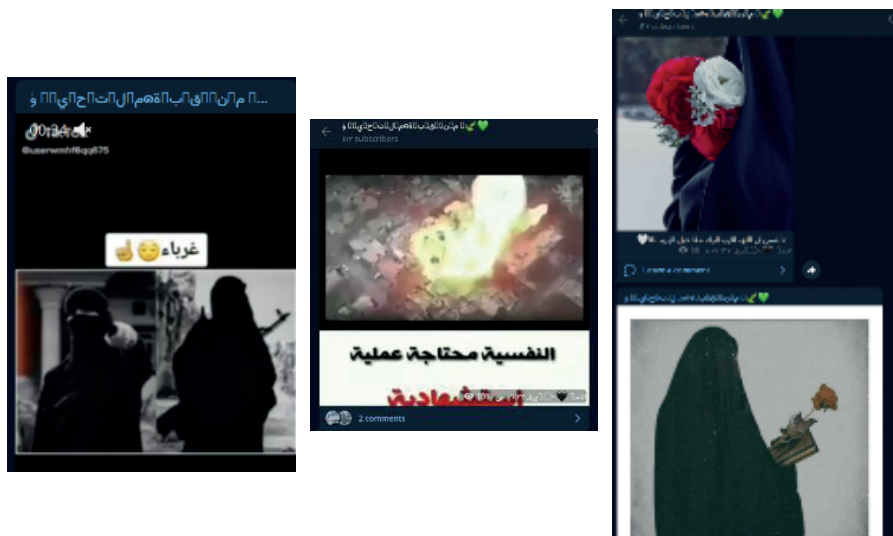
Some of the links shared by Salafi channels connect to Telegram channels which amongst Salafi content also reshare from TikTok a clip of an IS video, under the Arabic term *ghuraba'* with one emoji of a raised right index finger, to confess the oneness of God, and a satisfied smiley. *Ghuraba'* is the plural of *gharib* and can be translated in the sense of 'being strange' / estranged by worldly existence. It is a prominent theological concept at the heart of the Salafi-Jihadi nexus as it demands the individual believer to be of most pure intention of acting and living according to god's command. In western societies this can lead to a form of self-chosen isolation to avoid committing sinful acts, such as seeing humans violating the ultra-conservative dress codes, being exposed to places that serve alcohol etc. The term was coined by prophet Muhammad who stated, "Islam has begun as something strange (or alien) and will return as such." Salafis and especially Salafi-Jihadis consider themselves as the people who are actively applying theology through

every available means, and as part of those who bring back Islam despite it being seen as alien, strange or not taken seriously at all.

Other posts feature praise for suicide bombing attacks with images taken from drone footage of the explosion.

Some images resonate with both Salafi and Jihadi sides of the Salafi-Jihadi nexus, including content portraying the ideal woman or wife, often shown carrying roses. In addition to the beauty of God’s creation, roses symbolize life and eternity. The colour choice also references specific concepts, red often associated with blood and hence martyrs, white symbolizing life and purity.

Figure 6 - Screenshots from Telegram

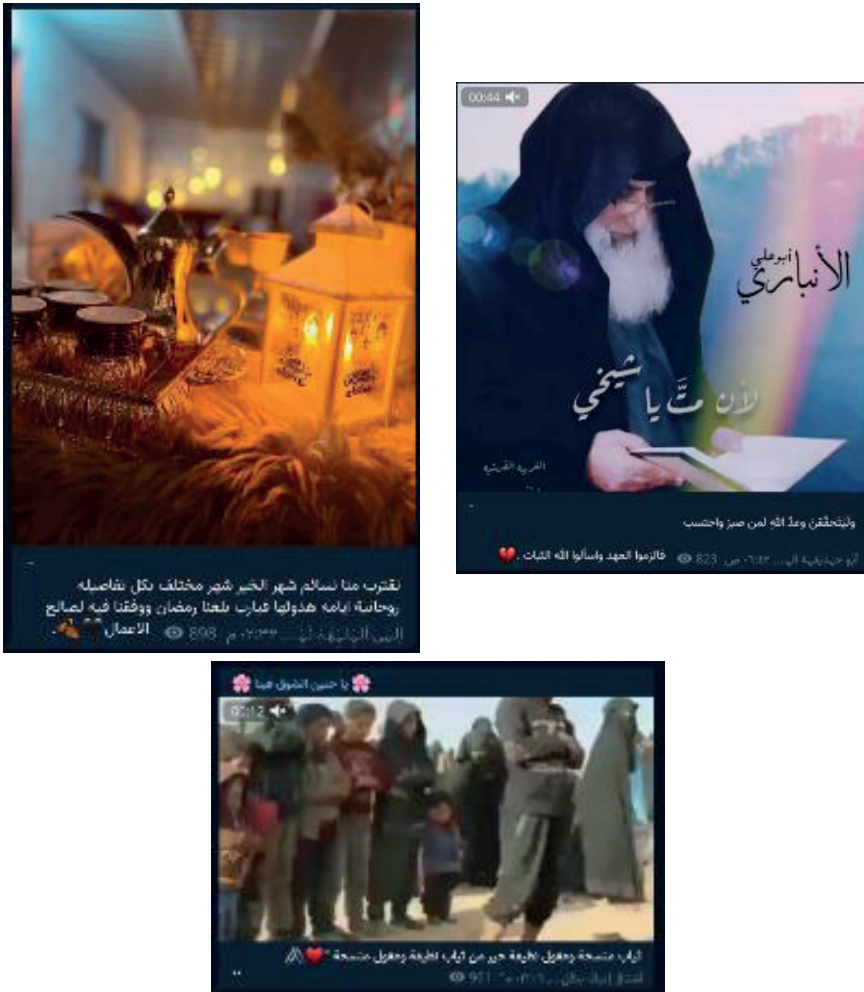


However, the images of combat are not the only parts of the Salafi-Jihadi content to feature in these predominantly Salafi channels. Nasheed, pictures of coffee being served and intermixed with jihadi content that – to the initiated consumer – is clear.

For example, Abu Ali al-Anbari (pictured below right) is one of the most important IS theologians, who is eulogized in a nasheed as man of great knowledge and respect. Within Islamic State online networks Abu Ali al-Anbari is heavily featured with al-Bayan radio programs dedicated to his speeches, writings and a lengthy biography was published as well. His anti-Shia theological tractates, for example, outline in detail how the practice of ‘polytheism’, the association of items, persons or good to God, leads to a total violation of the oneness of god. This is a fundamental allega-

tion lanced against Shiites in general who are accused as being ‘polytheists’ rather than ‘monotheist’ and hence are obligatory to be killed. The Arabic words, references and general rhetoric employed by al-Anbari are very similar and often the same to what ultra-conservative scholars from the Gulf region use and broadcast globally. Other posts feature brief IS video clips that emphasize the importance of theological aspects common to Salafi and Salafi-Jihadis alike.

