International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:9, No:7, 2015

Terrorism: A Threat in Constant Evolution Still Misunderstood

Manuel J. Gazapo Lapayese

***Abstract*—**It is a well-established fact that terrorism is one of the foremost threats to present-day international security. The creation of tools or mechanisms for confronting it in an effective and efficient manner will only be possible by way of an objective assessment of the phenomenon. In order to achieve this, this paper has the following three main objectives: Firstly, setting out to find the reasons that have prevented the establishment of a universally accepted definition of terrorism, and consequently trying to outline the main features defining the face of the terrorist threat in order to discover the fundamental goals of what is now a serious blight on world society. Secondly, trying to explain the differences between a terrorist movement and a terrorist organisation, and the reasons for which a terrorist movement can be led to transform itself into an organisation. After analysing these motivations and the characteristics of a terrorist organisation, an example of the latter will be succinctly analysed to help the reader understand the ideas expressed. Lastly, discovering and exposing the factors that can lead to the appearance of terrorist tendencies, and discussing the most efficient and effective responses that can be given to this global security threat.

***Keywords*—**Responses, resilience, security, terrorism.

I. On the Definition of Terrorism: Characteristics and Goals

THE first problem when trying to address the issue of terrorism is the absence of a generally accepted definition, which would allow us to discuss the threats that it poses to security from a consensus. It is worrying to realise that, while terrorism is one of the strongest threats to national and international security anywhere in the world, seemingly leaving nobody anywhere free from risk, no definition of it is accepted by all agents on the international scenario.

Were somebody to fight a given threat 'x' by all possible means - but with no more information than the name of the threat, it is highly unlikely that their actions would yield positive results. Similarly, in real life the absence of an international consensus on the definition of terrorism can render operations geared towards its prevention useless, since instruments may be deployed which do not work against its essence: a good example of this may be the choice by certain governments of the military as the backbone of their efforts against terrorism, as though the latter were comparable and equal to a nation-state. It is clear that this is certainly not so – the conflict is undoubtedly asymmetric. Yet, while acknowledging this, many governments still insist that the response to it be exclusively military in nature. This, which will be proven to be a misguided choice, is probably caused by the absence of a consensual definition of terrorism. The significance of this absence of definition was highlighted when the United Nations were unsuccessful at achieving one after 9/11.

As long as there is no globally accepted definition, international society will remain in the dark and continue to act in an incoherent, uncoordinated way against the grave threat posed by terrorism.

A. The Definition of Terrorism: Its Four Elements

It is vital to try to assess the factors which have prevented a consensus on the definition of terrorism. After doing this the main traits that define the contemporary terrorist threat will be outlined, elaborating on authors such as Luis de la Corte Ibáñez, Fernando Reinares Nestares and Cástor Díaz Barrado.

An interesting starting point may be Luis de la Corte Ibáñez's definition of terrorism: "terrorism is a premeditated succession of violent, intimidating actions exerted on non-combatant populations and designed to have a psychological influence on a number of people greatly exceeding their direct victims in order to reach a given, almost always political, goal" [1]. This covers the main traits defining the complex phenomenon of terrorism, and implies four factors:

- The first of these is an understanding of terrorism as violent human actions carried out in an, according to De la Corte, "deliberate and conscious" way and intent on causing harm. It is for this that terrorism is considered a threat to security.
- The second factor is an acknowledgement of the civilian population as the main target of terrorism – though this does not prevent the military from being targeted as well.
- The third factor is the fundamental role of propaganda. As its goal is to upset the balance of power within a society, the ability to communicate its messages and publicise its attacks through media channels is definitely relevant.
- The fourth and last factor is its "instrumental dimension". If, the goal of terrorism is usually to transform the balance of power within a society, it follows that "terrorism is hardly ever practised as an end unto itself", since it responds to a scheme bent not on thirst of death for death's sake, but on spreading chaos and insecurity through the populace to achieve a reaction that will upset the balance of power.

B. The Three Main Goals of Terrorist Groups

By analysing the aforementioned factors, the conclusion can be reached that psychologically weakening the population is the primary goal of terrorist organisations: terrorists plan their

Manuel Gazapo Lapayese is Chief Manager of the International Security Observatory and Researcher at GIPC- Universidad Politécnica de Madrid. Spain (Phone: +34- 686 675 249; e-mail: publicaffairs@international-security-observatory.com).

