ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

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

10
2019

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

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

10

ISSUE 2/2019

Milano 2019

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

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

ISSUE 2 – 10/2019

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)

© 2019 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: 978-88-9335-540-7

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

I.
Perspectives on Cultural Diplomacy
in conflict management and mitigation

Marco Lombardi
Culture and Action: Cultural Diplomacy and Cooperation 7

Barbara Lucini
Cultural Resilience and Cultural Diplomacy: the State of the Art 19

II.
Perspectives on Terrorism
and Counter-terrorism

Alessandro Boncio
The Italian shared house for combating terrorism 31

Daniele Barone
The decentralized finance-violent extremism nexus: ideologies,
technical skills, strong and weak points..... 41

Filippo Tansini
Conosci il tuo nemico: la rappresentazione del terrorismo
nei tweet della disinformazione russa..... 77

I.
PERSPECTIVES ON CULTURAL DIPLOMACY IN CONFLICT MANAGEMENT AND MITIGATION

Culture and Action: Cultural Diplomacy and Cooperation

Marco Lombardi[1]

Nota autore

Marco Lombardi, director of the Italian Team for Security, Terroristic Issues and Managing Emergencies (ITSTIME), 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 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. He is member of the Governmental Commission on Counter Radicalization and of the Strategic Policy Committee of the Italian Ministry of Foreign Affairs and International Cooperation. He is member of the board of "JD – Journal for Deradicalization" (www.journal-derad.com), "Journal of Mediterranean and Balkan Intelligence – JMBI" and "Sicurezza, Terrorismo e Società – STS" (www.sicurezzaterrorismosocieta.it)

Keywords

Culture, diplomacy, cultural diplomacy, crisis and conflict reduction.

1. Foreword

The new, uncertain structures of the reticular global world call for innovative strategies. In particular, the new forms of diffuse conflict demand that international diplomacy give effective answers in terms of handling the crisis and reducing conflicts. In this context, cooperation has to regain credibility and competence to prove itself as a system of intervention suited to the new challenges, able to project itself into the new scenarios that are changing significantly and rapidly.

This brief note proposes to highlight some important factors of the change taking place, followed by the description of recent experiences in the field, concluding with the proposal of new kinds of involvement expressed in the

[1] ITSTIME – Università Cattolica del Sacro Cuore, Milan, Italy and CAARI – Addoun University, Galkayo, Somalia.

Cultural Diplomacy Partnership, an experience of reticular cooperation formulated and promoted by our research centres, ITSTIME in the Università Cattolica, Milan, and CAARI at the Addoun University in Somalia.

2. The changing pattern: from globalisation to reticularisation

It may not yet be clear enough that globalisation – which is a daily topic of discussion – is an incomplete and not fully understood process, that we attempt to fit into the models of interpretation of the past without making the conceptual leap involving a change that is radical by its very nature. We could perhaps add that "we haven't wanted to make" this leap, in the hope of maintaining the forms of "previous order", corresponding with consolidated cognitive models. For this reason, globalisation is explained, in general, as "complexity", due to the intensification of the relationships among a network that is increasingly thick with nodes, and as "standardisation", a spread of uniformity guaranteeing linear relationships between the nodes. The result is the inevitability of an increasingly dense network, made up of nodes that tend to resemble one another. In either case, globalisation is interpreted as a paradigm of the "*pre-global*", we dream of restoration, i.e. normalisation and return, and not of changing the model in order to understand the world. In this view, globalisation is a positive orientation of the system or, at most, a future state that is inevitable and should be managed to exploit its advantages.

But this is mistaken. With our fear of novelty, we anchor ourselves to the customary way of reading the present, as a replica of the past, inebriated with the easy sense of security produced by habit.

However, the scenarios change before the cultural models are able to adapt to the new needs for interpreting reality, hence the increase in vulnerability.

In reality globalisation and reticularisation are different phenomena, each implying the other in certain respects but maintaining their autonomy, although the latter is generally considered to be the product of the former. In the present state, if globalisation can be contained, and combated successfully, reticularisation cannot be avoided without losses, with the degree of interdependence achieved by the parts in relation between them.

However, we must begin to change the idea of a network that leads to primacy of the concept of globalisation, and work out an autonomous view of the network itself. First of all, the nodes are not all equal, nor do they become so; each node is highly specific (different from the other nodes) and is necessarily in network with the other nodes. In this way the strategic attention for managing the process of reticularisation is focused on the specific nature of each node and on the characteristics of their links. Especially the latter, the

links, i.e. the relationships, are the key to access for understanding the reticular system: they must be able to handle the differences between the nodes because the relational forms – the relational processes – are the cultural and political "elastics" that permit the reticular form of the diversities.

The conceptual distance between global and reticular appears even greater if we consider that global is understood mainly as "extensive", while reticular is understood as "intensive". The former expands its frontiers while the latter deepens the relationships between the parts. As a result, the strategies giving preference to one or the other aspect are very different: one insists on the dimension of the control of the boundaries rather than on the definition of the relational protocols, one favours the channel of exchange rather than the object or value exchanged, space is preferred over time, etc. But in reality a radical dichotomy between the two aspects is as false as a univocal cause-effect relationship between them: the world is always more complicated than people would like it to be so they could understand it easily. Thus we are faced with scenarios where globalisation and reticularisation are processes correlated without a causal connection (one is not the cause of the other) but "cohabit" in that dynamic world which is represented as a functional connection between the two. This is expressed in the space-time relationship characterising them, and which we have learnt to consider right from childhood as linked by the expression of velocity (relationship between space and time), measuring transformation and change.

The conclusion from this first prompt is summed up in the fact that the global network does not homogenise anything, but on the contrary offers the possibility of a governance of the diversities, shifted from the "node" to the "relational link", to the degree that we want and are able to see the emergence of the new pattern: when the world changes more rapidly than our will to develop more adequate interpretative models, we are victims of our vulnerability.

3. The change in the conflict: the Hybrid War

Globalisation is interpreted in a manner that serves to find excuses for "refusing the novelties" that it involves; this can be seen in the refusal to apply the same "globalising" prerogatives to conflicts as to other phenomena: it is accepted that it produces an increase (circularity) of movement of people, goods, capital, information... but not of conflicts and violence; it is accepted that "everything" is in the network and connected, but not conflict and violence. And yet the world is increasingly characterised by that diffuse, pervasive and delocalised form of conflict known as Hybrid War, involving numerous players who "could not stay together" until now, in a context of

war that manifests itself in a non-conventional form. To explain, let us try to imagine a football field where one team comes to play rugby, another to play soccer, a third to play volleyball and then an international referee arrives to regulate this tennis match. All they have in common is the ball, and this in different shapes. It becomes evident that all the players in the field face each other without sharing any rule, or strategy, but each being aware of having to beat the others and be the sole winner. Outside this metaphor is the Hybrid War, where regular armies, terrorists, insurgents, freedom fighters, media, NGOs etc. face each other without rules; International Humanitarian Law, the Geneva Convention is now an outdated embellishment.

We are speaking of the war that provoked this comment from Pope Francis (30 November 2014, during his return trip from Turkey): "*It is an opinion of mine, but I am convinced that we are living through a third world war in pieces, in chapters, everywhere*". And this other comment by President Mattarella (19 August 2015, 36th Meeting at Rimini): "*Terrorism, fuelled also by fanatical distortions of faith in God, is trying to introduce the germs of a third world war into the Mediterranean, the Middle East and Africa*".

But this is an untenable narrative, both civilly and politically: what citizen or ruler today would willingly and consciously accept finding himself immersed in a third world war? Hence the denial of the evidence of the conflict, which is played out on a multiplicity of concurrent levels (military, economic, media, cultural, technological etc.). This permits each of us to feel safe without actually being safe and, above all, does not allow anyone to initiate appropriate strategies for peace and reduction of conflicts, unless adapted to the new form of "negated scenario".

The dramatic consequences of this situation are the exponential increase in victims among "civilians" (but who are the "formal" combatants?) and the expansion of that grey area that is neither war nor peace (but which of the two is declared now?), making up the new uncertain scenario in which to go and operate.

Thus war without rules arouses even greater fear, because it loses the perceivable limits of political and cognitive control, becoming a monster capable of swallowing up everything; from an "unpleasant" but regulatable event it is transformed into an uncertain and ungovernable event: a crisis.

4. The central role of culture: Cultural Diplomacy

Clearly at this time we are in a turbulent and uncertain global system seeking new forms of stability that must be entrusted to new forms of "diplomacy" as a process that favours functional relations between subjects interested in cooperating. For these general characteristics (crisis, uncertainty, turbulence

etc.) the cultural dimension is the perspective to be adopted: local identities are important cognitive anchoring points, so much so that we can state that a response to turbulence is obtained by strengthening local cultures – that reserve of identity that favours the interpretation of change – on condition that they are connected in a network through a facilitating cooperative system. In fact it is the social identity of the community, expressed in its cultural practices, that generates the resilience necessary to cope with the uncertainty of the conflict. And it is the reticular, i.e. relational, dimension that enables social identities to overcome their own particularisms and deploy their potential in the "network of diversities".

Over recent decades there has been an increased insistence, and weight, of so-called Public Diplomacy in the context of government practices in international relations: "soft power" has come alongside traditional "hard power" especially in areas of conflict, offering new instruments for dealing with the crisis. Even more in recent years, especially with the development of the modern diffuse and pervasive technology of communication, the term Public Diplomacy has been joined by Cultural Diplomacy. In fact, ICTs (Information and Communication Technologies) have given a potentially significant role to local cultures, understood as systems of knowledge, belief, arts, behaviour, ethical and moral orientation, or any other object, also immaterial, built by a community.

Unfortunately cooperation itself, understood as a strategy of diplomacy, is trapped in the old way of seeing, with the participation of a system of international relations and outdated political theories, and has not taken up the change. It pursues programmes and actions that do not produce anything because they look to a horizon that can no longer be such, in the light of the premises explained above.

The proposal presented here, concrete in terms of work of research and in the field, is to reposition ourselves towards a reticular world made up of nodes differing between them, in relationship through links able to contain diversity, where:

- cultural resilience is structured in a policy of local government;
- the global world is made up of strong singularities in a network, where the hegemonic model changes;
- cooperation is an instrument for renegotiating the forms of power;
- Cultural Diplomacy is the instrument of navigation for the difficult transition we are going through.

5. Thoughts from the field

The opportunity has arisen for comparing the considerations set out so far with the results obtained in the field over the last few years, engaged in cooperation with the International Solidarity Centre (Centro di Solidarietà Internazionale - CeSI) of the Università Cattolica, together with institutional partners, such as the Italian Armed Forces, or some non-government organizations, such as Perigeo IPC Ngo. These activities have always concerned interventions in crisis or post-conflict contexts, focusing above all on the cultural dimension of the interventions, developing in a period of about twenty years and embracing, among the various countries, Iraq and Kurdistan during the 2003 war, Sri Lanka for the tsunami in 2004 and 2005; Haiti for the 2010 earthquake; Afghanistan from 2009 to 2014. Numerous activities have been involved, which have enabled us to reconsider the activities carried out in those specific contexts, within a model which has then recently become topical in Syria, Oromia and Somalia, the areas referred to below.

5.1 Syria, Maaloula 2019

The experience accrued over the past few years in crisis contexts brought us, with Perigeo IPC Ngo and the Congregation of the Barnabite Fathers, into the Syrian War, at Maaloula in January 2019.

Maaloula is an ancient village about fifty kilometres from Damascus, 1,500 metres above sea level, considered to be the cradle of Syrian Christendom, where the Muslim, Greek-Catholic and Greek Orthodox communities have always lived together and where they still speak the "Syriac dialect of Maaloula". It was the venue of bitter battles with the Al Qaeda terrorists of Al Nusra, who occupied it for two years.

It is the cradle of Aramaic civilisation, it houses the Greek-orthodox monastery of Saint Thecla, where the remains of the saint, a disciple of St. Paul, are kept. Here is also the 6th century Greek-Catholic monastery of Saints Sergius and Bacchus, dedicated to two Roman army officers of Syrian origin, executed in 297 A.D. It is built on the ruins of an ancient temple to Apollo. On the walls, next to the very ancient altar, were 26 icons of the Syriac school, which have disappeared, perhaps destroyed or sold. Among these, that of the Mysterious Supper: a last supper in which Christ does not sit at the centre and the table is semi-circular but, above all, it was the symbol of the entire community, which met spiritually every day at that table. On our mission for Damascus, Homs and Aleppo we delivered a copy of this icon to the community, faithful not only in its form but also in the "methodology of writing", a real piece of local identity culture: the ceremony, which took place in the monastery before the ancient altar, brought back together the pieces of the

battered community, which reconstituted itself then as such, able to share a vision, a project and a future by rediscovering the cultural links that generated it. This initiative confirmed the priority of the process of symbolic-hereditary reconstruction as compared with that of post-emergency material reconstruction: the design of the infrastructures, which is associated with the vision of a future, is useful only where the roots of the community have been rediscovered. The cultural action was confirmed to be both the elective instrument of cooperation in the post-conflict phase, because it responds to the "urgency of peace" weaving a network of strong identifying singularities, and the concrete dimension orienting the action of Cultural Diplomacy.

5.2 Horn of Africa: Tigrai, Oromia and Puntland, 2016 -18

The Horn of Africa, with the violent complexity and cultural heritage that distinguishes it, is the destination of a significant activity; it is an important partner in the new network of the *Cultural Diplomacy Platform* with CAARI – Cultural and Archaeo-Anthropological Research Institute of the Addoun University of Galkayo, Puntland (Somalia). The project, promoted by Perigeo IPC Ngo in collaboration with the Università Cattolica, has set itself the task of promoting culture as a tool of development and empowerment of local ethnic minorities and as a means to support peace, dialogue and solidarity between different communities focusing on:

- Ethiopia in Tigrai, on the border with Eritrea, where centres for the development of the activities have been selected at Shiraro (Cunama ethnic group), at Dawhan (Irob ethnic group) and Alitena (site of the first monastery of Catholic religion), areas of criticality between Ethiopia and Eritrea and between the ethnic groups present;
- Ethiopia, in Oromia, at Kofale and in the border area with Somalia: a territory with a high inter-ethnic tension but with great possibilities for tourist development, crossed as it is by the course of the Webi Scebeli, whose sources were discovered ninety years ago by the Duke of the Abruzzi;
- Somalia, in Puntland at Garowe and Galkayo for the exploitation of a recent archaeological discovery that throws light on the most ancient civilisations of the Horn of Africa, in a country crossed and shaken by the violence of terrorism and tribal clashes;
- Somalia, at Jowhar (about 90 km from Mogadishu) with an intervention in the former "Duke of the Abruzzi" agricultural village, an area dense with history, both exemplary and problematic.

The project arose from an intuition by Perigeo, present in Somalia since 2010, with the "Museums for Peace" where it expresses the belief that recip-

rocal acquaintance represents a necessary condition for favouring peace in areas with a high inter-ethnic conflict. Hence the idea of promoting awareness, protection and use of the material and immaterial heritage belonging to the traditions of the various countries where Perigeo carries on its work.

Starting from this original idea, the activities focus on some specific objectives, namely:

1. To support the reconciliation process through the development and promotion of the cultural heritage;
2. To promote awareness of the value of the culture of their community and of the need to preserve it;
3. To promote positive relationships between generations through the exercise and transmission of cultural skills;
4. To promote tourism and community handicrafts, with particular attention to the possibilities offered by the region (e.g. the sources of the Webi Scebeli in Oromia)

The old idea of the "Museums for Peace" prompted the reflection that led to the development of Cultural Focal Points as a privileged instrument of Cultural Diplomacy and, above all, the cultural intervention demonstrates its undoubted added value in promoting those links that permit subsequent structural interventions for combating drought (wells), favouring medical care (setting up a laboratory for the production of medicines), relaunching the local economy on a sustainable basis (school of fishing and fish market) and setting up a network of sustainable cultural tourism.

The Horn of Africa has been the first laboratory experience in the use of culture as an instrument of cooperation in areas that are difficult due to a complex history of cultural conflicts, which has seen the involvement of all the actors of the project, albeit at different times. In this context, a relationship has been created between Somalian ethnic groups, between Ethiopian groups, between Ethiopian and Somalian ethnic groups, and also between Ethiopians and Somalians and Italians. The dynamics of this process of reciprocal acquaintance were not explained so much as governed in the very perspective of the project, highlighting how that cultural dimension was an asset preparatory to making subsequent structural cooperative activities effective.

6. Cultural Diplomacy and cooperation: the instruments of the intervention

It has been maintained that the recomposition of the local cultural heritage must be a priority for the interventions in crisis or (post-) conflict situations, through the use and dissemination of local knowledge.

An expression "in the field" of the previous perspectives indicates how projects, research-action, interventions whose aim is to achieve a possible reconciliation and socio-political-cultural stability in the medium-long term, and which are activated as a response to long-lasting conflict situations, can be based in the following methodological process:

1. A phase of analysis of the situation and of the cultural interpretative *drivers* typical of the context being considered, through the principles and the theoretical lines of *crisis management* and *risk analysis*;
2. The preparation of elements of cultural resilience, which can overcome the passage leading from the handling of conflicts to a resilient response in terms of *cultural diplomacy*, recalling that Chandler[2] asserts: *'Changing or adapting behaviour and understandings need to come from within; resilience cannot be "given" or "produced" by outside actors, only facilitated or inculcated through understanding the mechanisms through which problematic social practices are reproduced'*. In this specific phase, cultural resilience maintains its characteristic of multidimensionality, recognising a functional and systemic interdependence between the national, political, local and community levels.

This methodological line aims to promote a management and reduction of conflicts, placing at the centre of these interventions the exploitation of the cultural heritage and the historical-social memory of a community or social grouping whose main instrument is its own culture. The positive spinoff of this type of action is to be found in the awareness of knowing one's roots as an instrument of dialogue and peace.

Cultural-interpretative change, the factors of crisis management, the specificity of resilience have been expressed in a new operative model, which we identify in the so-called *Cultural Diplomacy Partnership (CDP)*, which is being constituted in an experimental phase as a network of partners interested in cooperating according to some principles as set out briefly below.

The aim of the CDP is to promote *Cross Cultural Country Development (CCCD)*, understood as a process of cooperative development between partners, requiring from each the ability to interact effectively with the bearers of a different culture and therefore in the respect and use of cultural specificities and diversities.

As a result, the working method gives a central place to the cultural dimension in which local identities are expressed, a reason for stability, able to relate with other specificities in a network (singularities in a network): this is

[2] David Chandler, *'International Statebuilding and the Ideology of Resilience'*, Politics, Vol. 33, No. 4 (2013).

a strategy realised by *Identity Based Actions (IBAs)*. IBAs use, promote, conserve and reproduce the signs of the material culture (objects) and immaterial culture (song, dance, rites, narrations, cuisine and traditional medicines, ways of thinking etc.) of a specific community.

Networking, understood as a necessary and autonomous prospect with respect to globalisation, underlines the specificity of the CDP model, defining itself as "inclusive" and making the "extreme areas" the target of the actions. The method and, together, the target of the action is therefore *Inclusive Networking of Extreme Areas (INEA)*. The definition of an Extreme Area departs from the customary one of a crisis or post-conflict area: they resemble each other for their characteristics of uncertainty and diffuse and latent conflict, but differentiate themselves for the marginality and singularity typical of the Extreme Area. This is a marginality understood only as the periphery by the infrastructural channels which favour exchanges/relationships, but not by the interests that motivate exchanges/relations; a singularity understood as a high specificity of the network node whose relational protocols must however be defined in order for its networking capacity to be effective. In this perspective we can talk of Geopolitics of the Extreme Areas, which become an object of penetration especially when they are peripheries of a number of centralities, characterised by a marginal economy of their own, with local market resources and possibilities. An example is the Nepalese region of Mustang, in the Himalayas, where a new road has connected it effectively with Tibet and the Chinese economy, rapidly decreeing its dependence. The present road connection, in fact, is effectively operative in the eastern area Mustang (Nepal) - Tibet (China), (about 50 km) and completely ineffective in the West Nepalese route (about 150 km) which ought to constitute the new way of Chinese penetration of India along the Kali Gandaki Corridor. The result is that this extreme area is being incorporated into the process of extension of the Chinese neighbour, losing its singularity, assimilated by the neighbouring nodes (Chinese region) to become an offshoot of penetration by the nearby giant. On the contrary, the form of cooperation founded on the *Cultural Diplomacy Partnership (CDP)*, aims to guarantee that all the peculiarities that make Mustang marginal and singular remain in the network, favouring the maintenance of the "potential" difference between the nodes.

The cardinal instrument, the most operative dimension of the CDP, is the so-called Cultural Focal Points (CFPs): a series of representative collections of the material and immaterial culture of a specific local community and of activities reproducing local culture, which are the prime movers of cultural exchange initiatives, promotion of dialogue and reciprocal acquaintance between the various ethnic areas involved.

The Cultural Focal Point is:

- static: it can be compared to a museum, insofar as it represents cultural processes and displays artefacts;
- dynamic: it is a place of encounter where what is preserved is reproduced, favouring the dialogue and vertical transmission of the memory together with the learning of "how to do";
- singular: it highlights the cultural peculiarities of a single community, which by reinforcing their own identities acquire awareness and resilience that are expressed as a "competent node" of the global network;
- plural: because each culture finds itself in a necessary relationship with the other nodes (cultures) of the network, maintaining functional reciprocal relations.

We are aware that the model put forward is complex and composite, in the phase of elaboration and experimentation, but we are also convinced both as to its sustainability and as to its "preventive" effectiveness. The latter is defined by the necessity of guaranteeing the survival of local culture as an increase in value of the reticular world and, precisely, an instrument for prevention of conflicts and a prerequisite, on the basis of mutual understanding of the different cultural codes, to the reciprocal satisfaction of material needs, favouring economic relations.

We therefore need to reposition ourselves in this reticular world, made up of nodes differing between them that are identified in strong singularities in the network, which relate through links able to contain the diversity, where cultural resilience is structured in a policy of local government and cooperation as an instrument of reorganisation of power, where Cultural Diplomacy is proposed as an instrument of negotiation in the difficult period of transition we are going through.

It is urgent on the other hand that we find new forms of collaboration between institutional actors and communities in this new, highly unpredictable scenario, because a delay is not ethically or functionally sustainable. And the local dimension, in its expression of cultural identity, is functional to local development and well-being founded on those specific skills, fed into the network.

Thus, cultural strategy, organised in the perspective of Cultural Diplomacy and made operative in the *Cultural Diplomacy Partnership*, with its different instruments, is adequate to the new reticular and complex scenario, orphan of *governance*, where precisely *Peace is Urgent*.

Bibliography

AA.VV. (2018), *Cultural Diplomacy and Trade: Making Connections*, NACDI, Kingston.

Beel, D.E. et al. (2015), *Cultural resilience: The production of rural community heritage, digital archives and the role of volunteers*, Vol. 54, Journal of Rural Studies, Elsavier, Science Direct, UK.

Brown, K. (2015), *Resilience, Development and Global Change*, Routledge, London.

Chandler, D. (2014), *Beyond neoliberalism: resilience, the new art of governing complexity*, Resilience International Policies, Practices and Discourses, 2:1, Taylor and Francis, UK.

Gienow-Hecht, J. e Donfried, M. C. (eds.) (2010), *Searching for a Cultural Diplomacy*, Oxford University Press, Oxford.

Holtorf, C. (2018), *Embracing change: how cultural resilience is increased through cultural heritage*, World Archaeology, Taylor and Francis, UK.

Lombardi, M e Lucini, B., *Cooperazione e Cultural Diplomacy: resilienza e cultural focal points*, in Sicurezza, Terrorismo e Società, 9, pg. 7-20.

Lucini, B. (2014)a, *Disaster Resilience from a Sociological Perspective Exploring Three Italian Earthquakes as Models for Disaster Resilience Planning*, Springer Int. Publishing, Cham (CH).

Mantovani, G. (2005), *L'elefante invisibile Alla scoperta delle differenze culturali*, Giunti, Firenze.

Olivares, F., e Zafirova D.A. (cur.), (2019), *Diplomazia culturale e Relazioni internazionali. Il caso dei rapporti tra l'Italia e la Bulgaria*, Avangard, Sofia.

Thiele, L.P. (2016), *Sustainability*, Polity, Cambridge, 2nd ed.

Wagner, W. and Anholt, R. (2016), *Resilience as the EU Global Strategy's new leitmotif: pragmatic, problematic or promising?*, Contemporary Security Policy, Vol. 37, No. 3.

Cultural Resilience and Cultural Diplomacy: the State of the Art

Barbara Lucini[1]

Nota autore

Barbara Lucini is postdoctoral fellow and PhD in Sociology and Methodology of Social Research at the Department of Sociology, Catholic University of the Sacred Heart, Milan. She is also adjunct professor of risk management and crisis communication. She has been involved in several research projects (European and others) focused on crisis management, risk communication, risk perception, security and resilience. Her research interests are directed at disaster resilience, disaster management, and civil protection systems. She also explored the relationship between terrorism or political extremism and resilience. She is the author of "Disaster Resilience from a Sociological Perspective: Exploring Three Italian Earthquakes as Models for Disaster Resilience Planning", Springer International Publishing 2014, and "The Other Side of Resilience to Terrorism: A Portrait of a Resilient-Healthy City", Springer International Publishing 2017.