Figure 7 - Screenshots from Telegram

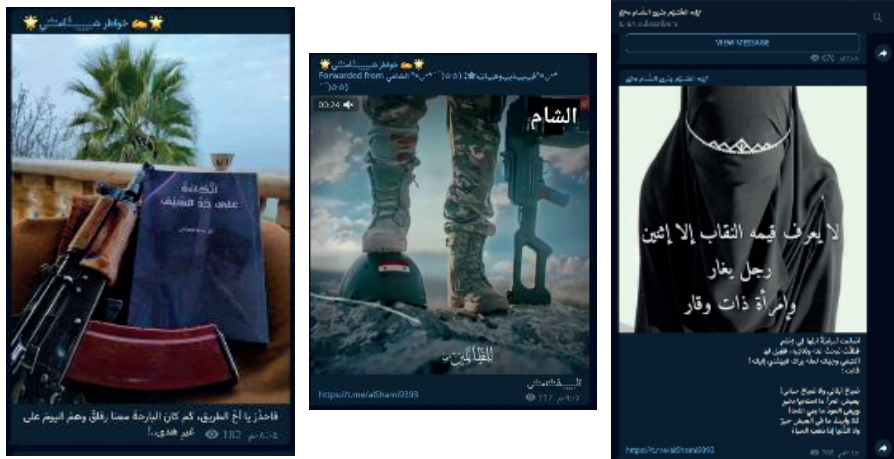


The importance of theology while expressed in writing, is also demonstrated through practical application. With the fall of what was often referred to as “the last IS stronghold”, al-Baghuz, images and video by the

mainstream media surfaced showing the families of male IS-fighters. Videos, for example, showing male children praying is framed as demonstrating steadfastness and unchallenged loyalty to God where the believer shall withstand the trials, torture and tribulation of this world to receive entry to paradise as reward in the afterlife.

The sharing of material in Salafi channels is not limited to IS, links shared by the most important Salafi channels in the network also lead to groups featuring AQ material interwoven with the Syrian revolution in general and Salafi content. Examples include, in a classical jihadi arrangement, a print copy of writing by Abu Hudhayfa al-Sudani, a core AQ theologian alongside a weapon. Another example features a boot on the helmet of the regular Syrian Arab Army showing disrespect to the conquered enemy in the eyes of the target audience, and the idealized image of a woman.

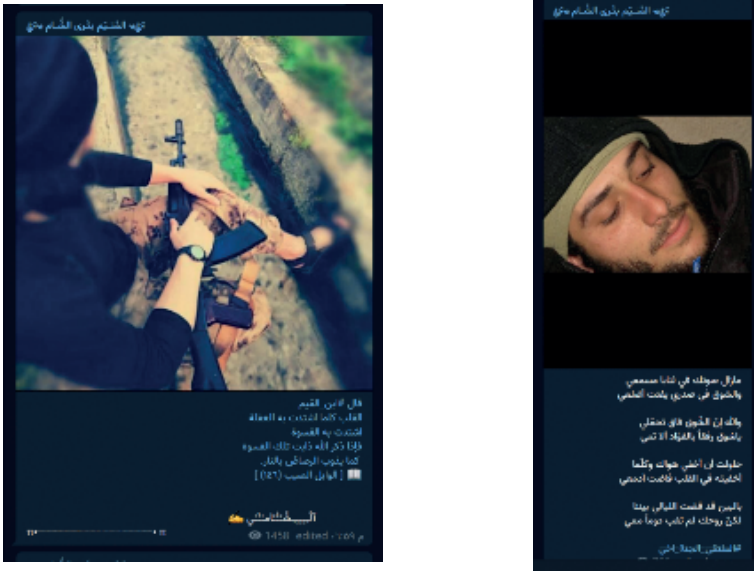
Figure 8 - Screenshots from Telegram



The writing by al-Sudani with the title “Bearing on the Blade of the Sword” is a theological book with the intention to offer divine guidance to the fighter – with a comment warning that yesterday’s brothers might be misguided today. The intellectual framework of AQ seeks to offer clarity on why and who to fight – and what for. The book was released by AQ’s media house Bayt al-Maqdis, a reference to Jerusalem, and was subsequently praised online.

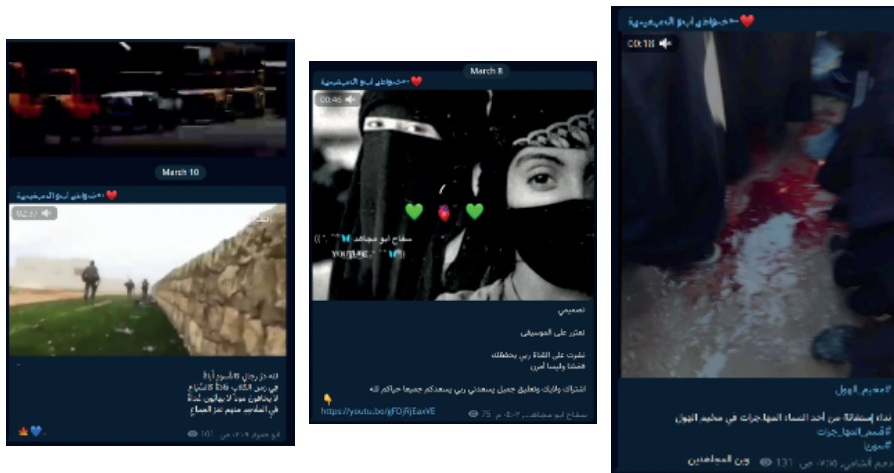
Another Syrian group sharing pro-AQ posts, include poems and commemoration of a martyr tagged by the statement “#in paradise we shall meet my brother” and cite Salafi authors, in this example, Ibn al-Qayyim.

Figure 9 - Screenshots from Telegram



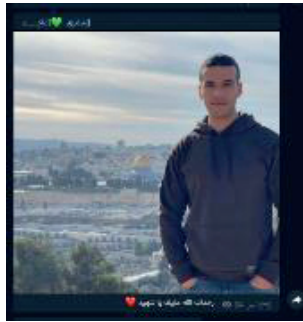
Another channel offers a combination of AQ and Amjad videos mixed with posts offering advice and religious role models juxtaposed with short videos from inside al-Hol detention camp and women calling for help.

