,

LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Department of Political Science

Major in Politics, Philosophy and Economics

Chair of International Relations

TERRORIST INFORMATION OPERATIONS IN CYBERSPACE.

THE ISIS CASE: FROM DABIQ TO RUMIYAH

Thesis Supervisor

Prof. Raffaele Marchetti

Candidate

Elettra Pelino

Student no. 078792

ACADEMIC YEAR 2017/2018

THIS PAGE IS INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

INTRODUCTION

The Information Age has witnessed an unrelenting growth of the Internet both in its traffic and topology[1]. The Internet of Things, connecting 8.4 billion devices as of February 2017 (Gartner, 2017), is expected to evolve into the more ambitious Internet of Everything, a concept conceived by CISCO and defined as "*the networked connection of people, process, data and things*" (CISCO, 2013, 1). Therefore, growing connections will cause the cyber domain to expand its value. Nowadays, cyberspace serves as the backbone underpinning social networking platforms, business engines, critical services, command and control warfare and the global economy. Moreover, its ability to allow for the storage and uninterrupted flow of information makes cyberspace vital for intelligence communities. In short, the cyber domain has successfully penetrated all the components of national power: Diplomacy, Information, the Military and the Economy (DIME).

As cyber dependency permeates our everyday lives and the physical and virtual worlds converge, our vulnerability to attacks that may engender radical and inevitable systemic shocks is enhanced.

Thus, a plethora of new challenges emerges, that alters the landscape of national security in a profound way. The traditional threat spectrum has been broadened to encompass cyber attacks, which, according to the 2018 Global Risks Report released by the World Economic Forum, are rated as one of the top five global risks by perceived likelihood. As a matter of fact, risks stemming from cyber threats have intensified in 2017, causing considerable economic damage, geopolitical tensions and widespread loss of trust in the Internet. Businesses have been subject to cyber breaches whose occurrence has almost doubled in five years, from 68 per business in 2012 to 130 per business in 2017 (Richards, LaSalle, Devost, van den Dool, Kennedy-White, 2017). Having been hampered by law enforcement successes in 2010–2012, "dark net" markets for malware goods and services have experienced a rebirth: in 2016 alone, 357 million new malware variants were released (Kessem, 2017).

[1] By the Internet topology we mean the arrangement of the physical network, including its nodes and connecting lines

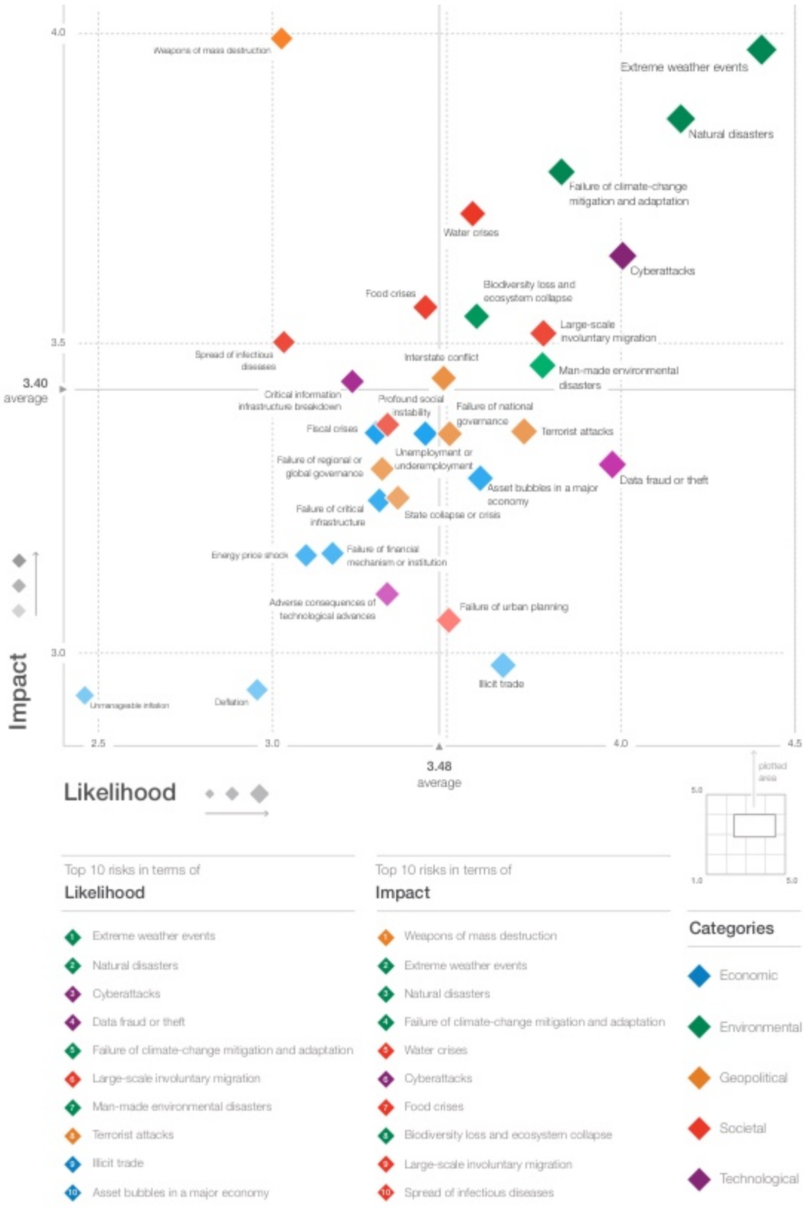


Fig. 1: The Global Risks Landscape 2018

Source: World Economic Forum (2018) *The Global Risks Report 2018, 13th Edition* [Online] Available from: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [7/06/2018]

Furthermore, recent cyber attacks have revealed a common denominator in targeting critical and strategic infrastructures sustaining a State's economy, health and safety, such as government ministries, railways, banks, telecommunications providers, energy companies, car manufacturers and hospitals (WEF). In impairing the functioning of assets that are vital to the continuity of services on a national scale, cyber attacks hold tremendous potential for delivering the same consequences of traditional, kinetic attacks. Above all, the complexity and unpredictability of cyber attacks, together with questions of speed and attribution, heighten the threat and make them an "unknown unknown", that is, " *the ones we don't know we don't* *know*" (Rumsfeld, 2002).

The emergence of cyberspace as a peculiar battlefield where actions can be undertaken instantaneously, globally and anonymously has produced new ways to advance state interests, through covert mechanism of coercion and influence in domestic political or economic affairs that might be regarded as acts of aggression if pursued by other means. Army Maj. Gen. Ashley Jr., the Director of the US Defense Intelligence Agency, called attention to the wide array of actors that might be empowered by "*the democratization of cyber capabilities worldwide*[1]" (Ashley, 2018). In fact, both States and violent non-state actors such as terrorist groups are increasingly drawing on cyber venues to alter the policy positions of other actors to their advantage.

States exploit the anonymity guaranteed by cyberspace to carry out operations aimed at achieving political utility, by swaying public opinion and politics in other states. In other words, States may apply cyber to the traditional DIME instruments of power owned by a State to manipulate conditions in the international system to their advantage. For instance, Russia has signaled that it intends to boost and refine the offensive as well as the defensive cyber capabilities of its armed force. Such confident cyber posture reflects the willingness to integrate cyberwarfare into a grand framework capable of achieving political objectives and is indicative of the strategy of the "weaponization of information".

Terrorists too take advantage of the asymmetric character of cyberspace, as they strongly rely on social networks to indoctrinate, spread news, fundraise, recruit and mobilize fighters. ISIS is the first terrorist group to have operationalized social media, drawing attention to itself by virtue of its propaganda, and has undertaken an evolution from territorial to ideological, cyber-based threat (from Physical to Virtual Caliphate). Thus, it is likely that the cyber domain will provide fertile ground for its ideological apparatus.

This research aims to analyze the impact of 'cyberization' of international relations and of information age on the new global terrorist threats.

Chapter 1 provides a general definition of the cyber domain, underlining its distinguishing features as a novel battlefield and exploring its political use by a plethora of actors. Chapter 2 reconstructs the activities in which terrorists engage within cyberspace. Chapter 3 delves into the information strategy designed by ISIS that carefully parallels and supports its military strategy, as shown by the evolution in the narrative of ISIS's magazines, Dabiq and Rumiyah, in light of territorial loss. ISIS has been selected as a case study because it presented itself as a state with a global political project, as opposed to the localized projects of rival jihadist groups, and as a "*powerful vanguard movement capable of delivering victory and salvation*" (Gerges, 2014, 342). Therefore, it gained an information momentum able to cut across economic classes, borders and ethnicities.

1. THE “CYBERIZATION” OF INTERNATIONAL RELATIONS: CYBERPOLITIK

> “*The realpolitik of the new era is cyberpolitik, in which the actors are no longer just states, and raw power can be countered or fortified by information power.”*
>
> David Rothkopf[2]

1.1 The unique domain of cyberspace

The term “cyber” has its roots in the Greek word κυβερνητικός- meaning skilled in steering (EastWest Institute and the Information Security Institute of Moscow State University, 2014). In the aftermath of World War Two, Wiener coined the term “cybernetics” to refer to “*the scientific study of control and communication in the animal and the machine*” (Wiener, 1948). Drawing on the notions of cybernetics and space, and foreseeing the global interconnectedness of systems and operators, Gibson conceived and portrayed cyberspace as *”a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding*” (Gibson, 1984, 69).

In 1969, the United States Department of Defense laid the foundation for a modest connection of a few computers called ARPANET, a pioneering network aimed at transferring digital resources, and in 1972 the codes for exchanging data (TCP/IP) were created to constitute an embryonic Internet capable of sharing packets of digital information. The domain name system of Internet addresses and the first computer viruses can be traced back to 1983. The World Wide Web came into being in 1989 and, simultaneously, businesses started using the new technology to ship production and procurement in complex global supply chains. Only recently has there been the bandwidth and server farms to sustain “cloud computing” in which companies and individuals can store their data and ware on the Web. Finally, ICANN (the Internet Corporation for Assigned Names and Numbers) was formed in 1998 (Nye, 2010).

The information revolution facilitated by Information and Communications Technologies (ICT) has paved the way for a paradigm shift in military affairs and capabilities. Warfare of the 21st century involving parties possessing even a modicum of modern technology would not be possible without access to cyberspace. Thus,

[2] Brantly, A., F. (2016) *The decision to attack: military and intelligence cyber decision-making.* Athens: University of Georgia Press

by virtue of its capacity to enable present-day warfare, as regards navigation, strike precision, communication and information gathering, cyberspace has become a crucial battlefield for global power in the 21st century. The Department of Defense (DoD) defines cyberspace as "*a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*" (DoD, 2016, 3). It results that cyberspace has been identified as the fifth domain along with land, sea, air, and space and it has been officially recognized as such by NATO in 2016 (Marchetti, Mulas, 2017).

Due to its pervasiveness, cyberspace has far-reaching implications across domains, yet it is qualitatively different from the other global commons. The unique character of cyber lies in "*the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infra-structures*" (Kuehl, 2009, 28). Thus, cyberspace is a manmade, replicable product that could not exist without the exploitation of the energies and properties of the electromagnetic spectrum (EMS). Kuehl's definition also makes information central to our understanding of cyberspace. In fact, with the advance of the information revolution and the expansion of its policy implications, information has been converted into a strategic resource and a "*fourth dimension of national power*" (Arquilla, Ronfeldt, 1997, 419) on which the political, economic and military components of a state's grand strategy rely to realize their power potential.

Within cyberspace, the classical constraints of time, space and distance are dramatically reduced. Conventional temporality is replaced with near instantaneity, geographical and organizational boundaries are overcome and jurisdictions are penetrated. Unlike the other four domains, cyberspace is not geographically bounded but increases in value and size with every new connection. On the other hand, it clearly follows that a disruption in the connections that link us to the domain can deeply affect our lives, causing the fifth domain to be more vulnerable compared to land, sea, air and space (Brantly, 2016).

Anonymity and by extension attribution represent two valuable aspects of cyber domain reinforcing the Clausewitzian fog of war, with the former playing a pivotal role for cyber offense - the execution of covert operations aimed at attaining a strategic or tactical objective without undermining a state's legitimacy- and the latter for cyber defense – the hampering of mechanisms of responsibility, as identity of actors and links to actions are obscured. As Edwards, Furnas, Forrest and Axelrod (2017), assigning blame for an attack or intrusion is made arduous by both technical factors and lack of agreement on basic definitions (e.g., what constitutes an attack or what counts as critical infrastructure). Moreover, the asymmetry inherent in the fifth domain, together with the low barriers to entry, grant non-state actors, small states and private individuals a significant role in the political stage at limited cost levels (Nye, 2011).

The permeating nature of cyberspace is such that the strategic effect of operations conducted in the domain is exponential when compared to the other domains. Through interdependence and interconnection with society, economy, technology and politics, cyberspace can enable single actors or states to produce, with a single event, "pathogenic" effects on the entire international system, as illustrated by the 2017 WannaCry computer virus. The latter marks a breakthrough in the scope and impact of ransomware, as it spread globally and with unprecedented speed, affecting, among others, automobile factories in France, the Russian Interior ministry, the FedEx in the United States and the National Health Service in the United Kingdom (Groll, 2017).

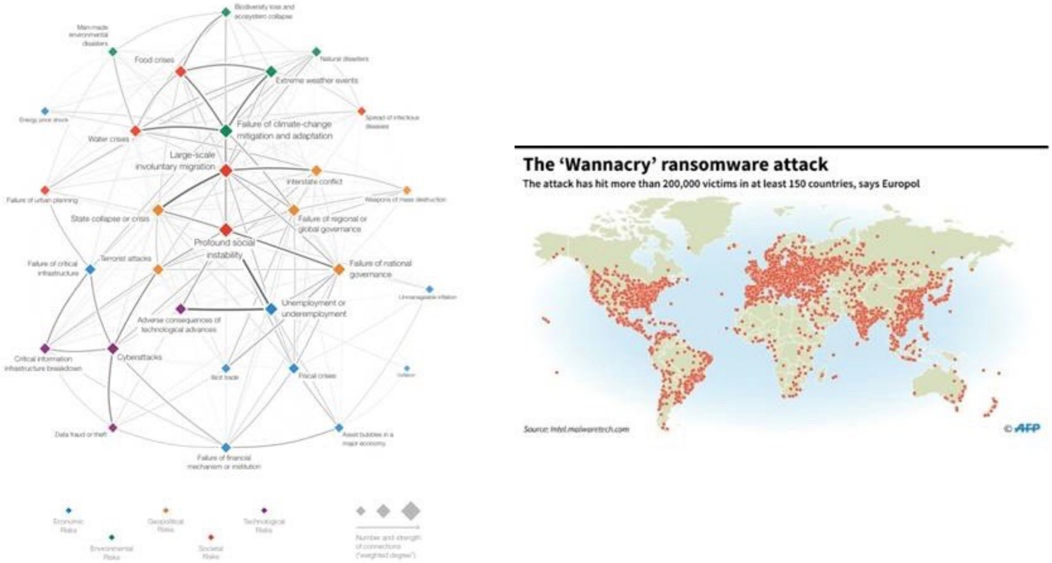

Biodiversity loss and ecosystem collapse
Man-made environmental disasters
Food crises
Natural disasters
Extreme weather events
Energy price shock
Spread of infectious diseases
Water crises
Failure of climate-change mitigation and adaptation
Large-scale involuntary migration
Interstate conflict
Failure of urban planning
Weapons of mass destruction
State collapse or crisis
Failure of regional or global governance
Profound social instability
Failure of critical infrastructure
Terrorist attacks
Failure of national governance
Unmanageable inflation
Adverse consequences of technological advances
Unemployment or underemployment
Critical information infrastructure breakdown
Cyberattacks
Illicit trade
Fiscal crises
Deflation
Data fraud or theft
Asset bubbles in a major economy
Failure of financial mechanism or institution
Economic Risks
Environmental Risks
Geopolitical Risks
Societal Risks
Technological Risks
Number and strength of connections ("weighted degree")
The 'Wannacry' ransomware attack
The attack has hit more than 200,000 victims in at least 150 countries, says Europol
Source: intel.malwaretech.com
© AFP

Fig.2: Left: cyber attacks and their links in the Global Risks Interconnection Map 2018.

Source: World Economic Forum Global Risk Perception Survey 2017-2018

Right: The 'Wannacry' ransomware attack seen in a graphic on May 14, 2017

Source: intel.malwaretech.com

Clark (2010) proposed a layered model of cyberspace combining physical and virtual properties and composed of:

1) the physical network coinciding with the hardware and empowering the cyber playing field;

2) the logical network supporting the platform nature of cyberspace and enabling services;

3) the information content stored, transmitted or transformed;

4) the cyber *persona* interacting in cyberspace.

The combination of these layers, functions and entities is actively framing cyberpolitics in international relations, turning cyberspace into a novel theatre that provides users with opportunities for competition and conflict. Accordingly, cyberspace represents both a virtual and physical domain, acting as an effective multiplier for the conduct of operations in the other four domains and being itself a locus that allows for the articulation of international relations officially and unofficially. Therefore, the fifth domain will be increasingly contested.