attacks so that psychological damage will greatly exceed physical or material destruction. The 2001 World Trade Center attacks did cause an exceptional amount of material damage; yet the psychological implications of the collapse of the Twin Towers with thousands of innocent lives inside them were much more devastating, and their consequences were unstoppable. Everybody still recalls how the whole world stood to a still against the images of hundreds of innocent office workers jumping to their deaths to avoid drowning in the flames. And this was exactly the main goal of the perpetrators: achieving a single image that would go round the world, sowing fear in all citizens of the world and making them realise that we are all potential targets for their atrocities. Secondly, the goal that terrorist organisations have of publicising their attacks should be paid attention to. As mentioned, if a terrorist group is unable to spread their message, their operations are unlikely to be successful. Finally, the third goal of terrorist groups is usually to fracture and weaken the system. Terrorism, in spite of being the theoretically weaker party to a conflict that is asymmetrical, tries to change the terms of the equation and destabilise the system supporting its opponent through attacks and media-driven fear-mongering and propaganda.

II. On the Nature of Terrorist Organisations: Structural Properties

After having drawn a profile of the terrorist threat and outlined its most characteristic traits, the second goal of this paper is to analyse the nature of terrorist organisations. The difference between a terrorist movement and a terrorist organisation may have a significant impact in our definition and research of the terrorist threat; the paper will now proceed to analyse the structural properties characterising a terrorist organisation, and to discuss one of the most representative.

A. Movement or Organisation?

Terrorist movements are social movements lacking exhaustive planning. As stated by Luis de la Corte Ibáñez, social movements are characterised by demands or "expression of a social conflict" [2]; the fact that the individuals within it "have constructed and/or assimilated a social identity common to all of them"; or the fact that "in order to achieve their goals of social change –or resistance thereto– they carry out activities of a non-institutional, or even anti-institutional, nature". However, these, "initially devoid of planning and order" may end up undergoing a transformation process leading them to establish themselves as an organisation, that is, "an association of individuals […] expressly created to achieve a number of explicitly defined objectives and aims", where there exists "a division of tasks and functions […] and a set of formal, explicit rules". Thus, the difference between a terrorist movement and a terrorist organisation is that the latter is a much more complex entity than the former. In an organisation, the acceptance that a series of functions have been strictly distributed and a command hierarchy led by an authority has been established means that an effective terrorist phenomenon will be much more likely to be achieved than in the case of a looser 'terrorist movement'. Having discussed this, the question now arises of what leads a terrorist movement to choose to become an organisation.

B. Reasons Leading a Terrorist Movement to Decide to Become an Organisation

Research has shown that the difficulty inherent to terrorist operations and propaganda, recruitment and indoctrination tasks are some of the key reasons behind a given terrorist movement becoming an organisation. A successful terrorist group would have to address all the following issues:

a) The inherent difficulty of terrorist operations: Logistically, a terrorist attack is a very complex operation. This calls for a solid backing organisation allowing recruiting and training the perpetrators, to gather funds and logistical support, and to plan, carry out and publicise the attack.
b) Propaganda: This extremely complex task requires the allocation of a great volume of resources, time and effort. If the terrorist group wishes to carry it out properly, it is only natural that the movement should become an organisation. Propaganda work is, in and of itself, a sufficient reason for movements to turn into organisations.

In order for the images of a terrorist attack to gain worldwide diffusion, the terrorist group must choose carefully the best place for the attack, analyse the way of carrying it out and study in which way it can draw a maximum of media attention. These three are the strategies that allow for the terrorist message to spread; to manage them properly some of the members of the terrorist group would have to specialise in intelligence duty, networking and target research. To carry out all these throughout a terrorist campaign a clear hierarchy of functions and responsibilities must be drawn between all the members of the terrorist entity: the terrorist movement must become an organisation, which, as De la Corte states, carries implicit a "a certain division of tasks and functions […] and a set of formal, explicit rules facilitating the coordination and supervision of the activities of each and every one of the members of the organisation" [3].

c) Recruitment and indoctrination: If a terrorist group wishes to broaden its goals and to achieve increasing psychological impact, the allocation of resources to the recruitment, training and indoctrination of new militants will grow in accordance. This will absorb a large volume of resources and require special attention from higher authorities. For this to be possible, the transformation of the terrorist movement into an organisation is clearly a prerequisite.
d) Locating and gathering economic resources: The greater the terrorist campaign, the more structured the group must be – thus, economic resources will have to be increasingly greater. As Luis de la Corte Ibáñez says, "terrorism would not be possible without money" [4] - for the acquisition of armament, propaganda operations, the recruitment and instruction of new militants and the establishment of

infrastructures require significant amounts of money. If the terrorist group seeks middle/long-term economic stability, it will have to structure its functions clearly.

Terrorist fundraising tasks are characterised by their extreme difficulty. Funding will come from activities such as extortion or kidnapping, front organisations, outright theft or association with organised crime. It is thus sensible that the terrorist movement should choose to transform itself into an organisation for a better coordination of financial affairs.

