ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

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

2
2015

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

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

2

ISSUE 2/2015

Milano 2015

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

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

ISSUE I – 2/2015

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri
Associato all'AIE – Associazione Italiana Editori
ISBN: 978-88-6780-958-5

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

Focus: Grandi Eventi

How cyberspace is used by terrorist organization: possible threats to critical infrastructures? The most recent activities of cyber counterterrorism

Mauro Pastorello[1]

Abstract

L'obiettivo di questo articolo è di mettere in luce le numerose criticità e vulnerabilità che possono essere sfruttate da organizzazioni terroristiche, che accompagnano la crescente importanza dell'universo cibernetico nella vita sociale quotidiana di ogni individuo e nei processi di business di ogni azienda. Nella prima parte sarà messa in luce la convergenza dell'universo fisico con l'universo logico e verrà offerta un'analisi del cyberspace, utilizzando la Teoria di Clark e fornendo esempi di alcuni recenti casi di attacchi cibernetici. Il corpo centrale dell'articolo fornirà una breve descrizione della strategia italiana sulla sicurezza cibernetica e introdurrà il concetto di Infrastruttura Critica, evidenziando come, ad oggi, non si possa più parlare di infrastrutture meramente fisiche ma di Infrastrutture Critiche Informatizzate. Nella terza ed ultima parte, l'articolo fornirà un'analisi delle attività terroristiche condotte nel cyberspace, applicando la Teoria di Barry Collin ed il concetto di cyberterrorism, evidenziando in ultimo le strategie difensive ed offensive attuate da Stati Uniti e Gran Bretagna e offrendo spunti di riflessione sulla necessità di applicare in misura maggiore le tecniche di cultural intelligence.

The paper aims to highlight the critical issues and vulnerabilities that can be exploited by terrorist organizations, which grow with increasing importance of cyberspace in all business processes and on the daylife of each of us.
In the first part will be highlighted the convergence of the physical world with the cyber world, where the phenomenon of cyberspace is being analyzed, according to Clark's Theory and providing some examples of recent cases of cyber attacks. The second part is dealing with a brief description of the Italian strategy on cyber security and introduce the concept of Critical Information Infrastructure, which means that we can no longer speak of merely physical infrastructure. In the last part, the paper will provide an analysis of terrorist activities conducted in cyberspace, according to Barry Collin's Theory and introducing the concept of cyberterrorism, highlighting the latest offensive and defensive strategies implemented by the United States and Britain and offering insights reflection on the need to apply techniques of cultural intelligence.

[1] Università Cattolica del Sacro Cuore – Milano
Largo Gemelli 1, 20123, Milano, (IT)
ITSTIME – Department of Sociology

Keywords

Cyberspace, Cyber-war, Cyber-weapons, Cyber-terrorism, Cyber-space, Cyber attack, Cyber security, Terrorism, IS, Critical Infrastructures, Social media.

1. Convergence of physical and logical security related domains

In the last 20 years, the massive introduction of computer systems to all business cycles has changed systems operations in many ways. This passage from the physical world to the physical-logical was initiated by the introduction of automation systems and remote controls. Attempts were made to minimize the risk in a cost-beneficial way, but concurrently physical systems security lost priority to the identification of new threats, arising from the cyber-world [29]. In these terms, we see a reduction in risk but also a shift [29]. Further, the evolution of critical infrastructure systems has brought to light the presence of a new layer to keep in mind: it is inseparably connected to the physical, works with and for it, and it brings new vulnerabilities to systems: it is the cyber layer [1, 25, 27, 29, 34]. We should also keep in mind that an internal information system could be damaged by malware introduced into the system by the synchronization of a manager's smartphone, regardless of the nature of the malware present in the smartphone. As we can see, there are multiple and varied points of access to the system which require a new approach to security, that includes an understanding that a cyber-physical system is not just the connection between the cyber world and physical world but it is the loci of interaction between them which gives rise to a "new system" [1]. This new cyber-physical system integrates the activities of processing and communication to control the structure of the physical world connected to them [1, 34].

1.1 The most exposed domain: networks and cyber space

The term cyberspace refers not only to the space in which millions of data per second travel, but it also extends to the equipment that enables these connections, applications that process data and decode the information and users.

This "space" is not used only by simple users but also by government agencies that manage critical infrastructures; the difficulty in finding an unambiguous definition of cyberspace depends on the nature of that domain, created by man and as such, very complex [42].

