
**RESEARCH PAPER**
**No. 117**

**JANUARY 2008**

# THE ROLE OF INTELLIGENCE IN THE BATTLE AGAINST TERRORISM ON THE INTERNET: REVISITING 3/11

**GUSTAVO DÍAZ**
**(Complutense University, Madrid)**

**ALFONSO MERLOS**
**(Complutense University, Madrid)**

**RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)**

**# 1, Kalavryton Street, Ano-Kalamaki, Athens, 17456, Greece**
**RIEAS URL: http://www.rieas.gr**

## RIEAS MISSION STATEMENT

### Objective

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

### Activities

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

### Status

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

**Dr. John M. Nomikos**
**Director**

**RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)**

**Postal Address:**

# 1, Kalavryton Street
Ano-Kalamaki
Athens, 17456
Greece

Tel/Fax: + 30 210 9911214

E-mail: **rieas@otenet.gr**

## Research Associates

**Mr. Ioannis Moutsos**, Independent Investigative Journalist
**Mr. Andreas Banoutsos**, Intelligence Studies
**Mr. Konstantopoulos Ioannis**, Intelligence Studies
**Mr. Nadim Hasbani**, Lebanon-Syria and North Africa Studies
**Mr. Nikos Lalazisis**, European Intelligence Cooperation
**Mr. Naveed Ahmad**, South & Central Asia and Muslim world

# THE ROLE OF INTELLIGENCE IN THE BATTLE AGAINST TERRORISM ON THE INTERNET: REVISITING 3/11

**GUSTAVO DÍAZ**
**(Complutense University, Madrid)**

**ALFONSO MERLOS**
**(Complutense University, Madrid)**

## Introduction

> *. . . In the past, the intelligence community's primary job was to know the Soviet Union. With the loss of the Soviet paradigm, other security issues have moved up in relative priority, and the built-in excuse for not concentrating on them is gone.*[1]

In this paper we argue that understanding terrorism within the new cyber environment of the twenty-first century is paramount for the intelligence services in the dawn of the 21st century. We believe that the intelligence services will have to confront this new trend in terrorism tactics in years to come whether they are fully prepared or not. This new type of threat will be one of the principal questions for intelligence services in the 21st Century.

Today, terrorist groups can access global information infrastructures owned and operated by the governments and corporations they want to target. Information systems, now serve as **both weapons and targets** of warfare.[2] The current terrorists have learned that nowadays the safety of the world depends on the infrastructures of computers and on networks all around the world.[3] A strategic assault on these systems would have undoubtedly devastating consequences for any country and its economy. Therefore as the economic structures of the democratic countries become more dependent on the computer systems, its protection and safety before the cybernetic assaults will be one of

1 See K. E. Scott, ''Paradigm shift: US strategic intelligence in the 1990's. Study Project'' http://www.osti.gov/energycitations/product.biblio.jsp?osti_id/6210758

2 The possibility of digital warfare and terrorism became a widespread concern in the early 1990s largely as a result of reports such as National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy Press, 1991) and books such as Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993).

3 Sullivant, J. (2007): *Strategies for protecting critical infrastructure assets*. Hoboken, NJ: Wiley.

the more important subjects for the security services, for this beginning of the 21st century.

On the other hand the cyberterrorist threat must not make us forget the daily use that this type of organization does of the network for communications, propaganda or the psychological warfare. As the use of new technologies applied to the traditional activities, as the propaganda on line, the establishment of former methods in new areas (physical attempts on systems of information), or the convergence of new technologies and new activities. These groups that need to establish minimally sure communications and to administer their funds from the anonymity, have found in the technology of the information an ally to cover these requirements. For example, the refugees of the opposition of Saudi Arabia in The United States have installed services of E-mail and exchange of information for the World Wide Web to receive information of their contacts, which they then will use as propaganda from the exile. Also the Sinn Fein, the political arm of the IRA (Irish Republican Army), established a site to receive donations on line and spread for this way, information on the positions of the British Army. Therefore we can affirm that the today terrorists take advantage of the Internet virtue to reach their aims.

## 1.- The first task for the intelligence services: Understanding the threat

Cyberterrorism, is a term that was relatively unknown before the September 11, 2001 terrorist attacks, has since become widespread, almost ordinary, just as the Internet has become more pervasive in all areas of human endeavour. Dr. Dorothy Denning defines cyberterrorism as "the convergence of terrorism and cyberspace", suggesting is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[4]

Currently, DoD of the United States does not have a definition of cyber-terrorism, but does define cyberspace as "the notional environment in which digitized information is communicated over computer networks."[5] In the U.S. Federal Government, the FBI describes cyber-terrorism as a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda."[6] In this sense, "cyberterrorism is the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)".[7]

---

[4] Denning, D. Cyberterrorism. Testimony before the House Terrorism Committee on Armed Services, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[5] 14 Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001, as amended through 17 December 2003.

[6] Harold M. Hendershot, "CyberCrime 2003 – Terrorists' Activity in Cyberspace" (Briefing slides from the Cyber Division, Federal Bureau of Investigation, Washington, D.C., 12 http://www.4law.co.il/L373.pdf; Also see: Keith Lourdeau, "Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security" ,February 2004, http://www.fbi.gov/congress/congress04/lourdeau022404.htm

[7] Michael Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?", *Crime, Law and Social Change* 46, Nº 4-5, 2006.

We understand cyber terrorism as any act of terrorism that uses information systems or digital technology (computers or computer networks) either as an instrument or a target. Following the lead of Peter Flemming and Michael Stohl we think that cyberterrorism should be understood as a new terrorist tactic rather than a new distinct form of terrorism.[8] Indeed, it is the last development of terrorist capabilities provided by new technologies and networked organizations.

