Review Article

Global Media Journal
ISSN 1550-7521

2022
Vol.20 No.52:313

Psychological Warfare and Innovation: A Constantly Evolving Combination

Williams Whitman*

Department of Media Journalism Ghana

***Corresponding author:**
Williams Whitman

✉ Williams_W@gmail.com

Department of Media Journalism Ghana.

Citation: Whitman W (2022) Psychological Warfare and Innovation: A Constantly Evolving Combination. Global Media Journal, 20:52.

Abstract

The Internet's great potential, including its extreme ease of access, monitoring deficit, legislative anomie, the wide audience it can reach and the large flow of information that inhabits it on a daily basis make it an indispensable tool for terrorist groups.

The Internet represents the media archetype of the democratic values of freedom of expression, an advocate of the neutralisation of the space-time dimension that unites and opposes any form of fragmentation. The new terrorists carry out their activities online, thus eliding the need for a central command and actualising a conflict characterised and marked by the doctrines, strategies and technologies of the Net.

This propaganda action aims at recruitment and radicalisation.

Keywords: Internet; Media; Propaganda; Communication; Recruitment

Received: 22-Jun-2022, Manuscript No. gmj-22-67347; **Editor assigned:** 24-Jun-2022, PreQC No. gmj-22-67347; **Reviewed:** 08-Jul-2022, QC No. gmj-22-67347; **Revised:** 13-Jul-2022, Manuscript No. gmj-22-67347(R); **Published:** 20-Jul-2022, DOI: 10.36648/1550-7521.20.52.313

Introduction

Globalization and the developments of Information Technology have revolutionized the concept of war and with it, that of security. The new terrorists, as can be seen from the media reports, have shown themselves to be extremely literate in the use of advanced technologies such as the Web, which, thanks to one of its intrinsic characteristics, interactivity, is actualized as a functional postulate for the planning of attacks and for the consequent actions of propaganda, enrolment and logistic support. We are facing the so-called Information Warfare [1].

The great potentialities of Internet, among which the extreme ease of access, the monitoring deficit, the legislative anomie, the ample attainable public and the great flow of information which inhabits it daily, make it an indispensable instrument for the terrorist groups[Chung-Yin Yeung J. (2015), A Critical Analysis on ISIS Propaganda and Social Media Strategies. University of Salford, Manchester.

The Internet represents, at least in its intentions, the media archetype of the democratic values of freedom of speech and expression, an advocate of the neutralisation of the space-time dimension that unites and opposes any form of fragmentation. The new terrorists are parcelled out into small units scattered around the world and coordinate their activities online, thus obviating the need for a central command. The netwar phenomenon is based on these dynamics, updating a conflict characterised and marked by the doctrines, strategies and technologies of the Net [2].

Communities have a rapid life cycle and grow at an uncontrollable rate; this process has heightened interest in analysing the communications exchanged in such digital agoras Gli Internet Centers e le battaglie di Intelligence, Gnosis.

This propaganda and loyalty-building action aims at recruitment, as mentioned above, and radicalisation, i.e. the process of adopting an extremist belief system including the decision to use, support or facilitate violence as a method to change society. It has become the lifeblood of extremist and globalised movements, an indispensable means of spreading their message to an increasingly wide and potentially global audience. Contingencies that activate a new socialisation of terror: social networks, chat rooms, blogs and forums are set to replace mosques, community centres and bars as places of contact and recruitment for terrorist groups such as Al-Qaeda. Initially, terrorists used the Web as a logistical support for their operations, but later they realised how the Web could become an ideological vector for their worldview.

Terrorism has perfectly translated the principle according to which the message is in the act itself, in the blind fear that it generates, conveyed by an ever faster and more intrusive communication.

This mechanism highlights and contains different meanings that follow one another respecting a sort of diachrony of evil: the need to glorify violence through the act followed by propaganda that praises violence itself, and perpetuates its effects, online recruitment, the search for funding and finally digital training.