Our description of cyberspace is based on the operating model proposed by Clark of four layers [10]:

1. physical entity that supports the logical elements, formed by all tangible entities: "PCs and servers, supercomputers and grids, sensors and transducers, and the Internet and other sorts of networks and communications channels";
2. logical layer includes software, bits and components scattered throughout cyberspace that perform and give orders for actions and reactions. We can consider this level as an intermediate level, which transforms input sent by the operators through the hardware and transforms them into information ready to be transmitted or in actions;
3. information[2] includes all traffic in the network of information of various kinds, from music and video to internet pages and so on;
4. users includes end users, who interact with the network and are responsible for each type of action carried out in cyberspace.

After this brief description of cyberspace, we must also identify the entities who act in this world and who can be a source of threats:

- Nation states: national actors such as government agencies that deal with cybersecurity, both offensive and defensive, play a very important role for their participation and for their investment in this area [37];
- Non-state organized threat groups: usually considered as "cyber-terrorists" [36], exploit the ease of attacking critical infrastructures through cyberlayers;
- Hacktivists: the term refers to an attacker that uses cyberlayers to cause damage to a system as a means of protest, usually politically motivated [37];
- Business-oriented attackers: are interested in cyberattacks to gain business advantages [37];
- Casual attackers: attack randomly websites for no apparent reason.

Another key element of cyberspace is that its inherent nature is the result of human mind, potentially unlimited and, therefore, has characteristics that can vary endlessly, changing the geography of the attack and the type of attack almost indefinitely.

Then, in a more tactical level, cyberspace allows great mobility of cyber weapons[3] and high capacity to fire[4]; to keep in mind, however, that, once used in a specific weapon cybernetics, it can not be used again (the so-called "one-shot") [13] because the potential victims will be aware of the "setting" of such a weapon and, thanks to the reverse engineering techniques, victims may postpone to the sender its cyberweapon.

[2] This layer is usually included in the logical layer, following the definition of the International Telecommunication Union (ITU).

[3] High mobility is intended to be the ability to launch an attack from anywhere useful, without geographical limits and therefore without the need for military bases or military vehicles.

[4] It should be noted that cyber weapons have not necessarily destructive purposes such as "conventional" weapons but can be used to steal or alter information defensive systems.

They were provided different definitions of cyberweapon and, as stated by Rid and McBurney[5], a clear and unambiguous definition of cyber-weapon is not easy to define.

According with Mele, a cyber-weapon is: "*a machine, a device, or any set of computer instructions designed to illegally damage an information or computer system having the character of critical infrastructure, its information, data or programs contained therein or relevant thereto, or to favor the total or partial interruption or alteration of its operation*" [22].

Considering also the cost of the cyber-weapons, we realize that there are significant advantages using cyber weapon than conventional weapons. Infact, a military plane can cost up to $ 120 million, with a cruise missile that is 1 to 2 million dollars; the average price of a cyber weapon ranges from 300 to 50,000 US dollars, ensuring anonymity and "silence" [22].

In a more technical level, each weapon Cybernetics consists of different types of codes, which depend on the type of intrusion and the launch path of the weapon. Specifically, the intrusion can be:

- direct, the intrusion is put in place using a device that transmits to the target system (USB, CDROM, etc..);
- Semi-direct, if sent by the network within the same system or from a domain connected to the target system;
- indirect, sent through cyberspace.

Any type of intrusion to exploit the vulnerabilities of the system; we can divide the vulnerabilities in technical and non-technical.

Technical vulnerabilities are divided into vulnerability of protocols, such as IP Internet protocol, Transmission Control Protocol (TCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and vulnerabilities in the application layer, used for gaining privileged access to remote control systems and to lock systems [18].

Non-technical vulnerabilities are related to people and their processes and for this reason they are difficult to counter and the only method— closely related to an efficient application of the ISO 27001—seems to be providing "education" on how to behave at work (remember that Stuxnet entered the system through a hard disk connected via USB) [18].

From what has been said, we can say that cyberspace involves the presence of new strategic vulnerability for each country, allowing global operations extremely fast, with the possibility of not being able to trace and contain the economic costs.