Abstract

Il presente articolo intende fornire un'analisi dell'importante contributo che la resilienza, soprattutto nella sua dimensione culturale, può fornire nei contesti di post- crisi e negli scenari di conflitto, in relazione con l'approccio operativo della *cultural diplomacy*.
La premessa importante riguarda il concetto di resilienza e il suo ruolo nell'ambito della gestione delle crisi e dell'analisi del rischio. La resilienza culturale si ritiene essere fattore imprescindibile per la costruzione di identità nazionali, collettive e individuali che siano in grado di definire, interpretare e gestire le nuove minacce ibride.
Lo stesso elemento culturale unito al concetto di identità sono da considerarsi, quali *driver* per una necessaria relazione fra la dimensione culturale della resilienza e la *cultural diplomacy*.
Le considerazioni finali consolidano la prospettiva socio- antropologica legata alla dimensione culturale e all'applicazione del concetto di resilienza nell'ambito della cultural diplomacy, per la gestione delle tensioni e conflitti socio – politici in molte parti del mondo.

This paper aims to provide an analysis of the contribution that resilience, especially in its cultural dimension, can provide in post-crises and conflict scenarios, along with the pragmatic approach of cultural diplomacy.
The key premise is the concept of resilience and its role in crisis management and risk analysis. Cultural resilience is regarded as an essential factor to build national, collective and individual identities that are able to define, interpret and manage new hybrid threats.

[1] ITSTIME – Università Cattolica del Sacro Cuore, Milan, Italy.

Both the cultural factor itself and the concept of identity need to be seen as drivers for the required relationship between the cultural dimension of resilience and cultural diplomacy. The final remarks consolidate a social anthropological perspective associated with the cultural dimension and the application of the concept of resilience in the framework of cultural diplomacy, with the aim to manage socio-political tensions and conflicts in many parts of the world.

Keywords

Cultural resilience, cultural diplomacy, security, adaptation, proactivity.

1. Foreword

The current state of the world and the increased instability at both national and international levels requires us to focus on the role played by resilience. Conflicts are pervasive, diffused and complex in this new and changing context of hybrid warfare.

An analysis of the concept of resilience requires using multidimensional perspectives as well as an adaptative attitude by the scholars themselves, yet it is a worthwhile opportunity to explore new views of the same concept applied to various scientific domains.

Resilience and its cultural dimension is affected by its own context-sensitive nature, which requires an attention to environmental variables and their effects on societal systems.

From this perspective, a world where threats derive from different sources, thus classified under the umbrella definition of hybrid threats, resilience appears to be the most necessary skill to deal with all post-crisis and post-conflict situations around the world.

2. Resilience and its cultural dimension

Defining resilience is challenging because of its context-sensitive nature and its wide range of application. It requires a specific contextualising of the scientific domain within which the concept will be analysed.

This approach is also determined by the historical background of the concept itself: the term resilience was used by scientific scholars involved in physics experiments. Therefore, ensuing studies on resilience took place within the scientific field of hard science.

Since the 70s, however, the concept of resilience has spread into the psychology and social science disciplines.

It is worth noting that the original definition of resilience was maintained in this context, while its area of application has changed.

For the purposes of this study, the definition of resilience is as follows:

a "*process, capacity or outcome of successful adaptation despite challenges or threatening circumstances*," and "*good outcomes despite high-risk status, sustained competence under threat and recovery from trauma*" (Masten, Best, & Garmezy, 1990) cited by Clauss-Ehlers (2008).

Studies conducted to further understand how the concept of resilience applies to the different societal systems found a few consistent attributes:

1. being context-sensitive
2. adaptability
3. being able to transform
4. flexibility
5. framing the opportunity
6. balance and order
7. proactivity
8. changing attitude depending on the cultural environment

These eight traits are universal in the concept of resilience and can be applied across scientific domains, painting a different picture depending on the context. This action brings the focus onto the characteristics of the system, as well as an awareness of where the resilience concept needs to be implemented: for instance it can be applied to the analysis of resilience within a private company as well as within a public institution.

Regardless of their application, studies on resilience have shown that it is a skill and competence that can be taught and learnt, depending on the inner characteristics of the target, whether that is a single person, a community, or a whole society.

This characteristic focuses on the way resilience can be taught and when it can be implemented according to the original attitudes of the people and the previous organisation of a system: the communication perspective is an essential tool and requirement to improve the effort of achieving resilience in multiple domains.

Moving on from a general definition of resilience, it is worthwhile to focus on the cultural dimension of resilience and its characteristics, as well as understanding the role played by culture (in its socio-anthropological definition) within the framework of resilience.

The main element distinguishing the connection between cultural resilience and cultural diplomacy as regards hybrid threats is the evidence based on previous studies[2], stating the influence that culture can have on resilience for individuals and systems. Specifically, Belgrave et al. (2000) cited by Clauss-Ehlers (2008) concluded that "*positive feelings about the self, one's*

[2] Cabrera and Padilla (2004), Belgrave et al. (2000), and Clauss-Ehlers et al. (2006).

culture, and one's ethnic group promote resiliency and are linked to positive behaviors (e.g., better school performance) and decreases in risky behaviors (e.g., early sexual activity, drug use)".

This finding prompts a reflection on the link between cultural resilience and cultural diplomacy, in that resilience can spread the activity of cultural diplomacy and support the understanding of the multiple identities that exist in geopolitical contexts.

For this reason, it is essential to define cultural resilience. One definition of the concept is provided by Holtorf (2018): "*I define cultural resilience as the capability of a cultural system (consisting of cultural processes in relevant communities) to absorb adversity, deal with change and continue to develop. Cultural resilience thus implies both continuity and change: disturbances that can be absorbed are not an enemy to be avoided but a partner in the dance of cultural sustainability*". (adapted from Thiele [2016, 36]).

A further model was developed to sustain this first evidence: Clauss-Ehlers (2004) presented a theoretical model that posits that culture and the sociocultural context affect resilience. This culturally-focused resilient adaptation model is described as "*a dynamic, interactive process in which the individual negotiates stress through a combination of character traits, cultural background, cultural values, and facilitating factors in the sociocultural environment*" (Clauss-Ehlers, 2008).

The importance of what was previously described as "*culturally-focused resilient adaptation model*" is linked to the current international scenario and its new threats. It focuses especially on the importance of strengthening cultural factors – detailed for each ethnic group, geopolitical framework and post-conflict areas – as they affect the ability to spread national, socio-political and community resilience.

Furthermore, Clauss-Ehlers (2008) clearly defines cultural resilience and the way its influence works within a framed context: "*Part of this contextual focus examines cultural influences involved in resilience and coping. Clauss-Ehlers (2004) presents the term cultural resilience as describing the degree to which the strengths of one's culture promote the development of coping. This type of resilience has a number of aspects including a developmental trajectory within a cultural matrix composed of norms, family structure, and peer relationships*".

The main aim of resilience is to enable people – at all levels, whether a single person, social groups or institutions – to cope with post-crisis and post-conflict times. The ability to cope becomes the main skill to pursue, when discussing the role played by cultural resilience within the scenario of cultural diplomacy.

Addressing the comprehensive contribution that cultural resilience can provide, it is worthwhile to focus on the role of identity and its social anthropological significance (Allovio et al. 2018).

The evolution of sociological theories demonstrates the relevance of identity – specifically social identity – in allowing people to interact and communicate with each other, promoting a common framing and understanding of a situation.

Referring to previous studies conducted about the influence of resilience on the capability of adaptation, Clauss-Ehlers (2008) states:

> Thus, it was the combination of both valuing one's culture as well as learning about the culture of the new system that helped the students be successful. Cabrera and Padilla (2004) wrote: "Some readers might argue that Erandi and Juan [i.e., the study participants] were the fortunate ones and that their success is atypical. We take the position, however, that Erandi and Juan succeeded only because they managed to learn what the middle class take for granted, that is, there is class- and culture-bound knowledge that is necessary to succeed in higher education

The study cited above confirms the bidirectional pattern of cultural resilience, stating the need to address both the individual culture and its view of the world and the collective culture deriving from group perceptions.

At the end of this short excursus, the new approach we introduce here maintains that resilience from a cultural dimension can be defined as the ability to rebuild identity – at individual, community, collective and institutional levels – after a crisis and/or a conflict (whatever its cause), evidencing that this is a specific competence that can be taught to and learnt by a community or a group of people.

This is the first step towards further theoretical and methodological research and activities in the field of *fostering cultural diplomacy through cultural resilience*.

3. Cultural Resilience and Cultural Diplomacy

Having provided a general definition of resilience and cultural resilience, the focus can now shift to a more specific analysis of the link between cultural resilience and cultural diplomacy, with an in-depth look at the role of culture and identity.

In order to develop a number of pragmatic insights and suggest further actions on this topic, we need to outline the scenario for this approach because of the context-sensitive nature of resilience.

Over the past decades, vulnerabilities, crises and fragilities that emerged as a result of various threats and local or national instabilities were mainly managed within political and/or technical perspectives.

The changing nature of the current scenario requires different, equally adequate, tools to prevent, manage, cope and respond to these unpredictable threats: "*[...] global, national and local systems must be strengthened to cope with a range of insurgent threats*" (Evans and Steven, 2009). This new situation requires cultural diplomacy tools to develop a holistic, resilient strategy for ongoing threats.

This scenario, characterized by the presence of pervasive conflicts, should be analysed with a focus on the behavioural patterns of social relations.

The challenges for conflict management in this era are the high levels of complexity and the chaotic set of motivations which lead to conflicts and crisis: interconnections and interdependency are the two main factors that affect an efficient response after impact.

Many significant conflicts are motivated by a combination of ethnic or ideological causes, showing that culture alone cannot be used as reference in dealing with crisis management and risk assessment.

Narrative and communication strategies also play a crucial role for both stages in this framework in understanding and managing the diffused instability and related threats.

Methodologically speaking, linking cultural resilience and cultural diplomacy means taking different levels of understanding into account:

1. Individual
2. Community
3. Society
4. Institutional

The institutional position brings us to the core topic of cultural diplomacy as part of a more general vision of public diplomacy.

Moreover, these levels exist within specific action areas: post-crisis, post-conflict, and extreme.

It is also important to stress the significance of the socio-political scenario's characteristics and cultural backdrop where the relationship between cultural resilience and cultural diplomacy manifests.

In accordance with this methodological framework and its drivers, we can link the cultural resilience domain to that of cultural diplomacy, with these postulates:

– this proposition should not focus on post-crisis responsiveness, but on a proactive approach for effective management that includes all phases, from prevention to planning for impact

– nations and countries with more socio-political instability need to develop adaptability to adverse situations caused by multiple threats, especially when managing ethnic conflicts
– adaptability is also needed for a new way of thinking about different geopolitical and international governance scenarios
– the context-sensitive nature of resilience demands a focus on the actual local situation and resources available in situ, promoting local knowledge in a view to cultural resilience

The combined approach of cultural resilience and cultural diplomacy is rooted into the following crucial points:

1. to manage complex crises and diffused threats, there needs to be interconnection and interdependence of both local and international situations. A social anthropological understanding of typical cultural representation is essential, in order to provide a cultural model of understanding that can be applied to different societal realities
2. the general characteristics of resilience can be combined with the detailed characteristics of cultural resilience, leading to a cultural model of adaptation to help go beyond conflicts and ethnic and social tensions, promoting *resilience-sensitive policies* at governance level (de Weijer, 2013)
3. from a methodological perspective, three aspects need to be developed:
   – promoting *culturally focused resilient adaptation actions* in areas of the world affected by multiple threats such as crises, instabilities, and conflicts
   – supporting the progress of what can be defined as *geopolitical ethnography*, where the three key elements of geographies, identities and cultures prevails over local and international instability management
   – combining the connection between cultural resilience and cultural diplomacy with the sub-categories of material culture (Ciabarri, 2018), where local artefacts become a concrete element linking back to the original nature of cultural diplomacy

These three aspects are tied together by the possibility to inform about the relationships emerging from the fieldwork, stressing the *cultural narratives* that influence both local and international levels.

4. Final Remarks on Future Research

The current piece of writing states the demand to promote an approach of cultural resilience within the domain of cultural diplomacy, with all the relevant challenges arising from this effort.

In particular, these are:

- the need to overcome the "old" understanding of resilience and international cooperation, addressing and including the essential role played by a cultural resilience dimension within the framework of cultural diplomacy, reflecting on more useful methods and tools to implement an international governance resilience framework, that will focus primarily on the *geopolitical ethnography* outlined above
- moving away from a more clinical approach to resilience and instead focusing on a cultural perspective and the impact that cultural factors, which vary from one society to another, have on resilience competences when reflecting on its contribution to social sciences
- it is not possible to ignore the influence that a context of crisis, instability and/or conflict has on the effect of resilience in cultural diplomacy, the original nature of the new global scenario and its threats must be acknowledged: *[Instead,] the concept of resilience should be at the heart of a new doctrine for managing transnational risk and global instability. Resilience offers a guiding principle for informing strategy and animating alliances. It also provides a yardstick for measuring success. At present, much of what governments do internationally inadvertently increases vulnerability. This must change if globalization is to be saved from itself (Evans and Steven, 2009).*

The future trend of cultural resilience and cultural diplomacy could develop in the following steps:

- developing a methodological framework – *geopolitical ethnography* – to enhance cultural resilience through cultural diplomacy (Thomas, 2016) in areas of the world affected by multiple situations of socio-political instabilities, growing as deep an awareness of context and intercultural communication as possible
- developing resilient identities in those countries affected by various threats and instability at an individual, community, societal and even national level, creating what could be defined as a *country profile of cultural resilience*
- promoting the development of a tool to assess cultural resilience from a double perspective: that of geopolitics and that of diplomacy

This roadmap for further development of this research area benefits from the bidirectional nature of resilience, which is on one hand a key element to support cultural diplomacy action and on the other the goal of those very actions.

Finally, the two new essential contributions – *geopolitical ethnography and a country profile of cultural resilience* – are the leading elements to develop the deep connection between cultural resilience and cultural diplomacy.

References

Allovio, S. et al. (2018), *Antropologia culturale: I temi fondamentali*, Raffaello Cortina Editore, Milano.

Beel, D.E. et al. (2015), *Cultural resilience: The production of rural community heritage, digital archives and the role of volunteer*, Journal of Rural Studies, ScienceDirect, Elsevier, UK.

Belgrave, F.Z., et. al. (2000), *The effectiveness of a culture-and gender-specific intervention for increasing resiliency among African American preadolescent females*, Vol. 26 Issue 2, Journal of Black Psychology.

Cabrera, N.L., and Padilla, A. M. (2004). *Entering and succeeding in the "culture of college": The story of two Mexican heritage students*, Vol. 26, Hispanic Journal of Behavioral Sciences.

Ciabarri, L. (2018), *Cultura materiale Oggetti, immaginari, desideri in viaggio tra mondi*, Raffaello Cortina Editore, Milano.

Clauss-Ehlers, C.S. (2004). Re-inventing resilience: A model of "culturally-focused resilient adaptation." In C.S. Clauss-Ehlers & M.D. Weist (Eds.), Community planning to foster resilience in children, New York, NY.

Clauss-Ehlers, C.S., Yang, Y.T., & Chen, W.J. (2006), Resilience from childhood stressors: The role of cultural resilience, ethnic identity, and gender identity, Vol.5, Journal of Infant, Child, and Adolescent Psychotherapy.

Clauss-Ehlers, C.S. (2008). Sociocultural factors, resilience, and coping: Support for a culturally sensitive measure of resilience, Vol. 29, Journal of Applied Developmental Psychology.

de Weijer, F. (2013), *Resilience: a Trojan horse for a new way of thinking?*, Discussion Paper, ecdpm, European Centre for Development Policy Management, n°139, Retrieved from: www.ecdpm.org/dp139.

Holtorf, C. (2018), *Embracing change: how cultural resilience is increased through cultural heritage*, World Archaeology, Taylor and Francis, UK.

Masten, A. et. al, (1990), *Resilience and development: Contributions from the study of children who overcome adversity*, Vol. 2, Development and Psychopathology.

Thiele, L.P. (2016), *Sustainability, Polity*, Cambridge, 2nd ed.

Thomas, D. et al., (2016) *Re-evaluating resilience: from individual vulnerabilities to the strength of cultures and collectivities among indigenous communities*, Vol. 4 Issue 2, Resilience, International Policies, Practices and Discourses, Taylor and Francis, UK.

Wagner, W. and Anholt, R. (2016), *Resilience as the EU Global Strategy's new leitmotif: pragmatic, problematic or promising? Contemporary Security Policy*, Vol. 37, n° 3, Routledge, Taylor & Francis, UK.

II.
PERSPECTIVES ON TERRORISM AND COUNTER-TERRORISM

The Italian shared house for combating terrorism[1]

Alessandro Boncio

Nota Autore

Alessandro Boncio, Inspector of Arma dei carabinieri is lecturer and counter-terrorism analyst at the Istituto Superiore dell'Arma dei Carabinieri. He is member of the European Expert Network on Terrorism Issues (EENeT) and part of the pool of expert on terrorism of the European Union Agency for Law Enforcement Training (CEPOL). He is the author of numerous researches published at the national and international level.

Abstract

Un aspetto spesso trascurato nello spiegare l'efficienza italiana nel contrasto e prevenzione del terrorismo, sia esso interno o internazionale, è rappresentato dalla struttura istituzionale creata nel 2004 per la gestione del problema. A tale proposito, il ruolo del Comitato di Analisi Strategica Antiterrorismo (CASA), il centro italiano di fusione antiterrorismo, si è rivelato essenziale. La necessità di tali organizzazioni fu una diretta conseguenza degli eventi dell'11 settembre 2001, quando gli Stati Uniti avviarono la costituzione di un "fusion center" antiterrorismo, successivamente seguiti da altri paesi europei a seguito degli attacchi jihadisti di Madrid e Londra.

Il compito principale del Comitato era originariamente quello di prevenire attentati terroristici attraverso la condivisione di informazioni in tempo reale tra gli attori statali del comparto sicurezza. Dalla sua creazione, tuttavia, i compiti del CASA sono cambiati ed ampliati: il terrorismo "homegrown" (la fase di leaderless jihad), i Foreign Terrorist Fighters e la recrudescenza dell'estremismo violento interno, hanno portato a un'evoluzione delle competenze del CASA. Il Comitato si è rivelato particolarmente utile nel rafforzare la sinergia tra tutti gli attori coinvolti nelle attività antiterrorismo, rappresentando anche un centro fiorente per "istituzionalizzare" la cultura del sistema di sicurezza nazionale derivante da precedenti esperienze nella lotta al terrorismo interno (Le Brigate rosse, Organizzazioni neofasciste) e di criminalità organizzata (Mafia, Camorra, N'drangheta).

[1] Disclaimer: The original paper was used as a contribution to a report commissioned by the International Centre for Counter Terrorism – The Hague; R. van der Veer, W. Bos, L. van der Heide, "Fusion Centres in Six European Countries: Emergence, Roles and Challenges", *International Centre for Counter Terrorism – The Hague*, February 4, 2019, *https://icct.nl/publication/fusion-centres-in-six-european-countries-emergence-roles-and-challenges/*. All the information originates from open sources and/or personal research and study. The contents of this publication, as well as any mistake or inaccuracy in the text, are the sole responsibility of the author.

A causa del numero non elevato di eventi legati al terrorismo in Italia, esiste solo una percezione generica del ruolo svolto dal CASA nell'opinione pubblica nazionale e, più in generale, tra gli osservatori internazionali, poiché il Comitato viene raramente menzionato come uno strumento sinergico antiterrorismo. Tuttavia, la struttura si è rivelata strumento flessibile ed efficiente e, nonostante la sua ambizione di istituzionalizzare l'approccio italiano al controterrorismo, non è stata gravata dalle pastoie burocratiche che troppo spesso caratterizzano la pubblica amministrazione.

An often overlooked aspect in explaining the Italian efficiency in countering and preventing terrorism, be it domestic or international, is the institutional setting established in 2004 to manage this issue. In this respect, the role of the Antiterrorism Strategic Analysis Committee (CASA – Comitato di Analisi Strategica Antiterrorismo), the Italian counterterrorism fusion centre, has proved to be essential. While the need for centers like this was a direct consequence of 9/11, indeed being the US those starting this kind of center, other European countries started working on similar centers as a consequence of homegrown jihadist attacks.
The Committee primary task was originally to prevent terrorist-related incidents through real-time information sharing among state security agencies.. Since its creation however, the CASA chores widened and changed; homegrown terrorism (leaderless jihad phase), Foreign Terrorist Fighters and the resurgence of domestic violent extremism led to an evolution in the CASA competencies. The Committee proved to be particularly useful in strengthening the synergy between all the actors involved in counterterrorism activities, also representing a thriving hub to 'institutionalise' the national security system culture originating from previous experiences in countering domestic terrorism (The Red Brigades, Neofascist Organizations) and organized crime groups (Mafia, Camorra, N'drangheta).
Due to the contained number of terrorism-related events in Italy, there is just a basic perception of the role played by CASA in the national public opinion and, more broadly, among international observers, as the Committee is seldom mentioned as a synergic counterterrorism tool. The Committee however, proved to be a flexible, efficient tool and, despite its ambition to institutionalise the Italian approach to counterterrorism, was not burdened by the classic bureaucratic problems often characterizing the public administration. An in-depth analysis of this fusion centre can also highlight lessons to be learned for other countries facing the same type of threat as Italy.

Keywords

Antiterrorism, jihadismo, estremismo violento, intelligence, forze di polizia

Counterterrorism, jihadism, violent extremism, intelligence, law enforcement

1. Introduction

On May 2018, fourteen people were arrested in two different counterterrorism operations in Italy. The Financial Police investigated an international *hawala* circuit, uncovering the collection of more than two millions of Euro as a money-laundering scheme intended to finance the acquisition

of firearms for terrorist use[2]; at the same time, the State Police investigation revealed a logistic cell in Sardinia that was responsible for the illegal money allocation to the former Jabhat al-Nusra terrorist group. Finally, police undercover personnel in cooperation with intelligence agencies successfully penetrated both cells and collected intelligence to corroborate the investigations[3].

On March 2019 instead, The State Police arrested the first Foreign Terrorist Fighter returnee on Italian soil, after receiving a detailed warning of his presence near Naples from the Internal Information and Security Agency, later corroborated by Interpol[4]. The Algerian national was apprehended after returning from Syria where he fought alongside ISIS; the man lived in Italy from 2003 to 2013 and was later radicalized in Algeria before leaving for the SIRAQ region.

Both police operations are just examples of recent counterterrorism activities prompted and coordinated by the Antiterrorism Strategic Analysis Committee (C.A.S.A. – Comitato di Analisi Strategica Antiterrorismo), the Italian counterterrorism fusion centre. Its acronym means "house" and the Committee is indeed the place where law enforcement and intelligence agencies are sharing real-time intelligence regarding terrorism[5].

National counterterrorism fusion centres were initially introduced in the United States after the catastrophic 9/11 events, but effective cooperation and information sharing later became a prominent subject of consideration also in Europe after the rise of homegrown jihadism; this led to the evaluations of existing counterterrorism structures in the wake of the homegrown terrorism generation emergence and to the establishment of CT fusion centres, often following deadly terrorist attacks.

In November 2003, a suicide attack against the Italian military contingent deployed in Al-Nassiriyah (Iraq) killed 28 (19 of whom where Carabinieri and Army personnel) and wounded 58 individuals; subsequently, the Political Authority realized that, to prevent further similar events in the country and

[2] Hawala is an Islamic informal system of value transfer via a network of brokers (hawaladars), without material exchange of cash. The transactions are based on the honor and system; trust and extensive use of connections, are the components that distinguish it from other remittance systems

[3] V.N., "Money transfer illegali per finanziare la jihad: arrestati 14 fiancheggiatori", *Il Sole 24 Ore*, May 10, 2018, https://www.ilsole24ore.com/art/notizie/2018-05-10/terrorismo-arrestati-14-fiancheggiatori-formazioni-jihadiste-081156.shtml?uuid=AEGPd1lE.

[4] "terrorista islamico arrestato dalla Polizia di Caserta. Era ricercato internazionale!, *Caserta Web*, March 1, 2019, https://casertaweb.com/notizie/terrorista-islamico-ricercato-internazionale-arrestato-dalla-polizia-caserta.

[5] Lower Chamber Report on the activities of the Counterterrorism Strategic Analysis Committee, March 11th, 2015, http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/html/30/indag/c30_flussi/2015/03/11/indice_stenografico.0023.html.

abroad, an ad-hoc structure was required, to share and analyze all relevant information coming from different CT agencies. In May 2004, after a trial period, the Antiterrorism Strategic Analysis Committee was officially established with a Ministry of Interior Decree, which disciplined the National Plan for the Management of Terrorist Events[6]. The Committee is directly linked to the National Crisis Unit, another body summoned by the Interior Minister ahead of events with national security implications[7].

2. Mandate and competences

The C.A.S.A. strength originates from its legal mandate, that binds the whole Italian security information structure to cooperate with it. The Committee is a permanent structure, reporting directly to the Minister of Interiors, with meetings held on a weekly basis to share and analyze the most recent information associated with the domestic and international terrorist threat on Italian soil and abroad. Moreover, the Interior Minister can request additional meetings whenever deemed appropriate, due to ongoing or imminent events relevant for the national security[8].