## 2.- The Impact of the Technological Revolution in the Terrorist Threat

In the last decades, computer technology has expanded enormously, as has its role in everyday life and in the management of public and private infrastructure. The CIA pointed out in a statement for the Joint Economic Committee in 2001, "most experts agree that the Technological revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid-eighteenth century."[9] In the same way people use the Internet, terrorists use it as a tool for communication. Internet allows people with common interest raging form collecting to terrorism to find each other and share information. Terrorist organizations use the Internet in several ways, either as **arms or as targets**, with the aim of continuing their fight. They publicize the terrorist's cause, raise money, and recruit members.[10]

However, the increasingly indispensable nature of information technology, however, has transformed these systems into high value targets of cyber terrorists and presents a significant threat to the military, economy and national security all arround the world. Indeed, given the relevance of computers and the Internet, massively violent means are not needed to threaten important elements of national economic life and the basic functioning of society to create fear and insecurity. Computers viruses and hacking have become insidious threats of great concern.

The technological revolution has increased the terrorist ability to engage in activities such as recruitment, communication and especially financing without the knowledge of state authorities, which may lead to stronger operative action. Today terrorist groups may become, more elusive and **deadlier** than their earlier counterparts. Moreover, the advent of computer networks has spawned a new direction in the organizational structure of terrorist groups likely to move beyond hierarchical organizational structures and employ **networked** ones. Also the opportunities presented by the cyber environment have translated into more groups that **are less reliant on external sponsors**.

The rapidly emerging cyber environment brings many concerns and uncertainties. The technological revolution offers contemporary terrorist groups a wide range of

---

[8] Peter Flemming And Michael Stohl, in *Countering Terrorism Through International Cooperation*, Alex P. Schmid (ed.) (2001): ISPAC, International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program, Vienna, pp 70-105.

[9] Director of Central Intelligence, *Cyber Threat Trends and U.S. Network Security*, Statement for the Record for the Joint Economic Committee by Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, (Washington, D.C., 21 June 2001), 1, http://www.cia.gov/cia/public_affairs/speeches/2001/gershwin_speech_06222001.html

[10] Mockaitis, T. R. (2007). *The "new" terrorism: myths and reality*. Westport, Conn: Praeger Security International

opportunities. It will play a major role in providing a wider range of options. Cyber terrorists will try to capitalize on known weaknesses and continue dedicated research and mining to discover new vulnerabilities in Western security systems. As stated in an al Qaeda statement in February 2002, *"despite the fact that the jihadi movements prefer at this time to resort to conventional military operations", jihad on the Internet is a serious option for the terrorist in the future for the following reasons: Remote attacks on Internet networks are possible in complete anonymity; The needed equipment to conduct attacks on the Internet does not cost much; The attacks do not require extraordinary skill; The jihadist attacks on the Internet do not require large numbers of people to participate in them.*"[11]

Because it moves globally at the speed of light, information technology enables and facilitates the **operations of networked terrorist.** It allows terrorists to move openly without attracting attention (at least in liberal, multicultural, open Western democracies), while simultaneously strengthening their ability to attack in a coordinated fashion. In this sense, as **Brian A. Payne pointed out, "**the transparent nature of Western society and the development of globalized information systems provide Al-Qaida a tremendous advantage in gathering actionable intelligence".[12] The terrorist *intelligence* has augmented through the globalization of information networks. **The development of the World Wide Web** has also been a boon to terrorists. Today the availability of information contributing to an attack is **incredible.**[13] The ability to communicate and share this information via encrypted messaging has facilitated the planning and execution of several Al-Qaida attacks.[14]

**As Western nation's economy become more dependent on computers**, and the Internet becomes an increasingly more integral part of our society, new digital vulnerabilities make the Western networked systems potential targets to an increasing number of individuals including terrorists. The vulnerabilities to networked systems arise from a number of sources, such as: easy accessibility to those systems via the Internet; harmful tools that are widely available to anyone with a point-and-click ability; the globalization of Western infrastructures increases their exposure to potential harm; and the interdependencies of networked systems make attack consequences harder to predict and perhaps more severe.[15]

## 3.- Terrorist Recruiting and Training Using Internet

The original nature and the new structural and operative dimensions, up to which there has grown the threat of the new jihadism, are directly linked to the use of the new technologies. In the current strategic scene, the communication and the propaganda have turned into central elements of the strategy of the global jihadist movement to

---

11 Ben Venzke and Aimee Ibrahim, *The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics and Targets* (Alexandria: Tempest Publishing, LLC, 2003), 36, quoting Abu 'Ubeid al-Qurashi, "The Nightmares of America, 13 February 2002.

12 Schweitzer, Y., & Shai, S. (2003). The globalization of terror: the challenge of Al-Qaida and the response of the international community. New Brunswick [N.J.]: Transaction Publishers, P.134

13 www.globalsecurity.org

14 9/11 Commission Report, 88.

15 Sullivant, J. (2007). *Strategies for protecting critical infrastructure assets.* Hoboken, NJ: Wiley.

guarantee the efficiency in the search of the intimidation and the extortion, of the blackmail and the submission; also to reinforce the symbolic character of every big wave of political premeditated and systematically designed violence.

The communication and the propaganda are not sufficient factors but necessary to understand how monolithic, vertical and rigid Al Qaida has been capable of surviving an offensive of harassment without precedents not only keeping intact its capacity of movement and its operative potential but strengthening them up to the end, discovering, exploiting and controlling a new theatre of operations.

The cyberspace has turned into the ideal frame of operations for the terrorist organizations that have known to put to the service of its tactical and strategic interests the innumerable advantages that environment offers: facility of access and maintenance, scanty regulation and governmental control, anonymity, rapidity in the interchange of information, access to the public international opinion and, definitively, comfort for the planning and coordination of operations that turn out to be profitable in terms of resources used and the global scope, thanks to the multiply force of the Net[16]. Also it is necessary to add that Internet has managed to annul the ethical barriers that traditional mass media establish on the specially violent contents, something that re-dresses special given relevancy the allergy that the western governments show to the fact of which the impact of bloody images in the public opinion could determine his support to certain orientations of foreign policy.