Due of its nature, as anticipated above, this environment is created by man and his mind and, consequently, it can ensure a constant change of this space

[5] For further informations on this topic see Rid T., McBurney M (2011). Cyber-Weapons, The RUSI Journal, 157:1, 6-13.

and of arms related to it. Operate in this context, however, it requires high level of expertise and strong links with the private sector by the competent authorities.

In this regard it should be noted the importance of partnership between the private sector and the public sector.

1.2 Stuxnet and ARAMCO attacks and Tridium Niagara AX Framework

Stuxnet was a malware used in 2010 to attack Iran's nuclear plant that had the capability of infecting and therefore modifying the behavior of the PLC used to run and control the power plant. The goal of the deployment of such malicious code was to sabotage the nuclear power plant's process for enriching the uranium used for the production of energy by causing a permanent damage, especially at the physical level (possible explosions of the power plant with radioactive consequences) [37].

This worm exploited five different vulnerabilities of the SCADA system designed and manufactured by Siemens[6] and infected 59% of computers in Iran, spreading to Indonesia as well (19% of computers were infected) and India (9% infected) [18]:

- RPC Vulnerability, allowed a remote user rights equal to a local user;
- LNK Vulnerability, allowed remote insertion of malware;
- Spool Server Vulnerability, allowed a malicious print request to take control of a server;
- Win32k.sys Vulnerability, opened vulnerability to executing kernel privileges;
- Siemens SIMATIC Win CC Default Password Vulnerability, use of known default password to access the system.

The attack against ARAMCO (National Oil Company in Saudia Arabia) was conducted by a worm called Shamoon, that gathered files from the system, sent them to the attacker and replaced files with an image (the US flag in flames). Fortunately, the attack hit only the administration system and it took a few weeks to restore all services.

In February 2013, a critical vulnerability in the Industrial Control Systems called "Tridium Niagara AX Framework", used by the military and hospitals, was found. After a complete set of analyses and testing, the system was found to ber vulnerable to a specific zero-day vulnerability that permits complete control of machinery [2].

[6] Siemens is the largest engineering company in Europe and the most profitable unit is the industrial automation division and some of its products are automation equipment and systems and controls for production machinery and machine tools and power automation products.

1.3 Cyber security strategy in Italy

The characteristics of the domain cyber show that there are no defined boundaries that define precisely the beginning and the end of an attack. For this reason, the security strategy has to be shared and implemented between the various Member States [20, 37].

The parties involved can be classified into three basic areas: Network and Information Security (NIS), law enforcement and defense [37]. The basis of the European strategy for cyber security is information sharing and involving private actors in cybersecurity [20, 37] but with different relations and exchanges between the actors involved, at the European level and the national level [37].

At the European level, ENISA (European Network and Information Security Agency) is responsible for implementing and facilitating information security related best practices and procedures; the CERT-EU (Computer Emergency Response Team), is responsible for the security of the IT systems of EU agencies and institutions and the EP3R (European Public-Private Partnership for Resilience) is involved in information sharing [37].

In law enforcement we have the EC3 (European Cyber Crime Centre), which provides analysis and intelligence [37].

Italy was late in implementing these measures and created the first working group that deals with the security of communications and network security as late as 1999. It later became the *Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni*, within the Ministry of Economic Development and Ministry of Defense, the department of Public Service. The Department of Innovation and Technologies and Ministry of Productive Activities aiming to increase the level of knowledge and technological level on security of communications [36], transposed and implemented the Directive 58/2002 on the protection of privacy in the comunication sector in 2003.

This group has collaborated with the political-military unit called CITDC and a group founded in 2003, the Working Group on CIIP [37].

Closely linked to the protection of critical infrastructure is the CNAIPIC, a special unit formed within the Postal and Communications Police Service[7] and the UACI (Unit for Cyber Crime Analysis), specialized in the study of cyber attacks [36].

A key role is played by COPASIR (Comitato parlamentare per la sicurezza della Repubblica), which has advisory jurisdiction on every regulatory scheme concerning the organization and management of entities involved with sensitive information and security affairs; it reports directly to the Prime Minister. And then there are the national intelligence services, AISI (Agenzia Sicurez-

[7] Italian Ministry for the Interior Decree G.U. 30 Aprile 2008 *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*, n. 101, 2008.

za ed Informazioni Interna) and AISE (Agenzia Sicurezza ed Informazioni Esterna), coordinated by DIS (Dipartimento Informazioni e Sicurezza) with the aim of protecting the Republic against all kind of threats, from within the country and without [37].