Figure 10 - Screenshots from Telegram



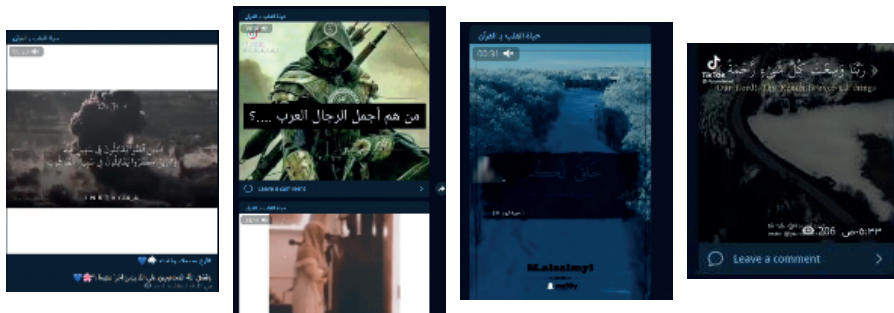
The commemoration of Palestinian martyrs, without any further information or context, can also be found in links shared by the top Salafi channels in the network. These draw on many of the same theological references as other parts of the Salafi-Jihadi network and thus suggest the young man died fighting (or violently) for the sake of the Dome of the Rock (seen in the background) in Jerusalem. As it turned out, the young man seen in the image was one of the perpetrators of random attacks against civilians in Israel in March 2022 and was shot to death.

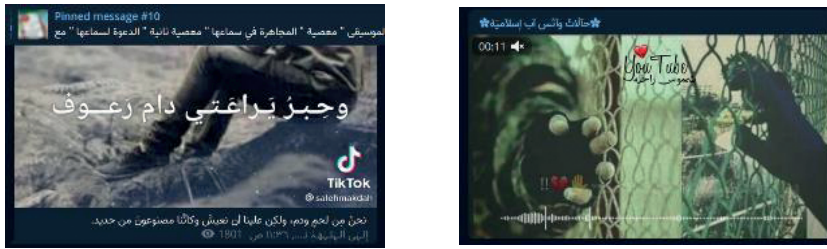
Figure 11 - Screenshot from Telegram



Some channels combine videos from Jihadi sub-cultural with material from preachers based in or from the Gulf region, drawing on the multiplatform nature of the Salafi-jihadi movement. This is evident in IS video scenes showing suicide bombing attacks with verses of the Quran embedded and a link to the Instagram account. It also appears in stylised imagery from TikTok juxtaposed with preachers. Resharing material from TikTok is also used for posts where scenes from nature are presented as proof of god’s creation, enriched with English Quran translations.

Figure 12 - Screenshots from Telegram





Other channels use common visual themes for example prisoners, particularly female, to express specific theological concepts which resonate with Salafi and Salafi-Jihadi audiences. These themes are obvious to the intended audience but can often pass by many researchers and social media filters as the material is not explicitly identified as from an FTO group nor is the imagery of a graphic nature.

Figure 13 - Screenshot from Telegram



A final series of images captures the nuance and challenge posed by the Salafi-Jihadi nexus as it is expressed through social media. The image of applied theology in the form of religious ritual (prayer) is immediately followed by imagery relating to another form of applied theology in the Salafi-Jihadi understanding.

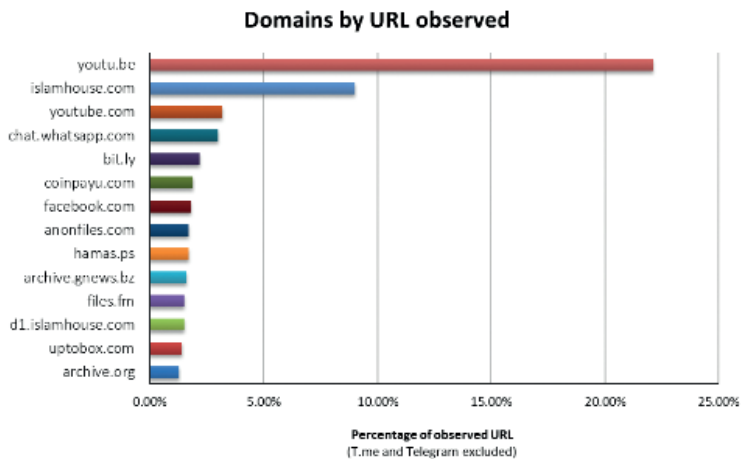
The juxtaposition of hand, watch and gun on the one side and red flower likely a reference to blood and martyrdom on the other in a channel which could be joined via links shared in a channel focused on sharing Salafi material highlights the role which some Salafi channels fulfil in sustaining access to Salafi-Jihadi theology. Not only are brief clips of IS and AQ content avail-

able via these channels, posted between material produced by Salafi authors, but the visual references and theological concepts which underpin them are also a familiar part of these Salafi channels.

The overview of material shared in channels promoted by the important Salafi elements of the network, highlights both the interplay between Salafi and Salafi-Jihadi content and the multiplatform communication paradigm in which this sharing occurs. Examining the URL shared in the channels that make up the Salafi-Jihadi ecosystem on Telegram provides another level of insight.

As a proportion of total sharing for the observed activity in 2021, YouTube remains an important element, for the Salafi-Jihadi information ecosystem, with many other familiar platforms including Facebook, Archive.org and WhatsApp also appearing in the most shared.²¹

Figure 14 - *On-line platforms most shared among the Salafi-Jihadi movement*



The most shared domains on Telegram include platforms fulfilling the main roles within the multiplatform communication paradigm; ‘beacon’, ‘content aggregator’, and ‘file store’. In addition to Telegram, WhatsApp chat links are shared frequently. Justpaste.it and Telegra.ph are the most frequently used aggregators, with YouTube, archive.org, anonfiles being prominent content stores.

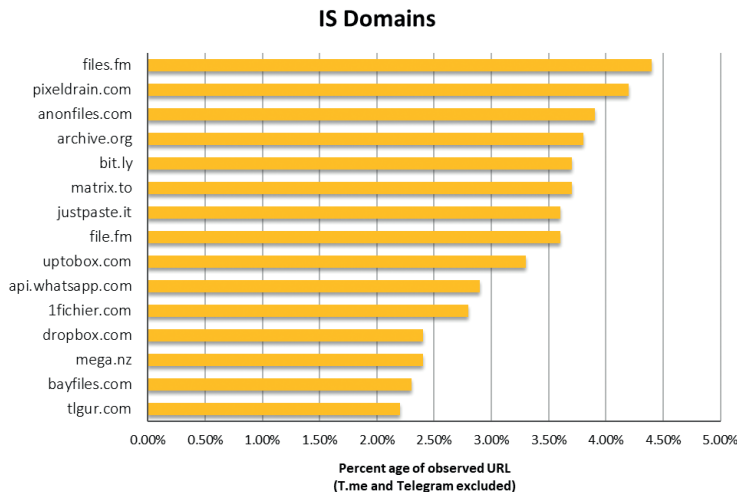
Other particularly noteworthy domains; Coinpayu.com enables users to earn cryptocurrency and gives access a number of cryptocurrency mining and exchange apps – cryptocurrency, NFT, and blockchain being prominent ele-

²¹ Telegram and T.me were removed from analysis.

ments of current Web3 applications.²² Second, Islamhouse.com describes itself as “The largest and the most authentic free reference to introduce Islam in the world languages on the internet”.²³ That it is part of the Salafi-Jihadi nexus should not be surprising given the theological nature of the movement and the tendency to use mainstream Salafi material alongside branded IS or AQ content.²⁴ Islamhouse.com offers mainly books in Arabic, and in another 120 languages, where selected Arabic writings are free to read online and download as translations. The site hosts the writings of Sunni Islamic scholars – hence the writings are all theological and offer a wide range of shared meaning with the Salafi-Jihadi movement, ranging from hatred against Shi’ites to historical books framing it a divine obligation for any Muslim to kill anyone accused of blasphemy, especially of insulting god or prophet Muhammad.