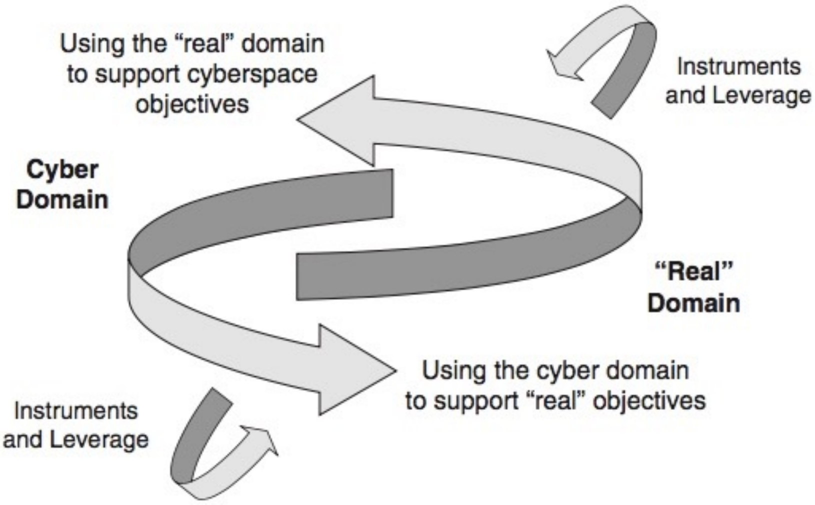
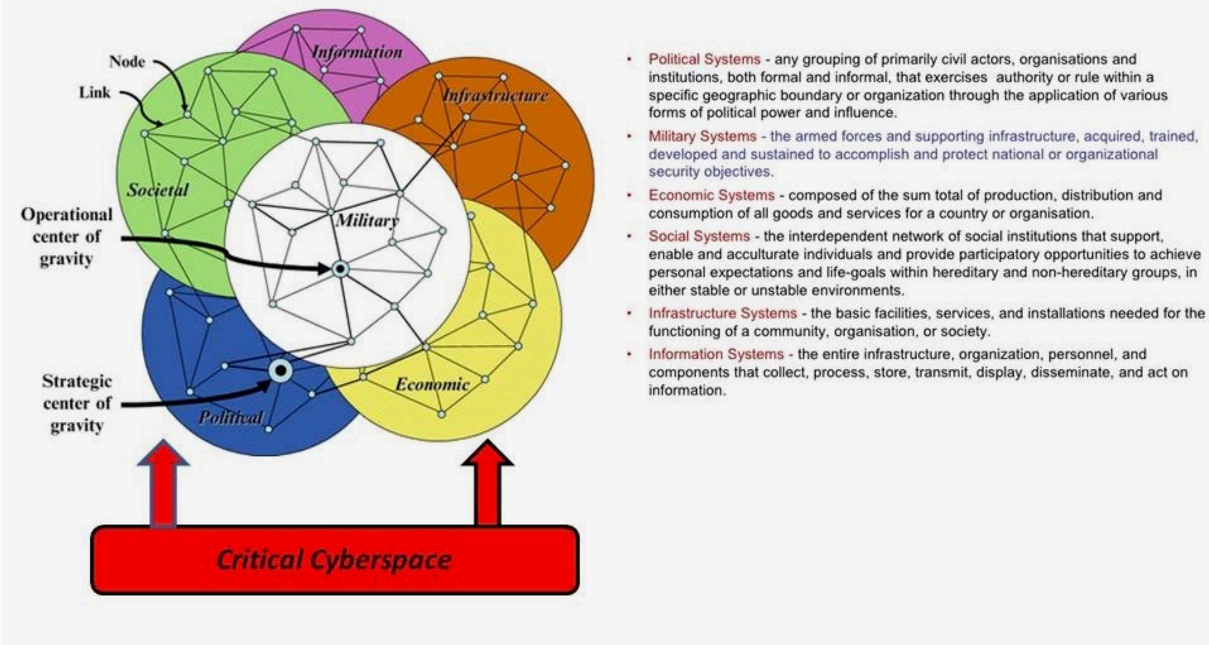

Using the "real" domain to support cyberspace objectives
Instruments and Leverage
Cyber Domain
"Real" Domain
Using the cyber domain to support "real" objectives
Instruments and Leverage

Fig.3: The interactions between the real and cyber domains of politics

Source: Choucri, N. (2012) *Cyberpolitics in International Relations* Cambridge, Massachusetts: The MIT Press

1.2 How cyberspace supports national security

Until recently, cyberspace was thought to belong to the realm of low politics, considering that it served as the basis for background conditions and routine decisions and processes (Choucri, 2012). With time, it has ascended to the ranks of "high politics" in international relations. As a matter of fact, increased dependence by states on computer technology to harness its benefits has made them vulnerable for exploitation by the adversary. Hence, cyberspace has increasingly turned into an unconventional domain of critical importance to the functioning of the national security of states, as it forms a modern infrastructure beneath the PMESII pillars, namely Political, Military, Economic, Social, Infrastructure and Information systems (Brantly, 2016). A subset of cyberspace can be identified, namely critical cyberspace, encompassing the "*cyber infrastructure and cyber services that are vital to preservation of public safety, economic stability, national security and international stability*" (EastWest Institute and the Information Security Institute of Moscow State University, 2014). Its assets, systems and functions determine the core Center of Gravity (COG) of the whole nation, or "*a source of power that provides moral or physical strength, freedom of action, or will to act*" (Joint Publication, 2011).



- Political Systems - any grouping of primarily civil actors, organisations and institutions, both formal and informal, that exercises authority or rule within a specific geographic boundary or organization through the application of various forms of political power and influence.
- Military Systems - the armed forces and supporting infrastructure, acquired, trained, developed and sustained to accomplish and protect national or organizational security objectives.
- Economic Systems - composed of the sum total of production, distribution and consumption of all goods and services for a country or organisation.
- Social Systems - the interdependent network of social institutions that support, enable and acculturate individuals and provide participatory opportunities to achieve personal expectations and life-goals within hereditary and non-hereditary groups, in either stable or unstable environments.
- Infrastructure Systems - the basic facilities, services, and installations needed for the functioning of a community, organisation, or society.
- Information Systems - the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Fig. 4: How critical cyberspace sustains the PMESII pillars

The conjunction of cyberspace and politics offers new possibilities for voicing political positions, enhances the demand for political participation, facilitating the aggregation of interests and group formation, and enables the supply of policy responses to be manifest (Choucri, 2012). In democratic countries, individuals can avail themselves of political blogs to bypass the power of the state and pursue their goals directly.

The awareness of the military potential of cyberspace has induced a plethora of decision-makers to adapt their offensive and defensive doctrines to the cyber age. The digitalized battlefield has come to comprise dominant maneuver, precision engagement, logistical support, real-time provision of intelligence and full-dimensional protection. Most importantly, by allowing the global command and control of forces and operations, cyberspace has turned into a new operational COG.

The adage that if one economy catches a cold the world economy gets sick derives from the interconnection of global markets within cyber. According to Friedman (2005), modern global economics has been flattened by cyber, as the latter constitutes the backbone of everything from currency markets and stock exchanges, to production lines. Multinational corporations have enlarged their supply chains with electronic data interchanges (EDIs) around the world traversing physical borders using the relatively borderless domain of cyberspace. Among the beneficiaries of this digital revolution are also small businesses and individuals, now able to gain access to information and products from around the world.

From online petitions to social networks, ICT has profoundly shaped social movements through its communicative ability to greatly broaden the potential audience. New communication technologies have afforded highly interactive platforms through which individuals and communities create and exchange content, socialize and organize themselves. In addition, by participating in cyber venues, individuals manage to surpass the bounds of sovereign territoriality and even formal identity.

Cyber technologies are integrated with critical infrastructures in key areas, such as the electric grid, the oil and natural gas, water, transportation, telecommunications, and financial sectors. Cyber attacks on critical infrastructures pose a relevant threat to an entire countrywide system. Furthermore, civilian cyberspace infrastructures are central to the functioning of the military, while civilian infrastructures can only properly be secured with military involvement. During his testimony before Congress on April 15, 2010, US Lieutenant General Alexander, the first Commander of the U.S. Cyber Command, highlighted that it is the combination of military and civilian targets that makes the deterrence measures implemented in the other domains of warfare inadequate in cyberspace (Institute for National Security Studies, 2012).

Finally, information transference has flourished in the fifth domain, to the point that it has saturated the capabilities of a state to supervise what goes in and out of its territory. According to Sun Tzu, "[…] To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting" (Sun Tzu, 2000, 8). This aptly fits the information age scenario, where information serves as "*the organizing principle of war and postmodernity*" (Osinga, 2007, 244).

Actors capable of mapping the entire PMESII pillars of a rival state through the monitoring of its critical cyberspace can ultimately attain the information superiority necessary to conduct a full-spectrum exploitation of it and consolidate political influence.

1.3 Actors and political utility in cyberspace

Under the propulsive thrust of the information revolution, the architecture of the international system is radically evolving towards a multipolar world order, with a plurality of actors capable of transforming and modelling decision-making processes. The democratization of information has brought about a "diffusion of power" that is eroding the prerogative of the monopoly of power and violence historically enjoyed by Nation-states (Nye, 2010). In fact, traditional power dynamics are being threatened by the greater involvement of individual criminals, organizations and non-state actors taking advance of the accessibility and asymmetry of the fifth domain (Eriksson, Giacomello, 2006). Since both the range of political expression and the volume of participation in cyber venues are mounting, the cyber arena can be considered a natural extension of politics and accordingly cannot be free from the inexorable competitions that arise when a variety of interests collide.

Actors interacting in cyberspace in order to maximize their political utility could be divided into three categories: states, hacktivists and terrorist groups.

There is growing evidence of the resort to cyberspace in order to pursue a wide range of political objectives, both at the inter-state and intra-state level. For the sake of simplicity, political cyber operations undertaken by states will be divided into external if directed against rival states to alter their policy positions and internal if cyber facilities are used to influence politics within their own territorial boundaries.

With respect to external cyber operations, states employ covert actions that can serve as a tool to advance the bargaining position of a state or to bring other states to the bargaining table. By entailing activities that affect outcomes in foreign countries, covert actions fill the gray zone between public diplomacy and outright war. The idea of making strategic gains without reaching the conflict threshold laid down by NATO in Article 5 is best reflected in the idiom "*On the Internet no one knows you're a dog*" (Fitton, 2016, 114). The 2009 Stuxnet worm makes a clear example of an external covert cyber action intended to have political effect. In fact, a malware specifically targeted Iranian nuclear facilities and led to the shutdown of 1000 centrifuges at Iran's Natanz nuclear fuel enrichment plant (Carr, 2012). It is essential to underline that Iran had been repeatedly denying that it was working towards the production of nuclear weapons capabilities. By contrast, it had consistently declared that it was working on nuclear production merely for peaceful purposes. Due to the fact that the Iranians would not allow inspectors from the IAEA into their facilities, a significant information asymmetry emerged between Iran and its main accusers, Israel and the United States. The situation was complicated by Iranian President Mahmoud Ahmadinejad's rhetoric that called for the destruction of Israel. This caused worries that a potential nuclear weapon would be directed against Israel. Against the background outlined above, the Stuxnet worm was able to provide political utility by exposing that Iran was enriching Uranium beyond civilian use. The reduction of the information asymmetry paved the way for higher sanctioning efforts and broke the diplomatic stalemate. New overt alternatives were available and profitable as a function of the second aspect of Stuxnet, namely time. As a matter of fact, because Stuxnet delayed the production of highly enriched uranium (HEU**)**, it provided time for diplomacy to have a chance at hindering the breaking out of a conflict.

At the intra-state level, a distinction needs to be made between democratic and non-democratic countries. As for democratic countries, Cambridge Analytica's former director Wylie has revealed that misuse of personal data illegally collected by the voter-profiling company has helped change the outcome of both the 2016 United Kingdom Brexit Referendum and the United States presidential election (Scott, 2018). Essentially, through data available on social networks like Facebook, companies similar to Cambridge Analytica profile individuals and personalize political messaging.

As regards non-democratic countries, they often limit or prohibit their citizens' access to the Internet in order to restrict the free flow of information. The Chinese government stands out for its censorship regime reinforced by a "Great Firewall" to counter potential subversion of its authority and prevent digital dissidents from accomplishing political change (Xu, Albert, 2017).

The term "hacktivists" applies to politically motivated intruders diverging from other types of hackers who are driven by profit or intellectual pursuit. According to Wong and Brown (2013), they are representative of "*the politics of no one*", i.e. a politics of actors without identities. Perhaps the most prominent hacktivist collective is Anonymous, responsible for cyber attacks against several government institutions and agencies, corporations and the Church of Scientology.

Finally, the awareness of the potential of using the Internet as a strategic tool has led terrorists to leverage cyberspace in order to undertake operational activities to further political change, including training, planning and logistics for future attacks, financing, disseminating propaganda and swaying public opinion through information operations (Hoffman, 2006).

1.4 Information as the bedrock of cyber power

Cyber power can be characterized as "*the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power*" (Kuehl, 2009, 38). It relies on information to manoeuvre perceptions of the operational environment to one's advantage and deteriorate the ability of the opponent to comprehend the same environment. Hence, cyber power could be construed as "sharp power", a peculiar type of hard power classified by Walker and Ludwig (2017) that shapes public opinion and "*pierces, penetrates, or perforates the political and information environments in the targeted countries*".

Information has been a fundamental aspect of national and international political power since Sun Tzu, who had observed: "*If you know the enemy and know yourself, you need not fear the result of a hundred battles*" (Sun Tzu, 2000, 11). Nye (2011) argues that power based on information resources is not new, but acknowledges that cyber power originated precisely in an information revolution carrying conceptual and organizational dimensions and implying a qualitative metamorphosis of the role of information. Arquilla and Ronfeldt (1997) envision information as a force-reformer rather than as a force-modifier. Therefore, the information environment (IE)[3] has emerged as a strategic environment where adversaries can rapidly transmit information, misinformation and disinformation to domestic and international publics and communities of interest.

The deceitful use of information for hostile purposes has a long history (Nye, 2018). Both the United States and the former Soviet Union had recourse to the manipulation of ideas, political perceptions and electoral

[3] According to Joint Publication 3-61*, Public Affairs*, "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."

processes during the Cold War. Afterwards, especially authoritarian countries such as China and Russia have tried to develop a vast array of influence techniques, including dispersing fake news and causing social disruption to lessen the attractiveness of democracy.

Nowadays, the Internet allows manipulation to take place on previously unthinkable scales of time, space and intentionality. As Lal (2002) put it, "*Conflicts on the ground are echoed, as one can imagine, in cyberspace…. Cyberspace offers even more fertile territory for sabotage, misinformation, and what in the clichéd formulation is termed the war over mind*". As a consequence, threat actors, both state and non-state ones, are expected to cultivate influence by increasingly incorporating Information Operations (IO) – defined as "*the integrated employment, during military operations, of information-related capabilities in concert with other of adversaries and potential adversaries while protecting [one's] own*"[4]- into their overall strategy. Therefore, military and information operations will be synchronized to respond effectively to world events and military successes will be tied ever more to the effectiveness of information operations to disrupt or influence the adversaries' leadership and decision-making processes.

[4] Defense Technical Information Center (2014) Information Operations November 20. Available from: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [2/04/2018]

2. THE INTERNET: A TERRORIST SAFE HAVEN

"*Tomorrow's terrorist may be able to do more with a keyboard than with a bomb*"

National Research Council[5]

2.1 Terrorism enters cyberspace.

Due to their nature of subnational group or non-state entity, terrorists lack the influence and leverage necessary to achieve their goal of generating or consolidating power. Thus, a thoughtfully choreographed act of violence, including elements of great drama, represents an essential requirement to penetrate the global political stage and attract attention to the group's cause. In consonance with the theory of "propaganda by deed" attributed to the Italian republican extremist Carlo Pisacane (Hoffman, 2006), violence satisfies the twofold purpose of spawning publicity for a cause and educating the masses.

As Jenkins stated, "*Terrorism is theatre*" (Jenkins, 1974, 4). Terrorists perform with an audience in mind and aspire to generate an atmosphere of fear in order to magnify their power beyond their actual capabilities. The real objective behind the violence perpetrated lies in the "*people watching, not the actual victims*" (ibidem). In fact, the success of a terrorist act rests on the efficacy of the multiplier effect and is measured on the basis of its far-reaching psychological repercussions, not merely on the material destruction of the target.

Veres (2004) indicated that terrorism entails the overthrow of the traditional relationship between news and facts. News no longer depends on the facts; facts have turned into a function of the news-making process. In such a way, the news acquires an eternal presence that preserves the life of the fact beyond its expiration.

According to Hacker, terrorists "*play to and for an audience*" (Hacker, 1977, xi). The targeted audience comprises three main groups, namely sympathizers, governments and neutrals. Interestingly, the message conveyed may vary for each recipient, but it is always conceived to promote change and manipulate political behaviour.

[5] National Research Council (1991) *Computers at Risk: Safe Computing in the Information Age* Washington: The National Academies Press

Sympathizers constitute a relevant segment within the audience because they provide the terrorist group with material, financial or spiritual support. Hence, terrorists' communication fulfils an internal purpose, as it strengthens internal solidarity and fosters morale.

Governments are addressed to impede the enactment of policies unfavourable to terrorists and to undermine their legitimacy, by alienating public opinion. As a matter of fact, terrorists may induce governmental bodies to execute excessive counter-measures, guaranteeing the group the opportunity to depict itself as a victim. In this case, terrorists' communication serves a coercive function, as it intends to ensure compliance through intimidation.

Finally, terrorists strive to engage in a dialogue with neutrals in order to make new converts, inform by delivering alternative narrative and solicit support. The purpose of this peculiar type of communication is didactic.

Traditionally, the media had a monopoly on covering and depicting terrorist attacks. Therefore, terrorists' hopes of garnering publicity for their causes and activities depended on attracting the attention of television, radio, or the print media. In other words, terrorists had to reach the "selection thresholds" (multistage processes of editorial selection) held by media.

Now, terrorist groups can tailor their recruiting pitch with their usage of "narrowcasting", that is, delivering different messages to individuals based on their age, gender, location, or other factors (Lieberman, 2017). Indeed, the rise of "*media-wise terrorism*" (Weimann, 2015, 51) has been favoured by the peculiar design of the Internet. Unregulated, cost-effective and guaranteeing almost perfect anonymity, it has demonstrated to be an extremely advantageous medium for both external (propaganda for recruitment and fund-raising) and internal (command, control and logistics) purposes, turning into a sort of "*virtual sanctuary*" (Hoffman, 2006, 214). Above all, the interactive capabilities of the Internet, such as social networks, chat rooms and online communities, enable terrorists to assume a proactive position and portray themselves in the light they wish, managing their perception before the world.

2.2 Terrorism and media: a paradoxically symbiotic relationship

In line with Wilkinson, "*When one says "terrorism" in a democratic society, one also says "media." For terrorism by its very nature is a psychological weapon which depends upon communicating a threat to a wider society. This, in essence, is why terrorism and the media enjoy a symbiotic relationship."* (Wilkinson, 2001, 17)

Terrorism and media are intertwined in a dangerous relationship of mutual exploitation and manipulation: the former ontologically hinges on the presence of an audience, whereas the latter are a vulnerable vacuum to be filled with gripping, dramatic news. The ability to transmit breaking news and reports 24/7 spawned intense competition among rival networks. Together with the increasing constraints of news budgets, which need to be justified and compensated by a high number of views, this resulted in a "trivialization of television news" that inexorably focus on the "*human-interest angle*" rather than genuine analysis (Hoffman, 2006, 180). Thus, media want to ensure the longevity of a story, just like terrorists do.