Despite the evolution of our security apparatus and the work of numerous players, many experts criticize our choices, or rather criticize the lack of implementation of what was stated in various parliamentary hearings.

First of all, criticism is moved because in our country there is no GOV-CERT able to respond to emergencies and that interfaces directly with the government. Then, further criticism is leveled against the political class in general, accused of lacking the necessary skills in information security and apparently totally disinterested about it, ignorant of the fact that today the information warfare is real and waging in several countries because information has a very high value. More criticism is moved about the strategy adopted from Italy, which aims at a "mere defense" and omits the offensive aspect of information security, often proposed and promoted by military organizations involved. Italy is thus seeking a kind of total security, impossible by definition, without considering some substantial differences between this cyber universe and the classic "material" world to which we are accustomed: the goal here is not to steal something tangible and that then leads to easier detection of the attack and of what happened, but the target is to "copy" the information, and when you do not steal anything but simply copy, it is much more difficult to prevent or at least realize what has happened [6].

According to the Norton[8] report, the cost of cybercrime in Italy is around €2.45 billion [37]. Despite these numbers, the resources to invest in the field of information security and protection of CIs, are few and mostly are seen as costs that add nothing to the business and business processes [38]. This situation hinders the creation of a culture of proactive action, essential to increasing the level of resilience and "robustness" of critical infrastructure [38]; quite often management prefers to invest few resources in preventive security, being forced to spend huge resources to restore interrupted service, neglecting that preventive spending to prevent an event X is less than the expenditure to be incurred at a later time to restore service.

1.4 Definition of Critical Infrastructures

Giving a clear definition of CIs is not an easy thing; this difficulty comes from the many definitions provided over the years from various countries, po-

[8] Norton 2012 cybercrime report – italy. Available at: http://now-static.norton. com/now/en/pu/images/Promotions/2012/cybercrimeReport/NCR-Country_Fact_Sheet-Italy.pdf 2012.

tentially affected by their national interests [26] and ithe definition depends on the type of infrastructure under consideration. We can say that the definition of ECIs is the result of a technical political process, which has as its basis the potential impact that can be generated by a fault or a destruction of an CIs [31, 35]. The international CIIP hand book of 2008-2009 defines CIs as: "Whose incorrect functioning infrastructure, even for a limited time period, may negatively affect the economy of individual subjects or groups, involving economic losses and/or even expose them to safety and security risk"[4, 33].

After the UN resolution 58/199 "Creation of a global culture of cybersecurity and the protection of critical information infrastructures" adopted by the UN General Assembly on December 23, 2003, the Plan of Action Combating Terrorism and the 2004 European Program for CIP in 2005, in 2008 we have the Council Directive on European Critical Infrastructure 114 wasenacted for the designation of ECIs.

Law no. 34 of 14/2/2003, which was enacted by the United Nations in December 15, 1997, and ratified the International Convention for the Suppression of Terrorist mediated use of explosives provides a first legislative identification of critical infrastructure that are identified as "any public facility or private entity providing public services, such as supplying water, the removal of waste water, energy, fuel or communications" [34].

Based on the Council document CS/2008/10934, the CIs ensure deliver of basic services and their destruction would have a strong impact on society; if these effects are trans-boundary we can refer to them as ECIs [3]. Directive 114/08 is therefore the first step toward using common criteria for identification of the CIs in all member states and to improve their protection [26]. To give a clear definiton of CIs, is very important in highlighting the difference between physical CIs and cyber CIs. For physical CIs we consider different system and facilities, closely related with the cyber world; cyber CIs are virtual and related with the IT world [31, 34].

According to Article 2 of this Directive, CIs are: "*means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety,security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*".

1.4.1 The Italian case: from "Working group for Protection of Italian Critical Infrastructure (PIC)" to Interministerial Technical Commission of Civil Defense (CITDC), National Anti-Crime Computer Centre for Critical Infrastructure Protection (CNAIPIC) and Legislative Decree 61/2011 of the 11th of April 2011

In 2003, after the release of results[9] from the "Working Group for the protection of Italian Critical Infrastructure", the CITDC (*Commissione Inter Ministeriale Tecnica della Difesa Civile*) was designed to study the vulnerability of and threats to the CIs [4, 31, 34, 75]. After two years, the CNAIPIC (*Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*), was established with the D.L. 155/2005; this center has the aim of collating and comparing all criminal activites against the CIs, working in collaboration with the different operators of CIs during and before a crisis [4, 31, 34, 35].