Furthermore, Al-Qaeda reiterates the dynamics of the web also at a structural level, characterizing itself as a reticular organization, in which the annihilation of a single cell does not threaten the security of the others, since there is no hierarchical relationship between them based on a pyramidal logic[Fishman B. H. (2017), The Master Plan: Isis, Al-Qaeda, and the Jihadi Strategy for Final Victory, New Haven, Yale Univ. Press [3].

Its media strategy is designed to perform various functions and, therefore, it unravels through various channels according to a Trans medial logic: statements sent by fax, posts on the Internet, videos, production of articles and interviews, marketing and targeting of the public.

The cadence of the statements corresponds to the main international events and is aimed at making propaganda, as mentioned above, exacerbating tension, demonstrating that a leader of the organisation thought dead is alive, increasing supporters and launching attacks and condemnations. Targeted communication to make the masses aware of their cause, gain the support of sympathisers and generate fear terrorists need publicity.

After losing its logistical base in Afghanistan, Al-Qaeda fragmented into smaller, elusive micro-actor factions. As a result of these events, Al Qaeda has suffered a drastic reduction in the communicative capacity which had constituted its identity.

What catalyses a careful reflection in the sector is the activity of the operators that produce and post material on the Net and the means through which they publish this material, using a Media Production and Distribution Entity (MPDE), that is an entity in charge of externalising such contents. With its activity, it maximizes the synergies, the efforts of the groups and catalyses the visibility of the content which is intended to be diffused; then it creates a link connected to the content which is a guarantee of authenticity of the material, a sort of legitimate recognition of the news, only for the fact that it is made through a specific MPDE, known and reliable and attributable to the terrorist area [4].

Terrorists use these means for two main purposes: to attract attention and to generate fear. They usually hack into network servers to send untraceable messages, instruction manuals and tutorials on how, for example, to build a dirty bomb. When the terrorists are detected and the server is shut down, they hack another one. Blogs, chats, forums: digital places used to deal with a range of topics and interact directly with users.

Jihadists are using the Internet and the web to create a virtual tribe of radical Islamists, a sort of online umma, characterised by shared global affinities.

The Internet is mainly used as a tool to research pre-attack information, including nuclear plans, railway maps, water networks, airport flight schedules. Another important aspect to consider for the purposes of this analytical path is the creation of a training network for all those who adhere to the Jihad cause, uploading videos, manuals, logistic-strategic materials, hand-to-hand combat lessons and assault tactics onto the server Reid E Analysis of Jihadi Extremist Groups 'Videos, Forensic Science Communications, In addition, downloadable online newspapers in PDF format and written in English are also very popular.

In this sense, today we can count as a further declination of terrorism the holographic one which sees the figure of its leaders, think of Bin Laden, almost dematerialised and crystallised for years. In this way, he has strongly concentrated on himself the public image of Al Qaeda, almost personalizing it and creating, through his sacred figure in that context, a fertile activity of propaganda and proselytism, directing the direct operative functionality.

Obviously, Osama's media objective was to strongly influence the Islamic public opinion, whose socio-cultural characteristics are very different from those of the Western countries. In fact, it concerns an audience whose levels of schooling are still very low and for which it is necessary to use a simple, dry, clear language, but at the same time, strongly rhetorical and evocative.

The tragic events of that dramatic 11 September, in addition to an obvious conspiracy trail, revealed the unpreparedness of the US intelligence, unable to understand, analyse the phenomenon and then act preventively to foil it. In light of this tragic assumption, all the anti-terrorist strategies have been revised. Once the initial shock had passed, the United States reacted decisively, both on the political and military fronts, making the fight against terrorism an absolute and global priority, a war for freedom. Also our Country has moved in this direction, supplying, at an international level, political and military support, and at a domestic level, conducting an effective police action against the presumed Italian branches of Al-Qaeda.