The politicians, security agencies, academicians and journalists' principal worry has centred traditionally on the challenge that the cyberterrorism supposes underestimating the different "passive uses" that the terrorist organizations do of Internet. Precisely only across the analysis of the complete scale of manoeuvres opened in the cyberspace it will be possible to better understand the movements, the capacity and the intentions of the neosalafist, to offset if possible, their campaigns of propaganda and worldwide propaganda and, scope especially, their power of performance: the tracking and control of the jihadists communications circles from the services of information and intelligence of The United States and its allies has facilitated relevant detentions and the consequent break of terrorist plots in different phases of planning.

In the current strategic context, the terrorists control in a direct way the bottom and the form of their messages; they have a major margin of manoeuvre to manipulate their image and that of their enemies; they produce and edit their communications without intermediaries or filters and in occasions with the highest degree of sophistication, trying to dominate the way of influence and the impact over their potential hearings. Of episodic and intensive form, neosalafists raise that West has not left them another option any more than to resort to the violence, that The United States and its allies are those who exercise the real terrorism and the most brutal, inhuman and immoral aggressions and, definitively, that the resource by force against military and civil population is an instrumental, transitory and relating to the moment way to stop

[16] Weinmman, Gabriel. "How Modern Terrorism Uses the Internet". *USIP Special Report*, nº 116, 2004, p. 3.

repressive governments and, for extension, to the enemies of the Muslims. Jihadist have exploited the environment multimedia with multiple and complementary ends.

In the first place, it has been used to promote operations of *psychological war*. Across Internet, terrorists have been capable of supporting a campaign of disinformation that has combined systematically the recovery of attempts with the spread of new threats, founded or groundless. The clear aim has been to transmit an internal image of fortress and strength, trying to mine the morality of The United States and its allies and fomenting the perception of vulnerability in these societies.

Across this studied strategy, groups and cells of limited importance and of unknown structure have managed to amplify extraordinarily the scope of its message and its actions reaching a global impact. The videos of the tortures, the petitions and / or the murder of hostages like the Americans Nicholas Berg, Eugene Armstrong and Jack Hensley or the British Kenneth Bigley and Margaret Hassan that have circulated over-excited for numerous servants and Internet portal has reinforced cyclically and persistently the sensation of defencelessness of the western societies and there have questioned the legitimacy and the effects of the "Operation Iraqi Freedom"

Secondly, young islamist, enthusiastic with the informative wealth that flows across Internet have found in this system an inexhaustible source of *internal documentation*, a library from which they are extracting the information and the most complete recipes to obtain the most diverse goals: from hack electronic pages up to sabotaging nets, creating files protected by encrypt codes or develop chemical and biological agents capable of being used as weapons.

Across opened sources and without resorting to illegal means, as the DoD of the United States has recognized, it is possible to assemble up to 80 % of the necessary information, from a qualitative and quantitative point of view, to attack with efficiency the enemy. From the access to maps and planes on objective potentials happening for the inquiry of the schedules of means of transport or precise details on the functioning of critical infrastructures as airports, ports, hydroelectric head offices, refineries of oil, preys, nuclear plants or chemical plants, the terrorists have seen in the Net a window opened for the attainment of their aims of mass destruction.

In some computers seized to members of Al Qaida there have appeared the details of the architectural structure and of engineering of a prey, which had downloaded of an electronic page and which could allow the engineers and planners of the net to design catastrophic attempts to strike these facilities. Of other computers it has been known that they were used by jihadists to sail along pages that were offering instructions of programming of the digital switches that make work the water nets, energy, transport and communications, information that might facilitate the execution of cyber attempts to great scale with human and economic incalculable repercussions.

Thirdly, cyberspace has turned into a field opened for the service of the *planning of tactical and strategic coordination of operations of mass destruction*. Already in the scene before the attempts on Washington and New York, the Palestinian Abu Zubayda, at the head of the recruitment and the logistics of Al Qaida's counterfoil, used an

electronic page to communicate across encrypted messages with the cells under the control of the Egyptian Mohamed Atta. In the moment of his detention in Pakistan, on March 28, 2002, Zubayda was accumulating more than 2.300 messages in his computer with keys for its protection. His communications, many of them supported from *cyber coffees* in Pakistan, were intensified in May, 2000, reached their top in August, 2001 and went out on September 9, 2001.

The operative leader of four suicidal cells in the morning of September 11, 2001 in Washington and New York confirmed the date of the attempts, the number of terrorists involved in the plot and the identification of the aims across a succinct electronic message: “The semester begins in 3 weeks. We have obtained 19 confirmations to study in the Faculty of Laws, in that of Architecture, in that of Arts and in that of Engineering”. Also in the context of 9/11, the federal attorney of the District of Columbia, Ken Wainstein, revealed before the Commission of Criminal Activities, Terrorism and internal Security of the Congress of The United States that two of the abductors involved in this operation, Nawaf Al Hazmi y Khalid al Mihdar, did the reservations for the flight 77 of American Airlines that then they would star against The Pentagon from the Internet service of the library of a public university of New Jersey.

The offensive launched after 9/11 to dismantle the fields of training to opened sky managed by the organization Al Qaeda has propitiated that, in parallel and with the passage of time, Internet has had an impact very emphasized in the creation of new and effective forms of *recruitment*. The use of programs that allow to support to two or more speakers conversations in the intimacy of codified and restricted access has been a habitual system to close, from Europe and from the middle of 2003, the terrorists' sending to Iraq, in general Muslims without experience of combat that they had acceded by electronic means to manuals of military training under titles as “The art of the kidnapping”, "Military Instructions for the mujahideens", "The war inside the cities", "Manual of the terrorist", "Manual of poisons for the mujahideens" or "Manual for the sabotage ".