Lukaszewski, a public relations consultant to the U.S. military, compares the symbiotic relationship between the media and terrorists to a dance of death: "*Media coverage and terrorism are soul mates - virtually inseparable. They feed off each other. They together create a dance of death - the one for political or ideological motives, the other for commercial success*" (Chuipka, 2006, 52).

Nevertheless, this paradoxically symbiotic relationship proved to be a double-edged sword. On the one hand, by indirectly projecting terror into individuals' lives, media promote terrorism's self-empowerment. On the other hand, they release information that might pierce the veil of secrecy all terrorist groups need. In fact, the obsession with publicity often leads to the unmasking and arrest of members of the terrorist network, as in the case of the climax of the so-called Unabomber's terrorist campaign. As Hoffman reports, the author of a series of mail bombings between 1978 and 1995 came to be identified when his desire to publish his manifesto was recognized.

2.3 Terrorists' activities in cyberspace

Terrorist' use of the Internet can be classified into two categories, namely communicative and instrumental (Weimann, 2015). The former comprises the dissemination of propaganda, the waging of psychological warfare campaigns and the mobilization of potential group members, whereas the latter includes virtual indoctrination and training, cyber-planning and coordination as well as fund-raising.

Propaganda

One of the vital uses of online communication by terrorist groups lies in the spreading of propaganda to advance their radical agendas by leveraging the full media spectrum, including (but not limited to) social networks, magazines, online messages, audio files, streaming videos and, surprisingly, even video games developed by terrorists themselves. Propaganda is highly involved in the orchestration of terrorist activities, for it helps secure much-needed publicity but also draw attention to the group's cause with indeed minimal effort (Lumbaca and Gray, 2011). Thus, regardless of the terrorists' motives, terrorist messages seem to give priority to two *leitmotifs* above all: guilt transfer and invulnerability (Tugwell, 1986).

- Guilt transfer: terrorists claim that their violence constitutes a reluctant but inevitable reaction to that enacted by the regime they oppose. The terrorist organization is depicted as constantly persecuted, with its supporters killed and its freedom of expression curtailed. This tactic, which characterizes the organization as weak and hunted down by a strong power or a strong state, turns the terrorists into the underdogs. Thus, guilt transfer implies the rejection of the term 'terrorist' by the violent group – which rather identifies with freedom fighters or martyrs sacrificing themselves for the sake of a greater ideal - and the transfer of the term to the regime, accused of displaying its inhumanity.

- Invulnerability: this theme is directed at convincing the general public of the inevitability of victory as part of the ideological conditioning together with demoralizing the government and its supporters. The rhetoric emphasizes the powerlessness of the regime in the face of terrorist attacks and, on the other hand, involves messages conveying pride and accomplishment in order to win the hearts and minds of the population.

Psychological warfare

Terrorism has often been construed as a form of psychological warfare (Weimann, 2004). As a matter of fact, the Internet allows even small groups to exaggerate the threat they pose and to amplify their message. It is used to spread disinformation, to deliver threats intended to instill fear and helplessness within a community and to disseminate brutal images. In fact, Youtube, Facebook and Twitter have been found to be powerful platforms for documenting incidents of violence. Moreover, terrorists can launch psychological attacks through creating the fear of cyber terrorism. Defined as exploiting virtual tools to wreak destruction, cyber terrorism has thus far been rare. As a matter of fact, "*cyber attacks appear much less useful than physical attacks: they do not fill potential victims with terror, they are not photogenic, and they are not perceived by most people as highly emotional events*" (Lachow, 2009, 448). It is also far safer to send electrons rather than agents through customs and immigration controls. Nevertheless, former Director of National Intelligence Mike McConnell argues that the vulnerabilities of financial and electrical systems offer a huge target for any group willing to wreak destruction, and that such groups will develop the capabilities to become a greater threat than other nation states (Nye, 2011).

Recruitment

The availability of the Internet gave birth to a forum for "virtual jihad" discourse on which terrorist groups rely on for recruitment and radicalization. The prevailing strategy used to seduce potential recruits lies in the invocation of "defensive mobilization" to compel them with a duty (Borum and Fein, 2016). Terrorist recruitment-oriented communication is frequently conceived to appeal to vulnerable and isolated groups in society. Hence, this propaganda of recruitment and radicalization hinges on an individual's sentiments of injustice, alienation, or humiliation (Weimann, 2015). Interactive participation can nurture a sense of cohesion and create a sort of virtual community between the terrorists and potential recruits, thereby creating a sense of unity. As Olivier Roy (2010) affirms, the key place for radicalization is "*neither Pakistan nor Yemen nor Afghanistan ...but in a solitary experience of a virtual community: the ummah on the Web.*"

Online indoctrination and training

Activities that were once conducted face-to-face, such as indoctrinating and training, now take place on websites and readily accessible online training camps. In fact, the virtual forums provide an open venue for recruits to learn about and provide support to terrorist organizations and they encourage engagement in direct actions. A plethora of terrorist manuals and instructions on how to build explosive devices and carry out attacks is published on the Internet every month. Therefore, some experts have referred to the Internet as a "terrorist university," an environment where terrorists can acquire new techniques and skills to make them more effective in their attack methodologies (Weimann, 2015).

Cyber-planning and coordination

Terrorists avail of the Internet not only to learn how to build bombs but also to plan and coordinate specific attacks. Since the World Wide Web may be viewed as a vast digital library, terrorist groups are allowed to gather a wide variety of details about prospective targets that may be relevant to their cause or to future operations. Geospatial imagery, such as Google Earth, may be profitable to study locations and plan potential attacks.

Fund-raising

The Internet represents the simplest method of soliciting donations and contributions. Terrorists use many techniques to raise funds online for their activities. Many have added links to their sites that advise visitors on how to donate funds electronically, while others have resorted to e-commerce, selling CDs, DVDs, t-shirts and books. Terrorist groups also raise funds through cyber criminal activity: "*There is substantial evidence that terrorist organizations are using the proceeds from traditional cybercrime, such as online credit card fraud, identity theft and telecommunications fraud to fund their operations*" (United Nations Counter-Terrorism Implementation Task Force 2011, 34).

2.4 The virtual jihad

Global jihadism is regarded as one of the main radical movements to have capitalized on the communications revolution in order to diffuse its message (Hanieh, 2016).

Aaron Zelin (2013) distinguishes four phases in which jihadi media have been distributed since 1984, namely phase 1 (beginning in 1984), phase 2 (beginning in the mid-1990s), phase 3 (starting in the mid-2000s) and phase 4 (starting in the late 2000s).

In the 1980s, the first generation of *mujahideen* relied on traditional oral and written communications to circulate their propaganda.

The second generation has made use of the Internet since the mid-nineties by creating thousands of top-down jihadist websites. By 2000, all terrorist groups had established their presence on the Internet (Weimann, 2006).

Phase 3 saw the rise of interactive forums, where administrators release content on behalf of jihadi organizations, but they are not necessarily directly connected. They have the power to prevent users from being exposed to dissent, thereby steering the online community in a certain direction. At the same time, users can play a role in posting a growing array of materials, including their own views on events, and are entitled to share ideas with like-minded individuals across a wide geographic area.

With the third generation, which was forged by the Syrian revolution in 2011, individuals, and not organizations, take on a more relevant position as they fully exploit social media, most notably Facebook, Twitter, Youtube and blogs.

Hence, the crucial role played by media in the terrorists' calculus is witnessed by the efforts of jihadist groups such as al-Qaeda[6] and ISIS to incorporate the media imperative. In the battle for the hearts and minds of the *umma*, the war of narratives has gained more prominence than that of the classical bullets and fire weapons.

2.4.1 Al-Qaeda

Al-Qaeda's online debut occurred in February 2000, with the creation of maalemaljihad.com, followed in March 2001 by alneda.com. Registered in Singapore, it appeared on Web servers in Malaysia and Texas before it was removed at the request of US officials. It then modified its name and URL regularly, forced to move from server to server by citizens who denounced it to the Internet service providers (ISPs) that were hosting the sites. After losing the Internet domain in 2002, al-Qaeda later reappeared with a novel website named Faroq.

In the summer of 2001 al-Qaeda founded its media arm, the *As-Sahab* Foundation for Islamic Media Publication, and released its first video, 'The Destruction of the American Destroyer [USS] Cole'.

The organization explicitly recognizes the importance of the Internet as a propaganda tool and calls for contributions to its overall communication approach as it did on one of its numerous websites (the Azzam site):

[6] The English translation is "The Base"

"*Due to the advances of modern technology, it is easy to spread news, information, articles and other information over the internet. We strongly urge Muslim internet professionals to spread and disseminate news and information about the jihad through e-mail lists, discussion groups and their own websites. If you fail to do this, and our site closes down before you have done this, we may hold you to account before Allah on the Day of Judgment.... We expect our website to be opened and closed continuously. Therefore, we urgently recommend any Muslims that are interested in our material to copy all the articles from our site and disseminate them through their own websites, discussion boards and e-mail lists. This is something that any Muslim can participate in, easily, including sisters. This way, even if our sites are closed down, the material will live on with the Grace of Allah"* (Weimann, 2015).

Jenkins (2011) places al-Qaeda at the forefront among terrorist groups in cyber know-how: "*While almost all terrorist organizations have websites, al Qaeda is the first to fully exploit the Internet. This reflects al Qaeda's unique characteristics. It regards itself as a global movement and therefore depends on a global communications network to reach its perceived constituents. It sees its mission as not simply creating terror among its foes but awakening the Muslim community. Its leaders view communications as 90 percent of the struggle*" (Jenkins 2011, 1).

The war on terrorism dismantled al-Qaeda's sanctuary in Afghanistan and urged the organization to convert into a highly decentralized network of affiliated, semi-independent cells without a single commanding hierarchy. The Internet allows these loosely interconnected networks to function, converse, and cultivate their ideological solidarity. Furthermore, it connects not only members of the "hardcore al-Qaeda," but also associates of groups who manifest the jihadist spirit. Therefore, the Internet developed into an essential stage, carrier, and bonding mechanism.

With the emergence of Web 2.0, blogs, Web forums, Facebook, MySpace, Twitter, and YouTube were combined in innovative ways that helped form the new media landscape.

Amble (2012, 339) highlighted that *"[t]he similarities between these two structural transformations, one of a transnational terrorist group and the other of the Internet, are striking. Indeed, Al Qaeda seems to have acknowledged these similarities by increasingly operating with considerable effectiveness in the new media environment.*" In fact, the unique unstructured nature of al-Qaeda influenced its online production lines. Al-Qaeda features various branches, with the main ones being al-Qaeda in the Arabian Peninsula (AQAP), al-Qaeda in Iraq, and al-Qaeda in the Islamic Maghreb (AQIM). Each of them has its own media outlet—in Pakistan, al-Qaeda has As-Sahab Media; in Yemen, Al-Malahim; in Iraq, Al-Furqan; and in North Africa, Al-Andalus. The rationale for al-Qaeda's reliance on leading online forums is authentication: by promoting its messages through authorized online venues (such as the forums Shamukh al-Islam and al-Fida al-Islam), it assures viewers that the information is an official statement.

2.4.2. ISIS

If al-Qaeda has been one of the first terrorist organizations to equip itself with members dedicated to the masterful production and dissemination of media products, ISIS transformed "*a local ground war into a global phenomenon*" through a well-defined, coherent information strategy (Gambhir, 2016, 9). By advocating the immediate establishment of the Caliphate, ISIS gathered worldwide support and was able to position itself as the reference point of a scattered community. As of December 2015, ISIS had drawn about 30.000 foreign fighters from at least 85 countries to the Syrian and Iraqi battlefields by virtue of its profitable propaganda machine (Benmelech and Klor, 2016), based on the revolutionary development of custom-fit content for niche audiences, targeting the viewers' ethnicity or age.

Moreover, ISIS employed the full spectrum of mass media as a force multiplier: "*in the minds of foreign fighters, social media is not merely virtual: it has become an essential part of what happens on the ground"* (Carter, Maher, Neumann, 2014, 29).

ISIS has mastered the virtual world thanks to the dialectic between the centralized approach conducted by an official media branch integrated in the core of the operational apparatus and the decentralized dissemination of media products carried out by online supporters. The former granted the group the chance to guide its media employees with the same speed and method of military forces and has to be credited with ISIS's adaptive behaviour, while the latter secured the resiliency of ISIS's digital presence in spite of international efforts to restrict it. Therefore, a single media foundation complemented with multiple pockets was envisaged.

The Base Foundation, or al-Mu'asasat al-Um, is at the head of ISIS's media apparatus and is responsible for branding the self-styled Caliphate through the production of high-quality videos, battlefield photoshoots and appealing multilingual magazines. It is said to be located either in Iraq or Syria.

The Base Foundation was charged with the task of structuring media campaigns and setting the priorities. It also oversaw the formation of new media offices in the 35 governorates, or *wilayats*, of the Caliphate and directly supervised their work by receiving accurate monthly reports. The external provinces established in the lands conquered by ISIS's militias released content related to military operations, service provision, and daily life. In addition to that, they circulated hard copies of ISIS's official media to civilians under ISIS's control in order to mobilize local populations.

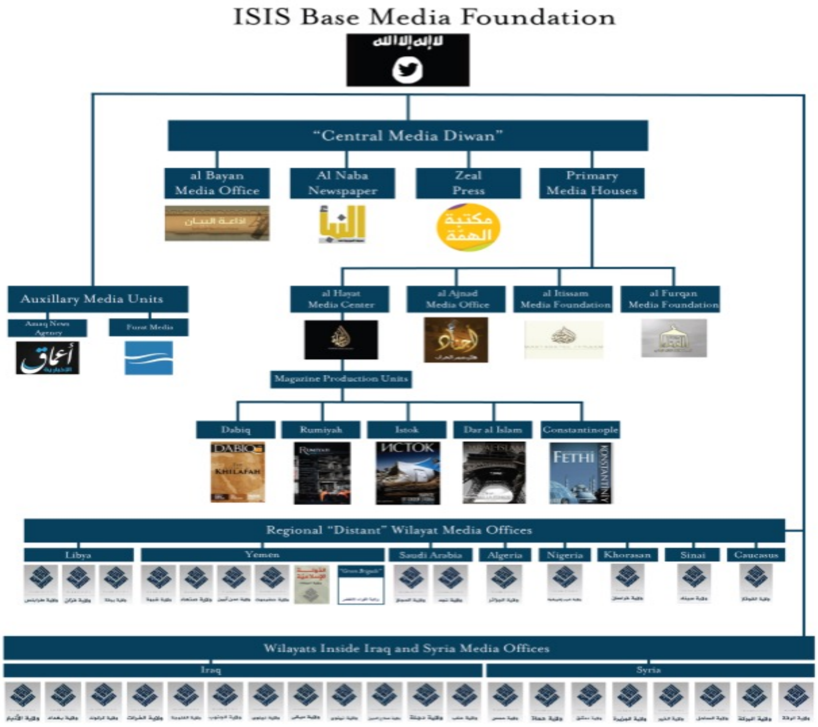


Fig.5: ISIS's Media Apparatus

Source: Forrest, C. (2016) *ISIS's media apparatus*

http://www.understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf [2/05/2018]

The Base Foundation managed ISIS's leading media houses, which include the Al-Furqan Institute for Media Production, the Al-Hayat Media Center, the Al-I'tisam Media Foundation and the auxiliary Amaq News Agency.

Founded in 2006, the Al-Furqan Institute of Media Production is ISIS's oldest media branch and represents "*a reliq of Al-Qaeda's heritage*" (Gambhir, 2016, 22). It is specialized in the making of videos of religious sermons and speeches from leading figures in the group. The Raqqa-based Al-Hayat Media Center was launched in 2014 and published ISIS's magazines Dabiq and Rumiyah in several multiple languages. Finally, Amaq News Agency is a news outlet linked to ISIS that has often been the first to claim responsibility for attacks on behalf of the group. The Base Foundation also administered ISIS's overseas al-Bayan radio, that broadcasted *nasheed* glorifying Islam as well as news updates.

The importance attributed to communication by ISIS is demonstrated by the economic privileges enjoyed by members of the media office, who earned a regular income - higher than that of soldiers - and were exempted from taxes.

Decentralized dissemination relies on the assumption that, even though a province is defeated both on the ground and in cyberspace, the leadership project will take roots easily elsewhere. Unlike other jihadist groups, ISIS's information operation successfully took into account real-world developments and, in order to prevent censorship, it did not consider the maintaining of an official website or single social media accounts. Alternatively, ISIS leveraged on a motivated "fan-base" that downloaded its online content and actively re-posted it on rapidly expanding set of platforms, including mainstream social networks, file-sharing websites or messaging applications. The removal of accounts loyal to ISIS was contrasted through a powerful resurgence plan that provided for the diffusion of "shout out" messages and the continuous regeneration of accounts with the same username and profile picture. As Bindner and Gluck (2017) explain, since the end of the 2000s jihadists emerged from not easily accessible deep web forums and migrated towards the surface web, enabling a massive spread of virtual jihad. Nonetheless, when faced with an increase in international attempts to suppress its online propaganda especially in the wake of terrorist attacks, ISIS's members landed to Telegram, an encrypted broadcasting application. The latter allows for an instantaneous sharing of contents without limit of size. Therefore, operational security was preferred to communication reach.

After conducting an extensive research on ISIS propaganda between July 17th and August 15th 2015, Winter (2015) found that ISIS's media apparatus articulates the group's narrative along six main lines, namely mercy, belonging, brutality, victimhood, war and utopia. Out of the 892 events examined - including audio statements, photosets, articles and videos - 861 prioritised victimhood, war and utopia.