C.A.S.A. primary competence is to analyze information originating from law enforcement and intelligence agencies, as well as from international cooperation and liaison officers contributions[9]. Ongoing investigations and monitoring activities are discussed during the meetings to assess the situation, foresee possible future evolutions and trends and analyze possible course of actions to be implemented. Warnings received are also examined and different actors are subsequently tasked with the evaluation of the information and the sources reliability.

Another C.A.S.A responsibility is to plan and coordinate activities for the prevention of terrorist incidents on Italian soil, monitoring (among others) radicalization hubs, online terrorist propaganda, prison situations and radi-

[6] The May 6, 2004 Ministry of Interior decree was classified on October 2, 2004 for national security reasons.

[7] Ministry of Interior official website http://www.interno.gov.it/it/temi/sicurezza/antiterrorismo.

[8] Parliamentary Annual report, XV Legislature (April 2006 - April 2008), pp.11-12, http://leg15.camera.it/_dati/leg15/lavori/documentiparlamentari/indiceetesti/033/001/00000001.pdf.

[9] For instance, after the Westminster attack on March 22, 2017, the C.A.S.A. was called for an extraordinary meeting and the Scotland Yard Liaison Officer in Rome participated to the reunion. Same thing happened after the Manchester terrorist attack on May 22, 2017; *Ministry of Interior press releases* http://www.interno.gov.it/it/sala-stampa/comunicati-stampa/antiterrorismo-comitato-analisi-strategica-intensifica-misure-sicurezza-e-vigilanza; http://www.interno.gov.it/it/sala-stampa/comunicati-stampa/comitato-analisi-strategica-antiterrorismo-dopo-i-tragici-fatti-manchester.

calized individuals. A Technical Working Group – composed by Committee representatives - establishes the procedures for implementing preventive measures approved by C.A.S.A. and delegated to the Police Authorities on the national territory[10].

Finally, the Committee mandate authorize it to establish bilateral relationships with other counterterrorism fusion centers, also outside the European borders. For instance, since the foundation of the Italian fusion center, Italy and the United States have signed a cooperation agreement to share information and monitor individuals investigated for terrorist activities; the data received are managed directly by the C.A.S.A., who provides the law enforcement agencies with all the necessary information to perform their duties[11].

3. Composition and evolution of the C.A.S.A.

The Committee is practically a joint operation room chaired by the Central Director of the Prevention Police or by the Interior Minister itself, and hosts the counterterrorism highest representatives of the law enforcement and intelligence agencies, the Financial Police and Penitentiary Administration Department (D.A.P.). Moreover, liaison officers from other countries might be invited to the meetings to provide qualified contributions. The minimalist structure and the weekly meetings make C.A.S.A. a flexible supra-agency working as a bottom up assessment tool and as top-down executive instrument at the same time.

Both Italian law enforcement agencies (Carabinieri Corps and State Police) have general jurisdiction on counterterrorism investigations, with national, regional and provincial specialized units fulfilling the investigative activities to counter domestic and international terrorism.

The intelligence agencies (Internal Information and Security Agency – A.I.S.I., and External Information and Security Agency – A.I.S.E.) counterterrorism main task is instead to collect and analyze information (intelligence activities), to be provided (also in cooperation with similar agencies abroad) to law enforcement agencies, to ensure police investigations and assess priorities in countering the risks.

[10] "A colloquio con il Presidente del Comitato Analisi Strategica Antiterrorismo", *Gnosis – Rivista Italiana di Intelligence*, op. cit.

[11] "A colloquio con il Presidente del Comitato Analisi Strategica Antiterrorismo", *Gnosis – Rivista Italiana di Intelligence*, op. cit.

The financial Police is a specialized force, usually tasked by the National Anti-Mafia and Anti-Terrorism Prosecutor for the investigations on the subject of money laundering and terrorism financing[12].

Finally, the Penitentiary Administration Department is responsible for monitoring and investigating inmates charged or convicted with terrorist offences, as well as common criminals presumed at risk of violent radicalization[13].

As already highlighted, since its establishment the Committee evaluates alerts and ongoing investigations for potential terrorist threats. In time however, the fusion center competences evolved and adapted to the changing terrorist landscape, so that the C.A.S.A. can be currently considered both a strategic and a tactical tool in preventing and countering terrorism.

At the strategic level the Committee "*analyze and evaluate relevant information related to domestic and international terrorism*" in an international cooperation framework, providing the Political Authority with the significant elements required to evaluate the risk and originate directives. In a top-down model, it is through the C.A.S.A. that coordination in the investigative activities is fulfilled and good practices from other countries are discussed[14]. Moreover, the national level of terrorism alert is eventually set by the Minister of Interior through advice from the Committee after its comprehensive assessment of the situation[15].

At the tactical level, the weekly meetings allow data to flow during the evaluation over the ongoing investigations and intelligence activities. Bottom-up information from law enforcement and intelligence agencies concerning individuals believed to be at risk of violent radicalization, also provide the Minister of Interiors with the elements to evaluate the adoption of possible courses of action and limit the terrorist threat. An important caveat to this activity is the tool of deportation for reasons of State Security, frequently used to prevent the spreading of jihadist ideology; the level of radicalization

[12] Guardia di Finanza website, http://www.gdf.gov.it/chi-siamo/organizzazione/compiti-istituzionali/antiterrorismo.

[13] "Relazione al Parlamento sull'attività delle Forze di Polizia e sullo stato dell'ordine e della sicurezza e sulla criminalità organizzata", *Dipartimento dell'Amministrazione Penitenziaria*, ed.2013, pp.1304-1307, http://www.camera.it/_dati/leg17/lavori/documentiparlamentari/indiceetesti/038/002v02/00000038.pdf; "Sventati attentati grazie al lavoro di prevenzione in carcere della Polizia Penitenziaria", *Polizia Penitenziaria*, January 19, 2019, https://www.poliziapenitenziaria.it/sventati-attentati-grazie-alla-prevenzione-in-carcere-cosi-il-procuratore-nazionale-cafiero-de-raho.

[14] F. Roberti, L. Giannini, "Manuale dell'antiterrorismo", *Laurus Robuffo*, 2016, pp. 39-40.

[15] "Come funziona il Comitato Antiterrorismo", *Il Sole 24 ore*, August 19, 2017, http://www.ilsole24ore.com/art/notizie/2017-08-18/come-funziona-comitato-antiterrorismo-211636.shtml?uuid=AEs9moEC.

reached by monitored individuals is discussed during the C.A.S.A. meetings and proposals of deportation decrees are consequently examined[16].

Since 2014 the Committee also implemented a list of foreign terrorist fighters (Italian citizens, foreigners resident in Italy and Italian citizens residing elsewhere), mapping routes to and from fighting zones, facilitators and other relevant investigative information.

To highlight some figures and activities of the C.A.S.A., in 2017 the Committee (summoned in permanent session since September 2014) held fifty regular meetings and ten emergency reunions; 806 topics were examined, 420 alerts were evaluated and 105 deportation decrees were issued as a result of consultation in the Committee[17].

4. Conclusions

The "new" terrorist threat is fluid in its semblance, transnational, cybernetic and often tangentially linked to criminality. To counter such complex phenomenon, the Italian C.A.S.A. ensure a perfect synergy between all actors involved in fighting terrorism and perfectly represent the national security system culture originating from its previous experience with past domestic terrorism and organized crime groups[18]. The Committee features, as a strategic structure and as an operative body tasked with investigative and intelligence analysis, makes it a ductile, effective, non-bureaucratic tool, characterized by the rapidity in the acquisition, sharing and verification of the information, that enables better operational analysis and the exchange of actionable intelligence that the Minister of Interior could implement through local units on the territory. As a former Director of the Italian Intelligence stated, "*We learned a very harsh lesson during our domestic terrorism years; from that we understood how important is it to maintain a constant dialogue at the operational level between intelligence and law enforcement actors*"[19].

[16] 2018 Intelligence Agencies Annual Report to the Parliament, *Sistema di Informazione per la Sicurezza della Repubblica*, February 2018, p.86, https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-2018.html.

[17] Annual report to the Parliament, "Law enforcement agencies activities, National Security and Public Order situation and organized crime groups overview", *Ministry of Interior*, 2017, p.11, http://www.interno.gov.it/sites/default/files/relazione_al_parlamento_anno_2017_.pdf.

[18] M. Minniti, "Le minacce per l'intelligence" p.163, in "L'Italia e la minaccia jihadista. Quale politica estera?", *Istituto per gli Studi di Politica Internazionale - ISPI*, January 28, 2015, https://www.ispionline.it/it/EBook/L%27italia%20e%20la%20minaccia%20jihadista.pdf.

[19] S. Kirchgaessner, L. Tondo, "why has Italy been spared mass terror attacks in recent years?" *The Guardian*, June 23, 2017, https://www.theguardian.com/world/2017/jun/23/why-has-italy-been-spared-mass-terror-attacks-in-recent-years.

Due to the lower numbers of terrorism related events in Italy, there is just a generic perception of the C.A.S.A. in the public opinion, as the Committee is seldom mentioned as a counterterrorism synergic tool. Political and judiciary officials however, praise the structure as a virtuous model and counterterrorism analysts are well aware of its inherent value. The Committee evolution in its 15 years of existence reflect the growth of homegrown terrorism (the *leaderless jihad* phase), the Foreign Terrorist Fighters phenomenon, the resurgence of right wing extremism, and confirm the commitment to the prevention of terrorist related risks, highlighted by the extent of the information exchange held, regarding the entire spectrum of the jihadist declinations, be it current or potential[20].

References

"A colloquio con il Presidente del Comitato Analisi Strategica Antiterrorismo", Gnosis – Rivista Italiana di Intelligence, op. cit, 2010

Annual report to the Parliament, "Law enforcement agencies activities, National Security and Public Order situation and organized crime groups overview", Ministry of Interior, 2017, p.11, http://www.interno.gov.it/sites/default/files/relazione_al_parlamento_anno_2017_.pdf

"Come funziona il Comitato Antiterrorismo", Il Sole 24 ore, August 19, 2017, http://www.ilsole24ore.com/art/notizie/2017-08-18/come-funziona-comitato-antiterrorismo-211636.shtml?uuid=AEs9moEC

F. Roberti, L. Giannini, "Manuale dell'antiterrorismo", Laurus Robuffo, 2016

Guardia di Finanza website, http://www.gdf.gov.it/chi-siamo/organizzazione/compiti-istituzionali/antiterrorismo

Intelligence Agencies Annual Report to the Parliament, Sistema di Informazione per la Sicurezza della Repubblica, February 2018, p.86, https://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-2018.html

Lower Chamber Report on the activities of the Counterterrorism Strategic Analysis Committee, March 11th, 2015, http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/html/30/indag/c30_flussi/2015/03/11/indice_stenografico.0023.html

M. Minniti, "Le minacce per l'intelligence" in "L'Italia e la minaccia jihadista. Quale politica estera?", ISPI, 2015, https://www.ispionline.it/it/EBook/L%27italia%20e%20la%20minaccia%20jihadista.pdf

Ministry of Interior official website http://www.interno.gov.it/it/temi/sicurezza/antiterrorismo

Ministry of Interior press releases http://www.interno.gov.it/it/sala-stampa/comunicati-stampa/antiterrorismo-comitato-analisi-strategica-intensifica-misure-sicurez-

[20] 2018 Intelligence Agencies Annual Report to the Parliament, *Sistema di Informazione per la Sicurezza della Repubblica*, op. cit. p. 76.

za-e-vigilanza; http://www.interno.gov.it/it/sala-stampa/comunicati-stampa/comitato-analisi-strategica-antiterrorismo-dopo-i-tragici-fatti-manchester

"Money transfer illegali per finanziare la jihad: arrestati 14 fiancheggiatori", Il Sole 24 Ore, May 10, 2018, https://www.ilsole24ore.com/art/notizie/2018-05-10/terrorismo-arrestati-14-fiancheggiatori-formazioni-jihadiste-081156.shtml?uuid=AEGPd1lE

Parliamentary Annual report, XV Legislature (April 2006 - April 2008), pp.11-12, http://leg15.camera.it/_dati/leg15/lavori/documentiparlamentari/indiceetesti/033/001/00000001.pdf

"Relazione al Parlamento sull'attività delle Forze di Polizia e sullo stato dell'ordine e della sicurezza e sulla criminalità organizzata", Dipartimento dell'Amministrazione Penitenziaria, ed.2013, pp.1304-1307, http://www.camera.it/_dati/leg17/lavori/documentiparlamentari/indiceetesti/038/002v02/00000038.pdf

S. Kirchgaessner, L. Tondo, "why has Italy been spared mass terror attacks in recent years?" The Guardian, June 23, 2017, https://www.theguardian.com/world/2017/jun/23/why-has-italy-been-spared-mass-terror-attacks-in-recent-years

"Sventati attentati grazie al lavoro di prevenzione in carcere della Polizia Penitenziaria", Polizia Penitenziaria, January 19, 2019, https://www.poliziapenitenziaria.it/sventati-attentati-grazie-alla-prevenzione-in-carcere-cosi-il-procuratore-nazionale-cafiero-de-raho/

"Terrorista islamico arrestato dalla Polizia di Caserta. Era ricercato internazionale!, Caserta Web, March 1, 2019, https://casertaweb.com/notizie/terrorista-islamico-ricercato-internazionale-arrestato-dalla-polizia-caserta/

The decentralized finance-violent extremism nexus: ideologies, technical skills, strong and weak points

Daniele Barone

Nota autore

Daniele Barone is a researcher and an analyst in the security sector. Graduated in Marketing & Communication at IULM University, he has a master's degree in International Relations at ASERI Graduate School of Economics and International Relations – Catholic University of the Sacred Heart. He specialized in homeland security and counter-terrorism studies earning an Executive Certificate in Counter-Terrorism studies at the International Institute for Counter-Terrorism (ICT) – Herzliya.
He has worked, for more than five years, as a project manager and a digital marketing specialist in the private sector.
Given his experience in online communication, economics, and geopolitics, his research interests are related to cyber-jihad, terrorism financing, and terrorist groups' communication strategies.

Abstract

Il comune denominatore dell'utilizzo delle criptovalute da parte dei gruppi terroristici ha origine dall'inquadramento legale poco chiaro in cui le criptovalute attualmente operano. Tale contesto permette, seppur indirettamente, la proliferazione di una propaganda basta sul rifiuto dell'idea di Stato, descrivendo la gestione decentralizzata delle criptovalute come un mezzo di pagamento che appartiene esclusivamente al popolo e supera le interferenze prodotte dal controllo centralizzato del governo o di altri intermediari.
Concentrando l'analisi sulla giustificazione ideologica e gli opachi schemi di finanziamento messi in atto da organizzazioni terroristiche internazionali come Hamas, movimenti globali come i gruppi estremisti di estrema destra ed i loro simpatizzanti, poi descrivendo come piccoli gruppi mercenari jihadisti come il Malhama Tactical Team o campagne di donazione con scopi umanitari sospette stanno evolvendo le proprie competenze nei settori della comunicazione online e delle criptovalute, questa ricerca fornirà una visione sia generale che particolare degli attuali collegamenti terrorismo-FinTech. L'analisi spiegherà come, nonostante le competenze tecniche dei gruppi estremisti in questo settore sembrino essere ancora in fase embrionale, presentano imminenti prospettive di miglioramento, creando una diffusione a cascata di know-how e giustificazioni ideologiche e politiche. Queste caratteristiche del fenomeno possono generare un duplice risultato: trasformare il finanziamento al terrorismo in un'occasione senza precedenti per migliorare le tecniche investigative ed i metodi di analisi o, al contrario, rendere l'utilizzo per fini terroristici della finanza moderna un settore sempre più complesso da monitorare.

The common denominator in the exploitation of cryptocurrencies by terrorist groups, can be found in the grey legal framework where cryptocurrencies operate. This contest, even though indirectly, allows the diffusion of a propaganda related to the rejection of the idea of State, by depicting the decentralized control of cryptocurrencies as a mean of payment that belongs exclusively to the people, avoiding the interference of a centralized government control or any sort of middleman. Focusing on the analysis of the ideological justification and opaque financing patterns used by international organizations as Hamas, global movements as alt-right extremist groups and their sympathizers, then describing in depth how small jihadist private military contractors as the Malhama Tactical Team or suspicious online humanitarian crowdfunding campaigns are developing their skills both in the online communication and in the cryptocurrency field, this essay is aimed at providing an either overall or specific view of the current terrorism-FinTech nexus. It will explain how, even though extremist groups' skills in the cryptocurrency sector may seem at an infancy level, they are evolving very fast and creating a trickle-down diffusion of know-how and ideological or political justifications. These elements can generate a twofold outcome: turn terrorism financing into an unprecedented occasion to improve investigative and analysis methods or, on the other hand, turn exploitation of modern finance for terrorism purposes into a total undetectable sector.

Keywords

Jihad, Alt-right, Financing, Cryptocurrency, Cybercrime

Introduction

Between the end of 2018 and the first half of 2019, many extremist political or religious groups have exploited the anonymity of cryptocurrencies. In particular, small or structured international jihadist groups have been experimenting online financing methods to find alternative means to receive donations, while far-right extremist groups have been using them to store and invest money or organize international crowdfunding campaigns.

Besides these differences, the common denominator in terrorists exploitation of cryptocurrencies can be found in the grey legal framework where many areas of modern finance are currently operating, allowing the proliferation of factions promoting an extremist narrative related to the rejection of the idea of State, fuelled by displaying and encouraging the use of a mean of payment that belongs exclusively to the people, overlapping the interference of a centralized governmental control or middleman.

Furthermore, the need for extremist groups to spread their propaganda through the web is giving them more and more access to cutting-edge technical expertise. The two areas are linked by an ongoing innovation process of their ability aimed at evading detection, developing their technical capabilities and calling for donations in cryptocurrencies through legitimate services like social media or public websites, increasing the chances to freely interact with many actors involved in cybercrime or hacking at various levels.

Indeed, international extremist groups (both political and religious), activists, and sympathizers scattered across the globe are still adapting more and more to either the developments in the ICT sector as a physiological response to the territorial instability of their groups. From this lens, these violent organizations are not only taking advantage of online tools which are already mainstream as social media or end-to-end chats, but also evolving in using up-to-date and not yet widespread online products and services as cryptocurrencies, encryption keys, cybersecurity issues, and alternative web hosting services, which require a medium/high e-skills level. From this perspective, they are on the one hand transversally learning from their members or related groups (as, for instance, in the case of *Amaq News Agency* and alt-right groups, creating a ZeroNet account after *Cyber Caliphate* hacking group, *Ansar Al-Khilafah*, previously experimented it) on the other hand, teaching their audience how to use modern online tools to communicate, finance the organization, and access to violent contents in a climate of total anonymity through the web.

This paper will focus on the latest developments (2018/2019) of those either technical or ideological aspects which are likely to spread more and more the use of modern finance to raise money for violent extremist groups.

Focusing the analysis on the ideological justifications and financing patterns put into action by international organizations as Hamas or global movements as alt-right extremist groups, then describing in depth how small jihadist private military contractors as the Malhama Tactical Team or opaque online crowdfunding campaigns are developing their expertise both in the communication and in the cryptocurrency field, this essay is aimed at providing an either overall or specific view of the current terrorism-FinTech nexus. It will explain how, even though extremist groups' technical skills in the cryptocurrency sector may seem at an infancy level, they are still evolving fast and creating a trickle-down diffusion of skills and ideological justifications which may turn terrorism financing into a more and more undetectable sector.

1. Latest technical developments in the illegal exploitation of cryptocurrencies: Europol IOCTA 2018

The latest report of Europol on Internet Organized Cyber Crime (IOCTA 2018)[1] discusses, among other issues, the weak points that modern financial

[1] Europol (2018) I*nternet Organised Crime Threat Assessment (IOCTA) 2018*. European Union Agency for Law Enforcement Cooperation. Available at https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

tools and a lack of either an up-to-date legal framework or cooperation among institutions and the private sector, brings to the cybercrime field.

The report highlights many sectors which are likely to become a target for criminal and terrorist purposes and depicts the latest development in the misuse of cryptocurrencies at different levels: Cybercrime in general (petty or organized crime) - Jihadist networks (local or international) - modern cyber-threats cryptocurrency related.

According to IOCTA 2018, even though Bitcoin has lost its majority of the overall cryptocurrency market share (Bitcoin enjoyed over 80% of the cryptocurrency market share, but by the start of 2017 this had dropped to less than 35%), it still remains the primary cryptocurrency encountered by law enforcement.

In particular, Bitcoin is still the most widely used cryptocurrency on **Darknet illegal markets**. According to Europol, even though law enforcement has taken down three major Darknet markets (i.e. AlphaBay, Hansa, and RAMP), it is reported a significant growth in both the number of small vendor shops (shops run by a single vendor) and secondary markets (i.e. non-English language markets) dedicated to a particular nationality or language group.

Nevertheless, nowadays Bitcoin is not anymore able to provide as much anonymity as it did in the past. As demonstrated by Philip and Diana Koshy in 2014, which were able to identify the IP addresses connected to more than 1000 Bitcoin addresses[2], it is possible to find a breach in the wall of the partially anonymous Bitcoin transactions flow.[3] Moreover, law enforcement has already proved to be able to track down and reveal Bitcoin **mixing services** (i.e. protect the anonymity of transactions by mixing many users' Bitcoin reserves with each other) used by criminals to launder money.

Furthermore, Bitcoin is developed with the Blockchain technology where data flow between computers (called "nodes") like gossip in a crowd, becoming immutable and unchangeably bound with each other. In this term, even though Blockchain is structured in order to protect users' real identity behind encryption codes, it also allows making public information (and public record) of their entire financial history[4]. Hence, from an investigative and monitoring perspective, get only once a criminal committing a crime by using Bitcoins, allows to uncover his whole criminal history.

[2] P. Koshy D. Koshy P. McDaniel (2014) *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. Pennsylvania State University, University Park, PA 16802, USA. Available at https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf.

[3] J. Bohannon (March 9, 2016) Why criminals can't hide behind Bitcoin. ScienceMag. Available at http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

[4] K. Marinos (March 23, 2016) *Are Bitcoin Transactions Traceable?*. CoinTelegraph. Available at https://cointelegraph.com/news/are-bitcoin-transactions-traceable.

This is likely to cause a significant shift of cybercriminals to more privacy-centric types of cryptocurrencies in the very near future[5].

1.1 Every internet user is unwittingly becoming a victim: Cryptojacking, a hallmark for modern cybercrime

Cryptojacking is the unauthorized use of a computer, tablet, mobile phone, or connected home devices by cybercriminals to mine for cryptocurrency.

There are only a finite number of Bitcoins that have not been completely mined and they can be mined only by solving a complex and ever-growing math task "**proof of work",** which requires elevated electricity bills and expensive computer equipment. Thus, the more devices are working, the faster is possible to mine coins, and cryptojacking allows cybercriminals to use other people's devices to pursue this task. Cryptojacking can occur in two ways:

- **Phishing tactics**, running a code that downloads the cryptomining script on the victims' computer, the most common method is to send the malware by email.
- **In-browser miner**, injecting a cryptomining script on a website or on an online advertisement that is placed on multiple websites. The script runs on the visited website, so the code does not need to be installed or the user doesn't even have to opt-in[6].

In both cases, the code solves complex mathematical problems and sends the results to the hacker's server while the victim is completely unaware.[7]

In-browser based cryptojacking **is not illegal**, thus it is more appealing to cybercriminals wishing to keep a low profile, requiring little or no victim engagement and, at least currently, minimal law enforcement attention.

Hence, for all these reasons, cryptojacking is expected to become a regular, low-risk revenue resource for cybercriminals.

1.2 Cyber-attacks targeting users and facilitators

Quoting Europol IOCTA 2018 "in a trend mirroring attacks on banks and their customers, cryptocurrency users and facilitators have become victims of cybercrimes themselves... Money launderers have evolved to use cryptocur-

[5] O. Kharif (January 2, 2018) *The Criminal Underworld Is Dropping Bitcoin for Another Currency*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

[6] https://hackerbits.com/programming/what-is-cryptojacking.

[7] https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html.

rencies in their operations and are increasingly facilitated by new developments such as decentralized exchanges which allow exchanges without any Know Your Customer requirements".

Indeed, a consequence of the decentralized and unregulated system of cryptocurrencies and the fact that they are becoming more mainstream (almost **1600 listed cryptocurrencies**), is that cryptocurrency users, exchange platforms and mining services are now subjected to the same attacks aimed at traditional financial instruments.

The most commons kinds of cyber-attacks and targets are the following:

- Phishing tactics aimed at taking over users' **login credentials for their online exchanger accounts, electronic wallets, and private keys.**
- **Exchange services**, which hold their own number of cryptocurrencies for trading and the fund of their customers who purchased cryptocurrencies, are key targets for cybercriminals given the huge amount of money that they administrate ore store for their customers. As the hacking attack to the Italian exchanger **BitGrail** that resulted in the correspondent loss of USD 195.000.000.
- Attack to cryptocurrency exchange services to **steal customers' data to further fraud** as, for instance, "phishing customers for their account login credentials and subsequent currency theft".