The permanent increase of the number of participants in cyberjihadist circles that communicate in English, French or German is a direct consequence of the process of radicalization and conversion to the salafism armed with a worrying segment of the *muslim Diaspora* seated in Europe. To the Muslims' sectors with an intellectual acceptable preparation and a technical training they have been persuaded by messages that offer the possibility of adding to the projects of the movement jihadist globally in the recording, the edition and the production of videos, functions for those that the authority has proclaimed itself both as the English and as the Arabic and the full disposition to travel to conflict zones.[17]

The creation of a virtual universe jihadist has increased the degree of physical isolation of the terrorists or recruited potentials I concern of the societies into whom they are infiltrated and it has shot the process of radicalization at the margin of any possibility of social integration, especially in the European communities. Internet not only has fomented the phenomenon of the terrorist self-radicalization but very specially that of the auto-recruitment and the self-training.

[17] La Guardia, Anton. “Al Qaeda Places Recruiting Ads”. *The London Telegraph*, august 10, 2005.

One of the most complete terrorist manuals for the training that circulate along the Net is the acquaintance as “Al Qaeda's Encyclopaedia” of preparation for the jihad, who gathers the experience and the educations derived from the guerrilla warfare against the Soviet troops parked in Afghanistan from 1979 to 1989. It is a document that is permanently completed and updated and that teaches jihadists about complete field of action, from the managing of light armament up to the manufacture of explosive appliances, the preparation of electronic circuits or the elaboration of chemical compounds capable of being used by major or minor efficiency as armament. Especially profuse they are the chapters in that the complete and complex process is detailed for the acquisition, the analysis and the presentation of information as a product of intelligence to be exploited by the organization.[18]

European information services have certified that this material not only has been used for jihadists whose actions are stimulated by a political motivation but for criminals who move with merely economic purposes. In parallel they have stated the appearance in certain pages of instructions detailed in Arabic to develop nuclear armament or to make 'dirty bombs'. On December 26, 2002, Abu Shihab Al Kandahari was publishing an article under the title “The nuclear warfare is the solution for the destruction of The United States “.

It was not a question strictly of a manual for the production of atomic armament but a document of the one that was parting that the global jihadist movement already had done to itself with some type of not conventional ammunitions which destiny was to be used in a mega operation against Washington or, in the second term, against 'the atheistic government of Moscow'[19].

In June, 2005 it began to circulate on the Net a document in Arabic of 15 pages tilted “Biological Weapon” that, attributed to Setmarian Nasar, described, for example, how the plague of the pneumonia could be transformed into a weapon. After revising the biological arsenal used by The United States and Japan during the World War II, the text was detailing how test injecting virus to rates or how to extract microbes of infected blood and to isolate them in order they could be compressed and spread across a system of aerosol.

With pragmatic and operative character, on October 6, 2005 someone made circulate along a page of jihadist debate, *Al Firdaws* ('The Paradise'), a document of 80 pages divided in nine chapters, under the title “The nuclear bomb of the jihad and the method to enrich uranium”, with exhaustive methods, included graphical procedures, to develop this type of unconventional weapon. The author, who was identifying with the pseudonym of *Layth al Islam* or Lion of Islam, was assuring to belong organically to the group 'Black Flags' and declared that in spite of the fact that the nuclear weapon was the

---

[18] Bakier, Abdul Hamied. “Jihadis Adapt to Counter Terror Measures and Create New Intelligence Manuals”. *Terrorism Monitor*, vol. 4, nº 14, july 13, 2006, pp. 1-2.

[19] Paz, Reuven. “Global Jihad and WMD: Between Martyrdom and Mass Destruction”. *Current Trends in Islamist Ideology*, vol. 2, 2006, p. 77.

symbol of the old technology of the 40's, the crusades had pledged in an unjust and systematically way in denying the jihadists access. [20]

Internet not only has served for the training in terrorist tactics but to reason the resource to each of them according to the context and the scene of the moment. In May, 2004, the tenth number of *Al Battar* was assuring that the importance of the kidnapping was taking root in that it could serve to different purposes, principally: a) to force an enemy government to succumb before the demands of the authentic Muslims, b) to create a shock among an enemy government and the feelings of his public opinion to provoke his delegitimation at the internal level, c) to obtain relevant information of the arrested capable of being exploited for future terrorist projects, d) to obtain an economic compensation for the liberation of hostages to continue financing the jihad and to facilitate his perpetuation, and e) to state before the public international opinion the injustices that the enemies of the Islam take to end[21].

The aim to facilitate the labours of training of the terrorists from Internet has been achieved across the diffusion not only of operative manuals but of critical documents in which one tries to extract lessons for the future of past conflicts. Paradigmatic case was the profusion of electronic texts that analyzed the battle developed at the end of 2004 by the control of Faluya, emphasizing the factors that can determine the victory in the defence of a low terrain, these are: 1) to have weapons adapted for the combat, 2) to dominate the skills of ambush, 3) to rely on skilful snipers, and 4) to enjoy the widespread support of the persecuted population[22].

The scene of Iraqi post-war period has used as base in order that they circulate profusely documents in which jihadists are recommended to face the combat in urban zones: a) to avoid the direct shock and the establishment of static zones, b) to centre in rapid operations and to avoid the immediate reprisal from the air for the enemy, c) to escape of instinctive form of the enclaves attacked in order to avoid the surrounding for land of the troops of The United States, and d) the harassment to look against those areas that the adversary believes that they have been effectively appeased preventing them in the theatre of operations from creating sensations of tranquillity, normality or stability.