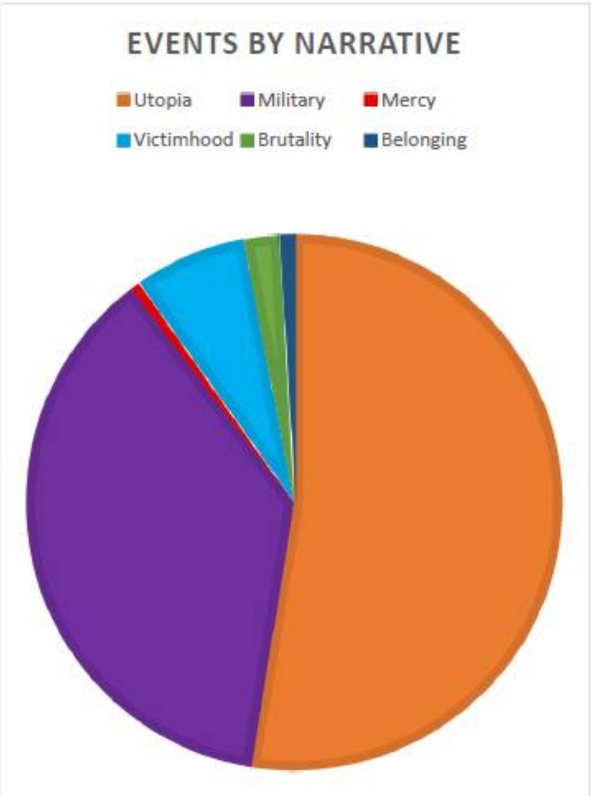


Fig.6: Main themes present in ISIS's narrative

Source: Winter, C. (2015) *Events by narrative* http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [3/05/2018]

As regards victimhood, the majority of the events was photographic in nature and depicted dead or injured, especially civilians. It represents a *leitmotiv* in jihadist narrative, because Sunni Muslims share the perception that they have always been made the scapegoats. In such a way, victimhood qualifies as a justifier for the group's existence.

War constitutes *"the Caliphate's raison d'être, its primary agent of change and revolution"* (Winter, 2015, 24). Therefore, ISIS must cultivate a triumphalist propaganda that idealises martyrdom in order to recruit foreign fighters.

Unsurprisingly, utopia appears to be the preeminent theme. By exalting all facets of everyday life in the new fully-fledged State - social life, religion, economic activity, implementation of the *shari'ah* and landscape-ISIS can succeed in exhibiting its supremacy over rival jihadist groups.

In conclusion, ISIS's propaganda machine works because it is flexible and thoroughly balances an institutional communication strategy and an emotional communication strategy (Lombardi, 2015). The former seeks to spread the ideological manifesto, project the image of a legitimate state and counter the dominant narrative. The latter, instead, is directed at enhancing in-group mythology, causing viral behaviours and provoking debates.

Notably, one of the preeminent features of ISIS's communication strategy lies in the parallelism between information and military operations in order to maximally sustain military objectives and adapt to territorial changes. This has been made possible by the synergy between ISIS's media, military and religious organs. As a matter of fact, the Base Foundation "*reported directly to the caliph, ISIS's shura, or advisory council, and ISIS's military commander and chief security officials*" (Gambhir, 2016).

By seeking to synchronize its messaging and actions, ISIS attempts to ensure that its information operations manifest as politico-military actions.

3. ISIS'S INFORMATION OPERATIONS

> *"This is a war of ideologies, as much as it is a physical war. And just as the physical war must be fought on the battlefield, so too must the ideological war be fought in the media."*
>
> Nasser Balochi, member of ISIS's social media team[7]

3.1 The rise and fall of ISIS

Emerging out of the war in Iraq (2003-2011), the Arab springs (2010- 2012) and the Syrian civil war (2011-present), ISIS constitutes a well-defined product of its time and geography. It may also be construed as the consequence of broader global trends of Islamization that accentuate the tensions between modernity and religiosity, compounded by a rise in Islamic militancy (Oosterveld and Bloem, 2017).

The roots of ISIS can be traced back to the 2003 Operation Iraqi Freedom (OIF) and to the radical Islamist group Jamat al-Tawhid wa-l-Jihad[8] (TwJ). Operating in northwestern Iraq, it comprised a few non-Iraqi operatives under the leadership of Jordanian-born Abu Musab al-Zarqawi (Plebani, 2014). Adopting an extremely aggressive stance, manifested in its multiple terrorist operations against Coalition forces, international personnel and targets, as well as embarking upon a captivating media campaign, the movement soon came to head the anti-US insurgency. Although Al-Zarqawi had succeeded in becoming one of the main players of he Iraq war, he had to withstand the restrictions stemming from the insufficient resources and fighters at his disposal, along with the predominantly foreign nature of the group. In other words, this *gharib* paradox, as Brian Fishman (2006) designated it, while safeguarding the cohesion of the movement and its allegiance to al-Zarqawi, precluded the Jordanian terrorist from accessing the wide pool of Iraqi militants operating against Coalition soldiers and the cadres of foreign fighters active on the ground but not allineated with his group. It is against this background that al-Qaeda in Iraq (AQI) came into being in 2004. In fact, al-Qaeda required a charismatic figure to lead the group against US forces in the aftermath of the setbacks suffered in Afghanistan, while Al-Zarqawi needed Osama bin Laden's blessing to increase his status in the radical jihadist galaxy.

[7] Stern, J., Berger, J. M. (2016) *ISIS: The State of Terror* [Online] Available from: https://www.researchgate.net/publication/308089080_ISIS_The_State_of_Terror [7/06/2018]

[8] The English translation is 'the Organization of Monotheism and Jihad'.

The Iraqi community's participation in the 2005 electoral process was deemed as an existential threat by al-Zarqawi, fully aware that his success hinged on the instability of the Iraqi system and on the collaboration of the Arab Sunni community. Therefore, he decided to widen the scope of the group's agenda, waging an all-out war against the Iraqi Shia community to foment inter-community hatred and competition. The hundreds of attacks against Shia civilian, religious and political objectives came to a climax in the June 2006 Samarra bombing, referred to as the event that heralded the beginning of Iraqi's civil war.

Shia militias ultimately got the upper hand, expanding their control over most of Baghdad and accomplishing a sectarian cleansing which heavily altered the demographic composition of a city that had always been marked by its 'mixed' heritage.

After the defeat at the battle of Baghdad, AQI was met with harsh criticism, both at the international and the local level. Jihadist groups expressed their disapproval of the ruthless tactics adopted as well as of the choice to strike at Shia militants. Abu Muhammad al-Maqdisi, identified as al-Zarqawi's mentor, denounced the *modus operandi* of the organization and Ayman al-Zawahiri – at the time Osama bin Laden's deputy – prompted the Jordanian leader to reconsider attacking the Shia population. At the Iraqi level, several insurgent groups condemned the movement for the fall of Baghdad and the opposition arising within its ranks. These internal fractures were exploited by AQI rivals who were able to infiltrate the group and kill its leader in June 2006. The death of al-Zarqawi inflicted a tremendous blow to the movement, that underwent re-configuration under the dual leadership of Abu Ayyub al-Masri, also known as Abu Hamza al-Muhajir, and Abu Omar al-Baghdadi. On the one hand, it launched an operation directed at 'Iraqifying' its core in order to mitigate the side effects of the '*gharib* paradox'; on the other, it integrated its military operations with management of the territory under its control. This led the organization to lay the foundations of the Islamic State of Iraq (ISI), an Islamic emirate that planned to extend its reach over the area around Mosul and the Niniveh plains, where it could rely on a profound historical presence, good relations with local insurgent groups and the benefits flowing from proximity to the Syrian border.

Despite its efforts the group was kneeling, with its members pursued throughout the country, its activities limited to racket, illicit trafficking and attacks against local minorities, and the flow of foreign volunteers drained. Amid the chaos unleashed over ISI's ranks by American and Iraqi officials, al-Baghdadi took on the leadership. He purged the group of the cadres whose loyalty could not be trusted and reinforced its internal bonds to build a brotherhood of foreign and Iraqi operatives with a single aim and willing to fight against anyone not sharing the same goal. By virtue of this internal re-organization as well of the growing polarization of Iraq's socio-political system and of the withdrawal of US troops, ISI was able to make a slow but steady return on the Iraqi scene.

When uprisings broke out in Syria in 2011, al-Baghdadi understood the opportunities the revolution could offer and decided to dispatch representatives to face pro-Assad forces and install a visible presence in Sunni majority regions, with the Raqqa, Idlib, Deir ez-Zor, and Aleppo provinces being the main areas of interest

(NATO Strategic Communications Centre of Excellence, 2016). Al-Baghdadi's militants – who fought under the banner of a new group named Jabhat al-Nusra[9] (JAN) led by Abu Muhammad al-Julani –came to be one of the preeminent groups of the anti-Assad insurgency, as they invested conspicuous resources in relieving the widespread scarcity of food and in imposing *shari'a* in the areas under their control. Moreover, they did not abstain from welcoming dedicated Syrian volunteers in its ranks. The achievements on the battlefield and the positive feedback from the Syrian population helped JAN advance its local and international stature, attracting a plethora of volunteers from Syria and all over the world, together with funding which replenished the movement's treasury and allowed al-Baghdadi to step-up his activities in Iraq, too. In fact, the movement commenced an intense anti-government campaign, which involved targeting Iraq's most important prisons. The co-optation of hundreds of prisoners coming from the ranks of Saddam Hussein's former army and equipped with military and strategic skills, coupled with good knowledge of Iraq's territories and dynamics, proved of extreme value for the future successes of the organization.

In light of the strength acquired by ISI forces on both sides of the Syrian-Iraqi border, on April 9, 2013 al-Baghdadi announced JAN's subservience to ISI and the merger of the two groups into the Islamic State of Iraq and al-Sham (ISIS). Nonetheless, the leader of the al-Nusra Front, Al-Julani, and al-Qaeda leader, al-Zawahiri, released a statement denying the merger and cutting all connections with al-Baghdadi's organization. Later, on February 2, 2014, al-Qaeda released a statement officially dissociating itself from ISIS (Bunzel, 2015).

In 2014 ISIS launched an an all-out offensive against the Iraqi state, which stood in stark contrast to the group's previous endeavours for its multi-pronged strategy that aimed at encircling Baghdad and, above all, at consolidating its hold over Mosul and the Niniveh plains. The invasion culminating in the fall of Mosul was preceded by months of violence and favoured by the gradual deterioration of the Iraqi social pact especially along the Shia-Sunni axis due to the Sunni marginalization by the Iraqi government of Nouri al-Maliki. On June 10, after less than 3 days of battle, Mosul –the political and economic capital of Sunni Iraq and the second largest Iraqi city - fell into the hands of a coalition headed by ISIS units and supported by important insurgent groups. Several weeks before the attack on Mosul, ISIS had engaged in information warfare that significantly affected the success of the imminent military operation. Social and mass media tools were employed to frighten the Iraqi army and other religious minorities including Shia, Christians, and Yazidis. Messages were broadcast in local markets and echoed by religious leaders in mosques during prayer services, compounded by pictures and videos showing the brutal execution of Iraqi and Syrian soldiers who had been captured by the group. The terror campaign urged many thousands of people to flee and caused morale depletion within the Iraqi Security Forces. The resulting fear and tension gave ISIS a psychological

[9] The English translation is "The Support Front for the People of Al-Sham".

advantage during the battle of Mosul. Being the brightest military success obtained by jihadi forces since the beginning of the new century, it enabled ISIS to access the enormous military deposits of the north, to collect over 450 million dollars stored in Mosul banks, to earn a set of oil-rich areas close to the ones it already administered in Syria and to kidnap the Turkish consul and several members of his staff. Above all, it allowed al- Baghdadi to extend his hold over a string of territories covering north-eastern Syria and reaching the very heart of Iraq's Arab Sunni domains, instituting an 'Islamic State'.

Furthermore, on June 29 – the first day of Ramadan – al-Baghdadi proclaimed the establishment of a pan-Islamic Caliphate under his rule as *Amir al-Mu'minin* (Commander of the Believers), inviting all the believers to join him in the fight against the oppressors of Islam and to emigrate to the newly declared proto-state. In the first message in his role of Caliph, titled 'A Message to the Mujahideen And the Muslim Ummah In the Month of Ramadan', he tried to present himself as the legitimate successor of the Prophet, justifying it by the genealogy of his tribe, which traced its lineage back to Muhammad's descendants. In doing so, he attempted to validate his legitimacy and assert his authority over the territories under ISIS's control as well as over alternative jihadi groups, as stated by ISIS spokesman and director of external operations Abu Muhammad al-Adnani: "*We clarify to the Muslims that with this declaration of khilafah, it is incumbent upon all Muslims to pledge allegiance to the khalifah Ibrahim and support him (may Allah preserve him). The legality of all emirates, groups, states, and organizations, becomes null by the expansion of the khilafah's authority and arrival of its troops to their areas*" (SITE, 2014a). In fact, from ISIS's perspective, al-Qaeda had become irrelevant to the pursuit of global jihad and its affiliates were ordered to give *bay'a* (the oath of allegiance) to al-Baghdadi. Significantly, the self-proclaimed Caliph issued 'a special call' to religious workers as well as to "*people with military, administrative, and service expertise, and medical doctors and engineers of all different specializations and fields*" (SITE, 2014b), reprised in ISIS's signature magazine, Dabiq.

In September 2014, US President Barack Obama announced the formation of an international coalition to degrade and defeat ISIS and the US and Arab allies launched air strikes on ISIS in Syria and on their positions in northern Iraq (McInnis, 2016).

According to Nair (2016), 2015 was a mixed year for ISIS fortunes. On the one hand, ISIS integrated local militant networks and added *wilayats* (provinces) in Afghanistan, Nigeria, Egypt and Libya (Jones, Dobbins, Byman, Chivvis, Connable, Martini, Robinson and Chandler, 2017). ISIS militants also seized Ramadi in Iraq, Palmyra in Syria and took full control of Sirte in Libya in May 2015. Majlis Shura Shabab al-Islam conquered Derna in Libya for ISIS in October 2015. On the other hand, ISIS suffered its first military setback when coalition forces drove it out of the Syrian border town of Kobane in January and Iraqi forces and Shiite militias freed Tikrit from ISIS in March 2015. By June 2015, Kurdish militia, supported by Syrian rebels and coalition air strikes, captured the town of Tal Abyad on the Syrian–Turkey border from ISIS, which it had held for more than a year. Liberation of Tal Abyad, one of two major transit points on a key supply route to the *de facto* ISIS capital in Syria Raqqa, was a major achievement. In July 2015, Turkey joined the war on ISIS and bombed ISIS positions inside Syria. In September 2015, on the request of the Assad regime, Russia began air strikes backing Syrian forces and participated in an Iranian-supported regime offensive near Aleppo. By then, the call by al-Adnani to ISIS members across the globe for attacks on citizens of the USA, France and other countries against the group was delivering results, as shown by the Sydney café hostage crisis, the suicide attack during a funeral north of Baghdad, the attack on the offices of French satirical newspaper, Charlie Hebdo, the armed assault on a luxury hotel in Tripoli and the beheading of 21 Egyptian Christians in Libya. Hence, rising territorial losses were counterbalanced by a proportional increment in terror-related activity by ISIS, thereby indicating intransigence towards the actions of the coalition and regional armies.

In March 2016, Syrian forces supported by Russia retook Palmyra and in May Kurdish and Arab units assembled in the Syrian Democratic Forces (SDF) and assisted by US-led air support launched a two-pronged attack against ISIS militias in north of Raqqa. In Iraq, Fallujah was declared fully liberated by the Iraqi government troops and paramilitary units in June, being the first major city to fall to ISIS. In Syria, the Syrian Army closed in towards the rebel-controlled part of east Aleppo. As for Libya, the UN-backed unity government had re-taken control of the Sirte Port by June. Therefore, by the end of 2016, Daesh had lost 43% of its total territory, including key cities in Iraq (Ramadi, Fallujah, and Tikrit) and Syria (Kobani, Tal Abyad, and Manbij). As it progressively lost more terrain, ISIS assigned its prolific global community a greater role: "*ISIS's brand in this case would not be contingent upon the existence of a physical caliphate, though it will likely endure, but rather upon ISIS's ability to encourage and facilitate terrorist attacks worldwide*" (Gambhir, 2016, 30). ISIS's followers were thus incited to plan attacks in their homeland rather than to leave for the Caliphate. Lone wolves promptly welcomed the new virtual strategy and executed a global wave of attacks during the Islamic holy month of Ramadan (Gambhir, 2016).

2016 also witnessed a stark decline in ISIS online propaganda activity in terms of quantity as well as quality. From January 2015 to August 2016, Milton (2016) collected over 9000 videos, picture reports and photographs embedded on Twitter. As shown in Figure 4, ISIS's media production reached its peak in July 2015 before dropping off quite steadily over the following months. By August 2016, the number of publications fell to 194, which marks the lowest number marked in the dataset.

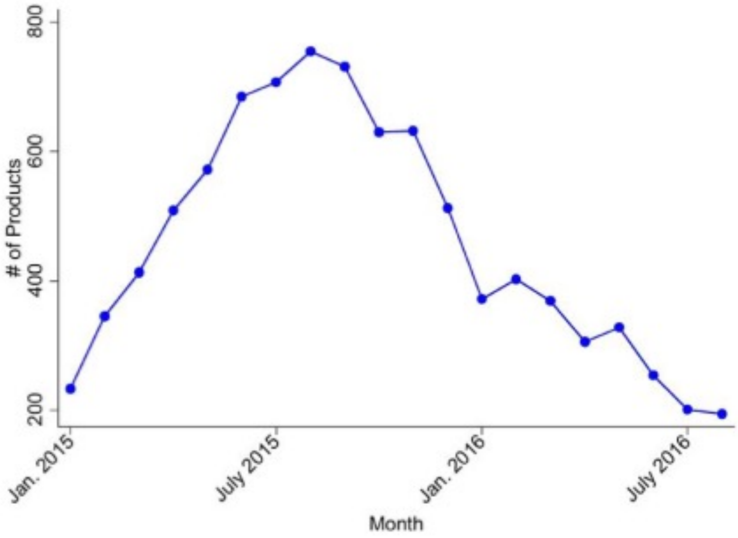


Fig.7: Number of official ISIS Visual Media Products by month

Source: Milton, D. (2016) *Communication Breakdown: Unraveling the Islamic State's Media Efforts* Combating Terrorism Center at West Point [Online] Available from: https://ctc.usma.edu/communication-breakdown-unraveling-the-islamic-states-media-efforts/ [7/06/2018]

According to the Pentagon, in 2017 ISIS lost over 70% of the territory it once held in Iraq, and 51% of its territory in Syria. In a substantial blow to the group, on 10 July 2017 Iraqi Security Forces liberated the Iraqi city of Mosul - ISIS's capital in Iraq- after nine months of fighting.