The core of the ideas stated above is that the intrinsic difficulty of terrorist operations, the effective implementation and spread of the terrorist message and the dedication and resources absorbed by recruitment and fundraising operations are all factors that can be important enough to make a terrorist movement crystallise into a terrorist organisation.

C. Structural Properties: The Characteristic Traits of a Terrorist Organisation

It has been shown above how, in order to be able to guarantee the success of a terrorist campaign, movements must become organisations. The fundamental traits characterising terrorist organisations will now be stated:

a) One of the concepts which have been discussed the most over the previous paragraphs is that of structure. The most notable element distinguishing a terrorist movement from a terrorist organisation is the existence of a clear hierarchy or structure.
b) The second most characteristic trait of terrorist organisations is derived from the concept of structure itself: the specialisation, or departmentalisation, of the organisation.
c) Another characteristic aspect of terrorist organisations is the existence of rules and regulations establishing how the different functions and operations are to be carried out.
d) Finally, the degree of centralisation / decentralisation of their decision-making structures is a defining trait of each specific terrorist organisation.

D. A Contemporary Example Analysed According to These Criteria

One of the clearest examples of the great importance acquired lately by decentralisation, formal structure and the development of operational autonomy is the radical transformation of its hierarchy undertaken by al-Qaeda over the last years. Although this meant shedding the hierarchical model once and for all and becoming a network, it must be remarked that al-Qaeda was network-like almost from the outset, being based on local and regional franchises even though these were subject to a central leader.

Documents from the Instituto Universitario Gutiérrez Mellado and texts by the likes of Fernando Reinares, Luis de la Corte Ibáñez, Walter Laqueur o Herfried Münkler lend credence to the idea that al-Qaeda's original pyramidal structure has given way to a reticular structure: a 'network of networks' [5].

This transformation is based on the key decision of leaving the upper echelons of the terrorist organisation in charge of planning, coordinating and executing the most relevant attacks only while delegating all other, lesser operations. Thus, it may be gleaned that al-Qaeda combines a diffuse, diluted pyramidal structure with an increasingly stronger, more consolidated and developed reticular structure, which allows it to act increasingly quickly on a broader action field: the al-Qaeda core acts in coordination with franchises, small cells indirectly inspired by the original. It must be remarked that this change would not have reached the degree it has without the use of cyberspace as a medium on which to work. The development of communication technologies, the reduction in the prices of hardware and the simplification of software and, fundamentally, the worldwide expansion of the Internet have marked a turning point - a change of paradigm in the dynamics of terrorism.

This example comes to show that the competitive advantage derived from the decentralisation of structures has a value that cannot be overstated, for it allows organisations to improve their security and their resilience, as well as to expand more easily.

III. On the Factors that Can Lead to the Appearance of Terrorist Tendencies

Here a series of factors will be discussed that have been identified as leading to the appearance of terrorist tendencies and propose efficient and effective responses to this global-reaching security challenge:

A. Urban Factor

The complex, dense fabric of the contemporary city entails a transformation of the relationships established within it. The highly densified city into which we are immersed is the ideal breeding ground for new types of social and political violence, for the execution of sophisticated terrorist actions and for groups or collectives operating unchecked and protected by urban anonymity.

It is important to emphasize that this does not imply a causal relation between the urban factor and the appearance of terrorist phenomena. What does exist is a strong correlation between a certain urban landscape and certain manifestations of political violence. It is absolutely necessary to develop tactics for reacting to, and anticipating, the anonymous, viral terrorist tactics springing up in contemporary cities.

B. Collaborative Factor

Another factor that must be considered when analysing the elements and situations favouring the appearance of terrorist phenomena is the presence, or lack thereof, of potential allies.

For a terrorist organisation it can be fundamental to have an environment of groups with which to collaborate in tasks such as the avoidance of police surveillance, information exchange and even mutual support in certain operations. Thus, the existence of allies might favour the organization's stability.

C. Technological Factor

Access to diversified means of transport and technologically advanced weaponry can be a determining factor for the

appearance of terrorist movements which will later become organisations.

Any technological advance is a window for opportunity, carrying with it ample benefits but also significant security issues that will have to be addressed: thus, the technological improvements that led to the invention of the plane gave terrorists a perfect tool for mass attacks; the technological improvements that enhanced the destructive capacity of high explosives allowed terrorist groups to carry out more powerful attacks with the same materials; the technological improvements that led to the Internet have eventually aided terrorist groups in many of their tasks. In other words, all advance has been, is and will be used by terrorists for their strikes. This may invite a reflection on the situation of terrorists: although it may seem an outlandish claim, their position is much more comfortable than ours. They only have to wait for us to develop new technologies and then reverse-engineer their algorithms to turn them against us. In a period such as the present day, marked by unstoppable development and R&D activity, there are more than enough incentives for the terrorists to strengthen their attacks. Although technological development is neither sufficient nor necessary for the existence of terrorism, it can be a factor inciting the apparition, evolution and increase of terrorist currents.