However, while the network exists predominantly as a single giant interconnected unit, there are specific clusters within it. The emphasis of these specific clusters is shown by the alignment or allegiance of the channels which comprise the cluster, but also by the material they share. The URL they share to sites outside Telegram highlights the difference in the sharing behaviour adopted by the different groups and the numerous distinctions between the sharing behaviours adopted by the different groups.

Figure 15 - *On-line platforms most shared among the Salafi-Jihadi movement.
Brakedown by organization*



²² For example, current options promoted on the site include: KuCoin, Bitdeer, Binance, HOO, Indoex

²³ <http://islamhouse.com/en>

²⁴ For description of Salafi-Jihadi Nexus see: Fisher, Prucha, ‘Understanding the Global Jihadist Movement 20 years after 9/11’, EICTP Expert Paper, October 2021. p. 23.

Figure 16 - *On-line platforms most shared among the Salafi-Jihadi movement.
Brakedown by organization*

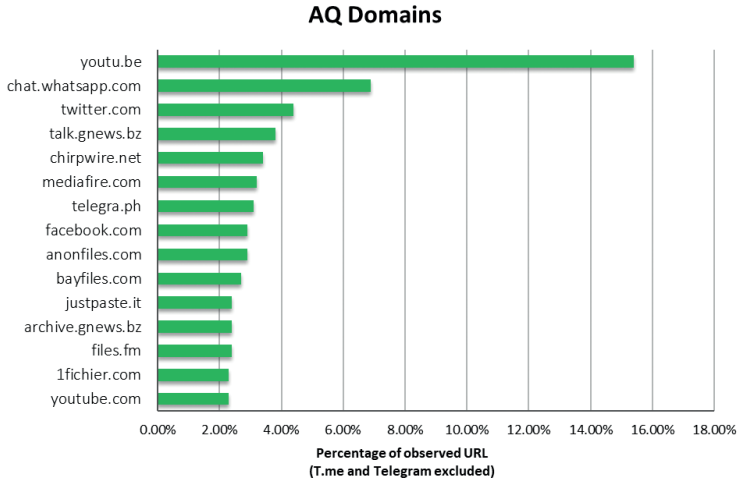


Figure 17 - *On-line platforms most shared among the Salafi-Jihadi movement.
Brakedown by organization*

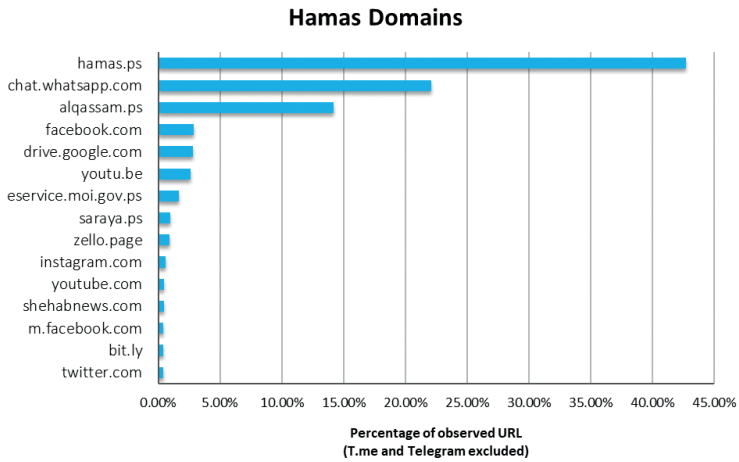
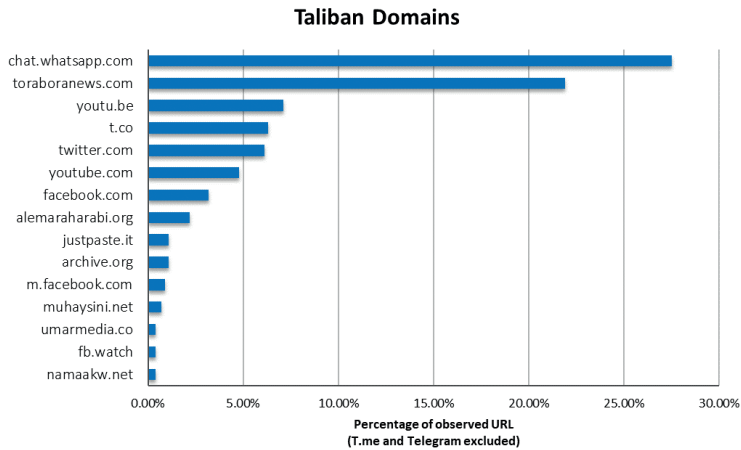


Figure 18 - *On-line platforms most shared among the Salafi-Jihadi movement. Brakedown by organization*



Observations from the specific groups show some commonalities and some specific nuances. First, WhatsApp is a prominent domain in the overall graph and in each of the graphs relating to specific groups.

Second, IS is the only example where a group specific URL does not appear in the most shared. This may have more to do with the constant pressure IS websites are under in comparison to the other groups. This may also account for the rapid cycling through many different types of platforms used a ‘content stores’ or filesharing platforms.²⁵ AQ, Taliban and Hamas respectively utilise a combination of their own specific websites, social media and file sharing platforms – with some sites or names of sites almost as old as the internet itself.

Third, the most used domains highlight the alternative communication options AQ and IS advertise to their supporters. AQ share links to Chirpwire and gnews.bz which is the former location of their Rocket Chat server. IS channels share links to Matrix, where users can access material via an IS run server.

4. Discussion

The evidence-based analysis of the Salafi-Jihadi information ecosystem on Telegram, and the URL shared to other domains highlights several important findings about the current state of the movement online and the multiplatform communication paradigm (MCP) which makes it possible to maintain

²⁵ Fisher, A., et al. “Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability.” Policy Brief, Royal United Services Institute, London (2019).

a persistent presence. Many of these findings challenge the orthodox ‘success narrative’ about the efforts taken against the Salafi-Jihadi movement online.