As of March 2018, ISIS has lost 98% of the territory it once occupied in Iraq and Syria, including Raqqa, which was liberated in October 2017 (Mills, 2018). In December 2017 the Iraqi government subsequently declared military victory over ISIS in Iraq and the USA declared the end of major combat operations. The strategic picture in Syria remains complex, as small pockets of ISIS resistance remain in the region, close to the Iraqi border around the town of Abu Kamal.

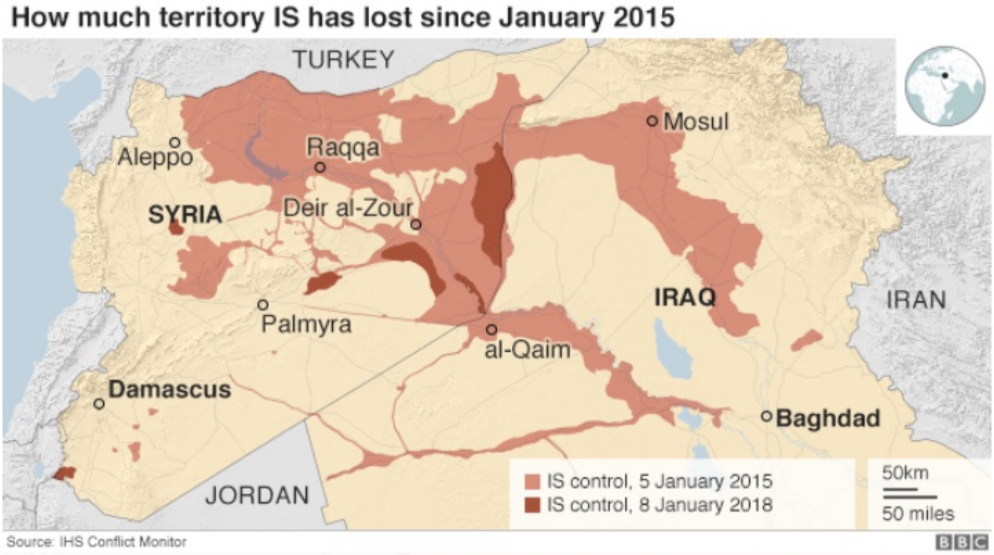

How much territory IS has lost since January 2015
TURKEY
Mosul
Aleppo
Raqqa
SYRIA
Deir al-Zour
IRAQ
IRAN
Palmyra
al-Qaim
Damascus
Baghdad
JORDAN
🟥 IS control, 5 January 2015
🟥 IS control, 8 January 2018
50km
50 miles
Source: IHS Conflict Monitor
BBC

Fig.8: How much territory ISIS has lost since January 2015

Source: IHS Conflict Monitor

Available from: https://www.bbc.com/news/world-middle-east-27838034 [7/06/2018]

The loss of territory was also coupled with loss of leadership. In May 2015, Abu Alaa al-Afri, the second-in-command of the group, was neutralised. Several other upper echelon commanders have been killed by the Iraqi and Syrian forces supported by coalition efforts in 2016, with al-Adnani being the latest in September (Nair, 2016).

In order to compensate for battlefield and territorial losses, in 2016 ISIS reinvented its military strategy and retooled its image, seeking to expand globally in both the physical space – relocating its centre of gravity to its numerous *wilayat*- and the cyber space. The change in name of ISIS's showpiece magazine from Dabiq to Rumiyah demonstrates continued momentum despite military defeats and reflects a significant shift in emphasis from a real, physical caliphate to a self-empowering virtual one.

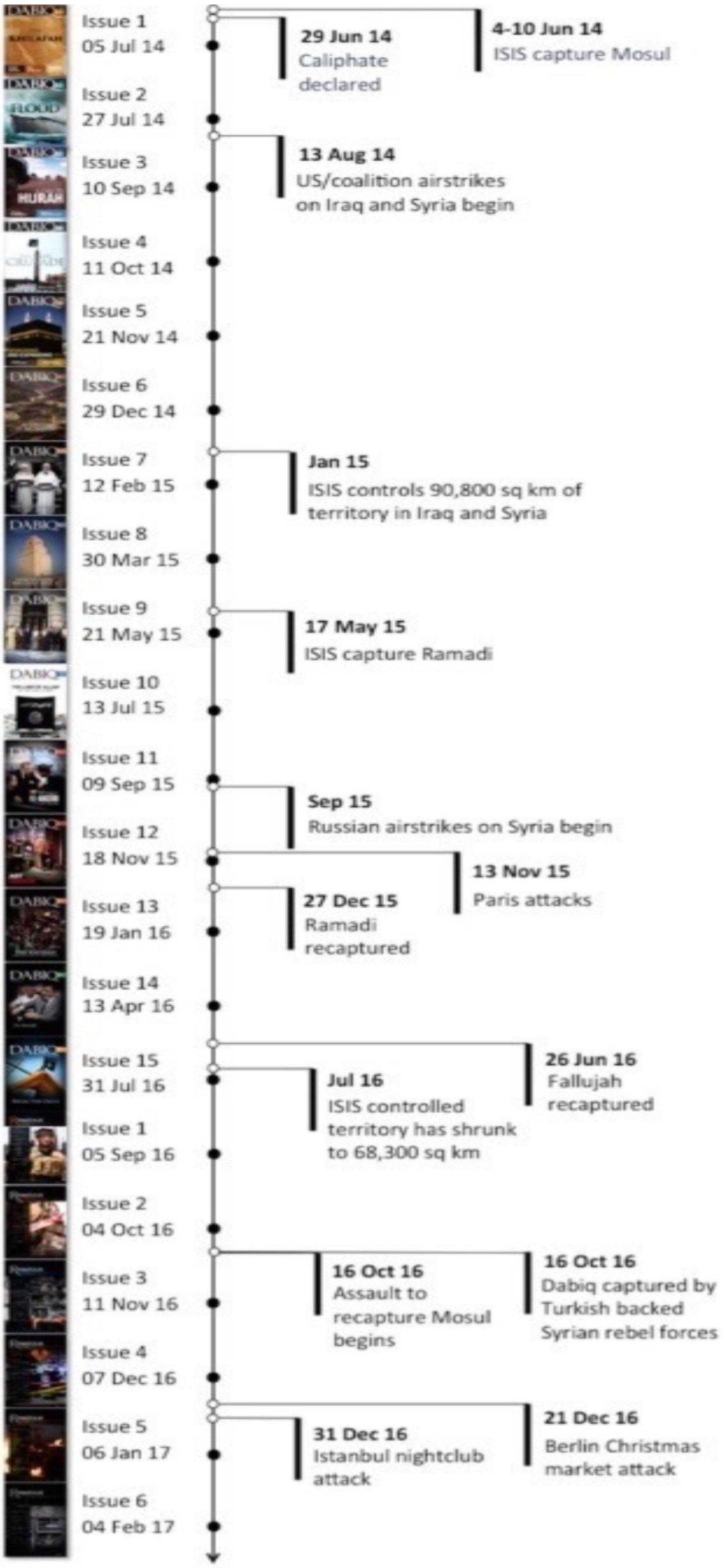


Fig.9: Timeline of issues of Dabiq and Rumiyah and key events in the changing fortunes of ISIS

Source: Wignell, P., Tan, S., O'Halloran, K., L. and Lange R (2017) A Mixed methods Empirical Examination of Changes in Emphasis and Style in the Extremist Magazines *Dabiq* and Rumiyah

Perspectives on terrorism Vol. 11 Issue 2 [Online] Available from: https://espace.curtin.edu.au/bitstream/handle/20.500.11937/53919/252631.pdf?sequence=2&isAllowed=y [7/06/2018]

3.2 Dabiq. The Physical Caliphate

Concurrent with the release of al-Baghdadi's speech, the Al Hayat Media Center published the first issue of Dabiq, a digital English-language monthly magazine series (Stern, Berger, 2016). It was disseminated in multiple languages, including Arabic, French, Turkish and Indonesian to address a vast target audience across the globe (Lombardi, 2015). Hence, Dabiq is "[*an] outreach to the Islamic State's potential fighters and future residents, as well as to its enemies. The magazine is not simply propaganda*" (Gambhir, 2014, 10). Defining itself as a "*magazine focusing on the issues of tawhid (unity), manhaj (truth-seeking), hijra (migration), jihad ('holy war') and jama'a (community)*", Dabiq provides an outward-looking articulation of the ISIS holistic state-building project (Maggioni, 2015). As a matter of fact, the magazine was conceived to brand ISIS as a functional Caliphate by asserting the group's legitimacy on the basis of its territorial control and ability to implement *shari'a* law. To this purpose, it justified the ideology upon which ISIS had been founded, provided battlefield updates and administrative reporting, and, in line with its counter-information campaign, celebrated the deceased fighters.

The first issue pays attention to the choice of the magazine's title. Dabiq, which lies in the Aleppo governorate, approximately 10km from the border with Turkey, features in Islamic apocalyptic prophecies as the site of a cataclysmic battle between Muslims and their Roman enemies based on *hadith* 6924. As reported by Shay (2016), the Prophet Muhammad is believed to have said that the last hour will not come until Muslims overcame the Romans at Dabiq or al-Amaq on their way to conquer Constantinople (Istanbul). Therefore, Celso (2014) has referred to Dabiq as "*IS's Apocalyptic 21st century jihadist manifesto*". The location also carries historical meaning as the site of a crucial battle in 1516 between the Ottomans and the Mamluks, which led to Ottoman victory and the consolidation of the last widely acknowledged Caliphate (Gambhir, 2014). Ironically, on October 16, 2016, ISIS lost control of Dabiq to Turkish backed Syrian rebel forces (Wignell, Tan, O'Halloran and Lange, 2017).

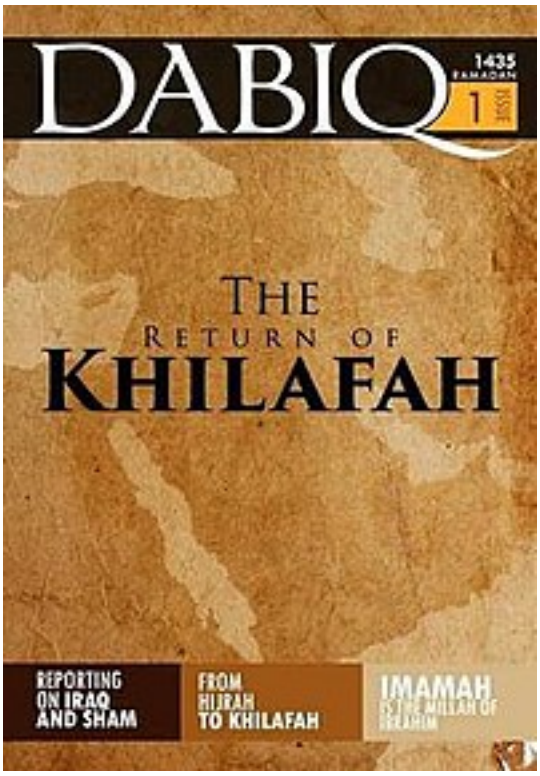


Fig. 10: Dabiq, Issue no.1: The return of Khilafah

Source: Jihadology.net (2014) *al-Ḥayāt Media Center presents a new issue of the Islamic State's magazine: "Dābiq #1"*[Online] Available from: https://jihadology.net/2014/07/05/al-ḥayat-media-center-presents-a-new-issue-of-the-islamic-states-magazine-dabiq-1/ [7/06/2018]

The Dabiq series enumerates fifteen issues published between July 5, 2014 and July 31, 2016. It is interesting to notice that they have not been released on a regular scale, with this mirroring ISIS's difficulty on the ground, especially from August 2015 onwards (Pedde, 2016).

A typical Dabiq issue consists of an introduction, 'Breaking News', 'Reports', 'Articles', 'Wisdoms', 'The Enemy's Words', 'Features', 'News', and a conclusion. To reiterate Dabiq's significance, every issue's table of contents is preceded by a quote of ISIS's spiritual founder, al-Zarqawi, affirming that "*The spark has been lit here in Iraq, and its heart will continue to intensify — by Allah's permission — until it burns the crusader armies in Dabiq*". The choice of this quote signals ISIS's desire to frame itself as an independent organization religiously preferable to other jihadist groups, particularly al-Qaeda.

Drawing on an analysis conducted by Bajrektarevic (2016), three dominant narratives conveyed by Dabiq may be identified: polarization, the glorious warriors and doomsday approaching. As a matter of fact, ISIS's Information Operations sought to polarize and recruit transnational populations by promoting its successes, portraying the group as fair and juxtaposing it with the actions of its opponents; to create a common Muslim heritage and, finally, to motivate readers to take part in the final battle against the infidels.

The first three issues were released during the time of major ISIS expansion (Wignell, Tan, O'Halloran and Lange, 2017). Issue 1 is devoted to explaining the basis of the authority of al-Baghdadi and laying out ISIS's strategy for the establishment of the Caliphate. Issues 2 and 3 solicit migration, which is presented as an obligation and warn of the consequences of not joining the so-called Islamic State. Issue 4 envisions both victory for ISIS and the forthcoming apocalypse. Issues 5 to 8 emphasize unity and disunity among jihadist groups and the deviance of those not allied to ISIS. Issue 9 shifts attention to 'conspiracy' between the near (Shi'a Muslims) and far enemy (the West). Together with Issue 10, it has robust apocalyptic and theological insights. From Issue 11 onwards the focus is firmly on ISIS's enemies. The title of Issue 11 invokes the historical Battle of al-Ahzāb in 627 CE, used as analogy for the conflict between ISIS and the coalition of enemies. Issue 12 gives prominence to the Paris attacks of November 13, 2015. Issue 13 and 14 feature an attack on the 'near enemy', relying on historical and scriptural arguments to predicate the apostasy of Arab leaders who are not aligned with ISIS. Finally, issue 15, '*Break the Cross'*, moves the attack back to the far enemy targeting Christianity and seeking to convert the non-Muslim audience.

3.3 Rumiyah. The Virtual Caliphate

On August 30, 2016 a US airstrike killed al-Adnani in Syria, raising questions about whether ISIS's media branch would continue to function effectively in his absence. Six days later ISIS replaced its longstanding signature magazine, Dabiq, with a new publication, Rumiyah. The title refers to Rome and indicates the deliberate reconsolidation of ISIS's worldwide broadcast. Since ISIS interprets the Western Civilization as a continuum of the ancient Roman Empire, "*aiming to take over Rome is alike taking down the West in its entirety emblematically*" (Latif, 2017, 19). Moreover, "Rumiyah" recalls "*Ar Risala ila Ahl ar Rumiyah*", the Arabic name for the Epistle to the Romans composed by the Apostle Paul, that might confirm ISIS's intention to project globally by converting Western non-believers to Islam (Santoro, 2016). To sum up, in order to avert attention on its military decline after the loss of Dabiq, ISIS produced Rumiyah to purvey thoroughly crafted narratives to amplify its strengths and reframe its setbacks, while reassuring its supporters of eventual victory.[10]

This becomes apparent in the rhetorical shift from Dabiq's initial proclamation, "*This jihad is not possible until you pack and move to Khilafah,*" (Dabiq, 2014, 31) to Rumiyah's "*mobilize from your dens to alleviate the pain afflicting the hearts of the Muslims by striking the kuffar in their homelands*," because, "*it is only from the hikmah of Allah that he has scattered you around the earth and in the various lands of the Crusaders to see which of you are best in deeds*" (Rumiyah, 2016b, 17). As Winter and Parker (2018) point

[10] In Issue 3 of Rumiyah, released on October 16, 2016, the fall of Dabiq is rationalised in a feature article titled '*Towards the Major Malhamah (battle) of Dabiq*' (Rumiyah, Issue 3, pp. 24–26). It warns that ISIS's enemies are mistaken in rejoicing for the fall of Dabiq as this was only the "*minor battle of Dabiq*" and not the "*Major Malhamah of Dabiq*" (Rumiyah, Issue 3, p. 25), which has yet to take place.

out, at its height ISIS deemed successful terrorist operations as a tactical bonus. Now, they represent a strategic imperative, both defensively and offensively.

Furthermore, Rumiyah complements two of ISIS publications released in Arabic, Al-Naba (a weekly newsletter) and Amaq News Agency. This further elucidates ISIS current media strategy: to dominate and grow in cyberspace through misinformation, and compete with mainstream news.

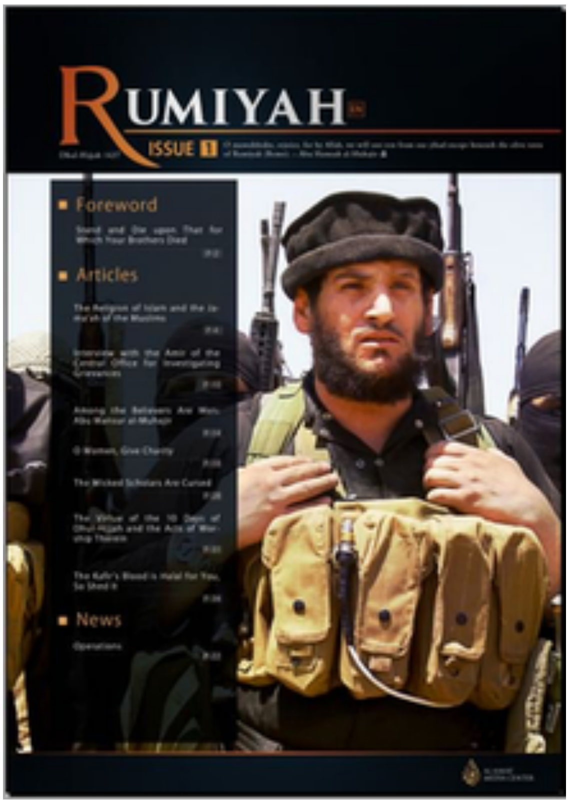

RUMIYAH
ISSUE 1
Foreword
Stand and Die upon That for Which Your Brothers Died
Articles
The Religion of Islam and the Jama'ah of the Muslims
Interview with the Amir of the Central Office for Investigating Grievances
Among the Believers Are Men: Abu Mansur al-Muhajir
O Women, Give Charity
The Wicked Scholars Are Cursed
The Virtue of the 10 Days of Dhul-Hijjah and the Acts of Worship Therein
The Kafir's Blood Is Halal for You, So Shed It
News
Operations

Fig. 11: Rumiyah, Issue no.1

Source: Jihadology.net (2014)

[Online] Available from: https://azelin.files.wordpress.com/2016/09/rome-magazine-1.pdf

[7/06/2018]

Streamlining the previous publication blueprint of the al-Hayat media office, ISIS published Rumiyah in nine languages: English, Arabic, Russian, French, Turkish, German, Indonesian, Uyghur, and Pashto (Mahzam, 2017). The last three languages deserve special attention, as Indonesia boasts the world's biggest Muslim population, Uyghur is spoken by the Chinese Muslim minority living in the Xinjiang Uygur Autonomous Region and Pashto is one of the two official languages of Afghanistan and the second-largest regional language of Pakistan.