D. Communications Factor

The current existence of international media and the extension of the Internet to the whole planet are neither sufficient nor necessary for the reappearance of old terrorist threats or for the birth of new campaigns; however, they can foster the appearance of such phenomena, as is happening with DAESH.

> *The global terrorist threat is highly amplified by an interconnected world, wherein an incident in one part can instantly provoke a reaction thousands of miles away – and where extremists can just connect to the Internet and learn how to carry out an attack from their own homes.* [6]

It can be argued that, in present-day cyberspace, the ease of access to the databases available is not only one of its defining traits, but also a first-rate factor to take into account when trying to understand why many terrorist organisations are starting to identify the digital world as a primary field for operation. In Magnus Ranstorp's words, "Cyberspace has allowed terrorist groups/movements to withstand the pressure of even the most stringent safety measures implemented by states" [7].

E. Financial Factor

Collecting and managing economic, material and human resources is a key element to the development and evolution of a terrorist organisation. Specifically, a stable and diverse supply of financial resources is arguably a precondition for the existence of any terrorist campaign. The financing of a terrorist organisation can come from the support of its social base, from front organisations or the collaboration with organised crime, from extorting 'revolutionary tax' or from ransom payments.

Jihadi networks are a living example of this: their funds do not come exclusively from extortion and looting, but are derived just as much from human trafficking, the drug trade and deals with organised crime: "the international networks of organised crime have also been taken advantage of by terrorists to launder their money" [8]. This is a showcase of a terrorist organisation doing all that is in their hands to diversify their sources of income; they will also require a variety of alternative channels for circulating it.

All in all, while it is neither sufficient nor necessary for the existence of terrorism, the existence in a conflict scenario of a variety of funding sources and channels is a significant factor that can explain the success of terrorist organisations.

IV. On Cyberspace as Terrorism's New Field of Operation

The notion that terrorism is a constantly evolving threat will be addressed over the following paragraphs, discussing both the characteristics of cyberspace and the reasons for which terrorism is incorporating this new dimension.

A. Characteristics of Cyberspace and Reasons Why Terrorism Is Incorporating It as a New Dimension

1. Immediacy

Cyberspace, a field for action based on electronic and digital interconnections, has as its first differentiating trait the speed at which interactions are carried out. It is evident to everybody that cyberspace can carry virtually instant communication, and can be taken advantage of as such by terrorists. Just as any private individual or company, terrorists use the Internet to exchange information, for they are well aware that no other way of communication is more effective than digital platforms for safe, real-time operation and interaction. Thus, the development of cyberspace has not only been a great improvement for society at large; it has also equipped terrorists with new channels through which to communicate without having to worry too much about the authorities eavesdropping on them.

The field of cyberspace is developing at impressive speed; as a consequence, control and cybersecurity mechanisms are always lagging behind the evolution of threats. Thus, even though it may be perceived that large security agencies control the flow of information on the Internet, these –in spite of filtering massive amounts of data- have been unable to prevent terrorists from communicating through cyberspace and skirting the barriers set up by counterterrorist computer analysts with relative ease.

All in all, the microseconds it takes to send and decrypt an e-mail, carry out a bank transfer or launch a cyberattack do not only set cyberspace apart from any other dimension or field for operation; they are also one of the key reasons for which terrorists are choosing to carry out an increasingly larger part of their operations through cyberspace. In a world where the grip of counterterrorist agencies is ever tighter, the immediacy offered by cyberspace for carrying out any operation is key to

understanding why the Internet is increasingly more interesting to terrorist factions.

2. Accessibility

Information and actions in cyberspace are completely open to anybody whatsoever, from private citizens to terrorists. The evolution of information technologies and constant investment in the development of the Internet have made cyberspace undergo exponential growth in its worldwide use. The leap in technological coverage has been such that access to cyberspace has been democratised all over the world. However, such democratisation does not only have positive effects; it also has implications that put international security at high risk. Any individual with access to the Internet can be recruited by a terrorist cell and become a potential 'lone wolf'. In this sense, internationally renowned terrorism experts such as Rohan Gunaratna –director of terrorism research at the Singapore Institute of Defence and Strategic Studies-, Magnus Ranstorp –director of the Saint Andrews University Centre for the Study of Terrorism and Political Violence- and David Rapoport have noted that virtually unlimited, uncontrolled access to cyberspace has become a key to explaining why so many terrorist organisations have taken so much interest in operating on the Internet.