1.3 Jihadist networks experiment

The Europol 2018 report defines Islamic terrorists' cyber attack expertise as at its infancy level. It describes Islamic terrorist groups as very high-skilled in terms of online propaganda through the masterly use of social media, surface or deep web forums or blogs, and end-to-end encrypted chat services, but still without an elevated overall harmful cybercrime potential. Nevertheless, IOCTA 2018 shows some interesting trends, about terrorist groups' cutting-edge technical expertise in the use of cryptocurrencies, which are worth explaining.

- **A few actors with high-degree technical know-how**: as already analysed by ITSTIME[8], since 2012 there have been a few cases related to terrorist groups' use of cryptocurrencies, mostly under the form of either more or less explicit online crowdfunding campaigns. The Europol report rightly defines this initial phase as the "Jihadist networks experiment with cryptocurrencies". During this experimental stage, a

[8] http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone.

common denominator can be identified in the difficulty to track terrorists' transaction movements.

– **Privacy-centric cryptocurrencies**: as previously explained, Bitcoin is not the most anonymous choice in the cryptocurrency landscape. There already exist other types of cryptocurrency created with the primary purpose of protecting users' privacy. The most popular are Monero (launched in 2013) and Zcash (launched in 2016). Monero and Zcash respectively use *CryptoNote protocol*, which allows seeing only an approximate amount of money that was sent in the transaction,[9] and *Zk-Snark*, "Zero-knowledge", which allows one party to prove to another that a statement is true, without revealing any other information beyond the validity of the statement itself[10]. The competition among these privacy-centric cryptocurrencies is causing a fast-paced development entirely aimed at increasing their users' privacy[11] while becoming more and more user-friendly and widespread[12]. As in the *Akhbar alMuslimin case*, Islamic Terrorist groups have already proved to have a high degree of sophistication in exploiting modern methods to obscure their illicit funding. In fact, Europol has noticed that Daesh requested donations in Zcash and also used such cryptocurrency to purchase website domains. Even though Europol underlines that there is no proof of Zcash, or any other type of cryptocurrency, being used to finance any attacks on European soil, the development in this field deserves to be carefully monitored.

The evolution in the field of online terrorism financing previously described, may be reassumed by the latest development regarding the pro-Daesh renewed deep web crowdfunding campaign, **Akhbar al-Muslimin (Muslim news)**, an IS-affiliated website which published news from the Islamic State. In November 2017, one month after the fall of Raqqa, a banner for donations of Bitcoins was launched on the website. In particular, it posted a link for Bitcoin donations claiming, "Click here to donate Bitcoins to the (*Akhbar al-Muslimin*) website – do not donate from *zakāt*[13] funds". The donations are presented as a support for the web-

[9] https://www.worldcryptoindex.com/what-is-cryptonote-technology.

[10] https://z.cash/technology/zksnarks.

[11] E. Spagnuolo (April 26, 2017) Addio Bitcoin, nel deep web ora si paga con Monero e Zcash. Wired - Italia. https://www.wired.it/economia/finanza/2017/04/26/bitcoin-monero-zcash.

[12] D. Manheim, P.B. Johnston, J. Baron, C. Dion-Schwarz (April 21, 2017) *Are Terrorists Using Cryptocurrencies?* RAND Corporation. Available at https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html.

[13] An Arabic word referring to a payment made annually under Islamic law on certain kinds of property and used for charitable and religious purposes, one of the Five Pillars of Islam. The

site, but may probably have been used by Daesh to restore its propaganda machine or fund terrorist attacks abroad[14]. The bitcoin address had no time to receive any donation because of two reasons: it was shut down after a while by authorities. Thus, it had no protection against Distributed Denial of Service attacks (DDoS) and only a bitcoin address to send donations, with no instructions or explanations available for users who were willing to donate to the website.

After the more consistent defeat of Daesh in Syria, on January 2019[15], the website reappeared online with a new bitcoin address. What is new is that, once the site has been accessed, now almost every page contains a request for a donation for "the activities of the website" that leads to the address of a virtual wallet for depositing the funds[16].

Furthermore, there are some new features added by the creators of the renewed website that give some interesting clues about an improved knowledge on how to facilitate the donation process:

- Because of the frequent closing of the *Akhbar al-Muslimin* website, the first window contains instructions for **finding the site's most updated links**: by sending an empty email to the address given, the user is automatically answered with an updated link to a mirror site of *Akhbar al-Muslimin*.
- There are more instructions available about how to exchange money into bitcoin with a link to explanatory videos about how cryptocurrencies work and to the designated exchange service platforms. On the first renewed version (January 2019) the exchange service used was VirWoX, a virtual currency trading company that allows buying **bitcoin via PayPal**[17]. Since March 9, 2019, the site referred potential donors to LocalBitcoins[18], a virtual currency money trading company where, to buy bitcoins, **providing identification is voluntary**.

word *zakāt* origins comes from Persian and Kurdu languages, meaning "almsgiving".

[14] D.M. Barone (2018) *Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism*. Sicurezza Terrorismo e Società. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

[15] (February 12, 2019) *Drive for donations using Bitcoin on an ISIS affiliated website*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/02/E_018_19.pdf.

[16] (March 7, 2019) *Funding Terrorism: ISIS raises funds through an affiliated website, using bitcoins*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/03/E_054_19.pdf.

[17] https://www.virwox.com/help.php.

[18] https://localbitcoins.com/faq.

1.4 Suggested Improvements

This year's happenings in the online extremist groups financing field are providing new strong and weak points related to the illegal use of cryptocurrencies along with scope for improvement.

- **Improve Public Awareness**: Cryptocurrencies are becoming widespread, user-friendly and, in many cases, developing through a privacy-centric protocol, while institutions have not yet enough tools to properly investigate or prevent their illegal use. Help investors to avoid becoming unknowing victims of criminal or terrorist networks is fundamental. Institutions should put more efforts in giving clear instructions to these modern customers aimed at avoiding credential or private keys theft and guide them through a conscious way to invest in cryptocurrencies.
- **Introduce mandatory KYC procedures:** even though in many cases governments can't impose strict rules on cryptocurrency development companies or cooperate with them, it is still possible to cooperate with exchange services. Obligatory Know Your Customer procedures for exchange services or crypto debit/credit cards providers, would definitely help to prevent jihadists' donation campaigns or criminal frauds.
- **An updated legal framework:** many frauds or theft committed in the cryptocurrency field can't even be prosecuted. A flexible legal framework updated to modern financial threats is crucial to isolate the dangers in this field and let either investors or prosecutors' freedom of movement inside a clearly legal environment. Furthermore, this would be a strong deterrence for many individuals planning to commit financial cybercrimes.

2. Structured and International jihadist groups: Hamas crowdfunding bitcoin

On January 29, 2019, Abu Obeida, the spokesman for *Izz ad-Din al-Qassam*, the armed wing of the Hamas, announced that the group is now accepting donations in bitcoin[19]. An attempt to get around international restrictions on funding the organization, by circumventing the banking system and international anti-money laundering (AML) measures.

Originating in 1987 after the beginning of the first Intifada as a spinoff of Egypt's Muslim Brotherhood, and funded on the long-term goal of establish-

[19] M. Arnold, S.A. Ramadan (January 30, 2018) *Hamas Calls on Supporters to Donate to Group in Bitcoin*. Bloomberg. https://www.bloomberg.com/news/articles/2019-01-30/hamas-calls-on-supporters-to-donate-to-group-in-bitcoin.

ing strong Islamic states on all Palestinian territories by declaring war to Israel[20], Hamas (*Ḥarakat al-Muqāwamah al-'Islāmiyyah*)[21] is the Islamist group that for eleven years has ruled the Gaza Strip.

Perceptions of the group differ: Israel, US[22], Canada, EU, Japan, Egypt, among others[23], say it's a terrorist group that poses a grave obstacle to peace between Israelis and Palestinians, others argue it is a true representative of Palestinians[24] that won credibility with its grassroots charitable work and for being less corrupt than its rival, the Fatah faction of Palestinian Authority, which was Israel's partner in peace talks[25].

2.1 The group's Economic Resources

Hamas raises money prevalently from taxes (e.g. cigarettes, auto registration fees, goods coming from Israel[26]) and also regulates many types of businesses (e.g. street vendors, money-changing companies) requiring them to pay license fees. Hamas has also control over various Gaza resources, such as leasing government-owned heavy machinery to private contractors for a daily fee (one of many ways the group has been able to indirectly benefit from the international reconstruction funds flowing into Gaza).

Nevertheless, most of the group's economic resources come from donations either from activists/sympathizers[27] or from some Arab States sponsor-

[20] M. Levitt, D. Ross (2007) *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*. Yale University Press.

[21] Hamas Covenant (1988) Yale Law School - Lillian Goldman Law Library. http://avalon.law.yale.edu/20th_century/hamas.asp.

[22] https://www.state.gov/j/ct/rls/other/des/123085.htm.

[23] Profile: Hamas Palestinian Movement (May 12, 2017) BBC. https://www.bbc.com/news/world-middle-east-13331522.

[24] J. Khoury (June 10, 2017) For Arab World, Hamas Is 'Legitimate Resistance Movement,' Not Terror Group, Qatar Says. Haaretz. https://www.haaretz.com/middle-east-news/palestinians/qatar-hamas-is-legitimate-resistance-movement-1.5482546.

[25] J. Ferziger (November 14, 2018) Hamas. Bloomberg. https://www.bloomberg.com/quicktake/hamas

[26] *"Hamas also takes a hefty cut from the Egyptian tunnel trade, imposing high "customs" duties and a daily fee on local tunnel contractors. Such trade has been dramatically reduced since June 2010, when Israel quadrupled the number of trucks permitted to bring goods to Gaza through legal terminals. To replace lost tunnel income, Hamas is reportedly taking advantage of the relative drop in prices on goods arriving via official Israeli channels, imposing new taxes on various items. For example, from early July to September 20, 2010, the group barred the importation of new cars from Israel until the taxation issues were resolved."* E. Year, E. Ofer (January 6, 2011) *Gaza's Economy: How Hamas Stays in Power*. The Washington Institute. https://www.washingtoninstitute.org/policy-analysis/view/gazas-economy-how-hamas-stays-in-power.

[27] E. Year, E. Ofer (January 6, 2011) *Gaza's Economy: How Hamas Stays in Power*. The Washington Institute. https://www.washingtoninstitute.org/policy-analysis/view/gazas-econo-

ships and private wealthy benefactors[28]as, for example: funding, weapons, and training from Iran[29]; donations from the Palestinian global diaspora; fundraising (and propaganda) activities in Western Europe and North America through global charities[30] affiliated with Hamas, which collect donations on its behalf.[31]

2.2 Hamas is calling for Bitcoin donations: the rules have changed

In economic terms, Hamas is finding itself pushed to the limit, facing unprecedented financial isolation due to banking bans against the Gaza Strip by Israel and the United States, while Iran is having financial trouble due to US sanctions. Even though Israel has allowed a $15 million monthly transfer from Qatar to the Gaza Strip in the framework of new understandings reached by Israel, Egypt, and Hamas, the terrorist group is still searching for more money to fund its activities[32].

Between these events, Abu Obeida calls for bitcoin donations to support Hamas.

Basing on the documented cases of jihadists' use of cryptocurrencies[33], in less than a week after making its e-wallet address, Hamas Bitcoin donation campaign has brought a radical change in this field.

The primary element able to turn cryptocurrencies from an experimental to a consolidated terrorism financing method, is an "institutional" approval coming from influent jihadist actors (e.g. extremist Islamic scholar or leaders of an international terrorist organization).

my-how- hamas-stays-in-power.

[28] BUREAU OF COUNTERTERRORISM AND COUNTERING VIOLENT EXTREMISM (2016) *Country Reports on Terrorism*. US Department of State. https://www.state.gov/j/ct/rls/crt/2016/272235.htm.

[29] Country Reports on Terrorism (2008) U.S. Department of State. https://www.state.gov/j/ct/rls/crt/2007/103714.htm.

[30] (October 4, 2012) *Treasury Sanctions Two Hamas-Controlled Charities*. U.S. Department of Treasury. https://www.treasury.gov/press-center/press-releases/pages/tg1725.aspx.

[31] Report - Hamas. Counter Extremism Project. https://www.counterextremism.com/threat/hamas.

[32] R. Katsiri (February 3, 2019) *Hamas raises bitcoin donations via US crypto exchange*. Globes. https://en.globes.co.il/en/article-hamas-raises-bitcoin-donations-via-us-crypto-exchange-1001271661.

[33] D.M. Barone (2018) *Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism*. Sicurezza Terrorismo e Società. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

Before Hamas call for bitcoin donations, in those cases documented since 2012, terrorism financing experiments through cryptocurrencies have always been conducted from activists at various levels or small groups but never directly from an international Islamic terrorist organization[34]. Indeed, the most relevant connections between cryptocurrency and an international terrorist organization are related only to a few cases, as the 4th issue released on October 2018 of al-Haqiqa magazine (an English-language magazine pro-al-Qaeda jihadists in Syria) asking for donations via either bitcoin or traditional currencies[35] or in the *Akhbar al-Muslimin* website, which used to publish news about Daesh, that launched an online fundraising campaign in November 2017 encouraging donations through Bitcoin[36]. Even though these two cases (as a very small number of other cases) seem to be strictly related to Daesh or al-Qaeda, none of their leaders has ever publicly encouraged the use of cryptocurrencies.

From this perspective, Hamas bitcoin donation campaign is already bringing to light some relevant elements of analysis.

The number of donations has highly increased: Hamas military wing issued via Telegram a request to donate to the organization by using Bitcoin. On January 31, 2019, it published a first virtual wallet address and a second one on February 2[37]. The bitcoin addresses provided by Hamas, to date, have already totally received 77 donations for the equivalent of $3.477,85.

It is relevant that, in the same day, also *Al-Nasser Salah al-Deen Brigades*, the military wing of the Popular Resistance Committees (a coalition of various armed Palestinian factions active since 2001 in the Gaza Strip, opposing to the conciliatory approach adopted by the Palestinian Authority and Fatah towards Israel)[38] used its Twitter account to call on the public to donate via bitcoin and

[34] D.M. Barone (October 22, 2018) Europol – Internet Organized Cyber Crime Threat Assessment 2018: new trends in the obscure sides of FinTech. ITSTIME. http://www.itstime.it/w/europol-internet-organized-cyber-crime-threat-assessment-2018-new-trends-in-the-obscure-sides-of-fintech-by-daniele-maria-barone.

[35] (October 15, 2018) 4th issue of al-Haqiqa magazine. Site Intel Group. https://ent.siteintelgroup.com/Western-Jihadists/4th-issue-of-al-haqiqa-magazine-features-interview-with-ttp-commander-promotes-password-security-and-bitcoin-donations.html.

[36] (December 6, 2017) Drive for Bitcoin Donations on an ISIS-affiliated website. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website.

[37] (February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

[38] Popular Resistance Committees - Palestine. TRAC. https://www.trackingterrorism.org/group/popular-resistance-committees-palestine.

share a link of a private Telegram account in order to give assistance or explanations. The call read: "*For those who love jihad and the resistance in occupied Palestine, you can send donations through Bitcoin.*" The address shows that the group is receiving bitcoin donations since 2015 almost on a daily basis (4170 transactions) for a total amount of 863.49824685 BTC, almost $3millions.

It has to be taken into account that the Popular Resistance Committees are strong allies of Hamas and Islamic Jihad[39], meaning that the terrorist organizations may have agreed in choosing the crypto-way (with a fair degree of success) to receive donations or launder money since more than 3 years ago and that only now, given the strict sanctions against Hamas, they've been forced to go public.

There's not a Lack of technical skills: the research conducted by the Israeli blockchain intelligence startup Whitestream shows some sophisticated procedures in the donation process to the Hamas bitcoin address. Some donations come from US cryptocurrency exchange Coinbase and US trading platform Bittrex, other are connected to the Chinese cryptocurrencies exchange Binance, to a Russian cryptocurrency exchange Vilkov, and to CoinPayments, a company registered in the Cayman Islands. Furthermore, the US exchange platform Coinbase is only available in US, Canada, Australia, Singapore, and 38 European countries, but is not available in Palestine, and Israel, showing that donations are not coming only from local activists but are likely to come from Western sympathizers.

Moreover, in some cases an efficient method of money laundering has been used to transfer Bitcoin to Hamas, through coinMixer.io mixing service, a technology able to mix different addresses of digital currencies, thereby making it difficult to identify their users[40].

Then, while many of the addresses involved in the bitcoin donations to Hamas are holding a small amount of Bitcoin, others are coming from wealthy donors.

2.3 Positive and negative aspects in the near future scenario

Further developments are likely to come soon in this field. The call for donations in bitcoin made by Hamas could be the beginning of a consolidated trend in terrorism financing or an occasion to improve prosecution and investigation methods of this crime.

[39] Mapping Palestinian Politics - Popular Resistance Committees (PRC). ECFR. https://www.ecfr.eu/mapping_palestinian_politics/detail/popular_resistance_committees.

[40] R. Katsiri (February 3, 2019) *Hamas raises bitcoin donations via US crypto exchange.* Globes. https://en.globes.co.il/en/article-hamas-raises-bitcoin-donations-via-us-crypto-exchange-1001271661.

From this analysis, it is possible to highlight either negative or positive aspects.

On the one hand, due to the anonymity provided by cryptocurrencies, terrorists are now freely calling for donations. Indeed, even though exchange platforms ban their bitcoin address, it is still possible for them to create a new one in a few minutes and keep on receiving donations. Terrorist groups and their affiliates can make public donation requests by exploiting social media or encrypted chats, reinforcing their cultural sense of community among their supporters while circumventing the conventional banking system.

On the other hand, maybe Hamas is still able to explicitly make calls for donation in bitcoin due to the fact that its goal is prevalently political and not only religious or ideological. But for other Islamic terrorist groups' leaders (as in the case of al-Qaeda or Daesh) explicit public call for cryptocurrencies could still be a risky move. There's not yet a broadly shared Islamic religious justification to consider mainstream virtual currencies (as Bitcoin, Zcasch or Monero) as a Sharia-compliant mean of payment: Islamic scholars are still considering cryptocurrencies as gambling due to their high price volatility. In these terms, their exploitation for jihadist purposes is not fully justified by the whole Islamic community, and their use could be leverage for de-radicalization and counter-narratives able to expose their economic and geopolitical "holy war".

3. Rejecting government and banking control: alt-right extremist groups, ethno-nationalism, and anarcho-capitalism

As explained by the Christchurch shooter in his manifesto, the rejection of paying taxes is defined in right extremism narrative as "*a sign of racial loyalty*". From this perspective, circumventing the tax system is depicted as a way to sustain the ethno-nationalist cause: a fight for a nation which is defined in terms of assumed blood ties and ethnicity.[41]

Indeed, before the Christchurch shooting, back in 2017, Tarrant seems to have adopted alternative methods to raise money[42], proving that, in practical terms, according to his ideology, avoid taxes to fight for his own ethnicity and

[41] UN Human Rights Office of the High Commissioner (July 2018) *Ethno-nationalism denies millions their citizenship rights - anti-racism expert*. https://www.ohchr.org/EN/NewsEvents/Pages/EthnoNationalismDeniesTheirCitizenshipRights.aspx.

[42] B. Kaye T. Allard (April 4, 2019) *New clues emerge of accused New Zealand gunman Tarrant's ties to far right groups*. Reuters. https://uk.reuters.com/article/uk-newzealand-shooting-australia-extremi/new-clues-emerge-of-accused-new-zealand-gunman-tarrants-ties-to-far-right-groups-idUKKCN1RG093.

oppose to present policies, can legitimize the exploitation of cryptocurrencies and, in some cases, defraud other people.

Even though the references throughout his manifesto indicate that he was mostly immersed in white nationalist internet forums[43], it is important to understand that, through his extremist angle, it is possible to draw a pattern of how white supremacist narrative can change the way people perceive the world around them causing an infinite number of possible outcomes. Violent acts, exploitation of unregulated financing systems, scams.

It is fundamental to take a step back in order to explain and understand the nexus between his views, ethno-nationalism, and the exploitation of anonymous and alternative economic resources.

3.1 The extremist and illicit side effects of defending ethnicity by mocking patriotism

A key part of the extremist ideology expressed on Tarrant's manifesto is related to the increasing and irreversible weakening of white people that, according to him, is caused by unjustified welfarism of governments towards foreign cultures. From this perspective, the incapacity of politicians of protecting average hardworking white people from economic and cultural threats posed, in particular, by immigrants and ethnic minorities[44], is causing a sort of "white genocide".

This point of view is the result of a political line of thought that is growing across Western countries,[45] which is shifting states border control or clash of civilizations from an issue related to State security to a matter of personal security, turning white people into victims or directly responsible for the loss of control over the perceived irreversible and spreading disappearance of white people's national identities[46].

[43] D. Kirkpatrick (March 15, 2019) *Massacre Suspect Traveled the World but Lived on the Internet*. The New York Times. https://www.nytimes.com/2019/03/15/world/asia/new-zealand-shooting-brenton-tarrant.html.

[44] Counter Extremism Project (2018) *European Ethno-Nationalist and White Supremacy Groups*. https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/European_Ethno-Nationalist_and_White_Supremacy_Groups_081618.pdf.

[45] A. Shalal (June 24, 2018) *Migration fight erodes support for German conservatives, far-right AfD gains*. Reuters. https://www.reuters.com/article/us-germany-politics/migration-fight-erodes-support-for-german-conservatives-far-right-afd-gains-idUSKBN1JK0HV.

[46] The Economist (March 21, 2019) *Why white nationalist terrorism is a global threat*. https://www.economist.com/international/2019/03/21/why-white-nationalist-terrorism-is-a-global-threat.

Indeed, as explained by the sociologist and anthropologist Anthony D. Smith: **ethno-nationalism, is a devotion to the ethnically defined nation**, as opposed to patriotism that invokes allegiance to the territorial state.[47]

Indeed, ethno-nationalism can be merged and fuelled with a widespread sentiment of individual responsibility or victimhood towards the perception of a lack of security, subsequently causing a feeling of an imminent call-to-action against the oppressing cultures. This feeling of individual responsibility is founded on the libertarian concept of **self-interest** (either in terms of ethnicity/heritage or in terms of private property) which, taken in absolute terms, can't really provide instructive rule of thought simply because, according to this principle, each person is free to achieve in any possible way what is in their best interest. It incites people to fight for their right to "be free to exercise complete control over their own person and property"[48] thus, even discriminating or fighting against foreign cultures can be interpreted as an essential right of any property owner.

3.2 A Decentralized currency for a Decentralized order

Then, the exacerbation of the idea of a nation founded exclusively on blood-ties and cultural heritage is able to depict current governments and politicians which are not able to provide any support to defend their people from foreigners physical and cultural assault, as useless bureaucrats, liars, and enemies.

As a consequence, the tax system and banking system become an unforgivable fraud against white people.

This vision of night-watchmen State (that should serve people only by defending them in the age of crisis)[49] whose alleged legal framework recognizes sovereignty of the individual, rejects the idea of a centralized state encompassing the political philosophy of **anarcho-capitalism** by embracing the utopia of establishing a free market: self-ownership, private property and free markets at the very basis of a society able to self-regulate and civilize through the spontaneous and organic discipline of the free market. Decentralize and privatize law enforcement, courts and all other security services which would

[47] A.D. Smith (2009) Ethno-symbolism and nationalism. Routledge (108-109).

[48] J. Ganz (September 19, 2017) Libertarians have more in common with the alt-right than they want you to think. The Washington Post. https://www.washingtonpost.com/news/posteverything/wp/2017/09/19/libertarians-have-more-in-common-with-the-alt-right-than-they-want-you-to-think/?utm_term=.1d9d3ac77b22.

[49] G. Iggers (1970) *The Cult of Authority: The Political Philosophy of the Saint-Simonians.* The Hauge Martinus Nijhoff (73-75).

be selected by consumers rather than centrally controlled by a government through confiscatory taxation[50].

Against this backdrop, Richard Spencer in 2017 claimed on his Twitter profile that "*Bitcoin is the currency of the alt-right*". Decentralized, anonymous (even though governments are increasing monitoring procedures on cryptocurrency transfers)[51], and detached from the banking and tax systems, many of the members and representatives of alt-right and neo-nazi groups[52] were early adopters and many of them cashed in as the currency's valuation rose in 2017[53]. With all the data collected so far, it is a truism that extremist white supremacist groups have understood how to capitalize on the exponential rise in the value of cryptocurrencies.[54]

As in the case of **Corey D. Wilson**, who gained notoriety for promoting the spread 3D printed guns, funding Hatreon, a website that allowed neo-Nazis, white nationalists, and other extremist figures to solicit crowdfunding online, and for being named by Wired magazine[55] one of the 15 most dangerous people in the world,[56] who recently emptied his personal cryptocurrency accounts and one related to his business, Defense Distributed, totaling almost $1million[57].

[50] H. Binswanger (January 24, 2014) *Sorry Libertarian Anarchists, Capitalism Requires Government*. Forbes. https://www.forbes.com/sites/harrybinswanger/2014/01/24/sorry-libertarian-anarchists-capitalism-requires-government-2/#6cb1ad7c7d89.

[51] S. Chandler (October 07, 2018) Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It. CoinTelegraph. https://cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it.

[52] M. Bell (December 19, 2016) Meet the identitarians, Europe's 'new right'. PRI Public Radio International. https://www.pri.org/stories/2016-12-19/meet-identitarians-europes-new-right.

[53] SPLC Southern Poverty Law Center. https://www.splcenter.org/bitcoin-and-alt-right.