First, is the breadth of the network identified. There is a tendency to separate ‘terrorist’ networks – those related to formally designated FTO – from Salafi or groups not considered FTO. The network data from Telegram in 2021 shows that on a network level there is no such distinction. This significantly challenges the idea of studying FTO networks separately from the material which is important to those networks, but which falls outside an FTO designation.

Homophily or similarity, is an important reason that networks form and individuals interact. At its simplest, “Similarity breeds connection. This principle – the homophily principle – structures network ties of every type”.²⁶ In addition to creating forms of relational ties, shared elements underpin collaborative or cooperative relationships.

Cooperation requires that individuals are able to identify, and preferentially associate with, others who have compatible preferences and the shared background knowledge needed to solve interpersonal coordination problems.²⁷

The creation of a single giant network component containing almost 90% of observed nodes and including AQ, IS, Hamas, Taliban and the Muslim Brotherhood alongside Salafi channels shows there is an element of importance to all groups. That is to say, being part of the network does not imply the specific group is aligned with the objectives of terrorists. It does, however, indicate there are elements of Salafi theology which are important to all.

Second, the dominant orthodox narrative has focused on how successful efforts have been in ‘deplatforming’ IS. It is widely accepted within the transatlantic orthodoxy of Terrorism Studies that “Broad improvements in the detection and removal of terrorist content on mainstream social media platforms has pushed such actors onto smaller online spaces”.²⁸ As “Tech Against Terrorism director Adam Hadley said smaller platforms and social media services are where extremists moved to after being shut down by giants like Facebook and Twitter”.²⁹ The primary difficulty with such a narrative is that

²⁶ McPherson, Miller, Lynn Smith-Lovin, and James M. Cook. “Birds of a feather: Homophily in social networks.” *Annual review of sociology* 27.1 (2001): 415-444.

²⁷ Curry, Oliver, and Robin IM Dunbar. “Do birds of a feather flock together?” *Human nature* 24.3 (2013): 336-347.

²⁸ THE THREAT OF TERRORIST AND VIOLENT EXTREMIST OPERATED WEBSITES, Tech Against Terrorism, January 2022, p. 4; <https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf>

²⁹ Dominic Giannini, ISIS app ignored by governments: inquiry, The Canberra Times, NOVEMBER 17 2021; <https://www.canberratimes.com.au/story/7515010/isis-app-ignored-by-gov->

Telegram was the 5th most downloaded mobile app globally in 2021, 13th most used social media platform, and claims 100 million more users than Twitter. As such, it is hard to consider Twitter a giant and Telegram a ‘small’ platform.

Furthermore, when the URL sharing behaviour of specific Salafi-Jihadi groups are analysed, it is clear they are all sharing links to WhatsApp, which boasts more than 2 billion people in over 180 countries. It was the third most used social platform and fourth most downloaded mobile app globally in Q3 2021.²⁰ In January 2022 Hootsuite reported WhatsApp was the world’s favourite social platform.²¹

TikTok and Instagram both featured heavily in the sample of channels which could be joined through URL shared by the top 5 Salafi channels. As shown above, this includes sharing non-branded material which resonates with Salafi-Jihadi audiences and posts which feature images from branded videos. TikTok reached a billion users faster than Facebook and, while still smaller than Facebook, is more than twice the size of the Twitter userbase.³⁰ Similarly, Instagram was the fourth most used social media platform in 2021, and the second most downloaded mobile app of the year.³¹ The platform claims to have over 1.4 billion users. Far from being deplatformed or driven to the fringes of social media, Salafi-Jihadi groups, supporters and aligned networks are still very much a feature on many of the world’s biggest and most popular platforms.

The third challenge is the ability of the mobile enabled Salafi-Jihadi Swarmcast to reconfigure to maintain a persistent presence and fulfil the strategic or intended purpose.

This swarm effect has many parallels to the speed and volume of content produced by jihadist groups. In addition, observable nature and computer simulations demonstrate that when a predator strikes, the swarm shifts to evade them.³² If the predator keeps looking in the same place, the number of avail-

ernments-inquiry/?utm_source=Tech+Against+Terrorism&utm_campaign=4e8f-78f06d-EMAIL_CAMPAIGN_2019_03_24_07_51_COPY_01&utm_medium=email&utm_term=0_cb464fdb7d-4e8f78f06d-68658615

³⁰ Simon Kemp, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 <https://blog.hootsuite.com/simon-kemp-social-media/>

³¹ The Global State of Digital 2022, Hootsuite, January 2022, <https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-233-App-Annie-App-Ranking-Downloads.png>; <https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-99-The-Worlds-Most-Used-Social-Platforms.png>

³² Chen, Yuxin and Theodore Kolokolnikov. “A minimal model of predator-swarm interactions.” *Journal of the Royal Society Interface*, vol. 11, no. 94, 2014; Milinski, Manfred. “A predator’s costs of overcoming the confusion-effect of swarming prey.” *Animal Behaviour*, vol. 32, no. 4, Nov. 1984, pp. 1157-1162; Parrish, Julia K. and Leah Edelstein-Keshet. “Complexity, pattern, and evolutionary trade-offs in animal aggregation.” *Science*, vol. 284, no. 5411, 1999, pp. 99-101.

able prey will appear to decline. But, if the predator shifts its perspective and looks elsewhere, it will be clear that the prey has not disappeared nor has the size of the swarm declined. Instead, the swarm has moved.³³

Based on the evidence, it is clear the assessments supporting the orthodox narrative do not equate to meaningful, strategic nor effective disruption of Media Mujahidin operations. As outlined in the Swarmcast metaphor, a swarm or flock reconfiguring does not mean they have disappeared. Yet OTS has consistently pursued the success narrative claiming that shifting position means disappearing. The success narrative began around 2014, when J.M. Berger believed “that Twitter suspensions have seriously degraded IS ability to game hashtags and distribute content”.³⁴ Following a similar approach, a VoxPol report concluded, “IS Twitter Community is now almost non-existent”.³⁵ At the time of the VoxPol research IS Ghazwat (raids) on Twitter were coordinated via Telegram, and the focal point of ISIS ‘community’ had been Telegram for 18 months by that point. As such, the majority of these accounts were never intended to serve a ‘community’ function. Instead, they follow the hit and move approach of classical horse backed raiders.