## 4.- Inspiring 3/11 Terrorist Attacks from the Net: An Investigation Hypothesis to Consider

As so many other fronts opened in the combat against the new jihadism, the Internet battle is for the intelligence services a decisive career. As the western security forces develop and apply with efficiency their systems of counter alertness discovering the weaknesses and the holes of jihadists, they perfect the systems of communication across an insistent testing method.

---

[20] Mahnaimi, Uzi y Walker, Tom. "Al Qaida Recruits with Nuclear Bomb Website". *The Times*, november 6, 2005.

[21] Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington. US Institute of Peace, 2006, p. 129.

[22] International Crisis Group, "In Their Own Words: Reading the Iraqi Insurgency". Middle East Report, nº 50, February 15, 2006, p. 15.

The valuable ones though incomplete and insufficient investigations that have derived in Spain of the 3/11 plot have allowed to determine the new coordinates in the area of the technology in which neosalafists move. Attila Turk, militant of the Islamic Moroccan Combatant Group (IMCG), has detailed some of the novel subterfuges for the internal communication used by an organization that interfered to the maximum level in the operation “trains of death". Hasan al Haski one of his leaders, used to contact across Internet a method that turns out to be extremely secret and that has surprised the agents of information: his communications were not transmitted from one account of mail to another, but they were coming from a unique account; both terrorists were using the same user's name and password (the same electronic door of access), leaving the terrorist / issuing messages in the paragraph "draft" and the terrorist / recipient in the paragraph "record", so they were avoiding the bidirectional transmission of the message.

This was the system used by a terrorist who was not a minor element in the networks of the Maghrebian salafist terrorism. The investigations developed by the Central Unit of Foreign Information in Spain, fitted organic and operatively in the General Police Station of Information, have determined that after the partial breaking up of the infrastructure of the IMCG as a direct consequence of the police and judicial offensive untied after 3/11, not only in operations completed in Spain but especially in France and Belgium. An element of the dome of the organization, as Al Haski, was starting constituting from a sure place as the Canary Isles and protected by followers as Abdalla Bourit the new structure of the IMCG in Europe, with the intention of being done by the absolute leadership in the continent.

The concrete use of Internet on the part of this Moroccans' cell is one of the certainties that the Spanish services of information could have stated in the intensive investigations that have as purpose dismantle the networks, essentially of Maghrebian origin, implanted clandestinely. It is for determining if, besides fulfilling this function of internal communication, the Net has fulfilled mobilization, inspiration, instigation and, especially, that of strategic orientation in case of the operation executed on March 11, 2004. In other terms: to reveal the scope of the plot, one of the most determinant questions happens for explaining when, who and from where one gave the order to commit an outrage in this date and not in other one, against the selected aim and not against other one.

The Spanish security agencies have handled as working hypothesis that one of the coordinators of the plot, concretely in charge of fixing the temporary coordinates of the attempt and of giving the order of execution might be the Syrian Moutaz Almallah Dabas, detained by the British police in March, 2005 by an international order dictated by the judge of the National Hearing Juan del Olmo. The brother of Mohannad Almallah, was also detained for his relation with 3/11. Moutaz could contact with Serhane Ben Abdelmajid "The Tunisian", Jamal Ahmidan “The Chinese” and Rabei Osman al Sayed “The Egyptian” at the time that he was involved in jihadist recruitment for their protection, training and infiltration in Iraq across the Syrian border.

Nevertheless, the control of the operation well might have had its origin in the Net. Few documents elaborated and emitted by the International Islamist analyze with

so many accuracy and clear-sightedness the political, social dynamics and informative search and generated by the 3/11: the aim was not only to kill innocents in a premeditated and systematical way but to reach a clear political purpose across a disproportionate influence in the public opinion. “Iraqi Jihad, Hopes and Thoughts: Analysis of the Reality and Visions for the Future, and Current Steps in the Path of the Blessed Jihad " is a key text to understand the dimensions of the intention, action and reaction untied after the massacre. It is a document written as draft in September, 2003 but that it is not published until December 8, 2003 in *Global Islamic Media* and later in *Al Farouq*, two of the electronic favourite directions of the Islamists[23].

It is a strategic text that defines with brightness and for stages the lines of performance of the Iraqi insurgency, signed by the “Media Committee for the Victory of the Iraqi People (Mujahideen Services Centre)” and dedicated to Yusuf to the-Ayiri, ideologist and coordinator of the media device of Al Qaida to whom the Saudi security forces shoot down in May, 2003 and who dedicated the last months of his life to design a strategy of ‘defensive jihad’ applied to Iraq from an eminently pragmatic and political approximation, with little attention to theological and religious references; an approximation put in his last and more influential works: "The Truth about the New Crusader War", in where he justifies 9/11, and "The Future of Iraq and the Arabian Peninsula after the Fall of Baghdad", in where he proposes to extend urgently the jihad to the Great Middle East.

The author or authors of the text follow the same line. They seek to contribute a realistic orientation to an international hearing of Islamism in disposition to implement assaults capable to defeat the will of the allies and their political, economic and military commitment in the Iraq post-Sadam. The analysis departs from the hypothesis from that not only the political or military cost of the occupation but especially the economic one will make to The United States fold its troops in a comparable movement to that of the Soviet Union in Afghanistan. In the second term, the text explicit the necessary means to reach the aim, and interprets that the US presence will not be sustainable if the number of allies limits himself to the maximum. After penetrating into the effects that an attempt would generate in United Kingdom, Poland and Spain, the text determines that the latter is “the weakest link of the chain".

Beyond the propaganda and the Islamist oratory, some kind of *realpolitik* in its more crude sense crosses the exposed arguments. It is a question of complex and multidimensional analysis demonstrating the highest degree of information and interpretive deep keys of domestic politics. Definitively, the lack of consensus in foreign policy and the distance between the position of the government and the public opinion in the case of ‘Iraq intervention’ placed Spain in the front of fire.