[54] J. Ebner (January 24, 2018) The currency of the far-right: why neo-Nazis love bitcoin. The Guardian. https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies.

[55] Wired magazine (December 19, 2012) *The 15 most dangerous people in the world*. https://www.wired.com/2012/12/most-dangerous-people.

[56] L. Beckett (September 19, 2018) *Gun rights activist Cody Wilson charged with sexual assault of teen*. The Guardian. https://www.theguardian.com/us-news/2018/sep/19/cody-wilson-3d-guns-sexual-assault-texas.

[57] Hatewatch Staff (September 20, 2018) *Notorious crypto-anarchist and antigovernment extremist Cody Rutledge Wilson left the country on a flight to Taiwan after he was alerted of an impending investigation against him for his alleged sexual assault of a minor.* SPLC Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2018/09/20/cody-wilson-lam-1-million-bitcoin.

3.3 Not only politics and philosophy but a head for business and popularity

The use of cryptocurrencies by far-right and neo-nazi groups is not at all only related to ideologies rooted in free-market, and aversion to the political establishment.

Indeed, far-right groups became more and more interested in bitcoin as its members were **cut off from more conventional payment channels**[58]: online payment services Paypal and Apple Pay stopped transactions and froze accounts belonging to organizations and right-wing extremist activists[59].

For instance, in 2017 the Austrian Identitarian Movement, Identitäre Bewegung Österreichs (IBÖ) which is part of a larger far-right Identitarian movement with branches in most Western European countries, North America and New Zealand (the group was calling for "Remigration" for European citizens with migrants background or non-white skin, spreading fear of a great replacement a few days after Christchurch shooting[60]) and their most famous leader, Martin Sellner (who counts over 90,000 YouTube subscribers and 16,000 followers on Telegram), have increasingly been campaigning for bitcoin donations.

Furthermore, recent investigations have led Austrian police to claim that Martin Sellner, received the equivalent of €1.500 donation in bitcoin from someone whose name was Tarrant[61].

Indeed, back to Tarrant's manifesto, he explains that he worked for a short time before making some money investing in BitConnect, an open-source cryptocurrency and a peer-to-peer payment protocol.

If it was true, he didn't raise money by investing in cryptocurrencies, but by defrauding other people by becoming part of a Ponzi scheme (an illegal scam in which belief in the success of a non-existent enterprise is fostered by the payment of quick returns to the first investors from money invested by lat-

[58] D. Gerard (March 19, 2019) *Neo-Nazis Bet Big on Bitcoin (And Lost)*. Foreign Policy. https://foreignpolicy.com/2019/03/19/neo-nazis-banked-on-bitcoin-cryptocurrency-farright-christchurch.

[59] M. Steinau (January 11, 2018) *How neo-Nazis and right-wing extremists profit from bitcoin*. Business Insider. https://www.businessinsider.com/neo-nazis-and-right-wing-extremists-profit-from-the-bitcoin-hype-2018-1?IR=T.

[60] J. Ebner (April 4, 2019) *Who are Europe's far-right identitarians?*. Politico. https://www.politico.eu/article/who-are-europe-far-right-identitarians-austria-generation-identity-martin-sellner.

[61] J. Wilson (March 28, 2019) *With links to the Christchurch attacker, what is the Identitarian Movement?* The Guardian. https://www.theguardian.com/world/2019/mar/28/with-links-to-the-christchurch-attacker-what-is-the-identitarian-movement.

er investors) that has been exposed in early 2018[62]. In fact, BitConnect was a fraudulent cryptocurrency that at its height in 2017 was worth approximately $2.5 billion but that after a chain of events that started with state securities regulators sending cease-and-desist letters to the company for fraud, led to the end of the project and a totally worthless cryptocurrency[63].

3.4 Connecting the dots

According to the elements that have been documented so far there are three main aspects that can be highlighted and accurately be monitored:

- As highlighted in the case of Hamas, bitcoin still allows to detect and gather clear information about any transactions and all e-wallet connected to any suspicious donation (as happened with the suspects of Tarrant's donation to IBÖ). On the other hand, there are many other cryptocurrencies, as Monero or Zcasch, which are competing more and more on providing the most privacy-centric product, becoming digital-currencies barely traceable.
- Extremist far-right movements are trying to push their communication efforts towards a target represented by young millennials, which are usually already cyber-literate and able to master new technologies very fast. In this context, introduce brand new privacy-centric cryptocurrencies to donate money could be a very easy and quick process.
- As in the case of BitConnect, cryptocurrencies, being uncontrolled nor regulated by any sort of institution or authority, represent a fertile ground for scammers. The idea of pursuing self-interest by circumventing governments could encourage activists and sympathizers of far-right groups to look for quick profit by defrauding internet users
- Focusing on the right to exercise complete control over their own person and property, as in the case of Corey D. Wilson's 3D printed guns, it is easy to connect cryptocurrencies to dark web illegal markets, in order to spread the use of unauthorized weapons.
  This may represent the most crucial aspect: the shift from a virtual/financial threat to a physical uncontrolled threat.

[62] G. Terzo (March 15, 2019) *Christchurch Terrorist Invested and Profited from Crypto Scam Bitconnect*. CCN. https://www.ccn.com/christchurch-terrorist-invested-and-profited-from-crypto-scam-bitconnect.
[63] BitConnect value https://coinmarketcap.com/it/currencies/bitconnect.

4. Small and independent jihadist groups: The Malhama Tactical Team

The Malhama Tactical was founded in May 2016, by **Abu Rofiq** (an Arabic pseudonym that means father of Rofiq), a 24-year-old Uzbek who was killed in a Russian airstrike on February 2017. The group is known as the first private military contractor team working exclusively for extremist groups and the first one operating on Syrian soil. It consists of more or less ten well-trained fighters from Uzbekistan and the Muslim-majority republics of the Russian Caucasus.

The team has been contracted to fight, provide training, and other battlefield consulting by groups like the *Hay'at Tahrir al-Sham*, also known as al-Qaeda in Syria.

Since 2016, the Malhama Tactical has been characterized by a strong presence on social media, video sharing platforms, and encrypted chats as Telegram, Facebook, Twitter, and YouTube. Before his death, Abu Rofiq used to post videos showing the group's training courses or, covering his face by wearing a scarf, he used to describe Malhama Tactical's ongoing jobs and future projects.

The group also placed job ads on Facebook, looking for recruits who were willing to "constantly engage, develop, and learn" and join a "fun and friendly team" with vacation allowance and a day off per week.

During an interview that the former leader of the military team released via Telegram to Foreign Policy[64], he explained that Malhama Tactical was willing to take work wherever Sunni Muslims were oppressed as in China, Myanmar or North Caucasus to continue fighting against the Russian government.

After Abu Rofiq's death, the online presence of the group has been reduced for a while, until the group's new commander, **Abu Salman Belarus**, a year ago, made his first public appearance on social media.

The new leader had even more followers than his predecessor, and used to translate his messages in English, Turkish and Russian (which was the only language used by the previous leader) and now is even planning to learn French.

Abu Salam Belarus, in an interview released on Telegram to the European Eye on Radicalization[65] between July and August 2018, explained that Malhama Tactical is "primarily instructing insurgents in battle tactics, giving medical aid, working with armoured vehicles, mortars, sniper activity, and weapons

[64] R. Komar, C. Borys, E. Woods (February 10, 2017) *The Blackwater of Jihad*. Foreign Policy https://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military-contractor-syria-russia-malhama-tactical.

[65] P. Van Ostaeyen, N. Hauer (September 19, 2018) *Interview with Abu Salman Belarus, Military Leader of Malhama Tactical*. European Eye on Radicalization. https://eeradicalization.com/interview-with-abu-salman-belarus-military-leader-of-malhama-tactical.

modifications" and that they are currently "teaching fighters of HTS (*Hay'at Tahrir al-Sham*, also known as al-Qaeda in Syria) and other groups". He also said that "quite a few of our students have become instructors, already working independently in different places".

3.1 Bitcoin donations campaign

The Malhama Tactical, being the first jihadist private military contractor, has explicitly turned the jihad into a for-profit belief. Abu Salam Belarus on Twitter, among other contents, used to call quite often for **donations in Bitcoin**. Despite the very frequent donation requests, the Bitcoin address provided by the group only received the equivalent of more or less $50. After this awkward attempt to raise money, Abu Salam Belarus deleted all the tweets calling for Bitcoin donations, inviting his followers to contact him in private to receive the Bitcoin address to give financial aid.

Even though the group, in economic terms, is not relying only on Bitcoin, the case of the Malhama Tactical is relevant to either consolidate some of the information gathered so far or provide new elements to analyse the jihadists' use of cryptocurrencies.

– **A clear militaristic intent instead of a politically correct approach**
  Jihadist donation campaigns asking for cryptocurrencies are explicitly aimed at providing supplies, training facilities, and weapons for the mujahideen. A kind of communication strategy very different from those campaigns, remotely linked to a terrorist organization, calling for donations through the conventional banking system and usually disguised behind charitable or religious intents. The shift into a more explicit message is likely to be allowed by the anonymity provided by the blockchain or digital ledger technologies[66].

– **The limited use of cryptocurrencies is not always related to a lack of technical skills**[67]
  Cryptocurrencies, Bitcoin in particular, are becoming a mainstream asset in legal markets. In fact, over time, their use is requiring less and less technical skills, causing an expansion of their catchment area

[66] International Institute on Counter-Terrorism *Trends in Cyberspace*. IDC Herzliya – International Institute for Counter-Terrorism (ICT). https://www.ict.org.il/Article/2230/Trends_in_Cyberspace_Annual_Summary_2017#gsc.tab=0.

[67] S. Webb (November 23, 2018) *Market blow up - ISIS war chest decimated by Bitcoin crash after terror chiefs invested millions in collapsing cryptocurrency, an expert claims*. The Irish Sun. https://www.thesun.ie/news/3424201/isis-war-chest-decimated-by-bitcoin-crash-after-terror-chiefs-invested-millions-in-collapsing-cryptocurrency.

which is also reaching terrorist supporters. Indeed, jihadist donation campaigns calling for cryptocurrencies are increasing in numbers since 2012[68]. Nevertheless, many legal users (and also jihadist supporters and religious leaders) are being sceptical about cryptocurrencies, due to the risks related to their price volatility and, for the same reasons, they are not yet spreading as a broadly exploited instrument for terrorism financing. But these concerns are only keeping Islamic terrorists from using cryptocurrencies as a store of value, not from exploiting them to move small or big amounts of money in complete anonymity and in a short range of time. In these terms, FinTech sector is allowing the creation of a potential, faster, substitute of the *hawala* system.[69]

– **One man's terrorist is another man's freedom fighter**
It is a truism that propaganda and communication are able to strengthen Islamic terrorists' narrative, turning a small group using violence and religion to raise money, into an army bravely fighting against the *takfir* (infidels). The truth is that, behind the narrative and storytelling depicting a courageous leader who is defeating an oppressive regime, there is a global strategy aimed at getting the world attention. Freedom, self-determination and religion, added to an online friendly Western communication strategy (e.g. job ads or business-oriented catchy advertisements) are the pillars of this new type of jihadist brand.
Hence, even though calls for anonymous donations through cryptocurrencies are still explicitly militaristic, jihadist groups are always hiding behind lies, trying to represent themselves as romantic and appealing young warriors fighting in the name of liberation. But there's no liberation in their intent. There's only an oppressive, colonialist, and violent will that groups as Malhama Tactical, despite being very small, are promoting, financing, and fuelling with bloodshed.

[68] E. Azani N. Liv (January 30, 2018) *Jihadists' Use of Virtual Currency*. IDC Herzliya – International Institute for Counter-Terrorism (ICT). https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf.
[69] ITSTIME (June 7, 2018) *Bitcoin and other types of cryptocurrency: modern and undetectable ways to finance terrorism*. http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone.

4. Suspicious humanitarian crowdfunding campaigns in bitcoin and their exploitation of exchange services.

The world's attention to the war in Syria is allowing jihadist groups to change their narrative, by disguising their intents also behind a false image built around humanitarian aid or struggle against war criminals oppressing innocent people.

This is potentially giving terrorist organizations and their sympathizers the chance to widen the heterogeneity of their affiliates by globally leveraging through the internet on the atrocities and injustice brought by the war, overlapping issues exclusively concerning violent extremism or radicalization.

In economic terms, this branch of the global jihadist web communication strategy is translating into a growing number of apparently decentralized (i.e. carried out by individuals or small groups) crowdfunding campaigns accepting bitcoin for either explicit militaristic or charity purposes as in the case Isis suspects in Al-Hol camp raising money through online crowdfunding campaign[70].

These campaigns are very numerous and are generating more and more difficulties either in how to identify their real intent (if terrorist related or just scams) and in tracking down the total amount of funds received.

Indeed, on Telegram, these calls for donations are usually only advertised by explicit jihadist chat groups without ever interacting directly with them; create mirror groups to avoid the risk of being blocked or tracked; provide several donation methods (e.g. PayPal, fundraising platforms on the public web, various bitcoin addresses).

In order to better explain this trend, the following analysis will focus on a few topic cases related to this opaque calls for bitcoin, as **Sadaqa al-Kahir** and **al-Ikhwa**, self-proclaimed charity groups aimed at giving aid in Syria, and **al-Sadaqa**, a jihadist campaign raising money to support the mujahideen and some of the bitcoin addresses and transactions processed to finance these groups.

4.1 Binance bitcoin address (...*bu1s*)

Before deepening into the analysis of these campaigns, is worth doing a short explanation on the bitcoin address "...*bu1s*" (last four characters of the bitcoin address), which is where the most majority of the donations that will be traced are sent.

[70] R.Hall (July 25, 2019) *Isis suspects in Syrian camp raise thousands through online crowdfunding campaign*. The Independent. https://www.independent.co.uk/news/world/middle-east/isis-syria-camp-al-hol-paypal-telegram-online-crowdfunding-a9021006.html.

As explained by Bellingcat[71] and Cointelegraph[72], this address belongs to **Binance**, a very well-known crypto exchange service, which allows users to trade cryptocurrencies for fiat money or other digital currencies. In particular, it was discovered that this exchange service has been used to send bitcoin to *Izz ad-Din al-Qassam Brigades*, the military wing of Hamas[73].

This doesn't mean or proves at all a direct implication of the exchange service in terrorism financing, but it only means that these funds have been exchanged (after a few steps) into cash or other digital currencies by exploiting Binance.

The transactions of these campaigns, usually, before reaching Binance bitcoin address, made a donation to other bitcoin addresses. These bitcoin addresses may belong either to other exchange services working as middlemen between the crowdfunding campaign and Binance or could belong to a mixing service (to disguise the sender and the receiver)[74], to launder and hide the bitcoin donated before being cashed through Binance, or could also belong to private parties involved in this pattern.

Below, a description of each campaign and of some of the most significant transactions analysed.

4.2 Al-Sadaqah Donation Campaign (... *Nwpf*, ...*qLez*)

Since November 2017 a*l-Sadaqah* (the charity) organization, began a still ongoing fundraising campaign on Telegram, other social media such as Twitter, and on the deep web[75] to raise bitcoin from Western supporters. The explicit intent of the call for bitcoin is to finance the *mujahideen* fighting against the Assad regime in north-eastern Syria[76]. Nowadays, the organization's Twitter page has been shut down, but its English and French Telegram accounts are still online.

[71] B. Smith (March 26, 2019) How To Track Illegal Funding Campaigns Via Cryptocurrency. Bellingcat. https://www.bellingcat.com/resources/how-tos/2019/03/26/how-to-track-illegal-funding-campaigns-via-cryptocurrency.

[72] https://cointelegraph.com/news/binance-vs-mcafee-hack-rumors-refuted-cryptocurrency-trading-resumed.

[73] D.M. Barone (February 06, 2019) Hamas crowdfunding bitcoin: legitimizing cryptocurrencies from a jihadist perspective. ITSTIME http://www.itstime.it/w/hamas-crowdfunding-bitcoin-legitimizing-cryptocurrencies-from-a-jihadist-perspective-by-daniele-maria-barone.

[74] https://cryptalker.com/bitcoin-mixer.

[75] http://cjlab.memri.org/latest-reports/online-campaign-in-english-raising-funds-for-the-jihad-in-syria-in-bitcoin.

[76] http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

The campaign seems not to be very popular. The BTC address advertised on *al-Sadaqah*, "...*Nwpf*", shows that from November 2017 until its last donation on October 28, 2018, has received an amount equivalent to more or less $1,000 and processed 8 transactions (4 inputs and 4 outputs). Although most of the transfers were only worth a few dollars, one Bitcoin wallet from which a transaction was made to the wallet of Al-Sadaqa stood out ...*85oC*, which has totally received the equivalent of more or less $7millions.[77] This Bitcoin wallet was associated with the kidnapping of a child in South Africa in May 2018 and many frauds.[78]

The wallet linked to the jihadist donation campaign[79] includes also another address "...*qLez*" (total received roughly $150).

Going backward from the only one donation received by this address, it appears that small amount of bitcoin (a few hundred dollars) has been transferred from one bitcoin address to another and all of them have only one input and one output. The interesting data is that the more we go back to the source of the only donation made to ...*qLez*, the more we encounter an increasing number of wealthy bitcoin addresses (as *FkdG*), worth the equivalent of thousands of hundred dollars.

Given that these addresses belong to e-wallets with only one bitcoin address[80], they're likely to belong to private wealthy donors rather than to any crypto-exchange or trading platform.

About the outputs of al-Sadaqa BTC addressees, the amount of bitcoin that their call for donations raised has been donated in full and, 4 out of these 5 outputs, as to "...*nbQ*" - "...*WFDD8*" - "...*Xt6D*", carry out the same method to send their bitcoin to Binance wallet address:

- They periodically receive small amounts (from a few hundred to $1.500) from different BTC addresses.
- Then, that same day or the very next day, they do a multiple input transaction: send the small amount received to another bitcoin address and a larger amount (until $1 million) always to "...*bu1s*", i.e. Binance (the big orange dot in the picture below).

These first wallets, where the donations are directly made by al-Sadaqa, could not belong to any private receiver but, given the incredible amount

[77] N. Liv (July 2019) Jihadists' Use of Virtual Currency 2. International Institute for Counter Terrorism ICT. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf.
[78] B. Strick (June 18, 2018) Tracing a Jihadi cell, kidnappers and a scammer using the blockchain – an open source investigation. Medium. https://medium.com/@benjamindbrown/tracing-syrian-cell-kidnappers-scammers-finances-through-blockchain-e9c52fb6127d.
[79] https://www.walletexplorer.com/wallet/ae0f2ea8de2764e9/addresses.
[80] https://www.walletexplorer.com/wallet/6402b0d863591976/addresses.

of bitcoin addresses owned by their e-wallets, are very likely to belong to an exchange platform or a bitcoin tumbler (a mixing service).

4.3 Humanitarian aid requests advertised on independent jihadist Telegram groups: al-Khair charity group and al-Ikhwa

As previously mentioned, not only explicit jihadist campaigns are calling for bitcoin donations for Syria, but also independent self-proclaimed charity groups.

Al-Ikhwa (The Brothers) and Sadaqa al-Khair present themselves as non-profit organizations, which are collecting donations to help the Syrian population, soliciting money also via Bitcoin to support widows and orphans.[81]

They both made their first appearance on Telegram more or less one year ago, posting extreme war images and video, in English and German, of armed attacks against civilians and of their initiatives to give aid to the Muslim people in Syria. Furthermore, both of these crowdfunding humanitarian campaigns declare on their Telegram and Facebook pages that they prefer to use alternative and anonymous fundraising methods because the conventional banking system or non-anonymous ways to receive and call for donations are already preventing them from processing any sort of payment (i.e. donorbox.com or wire transfers). Indeed, in order to help the needy and avoid authorities controls, they're calling for donations via Paypal, money transfers, some crowdfunding platform on the clear web, and also in bitcoin.

Both of these charity campaigns have been advertised by Telegram chat groups which post explicit jihadist material, that have sponsored bitcoin donations to help the mujahideen by supporting military groups and crowdfunding campaigns as the **Malhama Tactical Team** (private military contractor team working exclusively for jihadist groups)[82] and **SadaqaCoins** (a cryptocurrencies crowdfunding website on the deep web, aimed at funding the mujahideen in Syria).[83] Even though most of these groups have among a few hundred to 2000 subscribers, their contents have been viewed by thousands of users. Some of these Telegram groups also promote the **use of bitcoins by**

[81] https://www.memri.org/jttm/charity-group-telegram-solicits-money-bitcoin-%E2%80%8Esupports-syrian-fighters-wives-martyrs%E2%80%8E.

[82] D.M. Barone (December 01, 2018) Jihad as a Business Segment: the Malhama Tactical Team. ITSTIME. http://www.itstime.it/w/jihad-as-a-business-segment-the-malhama-tactical-team-by-daniele-maria-barone.

[83] N. Liv (July 2019) Jihadists' Use of Virtual Currency 2. International Institute for Counter Terrorism ICT. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf.

sharing self-made user's manuals and explain the reasons why it is right to **use cryptocurrencies according to the Sharia**.

In terms of donations, it seems that this communication strategy is already paying off.

4.4 Sadaqa al-Khair charity group: ...*51u7*

In a few days (from May 21, 2019, until May 30, 2019) al-Khair BTC address ...*51u7*, at the time of writing, shows a total of 6 transactions (3 inputs and 3 outputs) and a total received of more or less the equivalent of $1,100.

After a few days, the charity group didn't publicly provide anymore its bitcoin address. Thus, it is possible that they're providing a new bitcoin address on a private chat in order to avoid being detected.

All of the funds received have been transferred to other bitcoin addresses ...*MUaC* (once) and ...*pXai* (twice).

Also, in this case, there is a common pattern which leads to ...*bu1s*, Binance, very similar to the one seen in al-Sadaqa, adding a few steps more.

In fact, the donations made by the al-Khair charity group, are firstly passing through two or three brand new BTC addresses, with two transactions each, at most, in order to be subsequently transferred to wealthier wallets which in the end move their funds to ...*bu1s* (the big orange dot in the picture below).[84]

Same as in al-Sadaqa, the transfers involving BTC addresses which seem to be owned by private donors is made in the first or the second step of this chain. Thus, it is more likely that the wealthiest bitcoin wallets involved in these specific donations already belong to Binance or to another exchange service/mixing service which uses Binance to exchange cryptocurrencies. Hence, it seems that this campaign is not directly involving any wealthy donor.

4.5 Al-Ikhwa Independent Charity (several BTC addresses)

The al-Ikhwa crowdfunding campaign is using different bitcoin public addresses that, after the first four months of activities (since November 2018), have been monthly updated on their Telegram group in rotation. (...*6p6S* ...*Vgea* ...*zcHH* ...*deKc* ...*8ELo* ...*AU5j* ...*XLRs* ...*zXyz* ...*zcHH*).

Starting since July 2018 the self-proclaimed charity group has received, ignoring non-public bitcoin addresses provided only through the private chat, a total amount of more or less $3000. The charity campaign received its first donation on ...*zcHH* on March 2019 and the last donations have been received at the beginning of June 2019.

[84] https://www.blockchain.com/it/btc/tree/453240296.

Many of these addresses belong to the same bitcoin wallet[85], and in some cases have been used to send a multiple inputs (a donation made simultaneously from different bitcoin addresses to one or many other wallets) of more or less totally $700 to ...*wwxi*.[86]

This donation was then split into two different transactions: one is more likely to already belong to an exchange service/mixing service (its wallet has 108.496 total addresses) and then transferred to ...*bu1s*.

Then, the other donation was sent to another bitcoin address with a total amount received of $200 in 1 input and 1 output which then repeated the same process seen before to reach Binance bitcoin address[87] (the bigger orange dots in the picture below).

This process is repeated in almost all the bitcoin transferred by al-Ikhwa campaign to other bitcoin addresses until Binance.

As opposed to Hamas bitcoin crowdfunding campaign, in these cases the exploitation of Binance is related to the final output, meaning that the money received could be directly exchanged or used to finance other e-wallets.

This analysis explained the modus operandi of only a very limited number of the BTC addresses involved in these crowdfunding campaigns. Indeed, there are many others either wealthy or relatively poor addresses operating through this pattern, which bring out a very complex and solid network.

Hence, it is possible to highlight the following main aspects:

– Opaque humanitarian calls for anonymous donations may increase the difficulty to evaluate if there's a nexus between their charity fundraising campaigns and terrorism financing by making more and more unclear which one is reliable (e.g. moved by a legitimate purpose) or connected to a jihadist group (as a smokescreen to disguise terrorism financing or money laundering) or just a major scam. In the cases of Sadaqa al-Khair and al-Ikhwa, being advertised and supported by explicit jihadist Telegram chat groups could mean both that they support a jihadist group and that they are just a fraud. In both cases, the fact that they are able to freely ask, send and receive bitcoins should be stopped just in the same way it already happens when they try to exploit the conventional banking system or public and legitimate crowdfunding websites.

[85] https://www.walletexplorer.com/wallet/3bfee78719643a94/addresses.

[86] https://www.blockchain.com/it/btc/tx/7ad7c55e8724e9db3ca54651a3d7ab0591c93ce2bc0e5c39f97d09f09df8cc7d.

[87] https://www.blockchain.com/it/btc/tree/431361274.