Herfried Münkler has stated that "the spread of terrorism over the last decades of the 20th century has not been the consequence of a revolution in the means for exerting violence, […] but of an exploitation of the media revolution" [9]. The development of cyberspace and unfiltered, uncontrolled access to it has allowed terrorist operations to spread dramatically all over the world. "Cyberspace has allowed terrorist groups/movements to withstand the pressure of even the most stringent safety measures implemented by states." [10]

Effectively, the ease of access to data is also a first-rate factor to consider when assessing why so many terrorist organisations have begun to identify the digital world as one of their main fields of operation.

3. Anonymity

As explained in a previous paper presented during the First International Conference on Military Studies, which took place in Granada in September, 2014, the characteristic anonymity offered by cyberspace and the unreliability of attribution processes are also a primary reason for which terrorists are increasingly often choosing to operate through the Internet.

In the paper read during said conference, it was stated that the ongoing increase in cyberattacks and in terrorist-oriented use of the Internet are due mostly to the anonymity with which it is possible to operate on the Internet and the inefficiency of the processes for establishing responsibilities after a cyberattack has been committed:

"95% of cybercrime goes unpunished […] This has a great national and international importance for the danger it poses to economy, the citizens and critical infrastructure" [11]. The impossibility, from the standpoint of international law, of controlling potential terrorist uses of the Internet -for any terminal with Internet access could be a potential threat- has made cyberattack prevention a task characterised by great difficulty, for "there will always be a possibility that somebody, from their own living room, will generate and spread a piece of code with catastrophic consequences" [12]. Thus, cyberspace is a systemic field in constant metastasis, where rebounds from the IPs of millions of computers generate a cloud of echoes where it is practically impossible to pinpoint the origin of a terrorist cyberattack.

> *Terrorist behaviour in a cyber-environment offers countless operational advantages for achieving tactical and strategic goals. With relative anonymity, these organisations use information technology as a multiplying force for supplying, conforming and disseminating political propaganda […]; and for ensuring stealth and anonymity both in their day-to-day activities and in tactical operations; as well as for making sure that operations will be cost-effective in terms of invested resources.* [13]

All in all, the anonymity presently characterising the digital dimension may at first sight appear positive for it allows, for instance, for users from all over the world to express their opinion on any topic without repercussions on their personal or professional life. However, from a cybersecurity-based standpoint, it poses a significant problem; for it prevents the authorities from identifying agents who are carrying out illegal activities with "sufficient capacity to launch a cyberattack from which would derive effects comparable to those of the use of armed force; and thus act with due diligence". [14]

4. Asymmetry

It can be argued that the virtual dimension is a battleground which promotes the existence of asymmetric confrontations. There, as opposed to what usually happens in the physical/real dimension, two parties with a radical imbalance in firepower and resources can face each other directly. As we know that terrorism is based on a confrontational logic stating that enemy forces cannot be fought directly but through "nonconventional methods for the use of violence" [15], cyberspace seems a perfect medium for reaching its goals.

The world is before a new scenario for confrontation, completely different from everything it had known. Cyberspace conflicts are characteristically open and asymmetrical, and the theoretically weaker part –in this case, terrorist organisations– can attack a conventionally stronger enemy. For this reason, it can be argued that cyberweapons are revolutionising international relations as well as warfare. "An unprotected computer, system or network is a cyberweapon waiting to be loaded and made use of; and until we accept this we are all at risk" [16].

Cyberspace is a scenario for confrontation where terrorists can face their enemies as equals. Mere access to a digital platform allows any terrorist to attack their enemies while free from the risk of being identified or neutralised.

B. E-Mails Instead of Bullets?

At this point it is fitting to discuss which kind of scenarios, virtual and physical, can be potential targets for terrorist operation. Terrorist organisations are unlikely to, in any case, detach their ballistic potential from their cyber-potential; what is going to thrive in the future, and is already starting to be seen, is a concerted combination of physical attacks and cyberattacks. As said in the aforementioned 1st International Conference on Military Studies, by combining armed attacks with cyberattacks terrorists would be able to drastically weaken their enemies' decision-making processes and thus come out victorious from the confrontation.

The Russia-Georgia conflict is an excellent example of this and showed how the combination of bullets and e-mails carried an unparalleled destructive capacity.