These factors were opening two scenes: a) a series of two or three attempts in Spanish territory or against Spanish interests would make the government of the Popular Party move back and withdraw its troops, or b) if the government was not

[23] Paz, Reuven. “A Message to the Spanish People: The Neglected Threat by Qa’idat al-Jihad”. *PRISM Series of Special Dispatches on Global Jihad*, vol. 2, 2004; BRYNJAR, Lia y HEGGHAMMER, Thomas. “Jihadi Strategic Studies: The Alleged Al Qaida Policy Study Preceding the Madrid Bombings”. *Studies in Conflict & Terrorism*, vol. 5, 2004, pp. 355-376.

deciding to yield and was ratifying the military board in Iraq, the victory of the principal opposition party that was including in its program the doubling of the brigade "Plus Ultra", was almost insured. Raised the situation in these terms, and in the opinion of the islamists, a step backwards of Spain or Italy would provoke a similar reaction in the United Kingdom and would untie irreversibly “domino effect”. The selection of Spain was not an accident: already in December, 2003, there were numerous islamist web sites showing the video in which a rabble of mujahideens was trampling on the bodies of seven agents of the Spanish National Centre of Intelligence shot and murdered in Lutaifiya; these pages and forums were celebrating the first important blow to the Spanish mission in Iraq and were predicting the possible exit of the troops. Come to this point it is necessary to ask if the material or intellectual authors of 3/11 knew this document or some similar other one that, though it was not contributing with operational details, was aiming at a series of decisive elements in two levels: ideological inspiration and strategic orientation. And there are reasons to think in an affirmative response.

First, some of the material authors of 3/11 were dedicating hours every day to the exploration of islamist pages and the navigation on the Net as what with great facility they might have had access to this text. Of not having done it on initiative or own wisdom, the international connections of elements as Jamal Zougam were relevant, so jihadists of third countries might have recommended his reading to the Spanish cell.

Secondly, the hooded one that appears in the video of March 13 appears with the unusual one but probably studied alias of “Abu Dujan Al Afghani”, indeed, one of the most combative warriors in the initial era of expansion of the Islam and the one that is mentioned explicitly in the page 2 of “Iraqi Jihad, Hopes and Thoughts”. The preliminary conclusions of the investigation developed by the Spanish information services aim that, in spite of the fact that the real identity of this military speaker of Al Qaida in Europe is not definitively established, it can be a question of Yousef Beldhaj, arrested in Brussels on February 1, 2005 and extradited to Spain in April, 2005 for his supposed relation with the 3/11 pacification. Of Moroccan nationality, Belhadj was born in Touzine in 1976 and was living in Belgium, where already he had been arrested as supposed member of a cell of the IMCG, before remaining at conditional freedom. In his declaration before the judge Del Olmo, Belhadj denied to be a member of the GICM and his participation in the terrorist attacks, besides assuring that he had never heard the alias “Abu Dujan Al Afghani". He added that, he had never stimulated to anybody to travel to Afghanistan, that *Al Jazeera* and *Al Arabiyya* were the only news channels in Arabic he followed.

He only knew the 3/11 by Mohamed Afallah and Abdelmajid Bouchar, both fled of Leganés. However, “Al Afghani” was an alias unknown for all European information agencies developing investigations about the networks of jihadist terrorism, and the General Police station of Information in Spain did not discard that it was the "war name" of a mujahideen died in Afghanistan, Bosnia or Chechenia who the cell that operated in Spain was trying to produce tribute.

Thirdly, it is necessary to consider that seven suicidal terrorists of Leganés were storing on the hard disk of the computer and several USB memories located in the safe

house numerous documents downloaded of the same electronic page, belonging to Zarqawi's environment, in the one that had been "hung" and debated the analysis advising, justifying and rationalizing a pre-electoral terrorist attack in Spain of which a segment of the society would do jointly responsible, of unusual form and giving satisfaction to the theses and the goals of the terrorists, to a democratically chosen government. On this hard disk reconstructed in London after having remained practically disintegrated as consequence of the suicide, there were located fatwas defending the use of weapons of mass destruction, a guide to make domestic dynamite, advices to camouflage bombs in rucksacks and bag packs, documents that rush forth at the Muslims who defend the living together with Christians and Jews, anonymous texts of jihadist exaltation for the mobilization and recruitment of terrorist potentials, images of the murder of seven agents of the National Centre of Intelligence in Iraq and documents in which the steps are marked to continuing to form, to manage a cell and to make it operative across three essential factors: the religious, security and military formation.

The example of "Iraqi Jihad" and other similar documents that circulate along hundreds of islamist pages symbolizes brightly the Internet potential in different vectors: not only as a tool facilitating the collaboration and the identity of dozens of jihadists that operate in local cells but as backbone in the instigation for the execution of attempts of mass destruction terrorist attacks. Western information services will have to redouble their aptitudes to catch the threat that they represent small cells and neosalafist activists, that have their own means and promise unpredictable behaviours.

## 5.- Revisiting Intelligence in a New Security Environment

The globalization and the technological revolution have concerned in a notable way the development of cyberterrorism. As consequence of the increase of the use of new technologies on the part of the developed societies, the fight against the terrorism and its tactics has met harmed enormously. Hereby, the Internet use has supposed an advantage anonymous and instantaneous communication, which it has favored enormously to this type of groups. Cyberterrorism should be placed high up on the agenda of the intelligence agencies around the world.