Raiders on the Arabian Peninsula at the time Islam began to spread, did not intend to hold territory but achieve a specific purpose and move on, these were Ghazwat. The Ghazwat of the Twitter era follow the same ethos, no account is intended to last but to make content available for a short time before the user moves on to another account. Losing accounts, just as raiders would abandon positions they had taken, were entirely expected and acceptable losses. This strategy was laid out by IS on Telegram, however, the authors of the VoxPol report by focusing on content distributed via Twitter as a ‘community’ misinterprets what IS was trying to achieve. Just as a Swarm or flock moves so the Swarmcast had reconfigured, with the IS community function existing on Telegram. In focusing on Twitter when the IS core was active on an alternative platform, the VoxPol evaluation reflects the desire within the Transatlantic orthodoxy to measure success of disruption efforts rather than evaluate IS activity against what IS was trying to achieve.

Now seven years later, OTS papers have continued to conclude each of the latest efforts to disrupt IS content distribution have been successful. Wit-

³³ Ali Fisher, *Netwar in Cyberia: decoding the media mujahidin*, paper 5, USC Center on Public Diplomacy, 2018, http://humanshuddle.com/wp-content/uploads/2020/Netwar%20in%20Cyberia%20Web%20Ready_with%20disclosure%20page%2011.08.18.pdf

³⁴ Critique at the time was offered in: Fisher, Ali. “No Respite on Social Media After ISIS Attacks in Paris.” CPD Blog, 9 Dec. 2017, uscpublicdiplomacy.org/blog/no-respite-social-media-after-isis-attacks-paris.

³⁵ Conway, Maura, et al. “Disrupting Daesh: measuring takedown of online terrorist material and it’s impacts.” (2017).

ness, following the Europol led efforts, the immediate bullish assessment that the operation had “resolutely trashed the Islamic State’s presence on Telegram”.³⁶ However, the evidence-based analysis of data for the year 2021 shows the Salafi-Jihadi movement has maintained a persistent presence and, undeterred, has reconfigured to enable continued operations in the face of pressure. In addition, as the 2021 network graph found almost 90% of channels connected to a single giant component, channels and users have not been trashed or scattered to the wind. Instead, they reconnected to the channels which remained to continue as before.

Fourth, researchers within the orthodoxy of Terrorism Studies have long struggled to explain how Salafi-Jihadi networks survive Western attempts at disruption – particularly given the virtual uniformity in assessments that these disruption efforts have been successful. For example, over the same time-period as one OTS paper claimed IS suffered high levels of disruption on Twitter,³⁷ one third of all known traffic to IS content was still coming from Twitter.³⁸ Equally, while Berger was claiming disruption of content dissemination, and the orthodox narrative questioned the “purported resilience” of the ISIS social network³⁹ a single video was downloaded or viewed approximately half a million times across multiple postings on Archive.org alone.⁴⁰ Similarly, while the orthodox interpretation claimed Salafi-Jihad groups had been ‘deplatformed’⁴¹ and content dissemination degraded, IS videos posted on Twitter were receiving tens of thousands of views.⁴² No explanation has yet been offered for the extent that to which users were still directed to IS content, while researchers could not find what they deemed relevant IS accounts on the platform.⁴³

³⁶ <https://www.wired.co.uk/article/isis-telegram-security>. For evaluation of disruption using a very short timescale see: Amarasingam, Amarnath, Shiraz Maher, and Charlie Winter. “How Telegram disruption impacts jihadist platform migration.” *Centre for Research and Evidence on Security Threats* (2021).

³⁷ Conway, Maura, et al. “Disrupting Daesh: measuring takedown of online terrorist material and it’s impacts.” (2017): 1-45.

³⁸ Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. *The New Netwar: Countering extremism online*. Policy Exchange, 2017.

³⁹ http://www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf

⁴⁰ <https://uscpublicdiplomacy.org/blog/no-respite-social-media-after-isis-attacks-paris>

⁴¹ <https://gnet-research.org/2021/01/15/why-deplatforming-the-extreme-right-is-a-lot-more-challenging-than-deplatforming-is/>

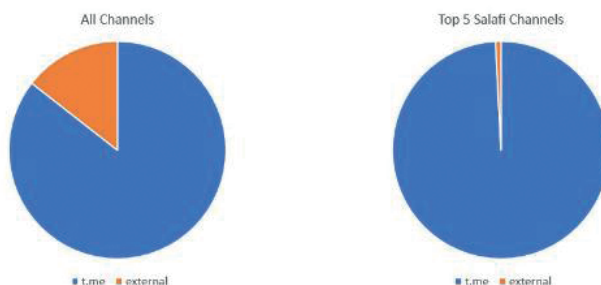
⁴² Ali Fisher, *Netwar in Cyberia: decoding the media mujahidin*, paper 5, USC Center on Public Diplomacy, 2018.

⁴³ Conway, Maura, et al. “Disrupting Daesh: measuring takedown of online terrorist material and it’s impacts.” (2017): 1-45.

The network analysis presented here demonstrates that the structure and the nature of the networks makes disruption difficult on a single platform – let alone across multiple platforms embodied by the Jihadi Multiplatform Communication Paradigm.⁴⁴ First, the data presented here reiterates previous findings that the sparse network structure makes it very hard to remove sufficient channels to destroy a network.⁴⁵ On Telegram, just as earlier on Twitter, elements of the network would likely remain, and as the early work on network resilience demonstrated, very low levels of redundancy were required for a network to survive attack.⁴⁶

The nature of the movement also contributes through the presence of Salafi material. The Salafi material is important due to the shared theological meaning,⁴⁷ and the tendency for Salafi channels to remain during the attempts to remove channels operated by Foreign Terrorist Organisations (FTO). The network data and key actor graph showed the many ways in which Salafi channels are important to the Salafi-Jihadi network. The Salafi channels are important bridges or conduits which connected different parts of the network (represented by betweenness centrality) as well as important to the core of the network (represented by PageRank).

Figure 19 - Network data – channels



⁴⁴ Fisher, A., et al. “Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability.” Policy Brief, Royal United Services Institute, London (2019).

⁴⁵ Ali Fisher, “Interrogating the electronic ribat: Data Science in the study of the Jihadist movement”, in Lohlker, R. (ed.) World wide warriors: How Jihadis operate online. (2019); Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018.

⁴⁶ The resilience of dispersed or distributed systems was demonstrated in: http://www.rand.org/pubs/research_memoranda/RM3420.html

⁴⁷ Ali Fisher, Nico Prucha, Pavel Tupek, The Salafi-Jihadi Nexus: An Evidence Based Approach of the Caliphate Library, EICTP Expert Paper, February 2022.

In addition to the network metrics, the URL shared by the Salafi Channels indicate another reason they are so important to the network. The URL from the top five Salafi channels (by PageRank) shows they are more likely to be sharing join links to other channels than the average behaviour by all channels. Within the top Salafi channels 99.2% of all URL shared were links to join Telegram channels or contact specific individuals. This comprised over 2,700 unique Telegram URL, or an average of 7.5 unique links to join other channels every day. This is contrast to 85.5% of the 725,000 URL shared by all channels observed.