The Legislative Decree 61/2001 transposing European Council Directive 114/08 into Italian national law describes the procedures for designating ECIs located within the Italian territory and other CIs, located in neighboring member states, but with the interest of Italy for reporting as ECIs.

It also points out the need to expand the components of the NISP (Interministerial Nucleus Situation and Planning), by the exponents of the Ministry of Interior, the Ministry of Defense, Ministry of Economic Development and the Ministry of Transport; a necessary for the proper implementation of the Directive 114/08 is the creation of a *responsible structure* for the CIs, a role temporarily played by the Secretariat of the Interministerial Coordination for Critical Infrastructure [16]. This *responsible structure* must liaise with the other member states about possible detections of ECIs that may affect the various countries and inform the European Commission of the intention of establishing bilateral talks on one or more ECIs and, annually, indicate the number of CIs by sector inside the Italian territory; this structure is also in charge of identifying potential critical infrastructures and reporting them to the NISP. Art. 2 of the Decree, gives us a definition of CIs:

> CI is an infrastructure located in a Member State of the European Union, which is essential for the maintenance of vital societal functions, health, safety and economic well-being of the population, and the disruption or destruction of which would have a significant impact in that country, due to its inability to maintain those functions.

Alongside the CIs we find the CIIs, which guarantee the full operation of the IC in normal conditions especially, in conditions of crisis [22]. Another

[9] Presidenza del Consiglio dei Ministri – Dip. Innovazione e Tecnologie "Protezione delle Infrastrutture Critiche Informatizzate: la realtà italiana", 2004 (estratto).

key point of this Decree is certainly the indication of the obligation, within the scope of the CIs detected, to adopt an OSP within a year and a review of the same every five years, drawn up by the officials responsible for security of the infrastructure, the owner of the infrastructure and the security liaison officer, that is a pre-requisite for the creation of OSP [3, 16].

Annex B of this Decree describes the minimum requirements for drafting and implementing an OSP, providing details on the implementation of risk analysis techniques, on the hierarchy of the security measures to be taken, distinguishing between permanent measures (physical protection systems, communication systems, training and awareness raising of the staff) and measures to apply graduated activations in relation to the level of threats and risks.

2. Terrorism threats in cyberspace

As described above, the cyberspace is the new frontier for all those criminal and terrorist organizations who want to pursue their malicious and evil interests [1, 5, 6, 9, 11, 12, 19, 25, 34, 35, 37, 38, 41, 43].

The cyber domain, and in particular Internet, from a sociological point of view, has no centralized governance but rather, is based on the service users themselves who are spread all over the world and then with totally different cultures [1]; precisely this decentralized governance based on various cultures and certainly influence the technological tool, both in the positive and negative senses [1].

Considering the wide use of cyber technologies to improve the performance of CIs, one might think of a willingness on the part of terrorist organizations, to exploit these cyber vulnerabilities to launch attacks on CIs or even aggravate the effects, without their direct involvement in these attacks [1].

All the intelligence agencies are moving in this direction, which represents the future and requires further study, but until now there has been no clear evidence or suspicion regarding cyber attacks *stricto sensu* against critical infrastructure by terrorist organizations [24, 38]; considering that cyberterrorism, according to Barry Collin, is "*the convergence of physical and virtual worlds where cyber weapons produce physical consequences*".

The Federal Bureau of Investigation (FBI) defines such activity as:

> a criminal act perpetrated with the use of computer and telecommunications capabilities, resulting in violence, destruction and / or interruption of services to create fear causing confusion and uncertainty within a given population, with the aim of influencing a government or of a population to conform to a particular political agenda, social or ideological.

Paradoxically, attacks and threats regarding this domain come from so-called "rogue states" such as North Korea and Iran. Iran is of considerable interest in a recent US report that points out an increase in attacks coming from Iran and indicates its technological evolution in the cyber world [26].

We could say that, at present, the cyber world does not seem to be used by any terrorist organizations to conduct any real attacks [38]. However, the cyberworld, according to Lombardi [1], offers different "operational" levels:

- we use cyber tools to attack the real world;
- we fight in the cyberworld with consequences that occur in the real world;
- the cyberworld is used to educate and inform.