> *The combination of armed operations and cyber-operations sought to cause a loss of operational capacity and of trust in the country's political, military and financial institutions; and to block the communications among these institutions, between the Estonian government and their citizens, and between Georgia and the outside world.* [17]

It would seem, as the media are indicating, that terrorists have taken good notice of this. Thus, as Magnus Ranstorp says, "the most probable scenario for the future is the use of cyberattacks to cause economic losses and amplify social commotion accompanying a conventional terrorist attack" [18]

Thus, it can be argued that those who claim that a large-scale cyberattack is still far from being real are probably out of touch with what already is the present experience. For instance, Jessica Stern and J.M. Berger, authors of the book Isis: The State of Terror, have already pointed out in numerous occasions how easy it would be to paralyse global trade through cyberattacks. As E. Graham remarked in *The Guardian*, "They have not yet been extremely visible carrying out more sophisticated activities such as high-level cybercrime or more destructive attacks, but I suspect this is just a matter of time" [19].

It is not necessary to wait for a Hiroshima bomb-like cyberattack. That cyberattacks are not conspicuous does not mean that they cannot be extremely harmful. It is just necessary to combine the physical and the virtual: "Security researchers have proven it is entirely possible for criminals 1.500 miles away to seize control of your car when you are driving 65 mph down the highway [...] What they do with your hacked vehicle is limited only by their imaginations".

Additionally, even if the technology in the hands of al-Qaeda or DAESH were not sufficient and the cyberattack could not reach their goal, the mere attempt at attacking the likes of New York's JFK Airport or the underwater optic-fibre cables would spread enormous economic insecurity and psychological fear, thus becoming an immense victory regardless. For it must be remembered that the ultimate goal of terrorism is to instil terror in their enemies through psychological warfare. It is irrelevant whether the cyberattack has succeeded or not: in any case, the panic derived from it would be unprecedented and, in and of itself, a fantastic victory for terrorists. Thus, developing a cyberindustry allowing them to carry out virtual attacks combined with physical attacks would not be "squandering finite resources" [20] but allocating them in a very efficient and effective way.

It would obviously be wrong to suggest that these arguments support the currents of thought that claim that, from now on, terrorists will exclusively focus "their energy in materialising cyberattacks" [21]. The stance of this paper is that terrorist movements and organisations are giving an increasing importance to carrying out cyberattacks, which does not mean that they are focusing only on these. The Internet is an increasingly greater priority, but this does not mean that terrorists will become computer hackers overnight; it does mean, however, that they are learning to draw greater benefits from social networks, electronic commerce, instant messaging services, databases or satellite positioning and navigation.

V. Conclusions, Proposals for Countering Terrorism

The results of research have shown the following:

- That the absence of a universally accepted definition of the terrorist phenomenon is due only to a lack of political will.
- That, if a terrorist movement seeks to ensure its long-term survival, it will have to undergo a process of structuring, formalisation and departmentalisation turning it into a terrorist organisation.
- That globalisation, the growth of cyberspace and the dissolution of the nation-state have all favoured the growth and expansion of terrorist initiatives. Therefore, solutions proposed should not be centred solely on military intervention but, first and foremost, on fostering economic cooperation and international transparency. If security is the first step towards development and vice versa, there is no other option than the urgent establishment of peaceful conflict-solving mechanisms.

A. Proposals for Countering Terrorism

1. First Proposal

While there is no case for legitimising terrorist actions, there is also no excuse for the current absence of an internationally-agreed-upon definition thereof. The choice not to define the terrorist threat is not a workable strategy. Terrorism requires a definition acknowledging it as a multidimensional threat to be faced with multidisciplinary measures, with military action taking up a secondary role.

For this reason, this paper's first proposal for its proper countering is to create a new international initiative, based on multicultural dialogue, gathering enough institutional maturity and political commitment to compile a globally accepted definition of the terrorist phenomenon.

2. Second Proposal

In theory, the whole of international society, and especially those actors that have been subject to the scourge of terrorism, are aware that this phenomenon cannot be fought through short-term measures but through long-term measures such as

the promotion of education, economic cooperation, agreements on migration, diplomatic relations, political support, conflict prevention or peaceful conflict resolution. However, in practice most international actors insist on short-term, mainly military measures. This is a great mistake – the fight against terrorism must be multidisciplinary in its perspective. This does not mean that warfare will never be necessary; but it should have a secondary, not central, nature.

Consequently, the second proposal is to promote the adoption of long-term peaceful and constructive measures and perspectives. Terrorism is not a threat that can be neutralised in the short term, for it has roots all over the planet and reaching into several generations. Thus, the only way to combat it would be through a peaceful approach to, and long-term dialogue with, the populations where the seed of terrorism has taken hold.