Law enforcement, security, and intelligence staff need to continually monitor the activities of cybercriminal gangs because future cyberterrorists may be drawn from them.[24] Indeed, a new ''market'' may emerge whereby cybercriminals are hired to undertake specific illegal acts. Money could, therefore, become the most important motivator for them. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services. Terrorists, at least in theory, could thus follow the hackers' lead, and then, having broken into government and private computer systems, could cripple or at least disable the military, financial, and service sectors of

[24] The primary difference between what law enforcement agencies and intelligence agencies collect is evidence versus information. Law enforcement agencies have long preferred evidence to information, and have used information only to obtain evidence. Intelligence agencies continue to work with information, sometimes substantiated, sometimes not. These differences notwithstanding, the greatest challenges facing law enforcement agencies relate to jurisdictional and legal issues.

advanced economies.[25] In other words, those fighting an ideological war may use free operatives to undertake their missions and, as a consequence, the job of the security and intelligence services monitoring the situation becomes even more difficult than it is at present, and the actions of such terrorists become even less predictable than they now are.[26] Tracking hackers via electronic or other means is not a simple task. Everything from e-mail to source address identity can be masked or spoofed. The protocols that drive the Internet were originally designed to allow for maximum connectivity and sharing among components with the maximum of privacy**.**

Another fundamental aspect that has not been sufficiently understood, is the need "*to connect the dots*" thus to identify the context and to locate something that leaves of the ordinary, in order to establish hypothesis. In the past the challenge was to complete the picture with little available information, but nowadays where the information is much more abundant, the complicated thing will be to be able to be spinning the pieces without hitting with the great number of barriers, of all kinds, to which the information is submitted, today the sources are great more abundant but the limitations and hobbles to these sources is very complicated.[27] The existence and availability vast amounts of information do not necessarily reflect its utility for intelligence collection. Rather, OSINT serves as a tool of corroboration for agents and assets in the field. The old adage, "you can't always believe what you read" has never been more true. Therefore, the need for corroboration has never been greater.

From a counterterrorist point of view, the bigger contribution that the intelligence indeed does is the collection of information about terrorist individual acts, leading terrorists, cells, and the groups that are used in order to be able to disintegrate terrorist organizations. Due to the fact that the terrorists have identities, they meet other persons, move, and communicate present a great quantity of available information that, though fragmentary and incomplete, it can provide tracks on the position, and the terrorist activities. Nevertheless the principal limitation for the intelligence resides in since choosing that persons are suspects of committing terrorist acts or being part members of terrorist cells when these do not have previous precedents. Weighing anchor to the suspicious individuals to the "screens" of the intelligence is nowadays very complicated: *"put up security countermeasures around one potential terrorist target and you have protected that one target from attack, for as long as you keep the security in place. Disrupt a terrorist cell and you have prevented that the cell from attacking any target, at any time, with any method"*[28.]

In any case, the ways and means by which relevant information regarding a terrorist' Internet activities is collected, like every other aspect of intelligence

---

[25] Nick Cullather, "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar", *Intelligence and National Security*, Vol.18, No.4 (Winter 2003), pp.141–154

[26] Peter R. J. Trim, "Public and Private Sector Cooperation in Counteracting Cyberterrorism", *International Journal of Intelligence and Counterintelligence*, 16: 594–608, 2003

[27] John Hollywood, Diane Snyder, Kenneth McKay, John Boon, "Out of the Ordinary Finding Hidden Threats by Analyzing Unusual Behaviour", *RAND Corporation*, http://www.rand.org/, (2004), pp.23

[28] Audrey Kurh Cronin and James M. Ludes, (eds) (2004): *Attacking Terrorism, Elements of a Grand Strategy*, Georgetown University Press, Washington D.C., p.117

collection, need revamping.[29] The technological barriers, combined with HUMINT challenges, pose a great challenge for the IC in the twenty-first century. The thought of cyber intelligence collection conjures images of electronic listening and watching devices in every corner of the world, reporting what they see and hear back to some ‘‘centralized intelligence computer system’’[30] is paramount. According to the United States Defensive Investigative Service (DIS), the Internet is one of the fastest growing areas of intelligence gathering by foreign governments and potential enemies of the U.S. and its allies.[31]

The technical intelligence, it has been used in the fight against the terrorism as a passive way of compilation. While the volume of communications has increased along the world of an exponential form, the agencies of analysis of technical intelligence have met exceeded in the quantity of information that they have to analyze.[32] As result of this trend the director of the National Security Agency (NSA) of the United States, Michael Hayden, had to admit in 1999 that the NSA was gathering many more information that it was capable of trying.[33] What briefly means that the major problem which the technical intelligence faces nowadays does not reside in the compilation, but rather in the selection and the analysis of the information collected.

The States can increase the value of the intelligence it collects is to ensure it gets into the hands of relevant users in a timely manner. Against a networked adversary that exploits the advantages of information technology, an intelligence collection and dissemination system with minimal obstacles is not a mere convenience: it is essential, perhaps even of paramount importance. In spite of best efforts to coordinate intelligence collection on terrorists, this is a massive failure of national cooperation”[34.]

Another important lesson consists of the fact that the services of intelligence must break the traditional existing barriers between human intelligence and technical intelligence.[35] Independently of the preferences of the consumers of intelligence, it is essential that the analysts of intelligence manage to integrate all the sources of intelligence, of an effective way, to be able to attack in a more effective way the terrorism.[36] For it the cooperation will be basic, not only between the agencies, but also between the different services of intelligence of the world.

---

[29] To monitor the activities and intentions of the extremist Islamic groups is really difficult, in great part because of their diverse origins.

[30] Thomas Winston, “Intelligence Challenges in Tracking Terrorist Internet Fund Transfer Activities”, *International Journal of Intelligence and Counterintelligence*, 20: 327–343, 2007

[31] Frederick L. Wettering, “The Internet and the Spy Business”, *International Journal of Intelligence and Counterintelligence*, 14, 2001

[32] Gregory Vistica and Evan Thomas, ‘Hard of Hearing’ Newsweek, 13 Dec 1999. Also see: Frank Tiboni ‘Difficulty Grows for US Intelligence Gathering’ Space News 12 June 2000, p.1

[33] Ackerman, ‘Security Agency transformations From Backer to Participant note 152.