The surprising aggregating and offensive potentiality of Osama's organization was based on a rocky religious faith of the militants, sharpened by the otherworldly symbolism of martyrdom, on a carefully compartmentalized organization, on the availability of considerable financial resources, on a vast area of supporters and mere sympathizers and, finally, as mentioned, on the capacity to exploit the great opportunities offered by the new means of communication.

Fundamental Role Assumed By the Internet

It is easy to understand how the advent of the Net has, in fact, favoured Al Qaeda, with all the terrorist organizations connected to it, and, in a specular way, has rendered the investigative activities of the anti-terrorist forces more difficult. In fact, thanks to its peculiar characteristics, the elision of the space-time dimension and the fact that it is free of charge, it has substantially neutralised the physical presence and therefore the potential identification of subjects involved in the above-mentioned actions. This makes evident the assumption according to which any strategy of attack on terrorism must take into account the fundamental role assumed by the Internet and the social networks: extraordinary instruments of strengthening the subversive dynamics, conducted by all the terrorist formations, which through the Net can improve both the organizational and logistic structure, as well as, the same offensive strategies. In fact, the terrorist universe progresses and develops with the same evolutionary rhythms as the society that generates and contextualizes it.

The presence on the Net of numerous sites containing ideological documents in support of the Islamic Jihad testifies to how the Internet is used with great skill by Al Qaeda, Isis and their sub-groups [5].

Another important aspect is the economic one: the financial network of Al-Qaeda and Isis is parcelled out and articulated in companies with offices in many European and American cities. They are perfectly integrated in the world financial system and apparently act in accordance with the laws of the market, thus avoiding the controls of the competent authorities. The Internet, therefore, becomes a fundamental tool also for operations aimed at self-financing.

New investigative scenery

The new investigative scenery which opposes terrorism tout court, therefore, seems to embrace, in parallel with organization charts and military bases, also the new area of cyberspace. Such a change of view implies a preparation and an organization characterized by innovative instruments of counteraction and equally immersed in the digital technological dimension [6], Gli Internet Centers e le battaglie di Intelligence, Gnosis.

The figure of the terrorist of the new millennium seems to differ from the traditional one: a subject no longer distinguished only by military qualities, but supported by considerable technical competence in the field of informatics. The capillary diffusion of Internet has, for some time, highlighted the problems connected to the integrity, the confidentiality of the data and the legitimate certainty of the informatics source.

Modern society

Modern society has reached, through information technology, very high levels of organization, especially in the tertiary and financial sectors, but, at the same time, it has become vulnerable to a new kind of terrorism, carried out no longer with firearms, but with computer keyboards. In this scenery, the beginning of a new form of terrorist antagonism is beginning to emerge, subversive and aggressive, able to threaten the most technologically advanced nations with just a click. A modality which no longer aims at the physical elimination of the adversaries, through purely military operations, but which focuses on the war of information and identifies in the above mentioned systems criticality and weak points of all those societies considered as possible targets of attack. We are dealing with a new generation of terrorists, in some ways much more dangerous than those of the past, able to wisely exploit such new opportunities. These possibilities seem to induce structural and organizational changes, above all, with regard to the modalities of compartmentalization, communication and proselytism, as already mentioned.

From what seems to be emerging on the world scene, and the attack on the Twin Towers corroborates this thesis, for many terrorist formations, the support activities offered by digitalisation are thus assuming a more important role than that played by analogue offensive activities[Chung-Yin Yeung J. (2015), A Critical Analysis on ISIS Propaganda and Social Media Strategies. Manchester, University of Salford.

The advent and development of the telematics networks, with their capacity to transcend spatial and temporal limits, has, in fact, rendered obsolete the theoretical and methodological frameworks relative to the research on the modalities of organization, recruitment and communication by many sodalities of the sector. Another interesting dimension that offers itself to such an analytical evaluation is represented by the new modalities of socialization of the terrorist groups in the ambit of the cyberspace.