– Crowdfunding campaigns as al-Sadaqa, al-Khair and al-Ikhwa don't seem to have received huge amounts of bitcoin but this doesn't necessarily mean that they can't be a part of a wider network. Cases like these are becoming more and more frequent since 2017: they ask for bitcoin in order to help the Muslim Syrian population either by arming them to fight against the Assad and Western governments or by giving aid to the orphans or widows; they receive an amount in bitcoin in a range from roughly $1.000 to $3.000; they usually operate for more or less a year. They could act as digital-money mules or bitcoin tumblers, transferring from time to time small amounts of bitcoin through an infinite number of e-wallets, in order to let wealthy jihad supporters to be disguised and act unopposed while moving huger amounts of wealth globally and anonymously through them. In this case, they could have the double role of being a smokescreen (able to hide wealthier transactions) and a fundamental tactical role in facilitating terrorism financing.

5. Summary

The most recent developments in the cryptocurrency/violent extremism ecosystem are highlighting, on the one hand, how a grey legal framework in the FinTech sector is currently keeping authorities and analysts from efficiently tracking down and prosecuting illicit financing methods, on the other hand, how the liquidity of terrorist groups strategies and tactics are constantly evolving. Moreover, as previously analysed in this essay, extremist groups are more and more becoming able to find either religious or political justifications to encourage their members or sympathizers to stay up to date on the most recent financing methods, by leveraging on their duties towards the organizations.

Focusing on the different areas and cases analysed in this essay, it is possible to understand that, even though every branch discussed has its peculiarity, they still present common denominators.

In the cases regarding the exploitation of cryptocurrencies by white supremacist groups, they are ideologically self-sustained by the refusal of a centralized economic control (e.g. taxes and policies unable to support white heritage and cultures) and the consequential will to establish an alternative source to finance, store and invest money while circumventing authorities or legal restrictions on conventional channels, increase privacy, and keep on spreading their propaganda.

Through this lens, cryptocurrencies become powerfully meaningful: a clandestine instrument to help their ethnicity. In these terms, crypto-

currencies are turned into a cornerstone of the communication strategies adopted by al-right groups.

On the contrary, in the events related to jihadist organizations as Hamas, they are overlapping the religious and ideological justification. In particular, it seems that after the first announcement made by Abu Obeida on January 29 about the incoming possibility to make donations via bitcoin to the organization, many activists and supporters have raised questions about cryptocurrencies. Indeed, the day after its first call for bitcoin, Hamas published an infographic about the Bitcoin on the Hamas-affiliated newspaper *Al-Resalah* explaining what Bitcoin is and, probably to reassure its supporters about their investment, stressing that the daily trade in bitcoin amounts is approximately $6 million, and that the total amount on the Internet is estimated at $61 billion.[88] Moreover, it is relevant that Hamas donation campaign in bitcoin is the first jihadist case in this field without any particular religious justification concerning the use of cryptocurrencies. Indeed, even though the debate about cryptocurrencies is still ongoing in the Islamic community and among Islamic scholars, it seems that, in this case, donors were prevalently worried about their investments rather than use a not yet fully recognized Sharia-compliant product as a mean of payment[89]. For Hamas it was enough to claim that "*The Zionist enemy fights the Palestinian resistance by trying to cut aid to the resistance by all means, but lovers of resistance around the world fight these Zionist attempts and seek all possible means to aid the resistance*" to convince its supporters that cryptocurrencies are a legitimate method to fund the jihad.[90]

Another important aspect is related to the diffusion of skills among these groups, which is not only regulated at an "institutional" level (e.g. violent extremist organizations leaders or endorsers) but it is autonomously also spreading through small independent clusters (as suspicious online humanitarian crowdfunding campaigns), individuals (as Tarrant), and

[88] (February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

[89] D.M. Barone (August 16, 2018) Cyber Jihad and Terrorism Financing: New Methods – Old Rules. ITSTIME. http://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone.

[90] (February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

small groups (as Malhama Tactical) which are causing the diffusion of a terrorism financing maze, similar to the phenomenon happening in the illegal deep web markets described in the IOCTA 2018.

All of these elements are creating a confusing environment, which can make investigations and prosecutions on terrorism financing even more difficult.

Focusing on small crowdfunding campaigns, it is still crucial to introduce stricter and updated Anti Money Laundering and Know Your Customer (KYC) policies applied to every user who wants to exchange or purchase even small amounts of bitcoin (e.g. less than the equivalent $2000). Binance, for instance, has already updated its account verification process, with the mandatory request of providing a valuable ID (e.g. National Identification Card, Permanent Residence Card, International Passport) even though, it is still not specified if there's a minimum expense required by the user to be obliged to provide a valid document to the platform[91]. Nevertheless, there are still many others exchange or mixing services available which still don't require, at the time of writing, any information about their users to purchase, receive or send either small or big amounts of digital currencies. This current situation allows the exploitation of digital money-mules or mixing services which can still easily scramble and hide wealthy illegitimate transactions.

It has to be stressed that, besides these complications, there are positive aspects to take into account. Blockchain technology is offering an unprecedented tool for investigations: from one single suspicious transaction, it is possible to track back all the financial history of the people involved in one crime. In these terms, the use of the web for terrorist purposes is still a double-edged sword; it can surely give a strong advantage to terrorist organizations in terms of anonymity and allow them to keep on widening their range through strengthening communication and crowdfunding practices, but authorities monitoring methods are subsequently improving. Even though the current legal framework makes it difficult to prosecute the illegal exploitation of many modern online tools, as long as the internet will be the primary way for violent extremist groups or individuals to keep an international unity among their members, they will still be exposed to controls and analysis.

[91] https://support.binance.je/hc/en-us/articles/360020832652-How-to-Complete-the-Account-Verification-KYC-Process.

References

A.D. Smith (2009) Ethno-symbolism and nationalism. Routledge (108-109).

A. Shalal (June 24, 2018) *Migration fight erodes support for German conservatives, far-right AfD gains*. Reuters. https://www.reuters.com/article/us-germany-politics/migration-fight-erodes-support-for-german-conservatives-far-right-afd-gains-idUSKBN1JK0HV.

B. Kaye T. Allard (April 4, 2019) *New clues emerge of accused New Zealand gunman Tarrant's ties to far right groups*. Reuters. https://uk.reuters.com/article/uk-newzealand-shooting-australia-extremi/new-clues-emerge-of-accused-new-zealand-gunman-tarrants-ties-to-far-right-groups-idUKKCN1RG093.

Bureau of Counterterrorism and Countering Violent Extremism (2016) *Country Reports on Terrorism*. US Department of State. https://www.state.gov/j/ct/rls/crt/2016/272235.htm.

B. Smith (March 26, 2019) How To Track Illegal Funding Campaigns Via Cryptocurrency. Bellingcat. https://www.bellingcat.com/resources/how-tos/2019/03/26/how-to-track-illegal-funding-campaigns-via-cryptocurrency.

B. Strick (June 18, 2018) *Tracing a Jihadi cell, kidnappers and a scammer using the blockchain – an open source investigation*. Medium. https://medium.com/@benjamindbrown/tracing-syrian-cell-kidnappers-scammers-finances-through-blockchain-e9c52fb6127d.

Country Reports on Terrorism (2008) U.S. Department of State. https://www.state.gov/j/ct/rls/crt/2007/103714.htm.

Counter Extremism Project (2018) *European Ethno-Nationalist and White Supremacy Groups*. https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/European_Ethno-Nationalist_and_White_Supremacy_Groups_081618.pdf.

D. Gerard (March 19, 2019) *Neo-Nazis Bet Big on Bitcoin (And Lost)*. Foreign Policy. https://foreignpolicy.com/2019/03/19/neo-nazis-banked-on-bitcoin-cryptocurrency-far-right-christchurch.

D. Kirkpatrick (March 15, 2019) *Massacre Suspect Traveled the World but Lived on the Internet*. The New York Times. https://www.nytimes.com/2019/03/15/world/asia/new-zealand-shooting-brenton-tarrant.html.

D. Manheim, P.B. Johnston, J. Baron, C. Dion-Schwarz (April 21, 2017) *Are Terrorists Using Cryptocurrencies?* RAND Corporation. Available at https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html.

D.M. Barone (2018) *Jihadists' use of cryptocurrencies: undetectable ways to finance terrorism*. Sicurezza Terrorismo e Società. http://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2018/11/Daniele-Maria-Barone-Jihadists%E2%80%99-use-of-cryptocurrencies_undetectable-ways-to-finance-terrorism.pdf.

D.M. Barone (August 16, 2018) Cyber Jihad and Terrorism Financing: New Methods – Old Rules. ITSTIME. http://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone.

D.M. Barone (June 7, 2018) *Bitcoin and other types of cryptocurrency: modern and undetectable ways to finance terrorism*. ITSTIME http://www.itstime.it/w/bitcoin-and-other-types-of-cryptocurrency-modern-and-undetectable-ways-to-finance-terrorism-by-daniele-maria-barone.

E. Azani N. Liv (January 30, 2018) *Jihadists' Use of Virtual Currency*. IDC Herzliya – International Institute for Counter-Terrorism (ICT) https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf.

Europol (2018) I*nternet Organised Crime Threat Assessment (IOCTA) 2018*. European Union Agency for Law Enforcement Cooperation. Available at https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

E. Year, E. Ofer (January 6, 2011) *Gaza's Economy: How Hamas Stays in Power*. The Washington Institute. https://www.washingtoninstitute.org/policy-analysis/view/gazas-economy-how-hamas-stays-in-power.

E. Spagnuolo (April 26, 2017) Addio Bitcoin, nel deep web ora si paga con Monero e Zcash. Wired - Italia. https://www.wired.it/economia/finanza/2017/04/26/bitcoin-monero-zcash.

G. Iggers (1970) *The Cult of Authority: The Political Philosophy of the Saint-Simonians*. The Hauge Martinus Nijhoff (73-75).

G. Terzo (March 15, 2019) *Christchurch Terrorist Invested and Profited from Crypto Scam Bitconnect*. CCN. https://www.ccn.com/christchurch-terrorist-invested-and-profited-from-crypto-scam-bitconnect.

Hamas Covenant (1988) Yale Law School - Lillian Goldman Law Library. http://avalon.law.yale.edu/20th_century/hamas.asp.

H. Binswanger (January 24, 2014) *Sorry Libertarian Anarchists, Capitalism Requires Government*. Forbes. https://www.forbes.com/sites/harrybinswanger/2014/01/24/sorry-libertarian-anarchists-capitalism-requires-government-2/#6cb1ad7c7d89.

Hatewatch Staff (September 20, 2018) *Notorious crypto-anarchist and antigovernment extremist Cody Rutledge Wilson left the country on a flight to Taiwan after he was alerted of an impending investigation against him for his alleged sexual assault of a minor*. SPLC Southern Poverty Law Center. https://www.splcenter.org/hatewatch/2018/09/20/cody-wilson-lam-1-million-bitcoin.

International Institute on Counter-Terrorism *Trends in Cyberspace*. IDC Herzliya – International Institute for Counter-Terrorism (ICT) https://www.ict.org.il/Article/2230/Trends_in_Cyberspace_Annual_Summary_2017#gsc.tab=0.

J. Bohannon (March 9, 2016) Why criminals can't hide behind Bitcoin. ScienceMag. Available at http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

J. Ebner (January 24, 2018) The currency of the far-right: why neo-Nazis love bitcoin. The Guardian. https://www.theguardian.com/commentisfree/2018/jan/24/bitcoin-currency-far-right-neo-nazis-cryptocurrencies.

J. Khoury (June 10, 2017) For Arab World, Hamas Is 'Legitimate Resistance Movement,' Not Terror Group, Qatar Says. Haaretz. https://www.haaretz.com/middle-east-news/palestinians/qatar-hamas-is-legitimate-resistance-movement-1.5482546.

J. Ganz (September 19, 2017) Libertarians have more in common with the alt-right than they want you to think. The Washington Post. https://www.washingtonpost.com/news/posteverything/wp/2017/09/19/libertarians-have-more-in-common-with-the-alt-right-than-they-want-you-to-think/?utm_term=.1d9d3ac77b22.

J. Wilson (March 28, 2019) *With links to the Christchurch attacker, what is the Identitarian Movement?* The Guardian. https://www.theguardian.com/world/2019/mar/28/with-links-to-the-christchurch-attacker-what-is-the-identitarian-movement.

K. Marinos (March 23, 2016) *Are Bitcoin Transactions Traceable?*. CoinTelegraph. Available at https://cointelegraph.com/news/are-bitcoin-transactions-traceable.

L. Beckett (September 19, 2018) *Gun rights activist Cody Wilson charged with sexual assault of teen*. The Guardian. https://www.theguardian.com/us-news/2018/sep/19/cody-wilson-3d-guns-sexual-assault-texas.

Mapping Palestinian Politics - Popular Resistance Committees (PRC). ECFR. https://www.ecfr.eu/mapping_palestinian_politics/detail/popular_resistance_committees.

M. Arnold, S.A. Ramadan (January 30, 2018) *Hamas Calls on Supporters to Donate to Group in Bitcoin*. Bloomberg. https://www.bloomberg.com/news/articles/2019-01-30/hamas-calls-on-supporters-to-donate-to-group-in-bitcoin.

M. Bell (December 19, 2016) Meet the identitarians, Europe's 'new right'. PRI Public Radio International. https://www.pri.org/stories/2016-12-19/meet-identitarians-europes-new-right.

M. Levitt, D. Ross (2007) *Hamas: Politics, Charity, and Terrorism in the Service of Jihad*. Yale University Press.

M. Steinau (January 11, 2018) *How neo-Nazis and right-wing extremists profit from bitcoin*. Business Insider. https://www.businessinsider.com/neo-nazis-and-right-wing-extremists-profit-from-the-bitcoin-hype-2018-1?IR=T.

N. Liv (July 2019) Jihadists' Use of Virtual Currency 2. International Institute for Counter Terrorism ICT. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf.

O. Kharif (January 2, 2018) *The Criminal Underworld Is Dropping Bitcoin for Another Currency*. Bloomberg. Available at https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

Popular Resistance Committees - Palestine. TRAC. https://www.trackingterrorism.org/group/popular-resistance-committees-palestine.

Profile: Hamas Palestinian Movement (May 12, 2017) BBC. https://www.bbc.com/news/world-middle-east-13331522.

P. Koshy D. Koshy P. McDaniel (2014) *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. Pennsylvania State University, University Park, PA 16802, USA. Available at https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf.

P. Van Ostaeyen, N. Hauer (September 19, 2018) *Interview with Abu Salman Belarus, Military Leader of Malhama Tactical*. European Eye on Radicalization. https://eeradicalization.com/interview-with-abu-salman-belarus-military-leader-of-malhama-tactical.

Report - Hamas. Counter Extremism Project. https://www.counterextremism.com/threat/hamas.

R.Hall (July 25, 2019) *Isis suspects in Syrian camp raise thousands through online crowdfunding campaign*. The Independent. https://www.independent.co.uk/news/world/middle-east/isis-syria-camp-al-hol-paypal-telegram-online-crowdfunding-a9021006.html.

R. Katsiri (February 3, 2019) *Hamas raises bitcoin donations via US crypto exchange*. Globes. https://en.globes.co.il/en/article-hamas-raises-bitcoin-donations-via-us-crypto-exchange-1001271661.

R. Komar, C. Borys, E. Woods (February 10, 2017) *The Blackwater of Jihad*. Foreign Policy https://foreignpolicy.com/2017/02/10/the-world-first-jihadi-private-military- contractor-syria-russia-malhama-tactical.

S. Chandler (October 07, 2018) Government Tracking of Crypto Is Growing, But There Are Ways to Avoid It. CoinTelegraph. https://cointelegraph.com/news/government-tracking-of-crypto-is-growing-but-there-are-ways-to-avoid-it.

SPLC Southern Poverty Law Center. https://www.splcenter.org/bitcoin-and-alt-right.

S. Webb (November 23, 2018) *Market blow up - ISIS war chest decimated by Bitcoin crash after terror chiefs invested millions in collapsing cryptocurrency, an expert claims*. The Irish Sun. https://www.thesun.ie/news/3424201/isis-war-chest-decimated-by-bitcoin-crash-after-terror-chiefs-invested-millions-in-collapsing-cryptocurrency.

The Economist (March 21, 2019) *Why white nationalist terrorism is a global threat*. https://www.economist.com/international/2019/03/21/why-white-nationalist-terrorism-is-a-global-threat.

UN Human Rights Office of the High Commissioner (July 2018) *Ethno-nationalism denies millions their citizenship rights - anti-racism expert*. https://www.ohchr.org/EN/NewsEvents/Pages/EthnoNationalismDeniesTheirCitizenshipRights.aspx.

Wired magazine (December 19, 2012) *The 15 most dangerous people in the world*. https://www.wired.com/2012/12/most-dangerous-people.

(March 7, 2019) *Funding Terrorism: ISIS raises funds through an affiliated website, using bitcoins*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/03/E_054_19.pdf.

(February 12, 2019) *Drive for donations using Bitcoin on an ISIS affiliated website*. The Meir Amit Intelligence and Terrorism Information Center. https://www.terrorism-info.org.il/app/uploads/2019/02/E_018_19.pdf.

(February 4, 2019) *Hamas and the popular resistance committees called on their supporters to donate money using the virtual currency bitcoin*. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/hamas-popular-resistance-committees-called-supporters-donate-money-using-virtual-currency-bitcoin.

(October 15, 2018) 4th issue of al-Haqiqa magazine. Site Intel Group. https://ent.siteintelgroup.com/Western-Jihadists/4th-issue-of-al-haqiqa-magazine-features-interview-with-ttp-commander-promotes-password-security-and-bitcoin-donations.html.

(December 6, 2017) Drive for Bitcoin Donations on an ISIS-affiliated website. The Meir Amit Intelligence and Information Center. https://www.terrorism-info.org.il/en/drive-bitcoin-donations-isis-affiliated-website.

(October 4, 2012) *Treasury Sanctions Two Hamas-Controlled Charities*. U.S. Department of Treasury. https://www.treasury.gov/press-center/press-releases/pages/tg1725.aspx.

Conosci il tuo nemico: la rappresentazione del terrorismo nei tweet della disinformazione russa

Filippo Tansini

Nota autore

Filippo Tansini, PhD in Theatrical Studies, is a Social Media Intelligence (SOCMINT) analyst. His research interests have mainly been focusing on strategic communication, social media dynamics and information warfare, Renaissance Theatre, Textual Criticism and Data Mining.

Abstract

All'interno di un quadro complesso di *Hybrid Warfare* e *Information Warfare*, questo studio prende in analisi un *dataset* di account Twitter impiegati dalla società russa Internet Research Agency (IRA), tra 2009 e 2018, in operazioni di *Information Warfare*.
Obiettivo dell'analisi è quello di studiare la rappresentazione del terrorismo costruita e diffusa dall'IRA attraverso le azioni svolte dagli account in esame. Utilizzando il costrutto delle Rappresentazioni Sociali e metodi di *Latent Semantic Analysis* (*cluster analysis* e analisi delle corrispondenze multiple) vengono esplorati temi espliciti e impliciti associati al concetto di terrorismo veicolato su Twitter. Su un campione generale di 8.768.633 di messaggi pubblicati, sono stati filtrati 22.764 messaggi contenenti il lemma «terror». I risultati mostrano dinamiche temporali peculiari e contenuti che sottendono due tematiche principali: la natura della minaccia rappresentata (nota/ignota) e il posizionamento del nemico (interno/esterno). I limiti e le implicazioni pratiche di questi risultati vengono discussi con particolare riferimento: alle modalità e ai contenuti delle comunicazioni online riferiti al concetto di terrorismo, alle capacità operative espresse dagli account analizzati, alle possibilità future di applicazione in prospettiva di contrasto a operazioni di *Information Warfare*.

Within the complex framework of the Hybrid and Information Warfare, this study analyses a Twitter account dataset related to the Russian company Internet Research Agency (IRA) that was potentially used for Information Warfare operations, from 2009 to 2018.
The objective of the analysis is to reconstruct the representation of terrorism disseminated by the IRA through the actions carried out by the analysed Twitter accounts. Using the construct of Social Representations and methods of Latent Semantic Analysis (cluster analysis and multiple correspondence analysis) explicit and implicit themes associated with the concept of terrorism are explored. Out of a general sample of 8,768,633, 22,764 messages were filtered containing the lemma «terror». The results show peculiar temporal dynamics and contents that subtend two main themes: the nature of the threat represented (known / unknown) and the positioning of the enemy (internal / external). The limits and the practical implications of these results are discussed with particular reference to: methods and contents of online communications related to the concept of terrorism, capability demonstrated by the accounts analysed, further applicability of the analysis with a perspective of countering Information Warfare operations.

Keywords

Hybrid Threat, Information Warfare, Latent Semantic Analysis, Social Media Intelligence, Social Representation, terrorism

Introduzione

> «Ogni èra ha il suo tipo di guerra, le sue condizioni di limite e i suoi preconcetti peculiari»
>
> Carl von Clausewitz, Della Guerra

Hybrid Warfare: un campo di azione complesso per definizione: «the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects» (Cullen e Reichborn-Kjennerud, 2017, p. 8).

Le operazioni coordinate e unificate dal concetto di scontro ibrido[1] sono rivolte trasversalmente all'intero complesso economico-sociale e militare dell'avversario. Gli esiti sono il prodotto di azioni volte a modificare un sistema complesso: non rispondono a logiche causa/effetto, ma tendono ad un improvviso e catastrofico collasso del sistema bersaglio. La guerra ibrida vive di attività in costante evoluzione, spesso riprogettate o adattate per rispondere all'immediata circostanza tattica: ne risultano azioni eterogenee, inaspettate, raramente «regolari» (e perciò prevedibili). Tra queste, rientrano certamente quelle comprese nello schema dell'*Information Warfare*[2]. La strategia si adatta alle esigenze del momento, capitalizzando gli eventi o costruendo le premesse da cui sviluppare nuove azioni. Citando l'esperto di *cybersecurity* Robert Graham (2018) a proposito di *Irregular Cyber Warfare*: «raggiungere uno specifico obiettivo è difficile, mentre è più facile provocare un qualsiasi risultato. Cercare di perseguire un'attività strettamente definita per danneggiare il nemico è complesso, più semplice è supportare un gruppo di hacker motivati e lasciare che facciano qualsiasi tipo di danno siano in grado di ottenere»[3].

[1] Per uno studio storico del termine si potrà consultare l'utile lavoro di Elie Tenenbaum (2015), *Hybrid Warfare in the Strategic Spectrum: An Historical Assessment*, in Guillaume Lasconjarias e Jeffrey A. Larsen a cura di (2015). *Nato's response to Hybrid Warfare*, NATO Defense College.: https://www.files.ethz.ch/isn/195405/fp_24.pdf.

[2] Si veda, ad esempio, lo schema costruito da Uwe Hartmann per descrivere da un punto di vista strategico le componenti di una operazione di Hybrid Warfare, specialmente «Executing strategies ambiguously», in Uwe Hartmann (2017). *The Evolution of the Hybrid Threat,and Resilience as a Countermeasure*. Rome: Nato Defense College, p. 2.

[3] «Accomplishing one *specific* goal is hard, but accomplishing *any* goal is easy. Trying to do a narrowly defined task to disrupt the enemy is hard, but it's easy to support a group of motivated hackers and let them do any sort of disruption they can come up with» [trad. dell'autore].

L'efficacia di queste azioni irregolari risiede proprio nell'ottenere risultati minimizzando le possibilità di identificazione preventiva, di ritorsioni sul piano internazionale, di dover fronteggiare strutturate azioni di resistenza.

Un punto decisivo riguarda proprio l'esito delle attività di guerra ibrida. L'influenza sulla capacità operativa o decisionale dell'avversario diventa evidente solo quando la strategia ha avuto già effetto, rendendo perciò complesso mitigare gli esiti di azioni già concluse. Inoltre, la spinta a seguire schemi indiziari locali legati al decorso di singoli episodi divenuti improvvisamente evidenti, aumenta il rischio di nascondere, alle analisi, le condizioni strategiche originarie che hanno condotto a quelle conseguenze in modo non lineare.

Il 17 ottobre 2018 Twitter decide di pubblicare attraverso il proprio blog ufficiale una serie di dati relativi a potenziali operazioni di *Information Warfare*. Uno di questi dataset riguarderebbe almeno una parte degli account utilizzati dalla Internet Research Agency (Adrian, 2015), azienda russa impegnata nella comunicazione online e considerata tra i principali agenti di applicazione della dottrina dell'*informatsionnaya voyna* [trad. Information warfare] (Ofer Fridman, 2017).

Gli account inclusi in questi dataset sono stati individuati a seguito delle indagini relative ai tentativi di influenza organizzati in occasione delle elezioni americane del 2016, ma la loro vita digitale non è circoscritta a quell'occasione. Questi account sono rimasti attivi per anni, prima e dopo il 2016: condividendo articoli, esprimendo opinioni, interagendo con utenti ignari. La complessità di questo panorama mostra la necessità di uno sguardo aereo nello studio delle azioni di *Information Warfare* che hanno coinvolto i profili Twitter appena menzionati. L'aspetto puramente tattico, legato alle azioni connesse all'evento elettorale statunitense, appiattisce il quadro più ampio delle dinamiche comunicative e nasconde la macrostruttura strategica entro cui le azioni svolte dai profili social sono da inquadrare.