Given the commonality in theological meaning, the audience for Salafi channels is one of the largest target audiences for Salafi-Jihadi groups. By contrast, conclusions from much of the orthodox terrorism studies research have undervalued or even ignored the role of the Salafi elements within the Salafi-Jihadi movement. It is unclear whether this is because the method focused on finding ‘official’ FTO material, looking for markers such as logos and flags in user profiles,⁴⁸ or, as Winter and others have attempted to do, have sought to ‘whittle away’ theology⁴⁹ to ‘uncloak’ alternative explanations for the movement including ice cream, Nutella, kittens, crime, and Utopia.⁵⁰ Whatever the cause of this effective blind spot in elements of the orthodox transatlantic understanding, Salafi-Jihadi groups exploit it to engage with audiences across their multiplatform communication paradigm (MCP).⁵¹

Finally, the evolution of a single giant network has occurred despite the various groups on both sides of the Salafi-Jihadi nexus being subject to very different pressures. This challenges the orthodox assumption that IS was driven to use Telegram, due to the difficulty of using Twitter. This pressure did not apply to Taliban and many Salafi organisations, but in spite of being free to use Twitter, these groups have built large networks on Telegram. This

⁴⁸ ‘Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts’, VOX-Pol, 2017, http://www.voxpol.eu/download/voxpola_publication/DCUJ5528-Disrupting-DAESH-1706-WEB-v2.pdf

⁴⁹ Ingram, Haroro J., Craig Whiteside, and Charlie Winter. *The ISIS Reader: Milestone texts of the Islamic state movement*. Oxford University Press, USA, 2020. pp. 7, 225.

⁵⁰ Smith, Samantha K., “Kittens and Nutella: Why Women Join ISIS” (2015). *What All Americans Should Know About Women in the Muslim World*. 7. <https://cupola.gettysburg.edu/islamandwomen/7/>; Amanda Taub, No, CNN, women are not joining ISIS because of “kittens and Nutella”, Vox, 18 February 2015 <https://www.vox.com/2014/10/20/6987673/isis-women>; Charlie Winter, quoted in: <https://www.bendigoadvertiser.com.au/story/3202519/isis-propaganda-to-push-a-new-utopia/>; Ingram, Haroro J., Craig Whiteside, and Charlie Winter. *The ISIS Reader: Milestone texts of the Islamic state movement*. Oxford University Press, USA, 2020. pp. 7, 225.

⁵¹ Fisher, A., et al. “Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability.” Policy Brief, Royal United Services Institute, London (2019).

indicates there are persuasive ‘pull’ factors for using Telegram beyond having difficulty using Twitter, and that there is a large target audience for Salafi, and Salafi-Jihadi content. This perspective is almost entirely absent from the orthodox interpretation due to the emphasis on ‘push’ factors and the ‘success narrative’.

Furthermore, that the giant component still exists despite Telegram targeting disruption efforts against some Salafi-Jihadi groups, indicates disruption has not been able to separate the FTO from the Salafi. FTO groups have been able to reconnect with those who share elements of theology, and the potential target audience which that provides.

5. Conclusion

This study has challenged the image of very insular Jihadi communities just talking to themselves. In 2021, far from being driven off Telegram (or the internet) by EUROPOL led disruption efforts the Salafi-Jihadi movement and the FTO elements within it, have reconfigured just as a flock of birds adjusts in flight to the attack of a predator. In 2022 they continue to exploit the platform.

Further studies will be required to understand the ecology of the Salafi-Jihadi ecosystem in greater depth. Specifically, how the interaction between Salafi and Salafi-Jihadi network clusters influences how future disruption is planned and evaluated.

The progressive, evidence-based approach to the Telegram data has reiterated the importance of elements of Salafi theology to the Salafi-Jihadi movement highlighted by previous research. As Adam Hoffman argued previously: “Ignoring the religiosity of ISIS and other Islamist movements is characteristic of many Western commentators and analysts, but discomfort in the face of religious belief is a major obstacle in the analysis of movements which see religion as the overall framework for interpreting and justifying their actions.”⁵² This is a problem because, as Rüdiger Lohlker put it, “It is crystal clear – to virtually anyone who has the linguistic capacity to grasp and the opportunity to witness what jihadists are actually saying, writing and doing, both online and offline – that religion matters.”⁵³

⁵² Adam Hoffman, ‘The Religiosity Challenge in Analyzing Islamist Movements’, 07/09/2017; <https://regthink.org/en/articles/the-religiosity-challenge-in-analyzing-islamist-movements>

⁵³ Rüdiger Lohlker, “Why Theology Matters – The Case of ISIS,” Strategic Review, July – September 2016; URL: <http://sr-indonesia.com/in-the-journal/view/europe-s-misunderstanding-of-islam-and-isis>

Given the importance of theology, the Telegram network is an online manifestation of the Salafi-Jihadi Nexus. As noted in a previous paper:

The Salafi materials are often quick and easy to find online – and in several languages. This enables jihadis to attain credibility as a religious movement fighting for ultraorthodox theological parameters while the networks online on the Salafi side of the nexus are rarely taken down or pushed offline. This reality strengthens Salafi-Jihadi networks online as it is one column, upon which they can rely to repopulate their content and continue to attract consumers of the Salafi world to their ‘enhanced’ world where religion is applied by force and based on theological constants and commandments that are explained in a soft-power fashion within the Salafi networks.⁵⁴

Bibliography

- ‘Disrupting Daesh: Measuring Takedown of Online Terrorist Material and its Impacts’, VOX-Pol, 2017,
- Amarasingam, Amarnath, Shiraz Maher, and Charlie Winter. “How Telegram disruption impacts jihadist platform migration.” *Centre for Research and Evidence on Security Threats* (2021).
- Blondel Vincent D, Guillaume Jean-Loup, Lambiotte Renaud, Lefebvre Etienne, ‘Fast unfolding of communities in large networks’, in *Journal of Statistical Mechanics: Theory and Experiment* 2008 (10),
- Bloom, Mia, and Chelsea Daymon. “Assessing the future threat: ISIS’s virtual caliphate.” *Orbis* 62.3 (2018): 372-388.
- Bloom, Mia, Hicham Tiflati, and John Horgan. “Navigating ISIS’s preferred platform: Telegram1.” *Terrorism and Political Violence* 31.6 (2019): 1242-1254.
- Chen, Yuxin and Theodore Kolokolnikov. “A minimal model of predator-swarm interactions.” *Journal of the Royal Society Interface*, vol. 11, no. 94, 2014
- Conway, Maura, et al. “Disrupting Daesh: measuring takedown of online terrorist material and it’s impacts.” (2017)
- Conway, Maura, et al. “Disrupting Daesh: measuring takedown of online terrorist material and it’s impacts.” (2017):
- Criezis, Meili. “Online Deceptions.” *Perspectives on Terrorism* 14.1 (2020): 67-73.
- Curry, Oliver, and Robin IM Dunbar. “Do birds of a feather flock together?” *Human nature* 24.3 (2013): 336-347.
- Fisher Ali, Prucha Nico, & Tupek Pavel, ‘The Salafi-Jihadi Nexus: An Evidence Based Approach to the Caliphate Library’, *EICTP Expert Paper*, February 2022.
- Fisher Ali, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018,

⁵⁴ Fisher, Prucha, ‘Understanding the Global Jihadist Movement 20 years after 9/11’, EICTP Expert Paper, October 2021. p. 23.