In fact, some new dynamics are highlighted, characterized by virtual interactions inserted within an information flow of planetary dimensions. This flow could be able to involve elements that in the past would never have had the opportunity of a direct connection and interaction, due to high, and then insurmountable, geographical, social, cultural and psychological distances.

In this context, the interaction of many individuals with communities characterised by a culture tending towards hatred, and the elimination of the generally understood different, could constitute a symbolic and factual context capable of favouring identification and, consequently, insertion in the above-mentioned association.

The first intuitive modification in the organizational dynamics of terrorism, induced by the advent of informatics, is represented by the generalized reduction of paper documents. Alongside the great capacity of data concentration offered by the digital supports to the terrorist groups, is the ductile functionality of the Internet, which constitutes, also for such organizations, a form of communication of extraordinary efficacy, which facilitates the principal objective they pursue: to communicate terror [7].

The attack is effective when it externalizes itself in all its bloody drama, goes viral and allows the material gesture to coexist with the symbolic one in an union which amplifies the effects and the irrational fear that derives from it. Starting from this assumption, it is easy to understand how the terrorists have kept up with the times by exploiting the great opportunities offered by technology.

The use of the Net allows the compression of the space-time dimension [Giddens A. (2000), mondo che cambia. Come la globalizzazione ridisegna la nostra vita, Bologna, Il Mulino.]. The communicative opportunities intrinsic to it have thus offered to the clandestine organizations that use it, a strong contraction of the points of vulnerability and an access to new areas of political consensus, through a contextual increase of the possibilities of virtual encounters, according to mechanistic dynamics.

Such scenery seems to exert an overbearing organizational pressure on the choices of the terror leaders. With the techniques of tactical-strategic communication, used by terrorists up to a decade ago, it was, in fact, necessary to physically go to the meeting places established, perhaps by telephone or mail, and in any case, to personally meet a conspicuous number of other members: such dynamics constituted the vulnus of the group itself. With the advent of the Internet, this meeting place has become volatile and dematerialised.

A fundamental opportunity offered by technology for evil communications is represented by cryptography. Encryption techniques are so sophisticated that they make it extremely difficult to intercept messages, and offer a complete guarantee of anonymity.

It is well known that the availability of powerful cryptographic algorithms is an extremely effective means of protecting information; a possibility within the reach of every cyber terrorist group. A strategy to counter this has been proposed in US government circles through the adoption of rules aimed at tightening the spread of cryptographic algorithms and the implementation of special systems allowing decryption. These solutions, apart from their questionable technical-scientific basis, risk being extremely damaging to the protection of personal liberties and sensitive data, Cyber espionage e cyber counterintelligence.

Normally, a terrorist group is articulated on a unanimously recognized leadership and on an indeterminate number of operative cores which provide for the implementation of the operations, the preservation of the structure, the research and the enlargement of a base of popular consensus.

At the present time, an organization has the concrete possibility of managing, with great ease, an indefinite number of sub-groups, through the constitution of fiduciary relations between the components which perpetuate their existence and with the implementation of mechanisms which foresee their rupture in the case of investigative compromise by the intelligence agencies. This opportunity leads us to hypothesize the birth of new organizational forms, more agile and impermeable, which entrust to telematics technology the function of monitoring the security of the structure itself.

In the past, the technical complexity of setting up a communication system of the kind outlined above ensured that it could only be built by very skilled leaders, literate in the new media and backed by huge amounts of capital. At the present time, the technical knowledge and economic resources have undergone an evident optimization which has neutralized the need for a professionalized expertise, opening to a new mass of actors. The new terrorist leader must, however, have a good mastery of the information flows that are articulated on the networks to manage them in such a way as to elude the countermeasures of the institutional agencies.

However, the objective danger that the western world is constantly running requires, in determined periods and with shared responsibility, the renunciation of a reasonable part of the privacy of the users, allowing the institutional agencies to carry out operations of access and wide control, fundamental for effective investigative activities.