In this sense, it must be pointed out that, although military intervention is absolutely necessary to stop the advance of certain terrorist organisations such as DAESH, it is only a containment measure. What is needed for their actual defeat is to establish a dialogue with the generations of potential future terrorists and help them change the context in which they live and which has led them, or may lead them, to choose terrorism as a way of life. These future generations will not be convinced by constant military invasion of their territory, but they may be drawn in by a peaceful, practical, proactive long-term project where they themselves can take the lead.

3. Third Proposal

Based on the arguments shown, it is fundamental to point out that a country need not wait to suffer the scourge of terrorism before it begins to act against it. As has been shown, terrorism is not a major cause of death, but its psychological impact is so inordinate and its effect on human rights so massive that it must be addressed by political agendas all over the world as a first-rate issue. Hence, since a state's security is linked to that of its neighbours and to the stability of its periphery, the proposal is for all the international community to coordinate urgently to treat the deeper causes behind terrorism.

4. Fourth Proposal

In spite of the fact that terrorism constitutes a massive violation of human rights, when measures are implemented to face it these are not to, under any circumstance, violate any fundamental rights or freedoms. This means that there is a limit in international law regarding counterterrorism: no matter how urgently terrorism must be weeded out, we cannot afford to become the same thing we are trying to combat. Free democratic states cannot forgo international law; they must preach with the example, for otherwise they would turn into what they are trying to eradicate; as Nietzsche said, "he who fights monsters should see to it that he himself does not become a monster" [22]. Respect for the rules is what sets them apart from their foes.

5. Fifth Proposal

We have to face up to the challenge of developing and generating new structures in international law allowing us to face terrorism in cyberspace. This is an extremely difficult enemy to attack; the adaptation of international law to new security issues such as the spread of terrorism through cyberspace must be a priority.

6. Sixth Proposal

Words hold massive power which often goes unrecognised – to prevent future bouts of terrorism it is crucial to be extremely careful with our choice of words. We cannot commit the same mistake as George W. Bush did when he declared the "War on Terror" in 2001. Terrorism is the perfect example of a modern asymmetrical conflict; if counterterrorism is understood as warfare, terrorist organisations are being put at the same level as states. And we cannot afford this to happen. Giving terrorists the same status as democratic states is, the first great mistake in the fight against terrorism, both in the physical and the virtual dimensions.

We cannot commit the mistake of equating our system to theirs, or of speaking to them as equals: in that way, the fight would begin with a defeat. Jihadi organisations such as DAESH or al-Qaeda seek to establish a caliphate reaching over the whole world and the first step to this is to be treated by states as equals. Consequently, regardless of how many attacks they may commit or casualties they may claim, we cannot give them the chance to become interlocutors at a state-like level.

Therefore, the international community must be more careful with the language it uses. Both the concept of war on terror and that of Islamic terrorism must be eradicated from our discourse, agendas and plans – for it may lead to an erroneous approach from the outset and compromise the chances of success in the fight against terrorism.

7. Seventh Proposal

As a consequence of what has been stated above, the fight against terrorism must be focused around six vectors:

- Multicultural dialogue
- Peaceful, non-invasive, multifaceted interventions
- Development and adaptation of international law
- International cooperation in the fields of intelligence and cyberspace
- Public-private police cooperation
- Military intervention as a last resource or containment measure

These six vectors have been proposed because their combination can allow, among others, to establish bases for dialogue, to develop legal and technical tools against the funding of terrorism, to protect critical infrastructures consistently at a global level and to perfect cybersecurity.

Ultimately, it is crucial to understand that against terrorism war cannot be waged – it is plainly and simply impossible. War cannot be waged against something nebulous: for terrorism, among other things, lacks both a professional army and a clearly delimited territory. However, it can be fought, neutralised and -especially- prevented. If we are so ready to

wage war, let us do it against the economic inequality and poverty running rampant where terrorism originates; let us wage war against radicalisation or discrimination; let us wage war against all elements that are liable to sow the seed of terrorism. Of course, these wars will be much more complex than military warfare against terrorism – chiefly because we have little interest in waging them, even if they would have a hugely greater middle and long-term benefit than the present, ill-advised wars against the terrorist phenomenon.

Until we realise that we are responsible for the present state of our international 'beehive' –and until we admit that we are indifferent to anything happening beyond our comfortable little cell– no efficient response to terrorism will be possible.