Gli obiettivi strategici delle operazioni della Guerra Ibrida possono restare celati o incerti. Sul campo di scontro, tuttavia, gli effetti e gli strumenti utilizzati lasciano tracce misurabili. È possibile, allora, ricostruire e indagare la struttura e le dinamiche che hanno connesso, in modo più o meno celato, l'obiettivo e le operazioni intraprese dall'avversario.

Una possibile formalizzazione concettuale e, allo stesso tempo, uno strumento di osservazione e analisi delle tracce di questi campi di scontro è accessibile attraverso il costrutto delle Rappresentazioni Sociali (RS) di Serge Moscovici, già utilizzato in altri studi per descrivere il modo in cui

i grandi temi del presente vengono narrati e rappresentati[4]. Questo concetto descrive il processo di nascita e trasformazione delle idee condivise localmente tra gli appartenenti ad un (qualsiasi) gruppo sociale. Secondo Moscovici (1998, 2005), infatti, le nozioni comuni tra gli individui di una società sono in continuo cambiamento, sotto la spinta comunicativa di mutazioni endogene o esogene. La creazione e trasformazione di questi concetti condivisi avviene di continuo, attraverso dinamiche connesse di ancoraggio[5] e oggettivazione[6] delle idee. Secondo Moscovici, la RS risponde a tre macro-dinamiche comunicative interne ad un gruppo sociale: rendere familiare un elemento estraneo; favorire la creazione di un terreno di comunicazione interno e condiviso, formare una identità comune all'interno di un gruppo (Moscovici 1973, p. XIII). Secondo la definizione di Denise Jodelet (1992) la RS «è una forma di conoscenza, socialmente elaborata e condivisa, avente un fine pratico e concorrente alla costruzione di una realtà comune ad un insieme sociale» (p. 48). La RS, insomma, è il momentaneo esito concreto e non definitivo di una dinamica comunicativa intercorsa tra le parti sociali coinvolte.

Da questo punto di vista, allora, la teoria delle RS è particolarmente preziosa al fine di affrontare in modo complesso le operazioni di *Information Warfare*: permette di considerare l'azione di comunicazione al tempo stesso in quanto processo (dinamica comunicativa) e in quanto oggetto (esito).

Si pensi alla nozione collettiva di «terrorista»: è differente in relazione al gruppo sociale in cui è discussa ed è in continuo cambiamento in relazione agli eventi esterni che colpiscono il gruppo in oggetto o all'esito di dinamiche relazionali interne. La mutazione è poi ovviamente oggetto

[4] Es. su immigrazione e Islam Cinnirella, M., (2013). Think 'terrorist', think 'Muslim'? Social-psychological mechanisms explaining anti-Islamic prejudice. In *Islamophobia in the West* (pp. 193-203). Routledge.; Kilby, L. (2017). Social representations of peace in terrorism talk: A United Kingdom talk-radio analysis. *Peace and Conflict: Journal of Peace Psychology*, 23(2), 106-116.; B. Hoijer, (2011). Social Representations Theory A New Theory for Media Research, *Nordicom Review* 32 2, pp. 3-16.

[5] Un elemento ignoto o estraneo viene confrontato con un elemento noto e parte del sistema di riferimento del gruppo ricevente (es. l'Isis come «la nuova Al Qaida» oppure l'immigrazione come «contagio»). In questo modo, riceve una nuova posizione all'interno della rappresentazione condivisa in relazione alla somiglianza con un modello di riferimento.

[6] L'appropriazione di un concetto o idea attraverso la sua concreta sintesi e figurazione in un oggetto/soggetto familiare al gruppo ricevente (es. il soggetto «Trump» usato per rappresentare politiche anti-immigrazione oppure l'oggetto «11 settembre» usato per descrivere eventi particolarmente traumatici per una nazione occidentale). Attraverso un processo dialogico ancoraggio e oggettivazione trasformano costantemente le rappresentazioni in elementi familiari per il gruppo sociale di riferimento.

di spinta diacronica con possibilità di adattarsi, cambiare o anche scomparire nel corso del tempo. La definizione di terrorista, inoltre, produce impatti diretti nella realtà sociale, civile e politica degli appartenenti all'ipotetico gruppo di riferimento.

Questo studio si occupa di una porzione del campo comunicativo creato dagli account Twitter utilizzati dall'Internet Research Agency, non dell'obiettivo strategico complessivo, né di una specifica attività tattica. Obiettivo dell'analisi è la rappresentazione dell'idea di terrorismo costruita da IRA attraverso le azioni svolte dagli account individuati da Twitter. In particolare, saranno approfondite tre domande di ricerca:

1. Quali eventi mondiali sono stati i più discussi nell'azione strategica di IRA?
2. Quale performance ha registrato nel tempo l'azione comunicativa perseguita?
3. Quali *cluster* tematici è possibile identificare nei messaggi pubblicati e quali dinamiche comunicative sottintendono?

Metodologia

Il dataset

Twitter offre, attraverso una sezione dedicata del proprio blog ufficiale denominata «Elections integrity», alcuni dataset relativi a possibili attività di *Information Warfare*. Per le analisi contenute in questo studio è stato utilizzato il file relativo ai tweet della sezione: «Internet Research Agency (October 2018)». Sono a disposizione degli utenti diversi database: un elenco degli account, un elenco dei tweet pubblicati, un archivio contenente tutte le immagini e i media che sono stati condivisi da questi profili. L'analisi proposta è stata realizzata sull'intero dataset dei tweet: 8.768.633 di messaggi pubblicati tra il 2009 e il 2018 anni da 3.613 profili unici. Ciascuna riga del foglio di calcolo presenta diversi *metadata* per ciascun tweet riportato, in questo studio sono stati considerati: *time stamp* (data e ora di pubblicazione al secondo), lingua utilizzata, identificativo unico del profilo Twitter, tipologia e numero di interazioni registrate dal messaggio (like, commenti, condivisioni, menzioni esterne).

L'intero elenco dei tweet è stato filtrato sulla base del lemma «terror». In questo modo è stato possibile selezionare solamente i messaggi contenenti parole chiave rilevanti per l'analisi (terrorist, terrorism, terror attack, terror*…). Il nuovo campione ristretto è formato da 22.764 messaggi e 1.215 utenti. I tweet analizzati hanno raccolto complessivamente 463.592 retweet, 53.714 repliche, 42.241 citazioni. Twitter identifica e

cataloga automaticamente le lingue utilizzate nei messaggi. Le prime cinque lingue, per numero di contenuti, riguardano il 98,27% dei tweet analizzati. Al primo posto l'inglese con l'85,05% (19.360), seguito da tedesco (2.503; 10.99%), lingua non rilevata (225; 0,99%), italiano (198; 0,87%), francese (85; 0,37%).

Analisi descrittive

Il dataset è stato analizzato nelle sue componenti utilizzando il programma di *Data Visualization* Tableau. Attraverso differenti tipologie di analisi grafiche si sono esplorati i trend della pubblicazione dei contenuti, l'andamento delle interazioni nel tempo.

Analisi semantiche

Uno degli obiettivi dell'analisi è lo studio dell'idea di terrorismo comunicata in modo esplicito attraverso le attività social degli account Twitter individuati, così da poter poi formulare ipotesi riguardo alle dinamiche implicitamente rappresentate da questi stessi messaggi. Al fine di analizzare le occorrenze semantiche più frequenti all'interno dei tweet si è scelta la LSA (*Latent Semantic Analysis*). In particolare, è stato impiegato un metodo di studio dei contenuti impliciti (ISMOC - Implicit Symbolic Meanings in Online Content[7]). Per questo, i messaggi sono stati uniformati nella lingua utilizzata e indagati attraverso l'analisi delle co-occorrenze lessicali. Lo sguardo delle *Latent Semantic Analysis* è panoramico: non mira alla valutazione di una singola occorrenza o messaggio pubblicato, ma ad intercettare rappresentazioni sociali condivise ed implicite, trasversali all'intero corpus testuale analizzato. L'insieme dei testi è analizzato nella sua completezza, quale prodotto di un discorso collettivo condiviso da un gruppo sociale definito (gli account impegnati nelle discussioni online su un certo argomento). Si è scelto di analizzare esclusivamente i tweet in inglese, considerando la percentuale rispetto al totale dei messaggi selezionati (19.360 tweet in inglese, l'85% del totale selezionato dal lemma «terror»). Il corpus così preparato è stato processato attraverso un software di analisi lessicometrica. Le analisi eseguite hanno un doppio scopo (Caputo *et al.*, 2019)[8]:

[7] Caputo Andrea, Fregonese Chiara, Tansini Filippo (2019). "A psychological approach to big data analysis: The Implicit Symbolic Meanings in Online Content (ISMOC) method", in New Developments in Psychology Research, Nova Publishing. 2019.
[8] *Ibidem*.

1. individuazione di pattern di co-occorrenza di parole in diverse parti del corpus analizzato. Questi gruppi testuali sono isolati sulla base di similarità semantica attraverso i metodi di *clustering* o classificazione
2. raggruppare le parti simili dei testi in classi di equivalenza in modo da ottenere una mappa semantica del discorso nel suo insieme. Questo consente di rilevare le dimensioni latenti attraverso il metodo degli «assi principali» o l'analisi delle corrispondenze.

Considerando obiettivi generali e domande di ricerca si è ritenuto utile, per descrivere le unità testuali, impiegare alcune variabili ottenute dal dataset originale a cui sono state aggiunte altre voci appositamente calcolate. Ciascuna unità testuale è descritta nell'analisi lessicale da 5 variabili illustrate in *Tabella 1*:

Tabella 1

Variabile	**Modalità (Percentuale di distribuzione)**
Account Date	nine (2009; 0,098%), eleven (2011; 0,005%), twelve (2012; 0,847%), thirteen (2013; 34,886%), fourteen (2014; 28,564%), fifteen (2015; 21,586%), sixteen (2016; 11,978%), seventeen (2017; 2,035%)
Time	A (2014, 3,44%), B (2015, 28,34%), C (2016, 39,75%), D (2017, 28,20%), E (2018, 0,27%) + first (primo semestre) / second (secondo semestre)
Retweet	False (52,365 %) True (47,634%)
OutlierInt	No (99,462%) Yes (0,537%)

La variabile «account date» ha otto possibili modalità in relazione all'anno di creazione del profilo che ha pubblicato il messaggio analizzato. La variabile «time» descrive il *timestamp* di pubblicazione dei contenuti. Il *dataset* originario presenta dati temporali fino al secondo, per ottimizzare le analisi i tweet sono stati suddivisi per anno e semestre (es. Afirst = primo semestre 2014, Bsecond = secondo semestre 2015). La variabile booleana «retweet» (due modalità «Yes» e «No») descrive la tipologia del contenuto analizzato distinguendo tra messaggi creati ex novo o condivisioni di messaggi pubblicati da altri utenti. L'ultima variabile è stata calcolata appositamente: il dataset originario indica per ciascun tweet il numero di like, citazioni, repliche e retweet. Al fine di identificare valori anomali nelle interazioni registrate dai messaggi pubblicati è stata creata la variabile «outlier_int». È stato standardizzato il numero di interazioni totali per ciascun

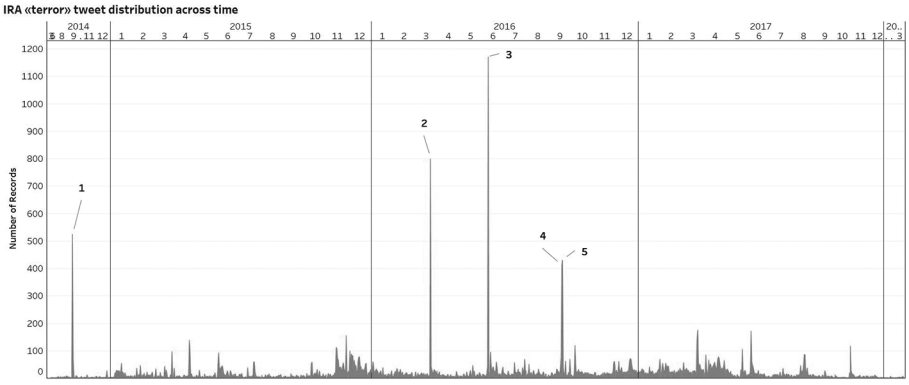
contenuto e identificati i messaggi fuori norma. Questa variabile presenta, perciò, due modalità, «Yes» e «No»[9].

Risultati

Analisi descrittive: momenti topici e argomenti salienti

Il dataset analizzato è composto da 22.764 tweet pubblicati da 1.215 account. Il numero medio di contenuti prodotti mensilmente è 455, in media 19 tweet al giorno. La frequenza di pubblicazione è stata analizzata con una risoluzione giornaliera alla ricerca di giornate *outlier*, cioè di giornate con un numero di tweet statisticamente anomalo in relazione al dataset selezionato. Sono stati così individuati 5 giorni con un numero di contenuti anomali. La complessiva distribuzione dei tweet nel corso del tempo è rappresentata nel grafico in *Fig. 1*

Figura 1



Sull'asse delle x è rappresentato il passare del tempo, con una risoluzione giornaliera, sull'asse delle y invece è rappresentato il numero di tweet registrati. Le giornate outlier emergono con chiarezza dal grafico e sono numerate da 1 a 5:

1. 11 settembre 2014, 524 tweet - Colombian Chemicals incident hoax (Z score 10,04)
2. 22 marzo 2016, 799 tweet - attentato a Bruxelles (Z score 15,53)
3. 9 giugno 2016, 1.171 tweet - tweet in tedesco su ISIS e terrorismo (Z score 22,93)

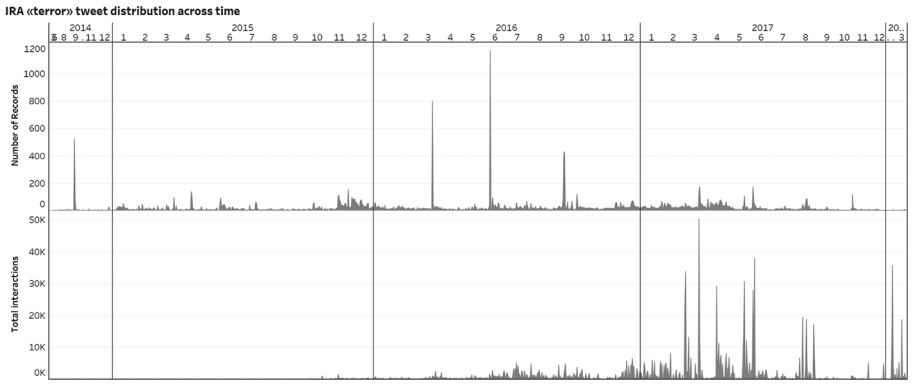
[9] Sono stati considerati anomali i messaggi con un valore di «Punto Z», relativo al totale delle interazioni registrate, superiore a 3,29. Barbara G. Tabachnick, Linda S. Fidell, *Using Multivariate Statistics*, 6th Edition, Pearson, 2013.

4. 18 settembre 2016, 430 tweet - attentato Chelsea, NYC (Z score 7,80)
5. 19 settembre 2016, 411 tweet - attentato Chelsea, NYC (Z score 8,18)

Ciascuna giornata in evidenza per la produzione di un numero anomalo di contenuti appare in risposta ad un preciso evento, unica eccezione i tweet relativi al dibattito politico in lingua tedesca, su terrorismo, Isis e rifugiati siriani.

Il dataset originario offre anche la possibilità di analizzare i tweet in relazione al numero di interazioni complessivamente raccolte, al fine di individuare momenti particolarmente virali e i contenuti di maggiore successo. In *Fig.* 2, il grafico relativo alla distribuzione dei contenuti quotidianamente pubblicati (in alto, lo stesso di *Fig.1*), è confrontato con l'andamento del totale delle interazioni registrate ogni giorno (istogramma in basso nel grafico).

Figura 2



Le scale dei due grafici sono sensibilmente differenti: nel grafico inferiore, alcune giornate arrivano a contare centinaia di migliaia di interazioni online, mentre si arrivano a pubblicare, al massimo, poco più di un migliaio di tweet al giorno in quello superiore. Inoltre, le giornate anomale per numero di contenuti presenti, non coincidono con performance particolarmente efficaci. Il grafico evidenzia un progressivo intensificarsi delle reazioni ai messaggi pubblicati dall'Internet Research Agency, con particolare efficacia ottenuta tra 2017 e 2018.

L'analisi della distribuzione delle interazioni totali raccolte giorno per giorno ha permesso di evidenziare la presenza di sedici giornate *outlier*, elencate nella *Tabella 2*

Tabella 2

Day	Month	Year	Total Interactions	Zpoints
22	Marzo	2017	50.346	14,93088
6	Giugno	2017	37.941	11,18751
15	Febbraio	2018	35.777	10,5345
4	Marzo	2017	33.833	9,947867
23	Maggio	2017	30.684	8,997615
15	Aprile	2017	29.230	8,558851
4	Giugno	2017	27.969	8,178328
3	Marzo	2017	25.151	7,327959
12	Agosto	2017	19.546	5,636576
17	Agosto	2017	18.792	5,409046
17	Marzo	2018	18.661	5,369515
27	Agosto	2017	17.222	4,935278
22	Maggio	2017	14.499	4,113576
8	Marzo	2017	13.220	3,727621
23	Marzo	2017	12.349	3,464785
26	Maggio	2017	12.117	3,394776

Per ciascuna giornata isolata in tabella, è possibile estrarre il tweet che ha ottenuto complessivamente il più alto numero di interazioni. Analizzando questo contenuto, si può ricostruire il tema più rappresentativo per il quale i profili IRA hanno registrato un numero anomalo di interazioni. Questi tweet sono organizzati nella *Tabella 3*, con data di pubblicazione, testo del tweet, dettaglio delle interazioni ricevute (il numero di tweet che citano il messaggio, il numero di repliche, il numero dei retweet e dei like ricevuti, la somma totale delle interazioni). I contenuti sono in ordine cronologico.

Tabella 3

Publish date (UTC)	Text	Retweet	Reply	Quote	Like	Total interactions
03 Mar 17	Here is Jewish bomb-threat suspect, Juan Thompson with Hillary Clinton! She must disavow the racist attacks against Jews! #LiberalTerrorism	5.548	394	605	5.021	11.568
04 Mar 17	Please RETWEET this video until @NancyPelosi steps down for lying about meeting with Russian ambassador Kislyak. #LiberalTerrorism	8.819	451	564	6.129	15.963
08 Mar 17	Islamic terrorist Linda Sarsour was just arrested outside Trump International for disorderly conduct #InternationalWomensDay #NotMyProtest	2.104	772	531	3.694	7.101
22 Mar 17	Mayor of London: "Terror attacks are part and parcel of living in a big city." Tokyo: biggest city in the world.. NO ISLAMIC TERRORISM.	6.400	1.156	759	7.596	15.911
23 Mar 17	Terrorist Khalid Masood was born in England; lived there for 52 years. Khalid Masood is a proof that a Muslim doesn't become an Englishman	1.308	198	128	1.193	2.827
15 Apr 17	Antifa terrorists threw a smoke bomb and didn't realize the wind was going their way. Probably the best thing that happened today😂 #Berkeley	4.008	621	528	6.078	11.235
22 May 17	Another day, another Muslim terrorist attack. RETWEET if you think that Islam needs to be banned RIGHT NOW! Manchester, we pray for you 🙏	3.254	1.195	2.894	3.003	10.346
23 May 17	Hey @David_Leavitt, you deleted this tweet about #Manchester terror attack. But you forgot to delete your account. Do it, please!	1.279	228	150	1.825	3.482
26 May 17	Milo destroyed @lsarsour today: "She is a sharia loving, terrorist embracing, jew hating, ticking time bomb of progressive horror."	3.954	260	241	5.967	10.422
04 Jun 17	7 more dead in London because of climate change. Oh wait, nope, it's Islamic terrorism again. #LondonAttacks	2.851	411	207	3.997	7.466

Publish date (UTC)	Text	Retweet	Reply	Quote	Like	Total interactions
06 Jun 17	Reminder: Mayor of London Sadiq Khan was a lawyer for a 9/11 terrorist Zacarias Moussaoui and has ties with Islamist movement worldwide.	13.532	1.089	1.888	9.353	25.862
12 Aug 17	RETWEET if you think that Antifa is a domestic terrorist organization!	8.310	630	734	5.260	14.934
17 Aug 17	About a week ago a horde of Moroccans landed on the beach in Spain. This week a terror attack by a Moroccan in #Barcelona.	4.597	414	437	4.124	9.572
27 Aug 17	Antifa terrorists attacking father and son in #Berkeley. No police in sight	7.808	1.729	1.935	5.666	17.138
15 Feb 18	A terrorist cell in America trained a man who killed 17 children yesterday. We don't have immigrant problem. We have WHITE SUPREMACY problem	5.502	273	149	10.849	16.773
17 Mar 18	Michael Flynn (convicted felon) gets a standing ovation at a republican fundraising event. Andrew McCabe (defended America from terrorist threats post 9/11) gets fired without a pension. This is a shining example of what the republican party has become.	6.581	1.019	655	9.937	18.192

Sette dei sedici tweet qui riportati sono relativi ad attentati terroristici compiuti al di fuori del suolo americano (6 riguardano Londra, 1 Barcellona). I rimanenti riguardano temi di politica interna americana: 4 attaccano direttamente figure pubbliche o politici statunitensi (Nancy Pelosi, Hillary Clinton, Linda Sarsour, Michael Flynn), 3 classificano il movimento politico «antifascista» come terrorista (con riferimento anche alle manifestazioni «Unite the Right» e agli scontri accaduti a Charlottesville ad agosto 2017), 1 tweet cita una sparatoria di massa su suolo statunitense (Marjory Stoneman Douglas High School).

Analisi semantiche: i temi e le dinamiche comunicative elementari

L'analisi semantica dei 19.360 tweet in inglese ha condotto all'individuazione di 5 diversi *cluster* tematici, illustrati in *Tab 4*.

Tabella 4

Cluster 1 (41,77%)		Cluster 2 (12,98%)		Cluster 3 (4,69%)		Cluster 4 (35.24%)		Cluster 5 (5,32%)	
Words	χ^2	Words	χ^2	Words	χ^2	Words	χ^2	Words	χ^2
Terrorism	1374,938	Group	1262,844	Refugee	7852,388	Attack	2377,413	Army	3648,299
Trump	597,091	List	1024,336	Welcome	864,54	Terror	1545,829	Destroy	1725,489
Radical	367,948	Organization	960,581	Pretend	805,661	News	899	Rocket	1693,977
Fight	318,007	White	766,146	Diversity	635,551	Suspect	648,525	Air	1574,175
Protect	166,662	Domestic	688,5	Enter	576,107	Police	456,592	Civilian	1229,034
President	165,473	Brotherhood	517,123	Pose	530,006	Plot	455,869	Countryside	1177,874
War	164,581	Bill	474,076	Tire	495,49	Shoot	433,401	Position	1104,622
Stop	162,86	Gun	434,41	Visa	437,643	Arrest	405,232	Kill	953,296
Call	162,442	Designate	372,052	Program	423,839	Man	399,651	Vehicle	946,431
Country	147,373	Supremacist	362,457	Lottery	324,965	Charge	396,741	Injure	884,439
Illustrative variables									
Retweet_True	131,015	Retweet_True	129,415	Time_Cfirst	574,173	Accountdate_Fourteen	638,621	Accountdate_Fifteen	1541,846
Accountdate_Sixteen	109,853	Time_Efirst	39,72	Accountdate_Thirteen	98,706	Time_Asecond	407,338	Retweet_False	281,11
Time_Csecond	69,439	Accountdate_Seventeen	27,435	Retweet_False	52,461	Time_Bfirst	171,405	Time_Cfirst	87,944
Time_Dfirst	55,869	Accountdate_Sixteen	27,406	Time_Dsecond	3,857	Retweet_False	76,31	Time_Bsecond	67,721
Accountdate_Thirteen	35,858	Time_Dsecond	23,02	Outlierint_No	3,249	Accountdate_Twelve	45,7	Time_Csecond	10,482
Time_Dsecond	20,119	Accountdate_Thirteen	19,954	Accountdate_Sixteen	1,113	Accountdate_Nine	20,231	Time_Afirst	3,073
Accountdate_Seventeen	4,787	Time_Dfirst	15,367			Outlierint_No	2,477	Outlierint_No	2,401
Time_Afirst	1,816	Outlierint_Yes	6,19			Time_Bsecond	2,226		
Outlierint_Yes	1,708	Time_Csecond	0,808						

La tabella illustra la struttura e la distribuzione dei *cluster*, elenca le 10 parole più frequenti e le variabili illustrative più associate a ciascun gruppo lessicale.