The absolute event, the attack on the World Trade Center, symbolically represented the watershed[Hoffman B. (2006), Inside Terrorism, New York, Columbia University Press.] between a free and secure everyday social life and a fluid future, in the Bauman sense, and therefore highly uncertain[Bauman Z. (2006), Modernità liquida, Bari, Laterza.]. Within the political debate, the media narrative and public opinion, an incontrovertible conviction has been perpetuated over time: since that day, nothing has been the same. That attack represented the vector of a change that changed the habits and relational dynamics between individuals, between cultures, and changed the perception of the very concept of security [8].

In today's scenery, dominated, as has been said, by an all-embracing and all-embracing uncertainty, a first objective fact emerges: terrorism represents a reality in constant evolution which pursues its objectives with new instruments and techniques, eluding technical, logistic and economic limits in the knowledge that it can strike the physical and digital places which characterize modern societies.

The strategy of terror, in its protean essence, is divided into different types: domestic terrorism, Islamic terrorism, bio-terrorism and cyber-terrorism.

It is a view where the fight takes place on new ground, where well-trained military groups are not enough, but knowledge and tools never used before, which inhabit and characterise the media-communication universe, become indispensable.

The web and terrorism are increasingly connected. The Islamic State has demonstrated this: the Internet not only permits a more capillary organization of the jihadist groups, but synchronically, also the invasive and planetary diffusion of its message.

The Net, with its processes of socialization and radicalization online, has made possible the birth of a molecular terrorism within the vast jihadist galaxy, as is evident, for example, from the so-called lone wolves: individuals who, inspired by the fundamentalist narrative, commit or prepare terrorist acts in support of a group, an ideology or a specific cause, acting, however, in isolation, outside of a collective logistic organization or structure and without any external assistance.

The impact of the Network, on the processes of radicalization and on the formation of terror networks, is absolutely remarkable and acts as a vector of growth in an impressive way. Furthermore, it has stimulated a new reality: the do-it-yourself terrorism. A sort of self-induced radicalizing process which is accompanied by training, also this self-taught, but at the same time, theoretical and technical. The analysts of the sector have elaborated this definition to categorize individuals trained in combat who, as components of sleeper cells within a foreign country and tendentially Western, are activated following precise signals sent by a terrorist centre. This evolution shows how Jihadism is now an always networked reality. It is a phenomenon that has the possibility of easily penetrating into the heart of Western countries and their societies, through the conversion and loyalty of individuals to radical Islam and the indoctrination of native terrorists on the web.

This process consists of several stages and shows how and how much the Internet has facilitated and speeded it up. However, in the age of digitalisation, face-to-face relationships still play a fundamental role.

In 2007, the Police Department of the City of New York, in collaboration with the Counter-Terrorism Division of the FBI, published the dossier, The Radicalization Process: From Conversion to Jihad, listing, as mentioned, four principal phases:

Pre-radicalisation: the first step consists in attracting the excluded who seek social acceptance in vain or the young converts to Islam who pursue, instead, an integralist interpretation of the faith. These people share a common social background of alienation, exclusion, discrimination, stigmatisation and unemployment. Moreover, they act out an all-encompassing logic: they feel they are innocent victims of a condition of submission that does not concern them alone, but extends to all Muslims, an element that stimulates them to react in order to change this situation [9].

The first approach with fundamentalists takes place on the web or in mosques, universities or prisons.

The second phase is that of identification: an individual identifies with the extremist cause, accepting the radical Islamic ideology. In this phase, a substantial isolation occurs together with a factual detachment from one's past. This path is accomplished autonomously. In the past, spiritual guides were necessary, such as, for example, a fundamentalist Imam, now their role is played by the enormous flow of information that the web receives on the subject.

The third step is indoctrination: after getting to know and identifying with the new cause, the goal is to become an active member, playing roles within the organisations' activities and contributing to their growth.