[34] Dan Verton and Bob Brewin, "Companies Warned About Possible Cyber attacks," *CNN*, 13 September, 2001, http://www.cnn.com/2001/TECH/internet/09/13/cyber.terrorism.idg/index.html?related

[35] Matthew M Aid, “All Glory is Fleeting: Signit and the fight against international terrorism”. *Intelligence and National Security* Vol 18. No 4 (Winter 2003), p. 81

[36] Michael Herman.”Counter-Terrorism, Information Technology and Intelligence Change”. *Intelligence &National Security* l 18. No 4 (Winter 2003), p. 42

A major method used in preventing cyberterrorism is the sharing of intelligence information. To share information between the different intelligence services, it will be what marks the difference. Because of the transnational nature of this threat a major cooperation will needed. But as aim Andrew Tan y Kumar Ramakrishna point out "all the information of the world will not be of any help, if it does not come with an imaginative thought and criticize of the first order.[37] It will be very important for the intelligence services to educate policy-makers of the necessity of conquer this tendency effetely. [38] Another of the key points in the fight against cyberterrorism consists in the development of international alliances, between countries involved in this type of fight, since we have raised previously, not all the countries perceive the terrorist threat of the same way.

> *"With the increased porosity of borders between terrorist organizations, the exchange of technical and human expertise between terrorist groups is increasing the threshold of violence. With enhanced terrorist cooperation, governments will be forced to collaborate by establishing common databases, exchange of personnel, joint training, combined operations and sharing of resources and experience"*[39]

## Conclusion

The rhetoric and the facts of the global jihadist movement show that the threat that has relieved the 'old Al Qaida' is that of a studding consisted of different levels always variable in that they come together from ideological leaders to operatives of field, technical personnel who complete tasks of logistics, specialists in funding, segments of the population sympathizers with the jihad or emirs that provide with religious content to the actions. Precisely the power of the jihadist networks derives from the interaction and the dynamics of wealth-producing communication, spontaneous and perfectly lubricated of the different components of a system designed to finish with the freedom of the opened and multicultural societies. The new technologies in general and the Internet especially, have been put to the service of the jihadism for the attainment of its global and totalitarian goals.

In many senses, Al Qaeda has recognized and exploited, together with other terrorist organizations, the tremendous instrumental advantages that the cyberspace can offer as for the significant improvement of the offensive own capacity in terms of intelligence, alertness and recognition. This Al Qaeda's multidimensional approximation allows him to support its structure of work in network with multiple nodes and "infinite" capacity while it is protected to yes same from infiltrations and detections by means of the technological anonymity and the hyper mobility. It allows to several branches of the doctrine salafista extreme to crystallize of joint form and to separate, mutating in different directions, turning into an entity multiplier force and changeable into the

---

[37] Andrew Tan & Kumar Ramakrishna (eds.) 2002, *the New Terrorism*, Eatern Universities Press, pp.18

[38] Dr. Bruce Hoffman "The Use of the Internet by Islamic Extremists", Before the Permanent Select Committee on Intelligence United States House of Representatives, May 4, 2006

[39] Rohan Gunaratna, "Global terrorist outlook for 2005" *UNISCI Discussion papers,* www.ucm.es/info/unisci

cyberspace that provides theological advice and moral inspiration for the violent action, and that the future generations will be able to exploit to will.

Al Qaeda's relation with the new technologies of the information and the cyberspace covers the entire spectrum of the operative defensive and offensive requirements. In terms of communications between networks, Al Qaeda used a great variety of simple and ingenious methods, whereas the top controls showed a deep knowledge of the technologies of alertness and of the technology of the technologies of western intelligence. [40]

The terrorist behaviour in a cyber-environment offers innumerable operative advantages to achieve tactical and strategic aims. With relative anonymity, these organizations use the computer technology as a multiplier force to facilitate, to agree and to spread political propaganda, capitation, funding and to control both the communication and the coordination intra and ínter group; for the withdrawal of information; to assure the seal and the anonymity both in the routine activities and in the tactical operations; and to facilitate operations that turn out to be profitable so much in terms of resources invested like by be constituting in a " multiplier force " regarding his aptitude to throb in the whole world.

The next generation of terrorists will have more powerful in cyberterrorism tactic. Their skill levels and knowledge will be greater. Hackers might be recruited by terrorists. Cyberterrorism could also become more attractive as the real and virtual worlds converge, with a greater number of physical devices attached to the Internet.[41] If

---

[40] Fernando Reinares y Antonio Elorza (2004): *El nuevo terrorismo Islamista*, Temas de hoy, p. 208

[41] Denning, D. "Cyberterrorism", *Testimony before the House Terrorism Committee on Armed Services*, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

the events of September 11th teach us one thing, it is that we should always consider the 'big picture' of the overall terrorist threat, rather than view one aspect in isolation. Although many of the current weaknesses in technological systems can be fixed, ever-evolving technological capabilities will continue to challenge cyber security and information assurance. Additionally, as one system is fixed, other vulnerabilities are often found.

---

## About the Authors:

**Gustavo Diaz and Alfonso Merlos do research at the Computense University, Madrid, Spain.**

## RIEAS Publications:

**RIEAS** welcomes short commentaries from young researchers/analysts for our web site **(about 700 words),** but we are also willing to consider publishing short papers (**about 5000 words**) in the English language as part of our publication policy. The topics that we are interested in are: transatlantic relations, intelligence studies, Mediterranean and Balkan issues, Middle East Affairs, European and NATO security, Greek foreign and defense policy as well as Russian Politics and Turkish domestic politics. Please visit: **www.rieas.gr** for more information (Publication Link)