Il *Cluster 1* (41,77% del totale delle unità testuali analizzate) sembra essere formato da discussioni relative all'ecosistema politico americano (si noti in particolare la presenza delle parole: Trump, president, country) e l'impegno dell'amministrazione Trump nei confronti del terrorismo (terrorism, radical, fight, protect, war, stop). Il lemma «terror» è qui associato all'area semantica dell'estremismo islamico. Un tipico segmento testuale di questo *cluster* è rappresentato dal tweet: «**democrats** won't cheer when **trump** says he will **defeat radical** islamic **terrorism** bc most of them are **funded** by these **radicals**». Le parole più frequentemente associate al *Cluster* 2 (12,98%) sembrano riguardare discussioni relative a dinamiche interne alla società statunitense (group, list, organization, white, domestic, brotherhood, gun, supremacist). Un tweet classificato come unità testuale rappresentativa del *cluster* ne chiarisce immediatamente l'orizzonte tematico: «**White House** rejects **petition** to **designate black lives matter** as a **terrorist group**». Il *Cluster* 3 (4,69%) sembra raccogliere messaggi relativi all'integrazione e all'accoglienza di profughi, così come ben rappresentato dalle parole più frequentemente associate a questo gruppo: refugee, welcome, pretend, diversity, enter, pose, tire, visa, program, lottery. Si tratta di discussioni a proposito di immigrazione e integrazione (diversity) e dei potenziali rischi ad essa connessi (pretend, pose). I testi tipicamente associati alla parola «refugee», la più frequente del *cluster*, illustrano con efficacia il *framing* costruito dagli account di IRA attorno a questo tema: «**terrorists penetrated** Paris also **pretending** to be **refugees** we must **prevent** it from happening #islamkills». Il quarto *cluster* raccoglie il 35,24% dei contenuti analizzati. Le 10 parole più rappresentative sono coerenti tra loro e sembrano indicare commenti e discussioni in occasione di attacchi terroristici: «attack, terror, news, suspect, police, plot, shoot, arrest, man, charge». Questa ipotesi è supportata dallo studio dei segmenti testuali tipici (ad esempio, «London **terror attack** 7 **victims killed** 3 **suspects shot dead** by **police**») e dalla lista delle forme testuali rilevate nel corso dell'analisi. Qui, compaiono parole chiave relative ad alcuni dei principali incidenti degli ultimi anni (Columbian chemicals[10], Paris, London, Boston, Belgium, French,

[10] Evento noto alle cronache per un procurato allarme, partito proprio da alcuni profili Twitter: l'11 settembre 2014 cominciarono a circolare via Social Network e Web messaggi e fotografie con notizie relative all'esplosione di un impianto chimico a Centerville, St. Mary Parish, Louisiana. La notizia era totalmente inventata. È passata alle cronache come

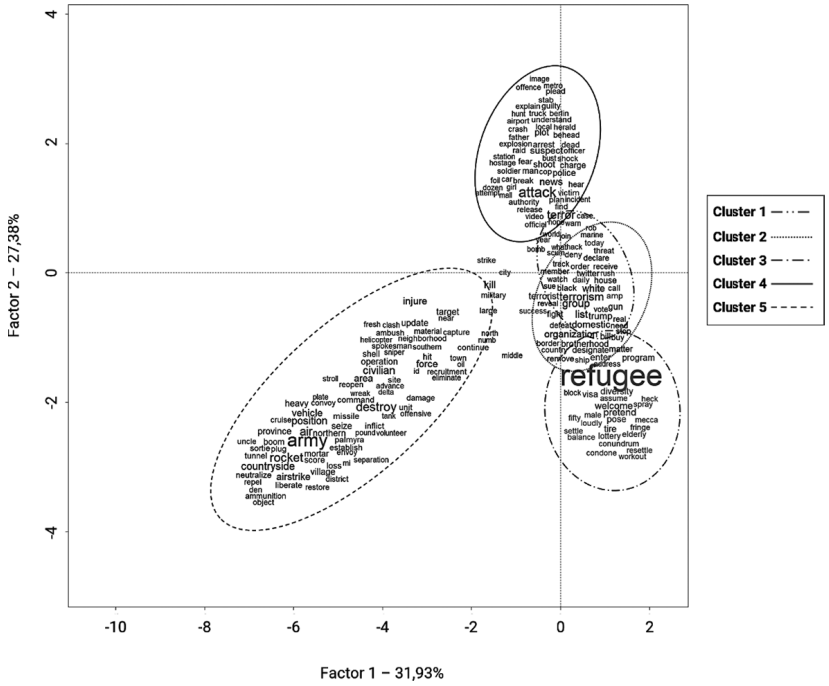
Westminster, Orlando, Belgian, California, Minnesota, Prayforbrussels, Stockholm). Il quinto ed ultimo *cluster* individuato riguarda il 5,32% dei tweet, le parole chiave più frequenti evocano una situazione di conflitto armato con perdite e feriti: army, destroy, rocket, air, civilian, countryside, position, kill, vehicle, injure. I segmenti testuali tipici aiutano ad identificare con più precisione questi contenuti: «syrian **army** and russian **air force kill terrorists leaders destroy** their **vehicles** and **positions**». Il lemma «terror» è identifica i terroristi coinvolti negli scontri in Siria.

Le variabili illustrative associate più frequentemente a ciascun *cluster* approfondiscono ulteriormente la comprensione della rappresentazione del terrorismo proposta. Facendo riferimento alla seconda parte della tabella 2, è possibile notare alcune differenze significative tra i vari gruppi emersi. Il *Cluster 1* presenta un numero significativo di retweet, i contenuti qui presenti sono stati pubblicati durante il secondo semestre del 2016 e il secondo del 2017 e condivisi da account creati nel 2016, 2013 e 2017. Anche il *cluster numero 2* condivide la presenza di retweet, con contenuti pubblicati tra primo e secondo semestre del 2017 da account creati nel 2013, 2016 e 2017. A differenza del primo, in questo secondo gruppo si concentrano anche gli *outlier* delle interazioni, ossia messaggi caratterizzati da un numero anomalo di interazioni. Il *cluster* 3 è composto da contenuti pubblicati nel primo semestre del 2016 e nel secondo del 2017 da account creati nel 2013. Tra il secondo semestre del 2014 e tutto il 2015 si registra la presenza di contenuti legati al *cluster numero 4*. Si registra anche una particolare presenza di account creati nel 2009, 2012 e 2014. L'ultimo gruppo testuale vede una concentrazione di contenuti del secondo semestre del 2015 e secondo semestre del 2016, pubblicati soprattutto da account Twitter creati nel 2015.

La distribuzione dei *cluster* su piano cartesiano (Fig.3) secondo i fattori 1 e 2, rappresenta il 59,31% dei contenuti analizzati. Considerando il fattore 2, si evidenzia una contrapposizione netta del *cluster* 4 rispetto a tutti gli altri, mentre si oppongono i *cluster* 1-2-3 al *cluster* 5 in relazione al fattore 1.

"Columbian Chemical Hoax". Wikipedia consultata online: https://en.wikipedia.org/wiki/Columbian_Chemicals_Plant_explosion_hoax aprile 2019.

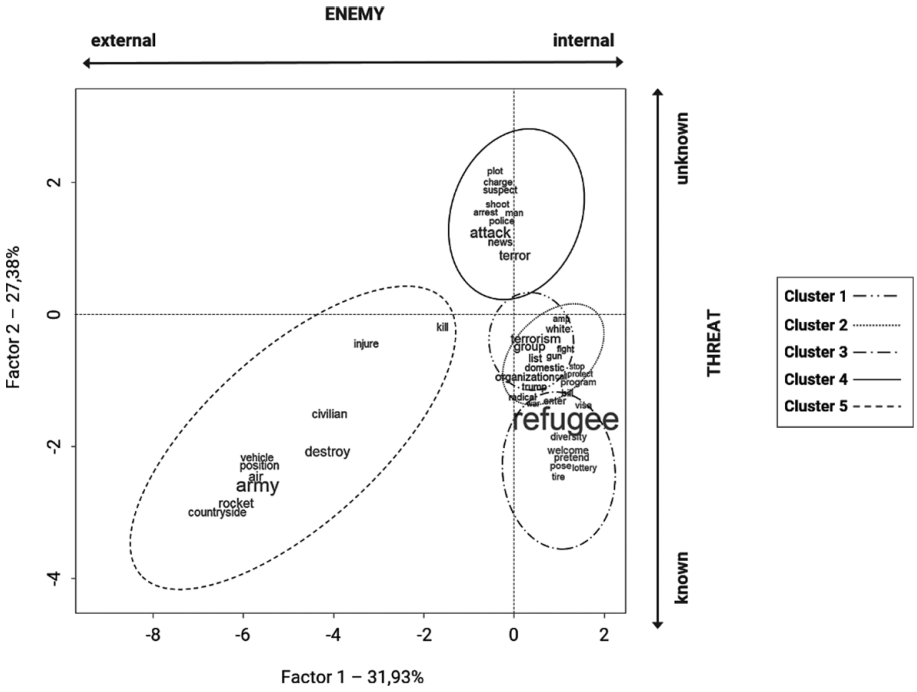
Figura 3



Le rappresentazioni implicite veicolate trasversalmente durante gli anni di attività da parte degli account analizzati cambiano in relazione all'oggetto della comunicazione. La rappresentazione del «terrore» assume diverse connotazioni nei testi analizzati. Il significato associato dagli account Twitter ai diversi temi, di volta in volta dato per scontato, costruisce progressivamente la possibilità di influenzare il modo in cui gli ignari partecipanti alle discussioni intendono concetti a loro familiari. Questo è precisamente uno degli obiettivi legati ad una operazione di disinformazione (John D. Gallacher *et al.*, 2019)[11]. Nel caso dei contenuti analizzati, la distribuzione dei *cluster* nello spazio fattoriale, in relazione ai diversi macro-temi rappresentati, può essere descritta come esito relazionale tra dinamiche comunicative contrapposte: minaccia esterna / minaccia interna (lungo l'asse orizzontale); nemico noto / nemico ignoto (lungo l'asse verticale) visualizzata in figura 4.

[11] «This difference between the IRA's activities spreading division abroad and cohesion at home can be further demonstrated by comparing how the organisation's Twitter activity in English and Russian responded to real-world events, such as terror attacks, political protests, and international military conflicts». John D. Gallacher e Rolf E. Fredheim (2019), *Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home*, in «Responding to cognitive security challenges». Riga: NATO STRATCOM, p. 73.

Figura 4



La minaccia può essere nota ed esterna, ad esempio nelle discussioni a proposito della guerra ai «terroristi» in Siria. Uno scontro tra attori specifici, in una terra lontana da quella degli interlocutori. All'opposto dell'asse orizzontale, il nemico può essere noto e domestico, così come rappresentato dai messaggi a proposito dei movimenti sociali statunitensi e alle politiche interne decise dal Presidente Trump. Interessante, in questo gruppo tematico, il *Cluster* 3 relativo ai «refugee». La comunicazione rappresenta una minaccia interna in senso geografico (gruppi sociali infiltrati nella società ospitante) e in senso figurato (la minaccia è legata al pericolo della dissimulazione e dell'inganno). I «refugee» sono discussi come minaccia interna ed esplicita: la rappresentazione condivisa è quella di un nemico interno di cui è già nota la traiettoria, attraverso l'inganno, verso il terrorismo. Il destino, insomma, è già segnato e rappresentato, nelle discussioni del *Cluster* 3, come scontato.
A questo orizzonte di minacce conosciute si contrappone l'attività comunicativa perseguita in occasione degli attentati internazionali: azione opportunistica tutta giocata sul registro della minaccia ignota, rappresentata dal *Cluster* 4. La rappresentazione veicolata da questi testi costruisce una precisa immagine degli attentati: quella del terrore minaccioso, imprevedibile e inarrestabile.

Discussione e conclusioni

Dallo studio dei risultati proposti, possono essere elaborate alcune considerazioni in risposta alle domande di ricerca che hanno guidato lo studio delle rappresentazioni implicite veicolate dalla comunicazione di account Twitter controllati dalla Internet Research Agency. L'analisi della distribuzione dei contenuti selezionati ha evidenziato 5 picchi di attività nella produzione di contenuti (domanda di ricerca 1). Il numero medio di contenuti prodotti giornalmente e mensilmente mostra come l'argomento del terrorismo sia un tema costantemente presente nel corso del periodo analizzato, presidiato e utilizzato soprattutto in modo opportunistico in relazione a specifici eventi. In occasione di alcuni incidenti terroristici internazionali, infatti, i profili si sono attivati producendo un numero anomalo di contenuti o provocando un numero anomalo di interazioni. In entrambi i casi, l'attività comunicativa segna una differenza rispetto alla normale routine. Lo studio della distribuzione dei contenuti prodotti mostra anomale attività in occasione di momenti ben definiti: il caso del «Columbian Chemicals accident» e l'attentato a Chelsea (NYC), il tentativo di inserirsi nel dibattito politico interno di un paese estero (tweet in tedesco su ISIS e terrorismo), i tweet pubblicati durante gli attentati a Bruxelles (22 marzo 2016). In quest'ultima occasione i tweet sostennero e accentuarono la diffusione degli hashtag #islamkills e #stopislam, entrati in breve tempo nella classifica *Trend Topic* a livello mondiale.

Se si analizzano i migliori tweet per *engagement*, il panorama tematico è analogo a quello evidenziato precedentemente (domanda di ricerca 2). Si dividono quasi equamente gli argomenti principali delle sedici giornate con un numero anomalo di interazioni: 9 relative alla politica interna statunitense, 7 in reazione a incidenti terroristici internazionali. Il tweet con engagement più elevato dell'intero dataset è quello pubblicato pochi giorni dopo l'attentato del 3 giugno 2017 a Londra («Reminder: Mayor of London Sadiq Khan was a lawyer for a 9/11 terrorist Zacarias Moussaoui and has ties with Islamist movement worldwide»). Lo studio dei tweet pubblicati in occasione degli incidenti terroristici internazionali mostra una interessante capacità reattiva degli account analizzati. Si prenda, ad esempio, i tweet pubblicati in occasione dell'attentato di Londra del 22 marzo o del 22 maggio 2017 a Manchester. Entrambi sono stati pubblicati a distanza di poche ore dagli eventi: il primo alle 18.12 del 22 marzo («Mayor of London: "Terror attacks are part and parcel of living in a big city." Tokyo: biggest city in the world... NO ISLAMIC TERRORISM»), il secondo addirittura alle 22.22 del 22 maggio 2017 («Another day, another Muslim terrorist attack. RETWEET if you think that Islam needs to be banned RIGHT NOW! Manchester, we pray for you»), entro un'ora dallo svolgersi degli eventi. Questo dimostra la volontà e capacità operativa di reagire con immediatezza

anche ad eventi imprevisti, così da approfittare e partecipare alle discussioni durante le prime fasi degli incidenti, con evidente vantaggio comunicativo e strategico dato dalla possibilità di partecipare e influenzare la creazione del *framing* degli eventi (John D. Gallacher *et al*., 2019)[12].

Lo studio delle interazioni ottenute dai tweet pubblicati segna, con il passare degli anni, una crescente efficacia dei contenuti pubblicati. Tra le ipotesi possibili per spiegare questo fenomeno: una migliore performance legata al consolidarsi della rete sociale organica (utenti reali) attorno profili IRA, un cambio nella strategia comunicativa (tra le possibilità: intervento opportunistico in occasione di eventi controversi, hashtag hijacking,...), utilizzo di tecniche non ortodosse o lecite per aumentare l'engagement e rendere più visibili i messaggi (es. utilizzo di account controllati o botnet per interagire con i messaggi da diffondere e rendere più visibili).

L'analisi semantica ha messo in luce la presenza di alcune dinamiche elementari, lungo i cui assi è possibile riordinare l'intero progetto comunicativo analizzato (domanda di ricerca 3). I contenuti studiati esprimono differenti gradazioni della minaccia terroristica in relazione a due variabili: la posizione del nemico rappresentato (interno / esterno), la possibilità di conoscerne le azioni (minaccia nota / ignota). All'interno di questo campo di forze contrapposte, emergono cinque differenti *cluster* tematici, cinque diversi modi di esprimere le possibili combinazioni delle dinamiche appena rilevate. L'azione del presidente Trump contro il terrorismo (pericolo interno / noto), la descrizione del pericolo sociale interno al paese a causa di gruppi politici o sociali caratterizzati come «terroristici» (interno / noto), il ruolo dei «refugee» (minaccia interna e nota), la guerra ai terroristi in Siria (nemico esterno e noto), il dramma degli attentati terroristici internazionali (minaccia ignota).

Questi gruppi tematici sono caratterizzati dalla presenza di variabili illustrative grazie alle quali è possibile formulare alcune ipotesi sulle caratteristiche operative degli account impegnati nelle attività di comunicazione. Il *cluster* tematico 5 (5,32% del totale) è composto soprattutto da contenuti relativi alla guerra siriana. Le variabili, caratteristiche di questo *cluster*, descrivono una presenza specifica di contenuti pubblicati nel secondo semestre 2015 e nel secondo semestre 2016, da account creati nel 2015. Questo è l'unico *cluster* in cui

[12] Da confrontare con le conclusioni simili raggiunte nel già citato studio John D. Gallacher e Rolf E. Fredheim (2019), *Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home*, in «Responding to cognitive security challenges». Riga: NATO, STRATCOM. In particolare a pp. 77-78: «Our research demonstrates that IRA activity was notably divisive in English, but showed a very different pattern in Russian. It did not seek to promote Russian interests or Russia's standing as a state directly, but instead sought to sow discord in overseas populations and drive groups apart. These efforts may well have been successful».

questi account compaiono: questo elemento potrebbe essere spiegato da una «specializzazione» di questi account. Potrebbero essere stati creati proprio per essere impiegati nella diffusione di contenuti relativi al conflitto siriano durante il 2015 e da allora aver mantenuto una specificità tematica. In modo analogo, il quarto *cluster* relativo agli assalti terroristici, presenta due specificità: la presenza di account creati in alcune annate che ricorrono solo in questo gruppo (2009, 2012, 2014) e la presenza di contenuti pubblicati tra la fine del 2014 e l'inizio del 2015. Anche in questo caso, una spiegazione possibile è la specializzazione di alcuni account nella trattazione di un tema specifico come quello degli attentati. Una ulteriore ipotesi potrebbe essere formulata osservando la specifica concentrazione in questo *cluster* di contenuti relativi a fine 2014 e di account creati proprio in quell'anno. A questo si può aggiungere la presenza delle parole: «Columbian Chemical» (l'operazione «Columbian Chemical Hoax», avvenuta proprio a settembre 2014). Una possibile spiegazione per l'assetto delle variabili illustrative del *Cluster* 4 potrebbe riguardare la presenza di account creati o utilizzati per costruire l'elaborato allarme inventato per l'inesistente esplosione nell'impianto chimico Columbian Chemical. In un secondo tempo, gli stessi account potrebbero essere stati reimpiegati nel dibattito pubblico in occasione di incidenti terroristici.

Anche in questo caso, insomma, una possibile spiegazione dei dati rilevati descriverebbe una struttura organizzativa degli account Twitter IRA con una specializzazione dettata da una logica di tipo tematico.

Limiti

Questo studio presenta alcune limitazioni relative alle caratteristiche intrinseche del dataset analizzato. Non è possibile valutare e perciò formulare ipotesi sulle caratteristiche dell'engagement ottenuto dai messaggi pubblicati poiché isolati ed eliminati da Twitter. Sono stati forniti i dati numerici delle diverse tipologie di interazioni, tuttavia, non è possibile stabilire se si tratti di interazioni organiche o di performance inflazionate in modo artificiale.

La natura avulsa dal resto dell'attuale rete sociale non permette di esplorare le dinamiche create dalla pubblicazione dei messaggi: si tratta di una fotografia isolata, un panorama artificiale estrapolato dall'ecosistema di riferimento. Un ambiente originariamente costituito non solo da questi account manipolati, ma anche dagli utenti comuni e animato dalle dinamiche evolutive della comunicazione digitale. Le caratteristiche artificiali del sistema analizzato obbligano ad uno studio statico, slegato dagli effetti e dalle dinamiche risultanti. Rappresenta, perciò, solo una parte del complessivo quadro comunicativo organizzato dalla Internet Research Agency.

Implicazioni pratiche

Lo studio delle rappresentazioni sociali legate al terrorismo ha mostrato alcuni elementi di cui tenere conto in un'ottica di contrasto ad operazioni di *Information Warfare*. La capacità operativa dimostrata in occasione degli incidenti terroristici mostra una notevole agilità organizzativa e capacità di reagire rapidamente agli eventi. In casi analoghi, istituzioni e forze pubbliche di riferimento per i cittadini dovrebbero avere la capacità di presidiare con analoga velocità e autorevolezza il campo delle opinioni digitali, così da mitigare la possibilità di inquinamento del panorama informativo. Diventare il punto di riferimento autorevole online per i cittadini è un'operazione complessa e con tempi di implementazione dilatati per qualsiasi istituzione. Il presidio del dominio digitale richiede preparazione preventiva, azioni costanti, capacità di risposta rapida e monitoraggio attivo.

Future linee di ricerca

Il risultato di questo studio non è la definizione delle motivazioni strategiche che hanno guidato le azioni analizzate. L'analisi ha esplorato le dinamiche comunicative relative al terrorismo, così come rappresentate nel corso di una operazione di *Information Warfare* durata cinque anni. La scelta del lemma «terror» racchiude un orizzonte parziale e limitato: questo è utile al fine della costruzione di una prima attività esplorativa che potrebbe, in futuro, essere sviluppata anche in senso più generale. Dal presente studio, emerge un profilo complesso dell'operazione di comunicazione strategica impostata: si sono alternati momenti di presenza costante a basso regime a momenti di performance anomale in grado di incidere significativamente anche a livello mondiale. Un panorama tematico altrettanto complesso si dispiega secondo due archetipi basilari: la minaccia nota o ignota, il nemico interno o esterno. Individuare tempestivamente le dinamiche elementari lungo cui si sviluppa un'azione di *Information Warfare* può costituire il primo passo di una complessa azione di mitigazione degli effetti.

Analisi con metodologia analoga possono essere estese a temi di più ampio respiro, al fine di indagare i messaggi implicitamente diffusi nel corso degli attacchi, le linee di forza perseguite, i feedback attivi prodotti dalla popolazione. Uno studio delle dinamiche profonde può consentire di scalare le azioni di contrasto dal piano tattico verso quello strategico; dall'inefficace *debunking* dei singoli casi (Zollo *et al.*, 2017)[13], elevare l'azione al fine di contribuire ad una migliore resilienza delle dinamiche sociali sotto attacco.

[13] Fabiana Zollo, Alessandro Bessi, Michela Del Vicario, Antonio Scala, Guido Caldarelli, Louis Shekhtman, Shlomo Havlin, and Walter Quattrociocchi. 2017. "Debunking in a World of Tribes". PLOS ONE. 12, no. 7.

Bibliografia

B. Hoijer, (2011). Social Representations Theory A New Theory for Media Research. *Nordicom Review* 32: 2, 3-16.

Caputo A., Fregonese C., Tansini F. (2019). A psychological approach to big data analysis: The Implicit Symbolic Meanings in Online Content (ISMOC) method. In: Grove L.E., a cura di, *New Developments in Psychology Research*, Nova Publishing.

Chen A. (2015). "The Agency", The New York Times Magazine. Link: https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Cinnirella, M., (2013). Think 'terrorist', think 'Muslim'? Social-psychological mechanisms explaining anti-Islamic prejudice. In: Helbling M, a cura di, *Islamophobia in the West*. Routledge.

Cullen P.J. e Reichborn-Kjennerud E., a cura di (2017). *Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, MCDC consultato online al link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Fridman O., (2017). Russian Perspective on Information Warfare: The Conceptual Roots of the Politicisation of "Information Warfare" in the Russian Academic, Political and Public Discourses', *Defence Strategic Communication*, 2.

Gallacher J.D. e Fredheim R. E. (2019). Division Abroad, Cohesion at Home: How the Russian Troll Factory Works to Divide Societies Overseas but Spread Pro-Regime Messages at Home, *Responding to cognitive security challenges*, Riga: NATO STRATCOM.

Graham R. (2018). *How to irregular cyber warfare*, https://blog.erratasec.com/2018/10/how-to-irregular-cyber-warfare.html

Hartmann U. (2017). *The Evolution of the Hybrid Threat,and Resilience as a Countermeasure*. Rome: Nato Defense College.

Jodelet D. (1992). *Le rappresentazioni sociali*. Napoli: Liguori Editori, p. 48

Kilby, L. (2017). Social representations of peace in terrorism talk: A United Kingdom talk-radio analysis. *Peace and Conflict: Journal of Peace Psychology*. 23: 2, 106-116.

Moscovici, S. (1973). Foreword. In C. Herzlich (Ed.), *Health and illness: A social psychological analysis* (pp. 9–14). London, United Kingdom: Academic Press.

Moscovici, S. (1998). The history and actuality of social representations. In U. Flick (Ed.), *The psychology of the social* (pp. 209–247). Cambridge, United Kingdom: Cambridge University Press.

Moscovici, S. (2005). *Le rappresentazioni sociali* [Social representations]. Bologna, Italy: Il Mulino.

Tabachnick B.G., Fidell L.S. (2013), *Using Multivariate Statistics*, 6th Edition, Pearson.

Tenenbaum E., (2015). *Hybrid Warfare in the Strategic Spectrum: An Historical Assessment*. In Lasconjarias G. e. Larsen J.A., a cura di, *Nato's response to Hybrid Warfare*, NATO Defense College, link: https://www.files.ethz.ch/isn/195405/fp_24.pdf

Zollo F., Bessi A., Vicario M., Scala A., Caldarelli G., Shekhtman L., Havlin S., e Quattrociocchi W. (2017). "Debunking in a World of Tribes". *Plos One*. 12, no. 7.

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-540-7

Euro 20,00