Isis is the reality that best represents the factual concretisation of the above-mentioned points, implementing a strategy that eliminates physical contact and fully embraces the digital dematerialisation of recruitment.

Through the Internet, the Islamic State has been able to attract more and more fighters, spread messages of terror, and reiterate its invasive presence through the continuous visibility of the web.

This activity has persuaded and recruited, above all, the younger generations, who, in addition to experiencing a condition of harassment and exclusion, have sought a consequent redemption in the promises and rhetoric of radicalized Islam.

Criminologist and expert in terrorism, underlines the central role that the web occupies in the strategy of terror: "Hierarchies exist, media producers, a centralized induction of communication. The innovation of the on-line Jihadism is in the fact that the audience participates, constructs, reconstructs, generates, and regenerates The great ability of Isis lies in the fidelity of the younger generations, mastering their media, using their linguistic codes, but above all, exploiting the cultural gaps and voids of those who use the web as their only and incontrovertible source of information [10].

Methodology

The Isis uses Telegram a lot, above all, thanks to the possibility of managing the passage between public and private chat, which allows an approach to potential audiences, first in a massive way and then in a personalized way[Chung-Yin Yeung J. (2015), A Critical Analysis on ISIS Propaganda and Social Media Strategies. University of Salford, Manchester, da In short, the Islamic State structures a communication that proposes itself, in its intentions and effects, as a totalizing and aggregating reality. The tools to counter such activities are, above all, preventive:

The major web giants should devise in advance methodologies dedicated to monitoring the dangerous content disseminated by terrorists, censoring it before it becomes widely available.

t seems necessary and imperative to intervene on the culture and training of digital natives. Provide them with interpretative antidotes to decode information correctly and resolve the conflict between what is right and what is wrong.

Facebook, Twitter, YouTube, Telegram, Line, Snap chat, Tik Tok, are all digital stages that terrorism occupies with ease, from which it plans and delivers its spectacle of death, as stated in the document The use of the internet for terrorist purposes produced by the United Nations. The purpose of the latter is to stimulate action by the international community given the immediate need for a level of cyber security that is far superior to that used until now. A dedicated control that can monitor the flow of information from social networks which, according to the report, are a veritable breeding ground for new terrorist cells.

Yury Fedotov, executive director of UNODC, the United Nations Office for Drug Control and Crime Prevention, says that terrorists use communication technologies, such as the Internet, to reach a potentially global audience, optimising costs and maintaining clear margins of anonymity. In recent years, the use of the Net has increased considerably among citizens and, in parallel; also the terrorist organizations have followed the same trend with decidedly different aims.

The report shows statistically how the above mentioned groups have actualized a systemic use of the Web to recruit new followers, find financing, conduct propaganda and awareness actions, but above all, according to mechanistic dynamics, to collect and diffuse information.

The Internet system no longer has any physical national borders, but uses connectivity, Connectography. Le mappe del futuro ordine mondiale, Roma, Fazi.] to increase its impact, its power and its destructive effects. A situation that requires greater synergy between the various institutional realities, reflected in effective legislation.

Within the document, social networks return, powerfully and once again, to the spotlight of governments and their control bodies, being the subject of analysis on a legislative, political and purely ethical basis. Orwellian scenarios have been repeatedly threatened on this issue with regard to the control of the Net and the use of social platforms [10].

Proposals that each time triggered protests from users, who put the protection of their freedoms before the fight against terrorism. The latest case in point was the discovery, by the European Digital Rights, the European association for the defence of civil and human rights and freedoms in the digital environment, of a proposal that should have remained secret, in which a sort of digital task force was set up to monitor the

Net, thanks to infiltrators, using false digital identities, within the social networks to check and report any violations or suspicious attitudes.

Faced with this possibility, Facebook, through a spokesperson, said on the All Things D website that the dialectic between control and user privacy is a problem for every communication platform, from mobile and social networks to search engines and video-sharing services. Their policies very clearly prohibit the support or representation of terrorism, terrorist groups, colluding individuals and all possible actions related to terrorism[Chung-Yin Yeung J. (2015), A Critical Analysis on ISIS Propaganda and Social Media Strategies. University of Salford, Manchester.