- Fisher, Ali & Prucha, Nico (2014, August): “The Call-up: The Roots of a Resilient and Persistent Jihadist Presence on Twitter“. *CTX*, 4(3), 73-88.
- Fisher, Ali, & Nico Prucha, “Follow the White Rabbit – Tracking IS Online and Insights into What Jihadists Share”, in Marone, Francesco (ed.) *Digital Jihad: Online Communication and Violent Extremism*. Ledizioni, (2019).
- Fisher, Ali, & Prucha, Nico, ‘Understanding the Global Jihadist Movement 20 years after 9/11’, *EICTP Expert Paper*, October 2021.
- Fisher, Ali, “Interrogating the electronic ribat: Data Science in the study of the Jihadist movement“, in Lohlker, R. (ed.) *Worldwide warriors: How Jihadis operate online*. (2019)
- Fisher, Ali, et al. “Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability.” *Policy Brief*, Royal United Services Institute, London (2019).
- Fisher, Ali, How Jihadist Groups exploit Western researchers to promote their theology, *Online Jihad*, February 2019, <https://onlinejihad.net/2019/02/18/how-jihadist-groups-exploit-western-researchers-to-promote-their-theology/>
- Fisher, Ali. “Mapping the great beyond: Identifying meaningful networks in public diplomacy” *CPD Perspectives in Public Diplomacy, Paper 2* (2010)
- Fisher, Ali. “No Respite on Social Media After ISIS Attacks in Paris.” CPD Blog, 9 Dec. 2017, usepublicdiplomacy.org/blog/no-respite-social-media-after-isis-attacks-paris.
- Fisher, Ali. “Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence.” *Perspectives on Terrorism*, vol. 9, no. 3.
- Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. *The New Netwar: Countering extremism online*. Policy Exchange, 2017.
- Giannini Dominic, ISIS app ignored by governments: inquiry, The Canberra Times, NOVEMBER 17 2021 https://www.canberratimes.com.au/story/7515010/isis-app-ignored-by-governments-inquiry/?utm_source=Tech+Against+Terrorism&utm_campaign=4e8f78f06d-EMAIL_CAMPAIGN_2019_03_24_07_51_COPY_01&utm_medium=email&utm_term=0_cb464fdb7d-4e8f78f06d-68658615
- Gillespie Marie et al., “Understanding the Changing Cultural Value of the BBC World Service and the British Council“, Open University Cultural Value Project, July 2014.
- Hoffman Adam, “The Religiosity Challenge in Analyzing Islamist Movements’, 07/09/2017 <https://regthink.org/en/articles/the-religiosity-challenge-in-analyzing-islamist-movements>
- Ingram, Haroro J., Craig Whiteside, and Charlie Winter. *The ISIS Reader: Milestone texts of the Islamic state movement*. Oxford University Press, USA, 2020. pp. 7, 225
- Jackson, R.D.W. “The Case for a Critical Terrorism Studies” (2007) <http://hdl.handle.net/2160/1945>
- Kemp Simon, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 <https://blog.hootsuite.com/simon-kemp-social-media/>

- Kemp, Simon, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 <https://blog.hootsuite.com/simon-kemp-social-media/>
- Lambiotte, R. Delvenne, J.-C. Barahona M. *Laplacian Dynamics and Multiscale Modular Structure in Networks* (2009)
- Lohlker, Rüdiger, “Why Theology Matters – The Case of ISIS”, Strategic Review, July – September 2016; URL: <http://sr-indonesia.com/in-the-journal/view/europe-s-misunderstanding-of-islam-and-isis>
- McPherson, Miller, Lynn Smith-Lovin, and James M. Cook. “Birds of a feather: Homophily in social networks.” *Annual review of sociology* 27.1 (2001): 415-444.
- Milinski, Manfred. “A predator’s costs of overcoming the confusion-effect of swarming prey.” *Animal Behaviour*, vol. 32, no. 4, Nov. 1984, pp: 1157-1162.
- Parrish, Julia K. and Leah Edelstein-Keshet. “Complexity, pattern, and evolutionary trade-offs in animal aggregation.” *Science*, vol. 284, no. 5411, 1999, pp: 99-101
- Prucha, Nico. “Is and the jihadist information highway—projecting influence and religious identity via telegram.” *Perspectives on Terrorism* 10.6 (2016): 48-58.
- Shehabat, Ahmad, Teodor Mitew, and Yahia Alzoubi. “Encrypted jihad: Investigating the role of Telegram App in lone wolf attacks in the West.” *Journal of strategic security* 10.3 (2017): 27-53.
- Smith, Samantha K., “Kittens and Nutella: Why Women Join ISIS” (2015). What All Americans Should Know About Women in the Muslim World. 7. <https://cupola.gettysburg.edu/islamandwomen/7>
- Spagna, Nicolo’ Giuseppe, *Ethnographizing Islamic State’s Digital Community on Telegram Platform; Socio-Organizational Anatomy and New Models of Threat*, BTT, (November 2021)
- Taub, Amanda, No, CNN, women are not joining ISIS because of “kittens and Nutella”, *Vox*, 18 February 2015 <https://www.vox.com/2014/10/20/6987673/isis-women>
- The Global State of Digital 2022, Hootsuite, January 2022, <https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-233-App-Annie-App-Ranking-Downloads.png>
- The Threat of Terrorist and Violent Extremist Operated Websites, Tech Against Terrorism, 28 January 2022. <https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf>
- Willis, Alistair, Fisher Ali, and Lvov Ilia. “Mapping networks of influence: tracking Twitter conversations through time and space.” *Participations: Journal of Audience & Reception Studies* 12.1 (2015): 494-530.
- Yayla, Ahmet S., and Anne Speckhard. “Telegram: The mighty application that ISIS loves.” *International Center for the Study of Violent Extremism* 9 (2017).

Questo volume è stato stampato
nel mese di maggio 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.sicurezzaerrorismosocieta.it
ISBN: 978-88-9335-956-6

Euro 20,00



9 788893 359566