Notably, Rumiyah is a stark example of ISIS's effort to tailor its propaganda to fit its objectives within peculiar regions. As a matter of fact, the English-language edition of Issue 1 features an article by the name "*The Kafir's blood is halal for you, so shed it",* which calls for ISIS sympathizers residing in the United Kingdom to execute indiscriminate attacks on *"the businessman riding to work in a taxicab, the young adults (post-pubescent "children") engaged in sports activities in the park, and the old man waiting in line to buy a sandwich*" (Rumiyah, 2016a, 36).

By contrast, the French-language edition highlights a different objective. Due to the increase in the level of security following the 2016 Nice attack, ISIS invites French-based lone wolves not to strike (Analisi Difesa, 2016).

Like Dabiq, each issue opens with a quote attributed to Abu Hamza al-Muhajir, who was appointed leader of al-Qaeda in Iraq after al-Zarqawi's death: "*O muwahhidin, rejoice, for by Allah, we will not rest from our jihad except beneath the olive trees of Rumiyah* (Rome)." The covers of Rumiyah contrast with the covers of Dabiq, because the issues have no title but a dominant image tied to one or more articles. The new magazine is less theological and shorter than the previous ISIS publication, with each issue averaging around 40 pages against Dabiq's 80 pages.

To date, 13 issues of Rumiyah circulate online. The last edition was issued in September 2017 and might be regarded as ISIS's strategic will that marks the end of the current mediatic series in light of de-territorialisation. The underlying focus on *hijra* is to be interpreted as an incitement to conduct the campaign of terror in *Dar al-Kufr*, i.e. territories which are not under the laws of Islam. In fact, ISIS adopted Rumiyah to boost successful terrorist attacks and foment its supporters to imitate these attacks and improvise where necessary, under what it calls "Just Terror Tactics". Issue 2 (October 2016) spells out instructions on how to carry out individual attacks with the exhortation to take readily accessible materials, whereas Issue 3 (released in November 2016) aims attention to the use of vehicles to kill. This modus operandi was adopted by Lahouaiej-Bouhlel who had pointedly rammed a 19-tonne cargo truck into the crowd during Bastille Day celebrations in Nice, France in July 2016. Similarly in Berlin, a truck driven by Anis Amri hit a crowd at a Christmas market. Both assailants of the truck attacks in Nice and Berlin were praised in Rumiyah as "*Soldiers of the Khilafah*" who carried out their just terror operations in response to calls to target the citizens of states engaged in the fight against ISIS. The Knife Attack strategy is explored in Rumiyah Issue 4 (December 2016), through an infographic providing advice on the usage of knives and choice of targets. Issue 5 of Rumiyah (January 2017) shifts the focus to arson attacks with readily accessible flammables. The article details how to make Molotov cocktail and Napalm explosives employing homemade items and explains how to claim responsibility after the attacks.

3.4 Evaluation of ISIS's change in strategy

The overarching purpose of ISIS's Information Strategy is to forge its audience's perceptions in line with its ideological tenets, polarize their support and rally them towards action by capitalizing on a combination of pragmatic and perceptual factors in its propaganda (Ingram, 2016). On the one hand, pragmatic factors, namely security, stability and livelihood, are leveraged in ISIS messaging by boosting the efficacy of its politico-military campaign and denigrating its enemies' efforts via a rational choice decision-making process based on a cost-benefit analysis. In fact, ISIS adheres to the understanding that its propaganda material should be directed at endorsing and propelling forward the group's political apparatus and, finally, winning over extensive support from the masses to advance the group's agenda. On the other hand, perceptual factors - linked to the interplay of in-group, Other, crisis and solution paradigms - are leveraged begging at identity-choice appeals that shape ISIS as the guardian of Sunni Muslims (the in-group identity), its enemies as Others accountable for Sunni perceptions of crisis, and ISIS as the only possessor of solutions to the crisis caused by Others.

ISIS seems to place major emphasis on pragmatic factors when targeting local populations and to prioritise perceptual factors when appealing to regional and transnational audiences. This makes perfect strategic sense because local audiences need to be convinced and coerced to support ISIS's politico-military efforts. At a global level, perceptual factors are more likely to resonate with transnational audiences that are outside of ISIS's direct sphere of control.

From the analysis of Dabiq and Rumiyah, a progressive increase in perceptual factors aimed at fortifying in-group identity at the expenses of pragmatic factors can be observed. It can be inferred that the focus was on recruitment and state-building when ISIS was rapidly expanding the territory under its control and could succesfully present itself as a triumphant and administratively competent organisation, seizing an ever-growing 'promised land' for its believers. Due to stagnation, ISIS switched focus to endorse affiliated organisations, particularly in Africa, to validate that the Caliphate was expanding globally. Finally, ISIS reconciled itself in face of shrinking territory in Syraq (Syria and Iraq) and prioritized attacking its enemies, near and far. By pushing operational tactics content –starkly absent in Dabiq – ISIS appeared to aspire to continue to spread its terror in foreign lands, relying also on what Clarke (2017) has defined "*the terrorist diaspora*", that is, the return of foreign fighters who might be committed to conduct homwgrown-style attacks or create new terror networks.

When seen against this backdrop, the change in ISIS's flagship magazine's name from Dabiq to Rumiyah can be read as strategic. With the highly likely fall of Dabiq, the apocalyptic theme foregrounded in the previous magazine had to be downplayed. The postponement of the imminent apocalypse was replaced with the promise of a longer-term victory, which does not have a definite date attached to it and can thus occur at any time in the future.

As Ingram (2016) mentions, Rumiyah carries the crucial message that regardless of what losses ISIS suffers on the groundi, its *jihad* is essentially a battle of opposing values and is unceasing.

CONCLUSION

Flexible information operations have shown themselves to be one of ISIS's greatest sources of resiliency, as they have supported the organization in rapidly adapting to changing circumstances and framed its victorious image in spite of military defeat. The loss of territory and the death of key leaders have only served to feed propaganda efforts.

The evolution in narrative focus across issues of Dabiq and Rumiyah, with the emphasis put on the call for terrorist attacks to be executed outside the physical caliphate, has allowed ISIS to achieve three purposes: first, to impose significant collateral damage on enemy infrastructure in multiple locations across the world; second, to promulgate ISIS enduring influence by promoting its branding through claims of responsibility for the attacks; third, to provide virtual training ground and inspire a new generation of Internet-savvy militants through the documentation of their activities and the declaration of allegiance to the Caliphate. In fact, the ISIS-inspired attacks that occurred from June to December 2016 echo those advocated in Rumiyah. 22-year-old Dahir Ahmed Adan employed steak knives in the mass stabbing attack at a shopping mall in Minnesota in September 2016 and was known to have had no previous connection to extremism (The Guardian, 2016). Furthermore, the perpetrator of the Ohio State University attack in November 2016, 18-year-old Abdul Razak Ali Artan, adopted both the knife and vehicle methods endorsed in Rumiyah when he drove his car into a crowd before charging out with a knife (CNN, 2016).

Thus, although it has posed a significant threat to one of the essential postulates of its existence, the loss of territory has not signaled the end of ISIS. The addition of Rumiyah to its ever-growing media apparatus has marked ISIS's transition to a Virtual Caliphate, a radicalized, cyber-based community that could reinforce the global Salafi-jihadi movement and function independently of ISIS (Gambhir, 2016).

The Virtual Caliphate would consist of a network of like-minded individuals connecting via chat rooms, jihadi forums, and social media. The group would benefit from ISIS's legacy and could incorporate some aspects of ISIS's present day online recruitment network and proliferation of content, but is likely to self-organize to prioritize target and attack types and boost best practices.

On the other hand, from its virtual safe haven ISIS will continue to coordinate and galvanise external attacks as well as create a solid support base until the organisation has the capability to reclaim physical territory (Coolsaet, 2017). Notably, ISIS's ideology, amplified through the execution of global information operations, will persist online and continue to inspire new generations of terrorists.

Clearly, the Virtual Caliphate will not necessarily be anchored to terrain. Many core aspects of the organization will be increasingly digitally executed, including communications, recruitment, cyberspace operations, public affairs, and possibly command and control. This new entity might re-characterize the threat of the global Salafi-jihadi movement.

If pre-2016 ISIS's online activities were merely a virtual means to a real-world end, the fall of territorial possessions in the Middle East has indeed changed the real-virtual relationship on the side of the cyber dimension. Hence the ISIS case validates the current trend that wars are no longer confined to the physical battlefield but have entered the digital realm. Unlike Al-Qaeda's Inspire or Jabhat Al-Nusra's Al-Risalah, Rumiyah and Dabiq have demonstrated that the global jihadist struggle involves not only military capacity but also a competence in crafting narratives through digital media. In other words, virtual *jihad* has not only gained credibility as a wholly legitimate alternative to traditional notions of *jihad* but has also surpassed physical *jihad.*

Nowadays all actors interacting in the international relations arena wage information-driven wars. This new wave of information warfare causes the world to be faced with serious repercussions. Digital peripherals, videos and info-graphics have become *sine qua non* medium to affect or transform strategic thinking and behavior, in a manner that is unlike coercive warfare in the physical space.

REFERENCES

- Amble, J.C., (2012) Combating Terrorism in the New Media Environment. *Studies in Conflict & Terrorism* [Online] 35 (5), p. 339- 353
- AnalisiDifesa (2016) *Rumiyah,* la rivista dell'ISIS per la conquista di Roma [Online] Available from: http://www.analisidifesa.it/2016/09/rumiyah-la-rivista-dellisis-per-la-conquista-di-roma/ [7/06/2018]
- Arquilla, J., Ronfeldt, D.F. (1997) *In Athena's Camp. Preparing for Conflict in the Information Age*. Santa Monica: Rand Coporation
- Bajrektarevic, A. (2016) Narratives in Extremist Propaganda. How Terrorist Groups Shape Propaganda Discourse. *Nordicom-Information* [Online] (38)2, p. 94-97. Available from: http://www.nordicom.gu.se/sites/default/files/kapitel-pdf/nordicom-information_38_2016_2_94-97.pdf [7/06/2018]
- Benmelech, E., Klor, E.F. (2016) What Explains the Flow of Foreign Fighters to ISIS? *NBER* [Online] Working Paper No. 22190, p. 1-25. Available from: http://www.kellogg.northwestern.edu/faculty/benmelech/html/BenmelechPapers/ISIS_April_13_2016_Effi_final.pdf [8/06/2018]
- Bindner L., Gluck R. (2017) Wilayat Internet: ISIS's Resilience across the Internet and Social Media *Bellingcat* [Online]. Available from: https://www.bellingcat.com/news/mena/2017/09/01/wilayat-internet-isis-resilience-across-internet-social-media/ [8/06/2018]
- Borum, R., Fein, R. (2017) The Psychology of Foreign Fighters *Studies in Conflict & Terrorism, 40:3*
- Brantly, A., F. (2016) *The decision to attack: military and intelligence cyber decision-making.* Athens: University of Georgia Press
- Bunzel, C. (2015) From Paper State to Caliphate: The Ideology of the Islamic State *Center for Middle East Policy at Brookings* [Online] No. 19, March. Available from: https://www.brookings.edu/wp-content/uploads/2016/06/The-ideology-of-the-Islamic-State.pdf [7/06/2018]
- Carmon, Y., Yehoshua, Y., Leone, A. (2014) Understanding Abu Bakr Al-Baghdadi and the Phenomenon of the Islamic State *MEMRI* [Online] Available from: https://www.memri.org/reports/understanding-abu-bakr-al-baghdadi-and-phenomenon-islamic-caliphate-state [1/12/2017]
- Carr, J. (2012) *Inside Cyber Warfare*. Second Edition. Newton, MA: O' Reilly Media
- Carter, J. A., Maher, S., Neumann, P., R. (2014), *#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks* [Online] The International Centre for the Study of Radicalization and Political Violence (ICSR) Available from: http://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf [8/06/2018]

- Celso, A. (2014) Dabiq: IS's Apocalyptic 21st Century Jihadist Manifesto *Political Sciences & Public Affairs,* (2) [Online] Available from: https://blackboard.angelo.edu/bbcswebdav/institution/LFA/CSS/Course%20Material/CCSS3312/Readings/dabiq-iss-apocalyptic-21st-century-jihadist-manifesto-2332-0761.1000e111.pdf [7/06/2018]
- Choucri, N. (2012) *Cyberpolitics in International Relations* Cambridge, Massachusetts: The MIT Press
- Chuipka, A. (2016) *The strategies of Cyberterrorism. Is Cyberterrorism an effective means to Achieving the Goals of Terrorists?* [Online] Graduate School of Public and International Affairs, University of Ottawa. Available from: https://ruor.uottawa.ca/bitstream/10393/35695/1/CHUIPKA%2C%20Adam%2020169.pdf [8/06/2018]
- CISCO (2013) *The Internet of Everything. Global Public Sector Economic Analysis* [Online]. Available from: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf [8/06/2018]
- Clark, D. D. (2010) Characterizing Cyberspace: Past, Present and Future *MIT/CSAIL Working Paper,* March 12
- CNN (2016) *Ohio State attacker when he was 'scared' to pray in public* [Online] Available from: https://edition.cnn.com/2016/11/28/us/ohio-state-attacker-abdul-razak-ali-artan/index.html [8/06/2018]
- Coolsaet, R. (2017) *Anticipating the Post-Daesh landscape* Egmont [Online] Paper 97. Available from: http://www.egmontinstitute.be/content/uploads/2017/10/Egmont-Paper-97.pdf?type=pdf [8/06/2018]
- Counter Extremism Project (2018) *ISIS* https://www.counterextremism.com/sites/default/files/threat_pdf/ISIS-01222018.pdf [8/06/2018]
- Dabiq (2014) *A Call to Hijrah* [Online] Available from: https://clarionproject.org/docs/isis-isil-islamic-state-magazine-Issue-3-the-call-to-hijrah.pdf
- Defense Technical Information Center (2014) Information Operations [Online] November 20. Available from: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [8/06/2018]
- EastWest Institute and the Information Security Institute of Moscow State University (2014) *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundation* [Online] *Issue 2.* Available from: https://www.files.ethz.ch/isn/178418/terminology2.pdf [3/04/2018]
- Edwards, B., Furnas, A., Forrest, S., Axelrod, R. (2017) Strategic aspects of Cyber Attack, Attribution and Blame *Proceedings of the National Academy of Sciences* [Online] Available from: http://www-personal.umich.edu/~axe/ [8/06/2018]
- Eriksson, J., Giacomello, G. (2006) The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review* [Online] 27(3), p. 221–44. Available from: http://journals.sagepub.com/doi/pdf/10.1177/0192512106064462 [8/06/2018]
- Fishman, B. (2006) After Zarqawi: The Dilemmas and Future of Al Qaeda in Iraq *The Washington Quarterly* [Online] Vol. 29, No. 4, Autumn. Available from: https://ctc.usma.edu/app/uploads/2010/06/After-Zarqawi_WashingtonQuarterly-FINAL.pdf [7/06/2018]

- Fitton, O. (2016) Cyber Operations and Gray Zones: Challenges for NATO *Connections: The Quarterly Journal* [Online] 15, no.2 p.109-119. Available from: https://connections-qj.org/system/files/15.2.08_fitton_cyber_gray_zones.pdf [3/04/2018]
- Friedman, T. L. (2005) *The world is flat: a brief history of the twenty-first century* New York: Farrar, Straus and Giroux
- Gambhir, H. (2014) Dabiq: the strategic messaging of the Islamic State [Online] Institute for the Study of War. Available from: http://www.understandingwar.org/sites/default/files/Dabiq%20Backgrounder_Harleen%20Final.pdf [8/06/2018]
- Gambhir, H. (2016) *The Virtual Caliphate: ISIS's information warfare* [Online] Institute for the Study of War. Available from: http://www.understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf [8/06/2018]
- Garamone, J. (2018) *Intel Chiefs Tell Senate Committee of Dangers to America* [Online] GlobalSecurity.org. March 6. Available from: https://www.globalsecurity.org/intell/library/news/2018/intell-180306-afps01.htm?_m=3n%2e002a%2e2243%2erh0ao0cyut%2e22ce [8/06/2018]
- Gartner (2017) *Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017* [Online]. February 7 Available from: https://www.gartner.com/newsroom/id/3598917 [8/06/2018]
- Gerges, F. A. (2014) 'ISIS and the Third Wave of Jihadism' *Current History* [Online] 113 (767), p. 339-343. Available from: http://currenthistory.com/Gerges_Current_History.pdf [8/06/2018]
- Gibson, W. (1984) *Neuromancer*. New York: Berkeley Publishing Group.
- Groll, E., (2017) Who is Really to Blame for the WannaCry Ransomware? *Foreign Policy* [Online] May 15. Available from: http://foreignpolicy.com/2017/05/15/who-is-really-to-blame-for-the-wannacry-ranswomware/ [8/06/2018]
- Hacker, F. J. (1977) *Crusaders, Criminals, Crazies: Terror and Terrorism in Our Time*. New York: W.W. Norton & Co Inc
- Hanieh, H. A. (2016) The Islamic State's Appeal: Theories of Attraction In: *The Secret of Attraction. ISIS Propaganda and Recruitment.* Friedrich-Ebert-Stiftung-Jordan and Iraq. Available from: http://library.fes.de/pdf-files/bueros/amman/12552-20160728.pdf [8/06/2018]
- Hoffman, B. (2006) *Inside terrorism*. Reviewed and expanded edition. New York: Columbia University Press
- Ingram, H. J. (2016) Learning from ISIS's virtual propaganda war for Western Muslims: A comparison of Inspire and Dabiq *Australian Institute of International Affairs* [Online] Available from https://icct.nl/wp-content/uploads/2017/07/INGRAM-nato-chapter-21JUL17.pdf [8/06/2018]
- Ingram, H. J. (2016) An analysis of Islamic State's Dabiq magazine *Australian Journal of Political Science* [Online] Available from: http://www.internationalaffairs.org.au/wp-content/uploads/2016/06/An-analysis-of-Islamic-State-s-Dabiq-magazine.pdf [8/06/2018]