The last point is of particular interest for the continuation of our analysis on the actual use of cyberspace by terrorist organizations; the possibility of training, through real training courses or manuals for creating IED (Improvised Explosive Device) and "informing" about the success of its suicide attacks or to spread the jihadi creed, it makes this dimension very attractive for the new terrorism 2.0, now accustomed to using the network and social networks to spread their beliefs.

2.1 Social media and cyber terrorism

Social media are therefore a useful tool for the terrorists of the new millennium.

Summarizing the many definitions of social networks, we can define them as instruments of mass communication that can be used only in cyberspace and that base their operations on the internet network, using various software [1]. Through them, users communicate, develop their own "virtual identity" and share various forms of content. The possibility of sharing ideas and content in real time anywhere in the world is the so-called "viral effect"of social media. This is the social media characteristic especially exploited by terrorists [1].

What makes these tools higly attractive is the ease of use and the absence of costs related to a wide range of features that allow users to "customize" their virtual space and their network [1].

Obviously, social media tools themselves are not threats but perhaps that is only because you do not know the real intentions of the end users. In fact, cyberterrorism are all those activities on social networks that aim to destabilize the civil society of different countries [1].

By definition, cyberterrorism is an offensive activity in cyberspace through the use of the network for propaganda purposes, affiliation, denigration, etc... [1,15].

Terrorist organizations that make significant use of social media are jihadist-Islamic organizations such as Al Qaeda and ISIS, engaged in massive operations of "cyberterrorism" aimed at destabilizing the civil society, through propaganda with video of executions, attacks and threats against Western

countries [1]; in this regard, it was only a very short time ago that photos were published on social media, immortalizing the landmarks of our country with the small paper containing claims by ISIS. Why? Spread terror through information (or misinformation, depending on your point of view) but without any concrete action, as mentioned by our Intelligence Services and reported by Lombardi[10] and other scholars [31].

According to Denning [17] and Lachow [28], cyber-terrorism would be more a myth than a real threat, as it seems to have not caused so far real dangers (equated to terrorism in the physical world). Even Tordjman, of the Institute for Counter-Terrorism in Israel of Herziliya, shared this opinion. The point is to define how the cyber-space is used by the terrorist organizations.

All experts agree that the main uses are: spread of propaganda, attracting new members and funds [1, 44].

Not everyone is for taking down IS propaganda, however. Some experts argue that the bloody videos cause the group more harm than good. Terrorism expert and noted it has actually led many countries to rise up against IS.

Experts wagered that if you showed your friend one of the IS execution videos, they'd probably be disgusted; so, the very typical response to this propaganda is not to be attracted to the Islamic State, but to be repulsed.

There's no doubt that IS is attracting new recruits through social media, yet they're mainly recruiting people who were already radicalized. The other side of the picture is that ISIS propaganda is causing nations to rise against it.

United States got involved in fighting IS, after the group released a video where they killed journalist James Foley. Jordanians started fighting IS after a video where they burned alive one of their pilots, Lt. Muath al-Kaseasbeh. Egypt started fighting IS, after it released a video of them beheading 21 Egyptian Coptic Christian migrant workers.

We need to consider that ISIS is the most active terror group on Facebook, Twitter, YouTube and Instagram account and their intention to create a cyber caliphate[11].

Another operation implemented by ISIS has been the creation of a smartphone application, called "The Dawn of Glad Tidings," which offer all the

[10] Available at: http://www.itstime.it/w/comicita-resiliente-is-minaccia-roma-e-milano-by-marco-lombardi/; For further informations on this topic: http://www.itstime.it/w/nuovo-video-is-contro-i-cristiani-until-there-came-to-them-clear-evidence-by-marco-lombardi/; see also http://www.itstime.it/w/is-lo-stato-islamico-pubblica-il-suo-magazine-dabiq-8-by-marco-lombardi/; http://www.itstime.it/w/da-foley-a-muad-al-kasaesbeh-cosa-cambia-nella-comunicazione-di-is-by-marco-lombardi/; http://www.itstime.it/w/lo-stato-islamico-una-realta-che-ti-vorrebbe-comunicare-il-documento-di-is-in-italiano-by-marco-lombardi/;

[11] http://thehackernews.com/2015/02/anonymous-isis-cyber-attack.html

news about the activities of the Islamic State and allow the use of twitter account users who downloaded this application, to spread their messages [44]; the other principal purpose is therefore to increase as much as possible the diffusion of their messages, and, above all, in the opinion of the author, spread the image of an organization stronger than it is in reality.