Facebook literally eliminates people in the social network who incite violence and devotes considerable resources to eliminating the few cases where these individuals try to exploit the service.

Google is also pursuing the same policy and, like Facebook, has implemented a self-regulation system on YouTube that allows users to report inappropriate content and possible misconduct, achieving a twofold objective: to make them accountable and, at the same time, to create an effective deterrent for any kind of violation. However, immediately visible platforms facilitate control, but other realities such as the dark web[Moore D., Rid T. (2015), Cryptopolitik e la Darknet, London, King's College.] hinder it and allow for greater dissemination of certain content.

The dark web is the part of the internet not indexed by the usual search engines, shielded by security measures that hide and anonymise users, documents, conversations and, above all, economic transactions.

The dark web only allows access through specific software and the exact address of the site in question that one intends to visit.

According to a 2015 study by Daniel Moore and Thomas Rid, radicalised groups are unlikely to use the dark web. The researchers developed a web crawler, a system that allows a mapping of the web and that allowed them to classify about 300 thousand services hidden on the Tor network, a network that allows safe navigation [Zanasi A. (2008), Gli Internet Centers e le battaglie di Intelligence, Gnosis, from http://gnosis.aisi.gov.it/Gnosis/Rivista15.nsf/ServNavig/17.]. Experts explained that terrorists prefer to share propaganda content on the usual web in order to reach a wider audience, including potential followers and onlookers interested in the groups' activities.

Another problem, when it comes to anonymous networks, is that they are often not very stable and slow. This is not to say that terrorists do not use the dark web; on the contrary, research has shown that ISIS militants routinely use Tor to anonymise their surfing [4].

The study by Moore and Rid states: "Propaganda running on the web is strictly limited, partly because beginners may be deterred by its illegality, especially in the initial phase.

Secondly, hidden services are often not stable or accessible enough for effective communication; other platforms seem to meet communication needs better. Islamic militants commonly use the Tor browser on the internet".

The researchers noted that jihadists paradoxically are not very active on the web. For instance, it is very difficult to find extremist content on the Tor network: a noteworthy finding was the confirmation of a residual presence of Islamic extremism on Tor's hidden services [5].

They prefer to use the classic web to achieve their dual purpose: propaganda and recruitment. These goals are easily achieved by using platforms and social media such as Twitter and Facebook. In fact, the research confirms that the dark web hosts a significant part of the services used by criminal organisations to implement and propose different contents related, for example, to the drug market, illegal finance and pornography often accompanied by violence against children and animals. About 1,547 of the 2,723 active dark web sites analysed by the researchers were used for such services Moore D., Rid T. (2015), Cryptopolitik e la Darknet, London, King's College.].

Discussion

Bin Laden's organisation produced in 2001 a sort of 11-volume encyclopaedia of Jihad containing information and techniques on the use of nerve gas, explosives and the conduct of urban guerrilla warfare. The documents were put on the Internet so that they could reach the various cells scattered around the world.

Investigations into some North African cells believed to be in contact with Osama's organisation revealed the existence of individuals who had taken root in the territory of various European nations, camouflaging themselves in their communities and carefully avoiding telephone contacts or meetings with other members of the terrorist association. Connections were maintained mainly through the Internet (with secret e-mails or web pages) with both the command structure and other members operating within it. Many of the messages were encrypted using special software. In 2001, investigations by the French police led to the arrest of Kamel Daoudi, a computer expert who had also received military training in Afghanistan. Daoudi, who lived in France, was responsible for the encrypted Internet links between the Afghan terrorist leadership and various sleeper cells in the Netherlands, Belgium and France[Fishman B. H. (2017), The Master Plan: Isis, Al-Qaeda, and the Jihadi Strategy for Final Victory, New Haven, Yale Univ. Press.