REFERENCES

[1] L. de la Corte, *La lógica del terrorismo*. Ed. Alianza, Madrid, 2006, pp. 42-43.
[2] L. de la Corte, *La lógica del terrorismo*. Ed. Alianza, Madrid, 2006, pp. 275-276.
[3] L. de la Corte, *La lógica del terrorismo*. Ed. Alianza, Madrid, 2006, p. 276.
[4] L. de la Corte, *La lógica del terrorismo*. Ed. Alianza, Madrid, 2006, p. 139.
[5] L. de la Corte, *La lógica del terrorismo*. Ed. Alianza, Madrid, 2006, p. 298.
[6] Europa Press, "El director de CIA dice que las redes sociales amplifican la amenaza terrorista", in Europa Press, 13 March 2015 http://www.europapress.es/internacional/noticia-director-cia-dice-redes-sociales-amplifican-amenaza-terrorista-20150313202208.html (consulted May 15, 2015)
[7] M. Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", in *El nuevo terrorismo islamista. Del 11-S al 11-M*. Ed. Reinares, F. & Elorza, A. Ediciones Temas de hoy, S.A., Madrid, 2004, p. 208.
[8] L. de la Corte, *La lógica del terrorismo*. Ed. Alianza, Madrid, 2006, p. 145.
[9] H. Münkler, Viejas y nuevas guerras. Asimetría y privatización de la violencia. Ed. Siglo XXI, Madrid, 2005, p. 149.
[10] M. Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", in *El nuevo terrorismo islamista. Del 11-S al 11-M*. Ed. Reinares, F. & Elorza, A. Ediciones Temas de hoy, S.A., Madrid, 2004, p. 208.
[11] J. Duva, "El 95% de los ciberdelitos cometidos quedan impunes", in El País, 4 May 2014 http://politica.elpais.com/politica/2014/05/03/actualidad/1399117342_852720.html (consulted June 26, 2015)
[12] J. López, "La evolución del conflicto hacia un nuevo escenario", in *El ciberespacio. Nuevo escenario de confrontación*. Ed. Ministerio de Defensa. Madrid, 2012, p. 142.
[13] M. Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", in *El nuevo terrorismo islamista. Del 11-S al 11-M*. Ed. Reinares, F. & Elorza, A. Ediciones Temas de hoy, S.A., Madrid, 2004, p. 208.
[14] S. Torrecuadrada, "Internet y el uso de la fuerza", in *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio*, Ed. Segura, A. & Gordo, F. Editorial Universidad de Granada, 2013, p. 108.
[15] H. Münkler, Viejas y nuevas guerras. Asimetría y privatización de la violencia. Ed. Siglo XXI, Madrid, 2005, p. 131.
[16] M. J. Caro, "Alcance y ámbito de la seguridad nacional en el ciberespacio", in *La seguridad un concepto amplio y dinámico. V Jornadas de Estudios de Seguridad*. Ed. Instituto Universitario General Gutiérrez Mellado de Investigación sobre la Paz, la Seguridad y la Defensa, Madrid, 2010, p. 79.
[17] N. Ganuza, "La situación de ciberseguridad en el ámbito internacional y en la OTAN", in *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Ed. Ministerio de Defensa: Cuadernos de Estrategia Nº 149, Madrid, 2010, p. 199.
[18] M. Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", in *El nuevo terrorismo islamista. Del 11-S al 11-M*. Ed. Reinares, F. & Elorza, A. Ediciones Temas de hoy, S.A., Madrid, 2004, p. 216.
[19] E. Graham, "Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?", in The Guardian , 12 April 2015 http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race (consulted May 5, 2015)
[20] M. Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", in *El nuevo terrorismo islamista. Del 11-S al 11-M*. Ed. Reinares, F. & Elorza, A. Ediciones Temas de hoy, S.A., Madrid, 2004, p. 217.
[21] M. Ranstorp, "Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información", in *El nuevo terrorismo islamista. Del 11-S al 11-M*. Ed. Reinares, F. & Elorza, A. Ediciones Temas de hoy, S.A., Madrid, 2004, p. 216.
[22] F. Nietzsche, *Beyond Good and Evil* (*Jenseits von Gut und Böse*). 1886, Aphorism 146.

Manuel J. Gazapo Lapayese (Madrid, 1992) holds a BSc in International Relations (Universidad Complutense de Madrid, Madrid, Spain, 2014) and an MSc in International Affairs: Economics, Politics and Law (ICADE, Madrid, Spain, 2015).

He is the Director of the International Security Observatory (Madrid), as well as an Ambassador for EU Careers Madrid. He has held a scholarship at the European Parliament under the direction of Ms Pilar del Castillo MEP. Among his latest publications are "El ciberespacio y la ciberseguridad: Estrategias comparadas entre España y Europa" in *I Congreso Internacional de Estudios Militares* (Granada, Spain, 2014) and "Cyberscape: cybersecurity as a field for contemporary confrontation" in *Strategies XXI* (Bucharest, Romania, 2015).

Mr Gazapo is a researcher for the Cultural Landscape Research Group (GIPC – Universidad Politécnica de Madrid).