Recently, IS has also announced the formation of a hacking division, led by British Junaid Hussein, also known as Abu Hussain Al Britani (killed in late August 2015 in Syria by US drone), which will handle their cyberwar; however, there were no significant attacks to critical infrastructures of NATO countries, but there have been numerous attacks against the Twitter profile of the US military command centers and their databases.

The last attack hit the Air Force; 156 soldiers of the US Air Force have seen their personal and sensitive information in the hands of IS.

In order to face this new threat related to IS, countries like the UK, have set up highly specialized departments, such as the 77th Cyber Brigades, created in April in England; this new department will be tasked to conduct psychological operations and to monitor the social networks, as well as to direct the behavior of some populations.

The 77th Brigade officially consists of:

- Headquarters Element
- The Media Operations Group [MOG] (MOG sends out teams to HQ or battlegroup teams to report the new or teach personnel how to deal with the media);
- The Security Capacity Building Team [SCBT];
- 15 Psychological Operations Group [15 POG] (focused on Psychological Warfare);
- Military Stabilisation Support Group [MSSG] (*"unique defence organisation that provides the UK with an array of skills and knowledge, that can be used to provide military support to the civilian efforts to stabilise countries around the world that are either emerging from conflict or are at risk of sliding into chaos"*)[12].

The British Government has also launched other programs, such as the Research, Information and Communications Unit (RICU), a trilateral unit owned jointly by the Foreign & Commonwealth Office (FCO), Home Office and the Department for Communities and Local Government (DCLG) based at the Office for Security and Counter-terrorism (OSCT) at the Home Office, *"with the aims to coordinate government-wide strategic and crisis communications activities – both domestic and foreign – to counter the appeal of*

[12] https://www.gov.uk/government/groups/military-stabilisation-support-group.

violent extremism and to strengthen inter-community relations at the grass-roots level"[13]. It is composed by three units:

- Monitoring and Coordination Team: responsible for providing analysis and insights of media and audience reactions;
- Domestic and International Campaigns Team: charged with the implementation of strategic
- communications activities targeted at vulnerable communities;
- Insights and Analysis Team: conducts research and analysis of target audiences both on and offline.

The United States, in September 2014, have created a cyber brigade, recalling all the soldiers who have knowledge in the field of information security and information technology and, as the British Government, has launched several different program strategic communications against terrorist extremism, such as the Center for Strategic Counterterrorism Communications (CSCC) and the Digital Outreach Team (DOT), that performs direct engagement through the Internet and social media to counter extremist propaganda and misinformation.

On this front, there is also the presence of "private" hacking company, as the GhostSec, born after the attacks on the headquarters of Charlie Hebdo.

The GhostSec seems to have managed to thwart possible attacks in Tunisia and the United States, getting information by hacking some jihadist forums and subsequently passing these reports to their respective governments.

GhostSec is divided into four divisions. Their operations team oversees the entire unit and gives directions, their technology team maintains tools to fight ISIS, their intelligence team infiltrates ISIS networks and gathers information (including on the Deep Web) while their research team collects data on ISIS news and propaganda.

The main feature of this type of organization is the complete freedom of action, regardless of constraints violations of privacy or similar legal restrictions, and these methods have certainly helped their work, which currently counts:

- 57,000 social media accounts related to IS closed;
- 100 websites reconnected to IS closed;
- 791 Twitter account linked to the IS discovered;
- 11 Facebook pages closed;
- 52 e-mail address directly connected to parties related to IS, in addition to the discovery that many sites are using IS servers on US territory.

All these activities are performed in a web little known, the so-called "deep web", known by many hackers and activists, used to create encrypted forum.

[13] Briggs R., Feve S. (2013). *Review of Programs to Counter Narratives of Violent Extremism. WHAT WORKS AND WHAT ARE THE IMPLICATIONS FOR GOVERNMENT?* Institute for Strategic Dialogue, UK.

It is then in this "deep web" that we must move to prevent further attacks and to monitor activities on social networks.