- Ingram, H. J. (2016) ISIS: Assessing Rumiyah *Australian Institute of International Affairs* [Online] September 12. Available from: http://www.internationalaffairs.org.au/australianoutlook/isis-assessing-the-rumiyah-magazine/ [8/06/2018]
- Institute for National Security Studies (2012) *Cyber Warfare: Concepts and Strategic Trends* [Online] Memorandum No.117. Available from: https://www.files.ethz.ch/isn/152953/INSS%20Memorandum_MAY2012_Nr117.pdf [8/06/2018]
- Jenkins, B. M. (1974) International terrorism: a new kind of warfare *The RAND Corporation* [Online] P-5621, p.1-13. Available from: https://www.rand.org/content/dam/rand/pubs/papers/2008/P5261.pdf [8/06/2018]
- Jenkins, B. M. (2011) Is Al Qaeda's Internet Strategy Working? *The RAND Corporation* [Online] Available from: https://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT371.pdf [8/06/2018]
- Jihadology.net (2014) *al-Ḥayāt Media Center presents a new issue of the Islamic State's magazine: "Dābiq #1"* [Online] Available from: https://jihadology.net/2014/07/05/al-ḥayat-media-center-presents-a-new-issue-of-the-islamic-states-magazine-dabiq-1/ [7/06/2018]
- Joint Publication (2011) 5-0 *Joint Operation Planning* [Online] August 11. Available from: https://grugq.github.io/resources/jp5_0.pdf [8/06/2018]
- Jones, S. G., Dobbins, J., Byman, D., Chivvis, C. S., Connable, B., Martini, J., Robinson, E., Chandler, N. (2017) *Rolling back the Islamic State* The RAND Corporation, Santa Monica [Online] Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1912/RAND_RR1912.pdf [7/06/2018]
- Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In Kramer F., Starr S., & Wentz L. (Eds.), *Cyberpower and National Security* (pp. 24-42) Washington D.C.: National Defense University Press, Potomac Books. Available from: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf [8/06/2018]
- Lachow, I. (2009) Cyber Terrorism: Menace or Myth? In: Kramer, F.,D., Starr, S.,H. and Wentz, L.,K. *Cyberpower and National Security*. Washington: NDU Press
- Lal, V. (2002) Terror and Its Networks: Disappearing Trails in Cyberspace (draft) *The Nautilus Institute* [Online] Available from: http://oldsite.nautilus.org/gps/virtual-diasporas/paper/Lal.html [8/06/2018]
- Latif, D. A. (2017) What do they say? Mapping the propaganda discourse of Islamic State publications: An analysis of Dabiq and Rumiyah [Online] *CEU eTD Collection* Available from: http://www.etd.ceu.hu/2017/latif_danish.pdf [8/06/2018]
- Lieberman, A. V. (2017) Terrorism, the Internet and Propaganda: A Deadly Combination *Journal of National Security Law & Policy* [Online] *Vol. 9:95, January, 1* Available from: http://jnslp.com/wp-content/uploads/2017/04/Terrorism_the_Internet_and_Propaganda_FINAL.pdf [8/06/2018]

- Lombardi, M. (2015) IS 2.0 e molto altro: il progetto di comunicazione del califfato. In: Maggioni, M., Magri, P., *Twitter e jihad: la comunicazione dell'Isis.* [Online] *ISPI*. Edizioni Epoké. Available from: http://www.ispionline.it/it/EBook/TWITTER_JIHAD_COMUNICAZIONE_ISIS.pdf [8/06/2018]
- Lumbaca, S., Gray, D. H. (2011) The Media as an Enabler for Acts of Terrorism *Global Security Studies* [Online] Volume 2, Issue 1. Available from: http://globalsecuritystudies.com/Media.pdf [8/06/2018]
- Maggioni, M. (2015) Lo Stato Islamico: una sorpresa solo per chi lo racconta. In: Magri, P., Maggioni, F. Twitter e Jihad: La comunicazione dell'ISIS *ISPI* [Online] Available from: https://www.ispionline.it/it/EBook/TWITTER_JIHAD_COMUNICAZIONE_ISIS.pdf[7/06/2018]
- Mahzam, R. (2017) Rumiyah: Jihadist Propaganda and Information Warfare in Cyberspace *RSIS* [Online] Available from: http://www.css.ethz.ch/en/services/digital-library/articles/article.html/f8a5b90d-29e3-47bb-a643-307673409cc5/pdf [7/06/2018]
- Marchetti, R., Mulas R. (2017) *Cyber Security. Hacker, terroristi, spie e le nuove minacce del web.* Roma: LUISS University Press
- McInnis, K., J. (2016) Coalition Contributions to Countering the Islamic State *Congressional Research Service* [Online] August 24. Available from: https://fas.org/sgp/crs/natsec/R44135.pdf [7/06/2018]
- Mills, C. (2018) ISIS/Daesh: what now for the military campaign in Iraq and Syria? *House of Commons Library* [Online] Briefing Paper, Number 8428, March 7. Available from: http://researchbriefings.files.parliament.uk/documents/CBP-8248/CBP-8248.pdf [8/06/2018]
- Milton, D. (2016) Communication Breakdown: Unraveling the Islamic State's Media Efforts *Combating Terrorism Center at West Point* [Online] Available from: https://ctc.usma.edu/communication-breakdown-unraveling-the-islamic-states-media-efforts/ [7/06/2018]
- Nair, K., N. (2016) The rise and future of ISIS *Journal of Defence Studies* [Online] Vol. 10 No. 4. Available from: https://idsa.in/system/files/jds/jds_10_4_2016_the-rise-and-future-of-isis.pdf [7/06/2018]
- National Research Council (1991) *Computers at Risk: Safe Computing in the Information Age* Washington: The National Academies Press
- NATO Strategic Communications Centre of Excellence (2016) *Daesh Information Campaign and Strategy. Results of the study* [Online] Available from: http://www.difesa.it/SMD_/CASD/IM/IASD/65sessioneordinaria/Documents/DaeshInformationCampaignanditsInfluence.pdf [7/06/2018]
- Nye, J. S., Jr (2010) Cyber power *Belfer Center for Science and International Affairs*, *Harvard Kennedy School* [Online] Available from: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [8/06/2018]
- Nye, J., S. Jr (2011) *The Future of Power* New York: Public Affairs
- Nye, J. S. Jr (2018) How Sharp Power Threatens Soft Power *Foreign Affairs* [Online] January 24. Available from: https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power [8/06/2018]
- Oosterveld, W., T., Bloem, W. (2017) The Rise and Fall of ISIS: From Evitability to Inevitability

The Hague Centre for Strategic Studies [Online] Available from: https://hcss.nl/sites/default/files/files/reports/The%20Rise%20and%20Fall%20of%20ISIS.pdf [8/06/2018]

- Osinga, F. P. B (2007) *Science, Strategy and War: The Strategic Theory of John Boyd.* London: Routledge

- Pedde, N. (2016) *Information Campaign del DAESH contro l'Occidente* Ce.Mi.S.S [Online] Available from: https://www.difesa.it/SMD_/CASD/IM/CeMiSS/DocumentiVis/Rcerche_da_pubblicare/Ricerche_2017/AL_SA_08_Pedde_information_campaign.pdf https://espace.curtin.edu.au/bitstream/handle/20.500.11937/53919/252631.pdf?sequence=2&isAllowed=y [7/06/2018]

- Plebani, A. (2014) New (and old) patterns of jihadism: al-Qa'ida, the Islamic State and beyond *ISPI* [Online] Available from: https://www.ispionline.it/it/documents/E_book_jihadism.pdf [7/06/2018]

- Roy, O. (2010) The Allure of Terrorism *The New York Times* [Online] *Jan, 10, 2010*. Available from: https://www.nytimes.com/2010/01/11/opinion/11iht-edroy.html [3/05/2018]

- Rumsfeld, D. (2002) DoD News Briefing – Secretary Rumsfeld and Gen. Myers *U.S. Department of Defense* [Online]. February 12. Available from: http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 [8/06/2018]

- Rumiyah (2016b) *Issue no.1* [Online] Available from: https://clarionproject.org/factsheets-files/Rumiyah-ISIS-Magazine-1st-issue.pdf [8/06/2018]

- Rumiyah (2016a) *Issue no. 3* [Online] Available from: https://azelin.files.wordpress.com/2016/11/rome-magazine-3.pdf [8/06/2018]

- Richards, LaSalle, Devost, van den Dool, Kennedy-White 2017. *Cost of Cyber Crime Study*. https://www.accenture.com/ t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/ Accenture-2017-CostCyberCrimeStudy.pdf

- Santoro, D. (2016) L'ISIS lancia una nuova rivista online denominata Rumiyah *Geopolitica.info* [Online] September, 12 Available from: https://www.geopolitica.info/rumiyah/ [7/06/2018]

- Scott, M. (2018) Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower *Politico* [Online] March 27. Available from: https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/ [3/04/2018]

- Shay, S. (2016) *The fall of Dabiq and the fall of the Caliphate* Institute for Policy and Strategy, Lauder School of Government, Diplomacy and Strategy IDC Herzliya [Online] Available from: http://www.herzliyaconference.org/eng/_Uploads/dbsAttachedFiles/ThefallofDabiq_Shay_19_10_16.pdf [7/06/2018]

- SITE (2014a) ISIS Spokesman declares Caliphate, rebrands group as 'Islamic State' [Online] June 29. Available from: https://news.siteintelgroup.com/Jihadist-News/isis-spokesman-declares-caliphate-rebrands-group-as-islamic-state.html [7/06/2018]

- SITE (2014b) Islamic State Leader Abu Bakr al-Baghdadi Encourages Emigration, Worldwide Action [Online] July 1. Available from: https://news.siteintelgroup.com/Jihadist-News/islamic-state-leader-abu-bakr-al-baghdadi-encourages-emigration-worldwide-action.html [7/06/2018]
- Stern, J., Berger, J. M. (2016) *ISIS: The State of Terror* [Online] Available from: https://www.researchgate.net/publication/308089080_ISIS_The_State_of_Terror [7/06/2018]
- The Guardian (2016) *Minnesota stabbing: Dahir Ahmed Adam was known for calm demeanor* [Online] Available from: https://www.theguardian.com/us-news/2016/sep/20/minnesota-stabbing-dahir-ahmed-adan-college-security-guard [7/06/2018]
- Tugwell, M. (1986) Terrorism and Propaganda: Problem and Response *Conflict Quarterly* [Online] Available from: https://journals.lib.unb.ca/index.php/JCS/article/viewFile/14713/15782 [7/06/2018]
- Tyagi, R K. (2013) *Understanding Cyber Warfare and its Implications for Indian Armed Forces* Vij Books India Pvt Ltd
- Tzu, S. (2000) *On the Art of War* Allandale Online Publishing. Available from: https://sites.ualberta.ca/~enoch/Readings/The_Art_Of_War.pdf [8/06/2018]
- United Nations Counter-Terrorism Implementation Task Force (2011) *Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects* [Online] May. Available from: http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf [8/06/2018]
- U.S. Department of Defense (2016) *Strategy for operations in the information environment.* Available from: https://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf [8/06/2018]
- Veres, L. (2004) Prensa, poder y terrorismo. *Amnis* [Online] 4. Available from: http://amnis.revues.org/706 [8/06/2018]
- Walker, C., Ludwig, J. (2017) The Meaning of Sharp Power: How Authoritarian States Project Influence *Foreign Affairs* [Online] November, 16. Available from: https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power [3/04/2018]
- Weimann, G. (2004) www.terror.net: How Modern Terrorism Uses the Internet *United States Institute of Peace* [Online] *Special Report 116, March 2004.* Available from: https://www.usip.org/sites/default/files/sr116.pdf [8/06/2018]
- Weimann, G. (2006) *Terror on the Internet: The New Arena. The New Challenges* [Online] Washington: United States Institute for Peace (USIP) Press.
- Weimann, G. (2015) *Terrorism in Cyberspace: the Next Generation* [Online] New York: Columbia University Press; Washington: Woodrow Wilson Center Press
- Wiener, N. (1948) *Cybernetics or control and communication in the animal and the machine.* Cambridge: The MIT Press
- Wilkinson, P. (2001) *Terrorism versus Democracy*. London: Frank Cass

- Wignell, P., Tan, S., O'Halloran, K., L., Lange R (2017) A Mixed methods Empirical Examination of Changes in Emphasis and Style in the Extremist Magazines *Dabiq* and *Rumiyah. Perspectives on terrorism* [Online] Vol. 11 Issue 2. Available from: https://espace.curtin.edu.au/bitstream/handle/20.500.11937/53919/252631.pdf?sequence=2&isAllowed=y [7/06/2018]
- Winter, C. (2015) *Documenting the Virtual Caliphate.* [Online] *Quilliam*. Available from: http://www.quilliaminternational.com/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf [8/06/2018]
- Winter, C., Parker, K. (2018) Virtual Caliphate Rebooted: The Islamic State's Evolving Online Strategy *Lawfare* [Online] Available from: https://lawfareblog.com/virtual-caliphate-rebooted-islamic-states-evolving-online-strategy [8/06/2018]
- Wong, W., H, Brown, P., A. (2013) E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One *American Political Science Association* 11(4) Available from: http://politics.utoronto.ca/wp-content/uploads/2013/12/wong-and-brown-2013.pdf [8/06/2018]
- World Economic Forum (2018) *The Global Risks Report 2018, 13th Edition* [Online] Available from: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [7/06/2018]
- Xu, B., Albert, E. (2017) Media Censorship in China *Council on Foreign Relations* [Online] February 17. Available from: https://www.cfr.org/backgrounder/media-censorship-china [8/06/2018]
- Zelin, A. (2013) The State of Global Jihad Online *New America Foundation* [Online] January. Available from: http://www.washingtoninstitute.org/uploads/Documents/opeds/Zelin20130201-NewAmericaFoundation.pdf [8/06/2018]

ABSTRACT

Nell'era dell'informazione, il cyberspazio costituisce la struttura portante delle piattaforme di social networking, dell'economia globale, dei servizi essenziali e della *command and control warfare*. Il dominio cyber ha dunque penetrato tutti gli strumenti del potere nazionale: Diplomatico, Informativo/Interno, Militare ed Economico (DIME). Dalla convergenza dei mondi virtuali e reali derivano numerose nuove minacce che alterano il panorama della sicurezza nazionale. Il tradizionale spettro della minaccia ha infatti inglobato gli attacchi cyber che, in base al rapporto sui rischi globali elaborato nel 2018 dal World Economic Forum, compaiono nella classifica dei primi cinque rischi globali per probabilità percepita. I recenti attacchi cyber hanno rivelato un denominatore comune nel colpire le infrastrutture critiche e strategiche degli Stati, dimostrando di poter produrre le stesse conseguenze dei tradizionali attacchi cinetici. La complessità e l'imprevedibilità degli attacchi cyber, insieme alle questioni legate alla velocità e all'attribuzione, li rendono un "*unknown unknown*", ovvero "rischi della cui esistenza siamo ignari".

L'emergere del cyberspazio come campo di battaglia in cui le azioni intraprese sono immediate, anonime e hanno ripercussioni globali ha generato nuovi modi.. per perseguire gli interessi di attori statuali e non-statuali.

I primi approfittano dell'anonimità garantita dal cyberspazio per manipolare le condizioni del sistema internazionale a proprio vantaggio, influenzando le decisioni politiche e l'opinione pubblica di altri Stati. Anche i secondi - in particolare i gruppi terroristici - si avvalgono del carattere asimmetrico del cyberspazio per indottrinare, diffondere notizie, raccogliere fondi, reclutare e mobilitare potenziali combattenti.

La presente tesi mira ad analizzare l'impatto della "cyberizzazione" delle relazioni internazionali e dell'età dell'informazione sulle nuove minacce terroristiche globali, riservando particolare attenzione alle *information operations* (IO) dell'ISIS, i cui obiettivi riflettono quelli delle operazioni militari, che coadiuvano, come mostrato dall'evoluzione della narrativa di Dabiq (il giornale rappresentativo del Califfato reale) e Rumiyah (in cui si delinea la creazione di un Califfato virtuale alla luce delle perdite territoriali).

L'ISIS è stato selezionato come caso studio perché rappresenta il primo gruppo terroristico ad aver reso operativi i social media, mostrando una sapiente capacità nell'utilizzo poliedrico dei mezzi di comunicazione riadattati alle proprie esigenze di propaganda e contro-informazione. Presentandosi come un'entità statuale con un disegno politico globale, in opposizione ai progetti locali di gruppi jihadisti rivali, ha catalizzato l'attenzione di un'audience multietnica, globale e interclasse.

Il Dipartimento della Difesa statunitense ha definito il cyberspazio come "un dominio globale all'interno del più ampio universo di informazioni composto dalle reti interdipendenti di infrastrutture basate sulla tecnologia informatica e dati residenti, compreso Internet, la rete delle telecomunicazioni, i sistemi di computer, processori e controller *embedded*". In passato, il cyberspazio era ritenuto un dominio della *low politics*, dato che fungeva puramente da base ai processi decisionali di routine. Successivamente, è stato elevato al rango della *high politics.* Di conseguenza, nel 2016 la NATO ha ufficialmente riconosciuto il cyberspazio come dominio delle operazioni insieme a quelli di terra, mare, aria e spazio. La natura pervasiva del cyberspazio amplifica gli effetti strategici delle operazioni condotte e comporta implicazioni di vasta portata negli altri domini, ma ne differisce qualitativamente. Il carattere peculiare del cyberspazio risiede nella sua artificialità e nella sua capacità di creare, archiviare, modificare, scambiare e sfruttare le informazioni. Quest'ultima è divenuta una risorsa strategica e una quarta dimensione del potere nazionale a cui le componenti politiche, economiche e militari di uno Stato si affidano per realizzare il loro potenziale. Nel cyberspazio, i concetti classici di tempo, spazio e distanza variano significativamente. Inoltre, il cosiddetto quinto dominio non è limitato geograficamente, ma aumenta di valore e dimensione con ogni nuova connessione.