After the attack on the Twin Towers in New York, Osama Bin Laden and other Islamic extremists, according to some American defence experts, turned to the use of information technology and used the Net to transmit orders and instructions for other attacks against the United States and its allies. Photos and maps of the targets to be hit were also encrypted and hidden on sites or transmitted through the most popular chat rooms. This activity was defined in military circles as 'e-Jihad', i.e. the holy war of the computer age.

The question of a greater control on the Internet as a means of prevention of international terrorism has always been the object of reflection for all those realities that fight any form of censorship on the Net. In the aftermath of the bombing of the Atlanta Olympics, the G7 proposed a series of restrictions on the Net, such as the prohibition and censorship of sources that might contain dangerous information, the imposition of the compulsory deposit of keys or other instruments that would allow governments to violate encrypted private correspondence. These measures were interpreted more as a violation of privacy and a form of restriction of freedom of communication than as a counter-terrorist strategy.

Currently, the balance between investigative needs and the protection of personal freedom is the subject of much institutional attention. If, on the one hand, the cyberterrorist threat calls for energetic initiatives, it seems essential that effective responses to the problem do not include censoring information and restricting its availability. In this case, any form of communication democratisation would be neutralised in favour of a biased and simplified selection of the aforementioned information, which, in turn, would undermine the very preventive operations of the actors dedicated to monitoring the phenomenon [10].

Conclusion

However, the Isis, suffering continuous defeats on the classical war plan, has been obliged to transform itself into something different and to concretize a process of dematerialisation from a digital point of view to fulfil its mission, starting to use also the dark web.

In fact, the Islamic State has decided to invest in the dark web to try to reorganize itself through a transformative shift from army to pure terrorist group. It has understood the necessity of such a change as the only solution to hope to survive in an unequal war.

In the beginning, jihadists used the Internet to spread propaganda widely, raise funds and recruit new fighters, particularly among the young.

Governments then reacted by involving key players in cyberspace and the social media leadership itself. In this way, many terrorist-communication strategies began to appear ineffective or even counterproductive.

The Islamic State was therefore forced to move some of its activities to less popular but certainly more productive digital locations: the dark web.

This scenario has caused further changes also in the economic field: Isis has felt the need to find new channels of financing, forced to leave the traditional ones, now obsolete and dangerous following the success of international law enforcement activities. Consequently, it has turned to a new currency, bit coins. There are several reasons for this. The first is that financial transactions on the dark web, at least for the time being, are anonymous, so it is more difficult to be detected by the controllers monitoring the internet.

In this sense, it is safer to receive funding from external parties, who run fewer risks. Moreover, it is money, albeit digital, that can be spent immediately and anywhere, without the need to transfer or convert it.

References

1 Antinori A (2007) Shahada suicide-bombing Fenomenologia del terrorismo suicida Roma Nuova Cultura.

2 Arquilla J, Ronfeldt D (1996) the Advent of Netwar Washington, Rand Corporation.

3 Bauman Z (2006) Modernita liquida Bari, Laterza.

4 Erelle A (2015) Nella testa di una jihadista Un’inchiesta shock sui meccanismi di reclutamento dello Stato Islamico, Milano, Tre 60.

5 Fishman B H (2017) The Master Plan: Isis, Al-Qaeda, and the Jihadi Strategy for Final Victory, New Haven, Yale Univ. Press.

6 Giddens A (2000) mondo che cambia. Come la globalizzazione ridisegna la nostra vita, Bologna, Il Mulino.

7 Hoffman B (2006) Inside Terrorism, New York, Columbia University Press.

8 Katz R (2015) Al-Qaeda and Internet in Terrorism and Counterterrorism, Georgetown University through EDx.

9 Khanna P (2016) Connectography. Le mappe del futuro ordine mondiale, Roma, Fazi.

10 Maggioni M (2015) Terrore mediatico, Bari, Editori Laterza.