La combinazione dei quattro strati del cyberspazio individuati da Clarke – la rete fisica, la rete logistica, il contenuto di informazioni e gli attori cyber – caratterizza attivamente la *cyberpolitics* convertendo il dominio cyber in una nuova arena che offre opportunità di competizione e conflitti e di articolazione delle relazioni internazionali.

La democratizzazione dell'informazione promossa dalla spinta propulsiva della rivoluzione informatica ha determinato una diffusione del potere che priva lo Stato-nazione della storica prerogativa del monopolio del potere e della violenza. Difatti, una pluralità di attori interagisce nel cyberspazio per massimizzare la propria utilità politica. Alle operazioni cyber condotte dagli Stati – distinte in esterne se dirette contro Stati rivali ed interne se tese ad orientare decisioni politiche all'interno dei propri confini territoriali – si affiancano hacktivisti motivati politicamente e terroristi che piegano lo strumento cyber ai propri interessi di cambiamento politico. Le attività politiche intraprese nel cyberspazio poggiano sul potere cyber, o "l'abilità di usare il cyberspazio per creare vantaggi e influenzare eventi in altri ambienti operativi e attraverso gli strumenti di potere", ritenuto un'originale manifestazione dell'*hard power*. A sua volta, il potere cyber dipende dall'informazione al fine di manovrare la percezione dell'ambiente operativo a proprio vantaggio e diminuire la capacità dell'avversario di comprendere lo stesso ambiente. L'informazione, declinata in misinformazione e disinformazione, ha costituito un aspetto fondamentale della politica nazionale e internazionale dai tempi di Sun Tzu. Tuttavia, Internet ha consentito che la manipolazione si svolgesse su scale precedentemente inconcepibili di tempo, spazio e intenzionalità. In conclusione, si prospetta che sia attori statuali che non-statuali integreranno progressivamente *information operations* nella loro *grand strategy*, sincronizzandole con quelle militari per reagire agli eventi mondiali. Allo stesso tempo i successi militari saranno sempre più legati all'efficacia delle *information operations* volte a condizionare la leadership e i processi decisionali degli avversari.

A causa della loro natura di gruppo subnazionale o di entità non-statuale, ai terroristi manca l'influenza necessaria per raggiungere l'obiettivo di generare o consolidare potere. Dunque, un atto di violenza scrupolosamente coreografato, che includa elementi teatrali, rappresenta un requisito essenziale per accedere al palcoscenico politico globale e attirare attenzione sulla causa del gruppo. Infatti, "*il terrorismo è teatro*": i terroristi si esibiscono avendo a mente una precisa audience e aspirano a suscitare un'atmosfera di paura per moltiplicare il loro potere oltre le loro reali capacità.

Inoltre, il terrorismo provoca il rovesciamento della tradizionale relazione tra notizie e fatti. Le notizie non dipendono più dai fatti; questi ultimi sono diventati una funzione del processo di *newsmaking*. Così, le notizie acquistano una presenza eterna che preserva la vita del fatto anche in seguito alla sua scadenza. Il terrorismo e i media sono dunque intrecciati in una pericolosa relazione simbiotica di sfruttamento reciproco e manipolazione, paragonata a una danza della morte, in un caso in funzione di motivazioni politiche o ideologiche, nell'altro per successi commerciali.

Se tradizionalmente le speranze dei terroristi di ottenere pubblicità per la propria causa erano legate al superamento della soglia di selezione fissata dai media, grazie a Internet i gruppi terroristici possono gestire la percezione della propria immagine di fronte al mondo e modellare la comunicazione sull'audience di riferimento. Internet rappresenta una sorta di santuario virtuale in cui i terroristi svolgono attività comunicative o strumentali. Alla prima categoria appartengono la disseminazione di propaganda, le campagne di guerra psicologica, la mobilitazione di potenziali membri del gruppo. Alla seconda, invece, fanno capo l'indottrinamento e l'addestramento virtuale, la pianificazione e il coordinamento cyber degli attacchi e la raccolta fondi.

Il jihadismo è uno dei principali movimenti radicali ad aver tratto profitto dalla rivoluzione della comunicazione per diffondere il proprio messaggio. E' possibile identificare quattro fasi in cui i media jihadisti sono stati distribuiti dal 1984. Nella prima fase, la prima generazione di mujaheddin faceva circolare documenti di propaganda in forma orale e scritta. La seconda generazione iniziò ad usare Internet attraverso siti *top-down*. La terza fase è contraddistinta dall'emergere di forum interattivi in cui gli amministratori postano contenuti per conto di organizzazioni jihadiste senza esserne direttamente connessi. Con la terza generazione, forgiata dalla rivoluzione siriana del 2011, gli individui, e non le organizzazioni, assumono un ruolo più rilevante attraverso i social media. Nella battaglia per i cuori e le menti della *ummah,* la guerra delle narrative riveste un ruolo maggiore di quello dei classici proiettili e delle armi da fuoco, come dimostrato dagli sforzi di al-Qaeda e dell'ISIS di incorporare l'imperativo mediatico. Il debutto online di al-Qaeda è avvenuto nel 2000. L'organizzazione ha esplicitamente riconosciuto l'importanza di Internet come strumento di propaganda e, in seguito alla distruzione del proprio santuario in Afghanistan, si è trasformata in una rete decentralizzata di cellule affiliate e semi-indipendenti prive di una singola gerarchia al comando. La nuova struttura ha influenzato le numerose produzioni online del gruppo. L'ISIS ha trasformato una guerra locale in un fenomeno globale tramite una strategia di informazione ben definita e coerente basata sulla dialettica tra l'approccio centralizzato condotto da un organo mediatico ufficiale integrato nel nucleo dell'apparato operativo e la disseminazione decentralizzata di prodotti mediatici realizzata da sostenitori *online*. Il primo ha garantito al gruppo l'opportunità di guidare i propri affiliati nel campo mediatico con la stessa rapidità e lo stesso metodo delle forze militari. All'approccio centralizzato si deve quindi la capacità di adattamento dell'ISIS, mentre alla disseminazione decentralizzata si riconduce la resilienza della presenza digitale dell'ISIS nonostante i tentativi internazionali di ridurla. La *Base Foundation*, o *al-Mu'asasat al-Um*, è a capo dell'apparato mediatico dell'ISIS ed è responsabile per la creazione del logo ISIS riprodotto in video di alta qualità, servizi fotografici sul campo di battaglia e riviste patinate multilingue. Ha anche supervisionato la formazione di nuovi uffici mediatici nei 35 governatorati, o *wilayat*, del Califfato e ha monitorato il loro lavoro ricevendo accurati report mensili. La *Base Foundation* amministrava le principali case di produzione dell'ISIS, tra cui l'Al-Furqan Institute for Media Production, l'Al-Hayat Media Center, l'Al-I'tisam Media Foundation e l'ausiliaria Amaq News Agency. Ha anche diretto la radio Al-Bayan, che trasmetteva *nasheed* celebrativi dell'Islam e aggiornamenti in tempo reale. Un'ampia ricerca sulla propaganda dell'ISIS tra il 17 luglio e il 15 agosto 2015 ha rilevato che l'apparato mediatico dell'ISIS articola la narrativa del gruppo secondo sei filoni principali, quali la misericordia, il senso di appartenenza, la brutalità, il vittimismo, la guerra e l'utopia. Degli 892 documenti esaminati – fotografie, video, audio, messaggi- 861 possono essere classificati all'interno delle categorie "vittimismo", "guerra" e "utopia". Una delle caratteristiche salienti della strategia comunicativa dell'ISIS consiste nel parallelismo tra operazioni di informazione e azioni cinetiche al fine di sostenere gli obiettivi militari e adattarsi ai cambiamenti territoriali. Ciò è stato reso possibile dalla sinergia tra gli organi mediatici, militari e religiosi dell'ISIS.

Le radici dell'ISIS si rintracciano nell'operazione Iraqi Freedom del 2003 e nel gruppo radicale islamista Jamat al-Tawhid wa-l-Jihad. Quest'ultimo era attivo nell'Iraq nord-occidentale e comprendeva pochi membri non iracheni sotto la guida del giordano Abu Musab al-Zarqawi. In virtù del carattere aggressivo manifestato in molteplici operazioni contro le forze della coalizione e della campagna mediatica accattivante, il gruppo divenne presto la guida dell'insurrezione anti-americana. Nel 2004, a causa della mancanza di risorse e di miliziani, al-Zarqawi si associò a Bin Laden: nasceva al-Qaeda in Iraq. Dato che la partecipazione della comunità irachena al processo elettorale del 2005 comprometteva le attività di AQI, al-Zarqawi ampliò l'agenda del gruppo e dichiarò guerra alla comunità sciita irachena. Dopo la sconfitta nella battaglia di Baghdad, al-Zarqawi fu criticato sia da gruppi jihadisti che da gruppi di ribelli iracheni. Le fratture interne al gruppo furono sfruttate da rivali di AQI che ne uccisero il leader nel 2006. Sotto la duplice guida di Abu Ayyub al-Masri e di Abu Omar al-Baghdadi, il gruppo subì una re-configurazione volta a integrare più soldati iracheni e ad amministrare il territorio sotto il proprio controllo, gettando le basi dello Stato Islamico dell'Iraq, un emirato islamico che pianificava di estendersi intorno all'area di Mosul e alla piana di Ninive. All'esplodere delle proteste in Siria nel 2011, al-Baghdadi stabilì di inviare rappresentanti dell'ISI a combattere le forze di Assad e di installare una presenza visibile nelle zone a maggioranza sunnita. I soldati di al-Baghdadi - che lottavano sotto il vessillo di un nuovo gruppo, Jabhat al-Nusra - divennero presto uno dei gruppi ribelli prominenti, imponendo la *shari'a* nei territori conquistati e accogliendo volontari siriani nelle proprie fila. I successi sul campo di battaglia e la risposta positiva della popolazione siriana fecero guadagnare a JAN numerosi fondi e soldati. Inoltre, al-Baghdadi riuscì a co-optare centinaia di prigionieri che erano stati soldati nell'esercito di Saddam Hussein e potevano garantire al gruppo un'ottima conoscenza delle dinamiche e dei territori iracheni oltreché capacità militari. Nel 2013 al-Baghdadi annunciò ufficialmente l'unione di ISI e JAN nello Stato Islamico dell'Iraq e del Levante (ISIS). Tuttavia, sia il leader del fronte al-Nusra, al-Julani, che il leader di al-Qaeda, al-Zawahiri, smentirono la fusione e si dissociarono dall'ISIS. Nel 2014 quest'ultimo lanciò un'offensiva totale contro lo Stato iracheno, consolidando la presa di Mosul e della piana di Ninive. La caduta di Mosul nelle mani dell'ISIS si deve anche all'efficace *information warfare* condotta dall'ISIS qualche giorno prima dell'operazione militare. Il 29 giugno al-Baghdadi proclamò la nascita di un Califfato pan-islamico sotto la sua guida e invitò i musulmani a raggiungere il neo-nato Stato. Nello stesso anno, il Presidente americano Barack Obama dichiarò la formazione di una coalizione internazionale per sconfiggere l'ISIS. Il 2015 è stato un anno di successi e sconfitte per l'ISIS. Da un lato, il gruppo ha integrato reti di militanti locali e ha aggiunto *wilayats* in Afghanistan, Nigeria, Egitto e Libia. Dall'altro, ha registrato le prime sconfitte militari, alla luce delle quali il portavoce dell'ISIS Abu Muhammad al-Adnani ha incitato a commettere attacchi terroristici negli Stati facenti parte della coalizione. Alla graduale perdita di terreno nel 2016 ha corrisposto un incremento degli attacchi terroristici realizzati da lupi solitari in tutto il mondo e un cambiamento della propaganda virtuale dell'ISIS, che ha interrotto la pubblicazione di Dabiq – la città ritenuta, nel *hadith* 6924, teatro della battaglia apocalittica contro i crociati – e ha iniziato quella di Rumiyah –Roma ed, emblematicamente, l'Occidente. All'attualità, l'ISIS ha perso il 98% dei territori che occupava in Iraq e Siria. Tuttavia, la situazione rimane complessa in Siria per la presenza di alcune tasche di resistenza in prossimità del confine iracheno.

Per compensare le perdite territoriali e di leadership, nel 2016 l'ISIS ha reinventato la propria strategia militare e aggiornato la propria immagine con l'obiettivo di espandersi globalmente sia nello spazio fisico – rilocalizzando il proprio centro di gravità verso le numerose *wilayats* – che in quello cyber. Il cambiamento del nome del giornale di spicco dell'ISIS da Dabiq a Rumiyah riflette il passaggio da Califfato reale e fisico a Califfato virtuale e auto-rinforzante.

Dabiq, rilasciato in varie lingue in concomitanza con il messaggio di chiamata ai musulmani di al-Baghdadi del 2014, fornisce un'articolata propaganda del progetto olistico di *state-building* dell'ISIS. Infatti, la rivista è stata concepita per promuovere la funzionalità dell'ISIS come Califfato basato sul controllo territoriale e sulla capacità di implementare la *shari'a*. Si impernia sui temi fondamentali della polarizzazione tra ISIS e Altri, dei soldati gloriosi e dell'imminente apocalisse. I primi tre numeri sono stati rilasciati nel periodo più produttivo dell'espansione dell'ISIS e sono dedicati al piano di attuazione del Califfato e all'*hijrah*, mentre gli ultimi tre sferrano attacchi ai nemici lontani e vicini.

Nato per distogliere l'attenzione dal suo declino militare dopo la perdita di Dabiq, Rumiyah indica una proiezione dell'ISIS all'estero, come dimostrato dalla pubblicazione in più lingue, tra cui meritano attenzione l'indonesiano, il pashtu e l'uiguro. L'Indonesia, il Paese a più grande densità musulmana, potrebbe essere considerata dall'ISIS il prossimo terreno fertile per i suoi scopi. Il pashtu è la lingua diffusa nei bastioni talebani e di Al-Qaeda tra Afghanistan e Pakistan, dove l'ISIS ha cercato di attecchire. Infine, l'uiguro è l'idioma dell'etnia turcofona di religione islamica che vive nel nord-ovest della Cina con ambizioni indipendentiste. E' significativo che la rivista contenga rubriche con sfumature differenti in base alle diverse audience a cui l'ISIS si rivolge. Ad esempio, la versione inglese del primo numero fomenta i simpatizzanti ad eseguire attacchi indiscriminati, mentre quella francofona esorta a interrompere le attività a causa dell'innalzamento delle misure di sicurezza.

Integrando Al-Naba e Amaq News Agency, Rumiyah chiarisce anche l'attuale strategia mediatica del gruppo: crescere nel cyberspazio attraverso la misinformazione e competere con le notizie *mainstream*.

Lo scopo primario della strategia informativa dell'ISIS consiste nell'allineare le percezioni dell'audience con i propri principi ideologici e spronare all'azione sfruttando una combinazione di fattori pragmatici e percettivi. I primi, ovvero sicurezza e stabilità, servono a promuovere l'efficacia della campagna politico-militare e denigrare gli sforzi dei nemici attraverso un processo decisionale razionale basato su un'analisi dei costi e dei benefici. Infatti, l'ISIS è consapevole che il proprio materiale di propaganda deve supportare l'apparato politico e acquisire il consenso delle masse per portare avanti l'agenda del gruppo. Sui secondi l'ISIS si sofferma per mostrarsi come guardiano dei musulmani sunniti e per ritrarre i suoi nemici come responsabili di una crisi a cui solo l'ISIS può porre fine. L'ISIS sembra porre maggiore enfasi sui fattori pragmatici nell'appellarsi alle popolazioni locali e sui fattori percettivi nell'interpellare un'audience regionale e transnazionale.

Dall'analisi di Dabiq e Rumiyah emerge un graduale aumento nei fattori percettivi mirati a rafforzare l'identità del gruppo ai danni dei fattori pragmatici. Di conseguenza, il focus era sul reclutamento e sullo *state-building* quando l'ISIS stava allargando rapidamente il territorio sotto il proprio controllo e poteva presentarsi come un'organizzazione trionfante e amministrativamente competente. Dopo la stagnazione, l'ISIS ha dato ufficialmente *l'endorsement* ad organizzazioni affiliate, specie in Africa, per avvalorare il progetto di espansione globale del Califfato. Infine, con la riduzione territoriale nel Syraq, ha dato priorità all'attacco dei nemici sia vicini che lontani attraverso l'introduzione di una nuova rubrica, "*Just Terror Tactics*".

Le *information operations* flessibili hanno dimostrato di essere una delle maggiori fonti di resilienza dell'ISIS, dato che hanno consentito all'organizzazione di adattarsi al mutare delle circostanze e ne hanno offerto un'immagine vittoriosa nonostante la sconfitta militare. L'aggiunta di Rumiyah al crescente apparato mediatico ha definito la transizione dell'ISIS verso un Califfato virtuale, una comunità radicalizzata e con base nel cyberspazio costituita da individui che interagiscono nelle *chat rooms*, nei forum jihadisti e sui social media. Pur traendo benefici dall'eredità dell'ISIS, il Califfato virtuale potrebbe rendersene indipendente. L’ISIS, invece, sfrutterà il Califfato virtuale per continuare a fomentare e coordinare attacchi all’estero e per costruire una solida base di supporto finché l’organizzazione non avrà la capacità di recuperare territori. In quanto entità non territoriale, il Califfato virtuale potrebbe ridefinire la minaccia del movimento salafita jihadista globale.

Legittimando la *jihad* virtuale, il caso ISIS è emblema del trend per cui le guerre non sono più confinate al campo di battaglia fisico ma sono entrate nel dominio cyber, dove le *information warfare* sono mezzi sine qua non per manipolare il pensiero strategico e il comportamento.