Other activity detected by the intelligence services is growing contact between cyber terrorists and organizations of cybercrime with the purpose of creating alliances or perhaps to sell the services offered by cybercriminals (phishing, etc.) to increase the financial resources of cyberterrorists [1].

This scenario has not gone unnoticed to intelligence analysts and all our security services and current Prefect Giovanni De Gennaro, when he was the General Director of the DIS (Dipartimento Informazioni e Sicurezza), stated:

> quanto più alto è il grado di informatizzazione di una collettività nazionale, quanto più diffuso è l'uso di apparecchiature telematiche da parte dei suoi cittadini, delle sue aziende e delle sue pubbliche amministrazioni, quanto più frequente è il ricorso al web per acquisire, trasferire o scambiare informazioni, tanto maggiore è la vulnerabilità di quel sistema-paese[14].

Analyzing the situation and becoming aware of the new scenario that is presented to us, with all its branches, it now seems essential and urgent to study and apply a Social Media Strategy at the national level, with proactive investigations, already active on the web and on social networks, aimed at preventing attacks and at identifying possible terrorist cells, thus allowing the implementation of a strategy that is both defensive and offensive. At the same time, an information campaign for the whole public administration should be implemented, in order to sensitize all to a careful use of social media, and so reduce the vulnerability of the system.

The use of Cultural Intelligence techniques conducted on the web, has a considerable importance to analyse the phenomenon and to follow the "propagator" of IS. An emblematic case was registered in December 2014, when an IS propagator (Shami Witness, Indian) was arrested and considered a key piece of the Islamic State propaganda by the intelligence agency. Subsequently, however, it was discovered that its activity was limited to disseminate materials and information on IS, along with the passion for American films of superheroes, nothing more.

Another case of non-use of cultural intelligence techniques is the use of the signal "stop" (raised arm and open hand with palm facing forward) used by all military checkpoints in Iraq; in fact, in the local culture this sign is not associated with "stop" or an "alt" but rather is a sign of welcome and hospitality.

[14] "The higher the degree of computerization of a national community, the more widespread is the use of telecommunication equipment by its citizens, its businesses and its public administration, the most common is the use of the web to acquire, transfer or exchange information, the greater is the vulnerability of that system – country".

From this kind of events, we note that the activities of study and investigation of intelligence can not and should not be limited to mere activities registered online or in the field but we need to analyze the environmental and cultural contest to better understand the situation in which we operate. In a word, activity of Cultural Intelligence, understood as intelligence activities conducted on the basis of information of a political and social, economic and demographic that help to understand the history and the behavior of a population[15] but, in this case, conducted in the cyberspace, that is by definition an intangible space, where different people with different cultures meet and interact, creating a new culture based on many cultural interaction and to difficult interpretation: the culture of cyberspace.

References

[1] Autori vari, Cur. di Osservatorio per la Sicurezza Nazionale. (2013) Cyberworld, *Capire proteggersi e prevenire gli attacchi in rete*. Hoepli, Milan.

[2] Bologna S., Lazari A., Mele S. (2014). *Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats*, NATO Workshop.

[3] Bouchon S., DI Mauro C., Loggtmeijer C., Nordvik J., Pride R., Shupp B., Thornton M. (2008). *Non-Binding Guidelines*, JRC, Italy.

[4] Brunner E.M., Suter M. (2009). *International CIIP HANDBOOK 2008/2009*, ETH, Zurich.

[5] Caleta S., Radosevic S. (2014). *Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection*, IOS Press.

[6] Chiesa R. (2014). *Quelle verità mai dette sulla cyber security*, available at: http://www.agendadigitale.eu/infrastrutture/757_quelle-verita-mai-dette-sulla-cyber-security.htm

[7] Choucri N. (2012) *Cyberpolitcs* in *International Relation*s. MIT Press, Chicago.

[8] Choucri N., Goldsmith D. (2012). *Lost in cyberspace: Harnessing the Internet, international relations, and global security* in Bulletin of the atomic scientists, vol.68, no.2, 70-77.

[9] CIS Sapienza [Cyber Intelligence and Information Security] (2014). 2014 Cyber Security Report, Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana, Italy.

[10] Clark D. (2010) *Characterizing Cyberspace: past, present and future*, MIT Review, Chicago. Available at: http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf

[11] Clusit (2012). Rapporto Clusit 2012 sulla sicurezza ICT in Italia, Italy.

[15] Coles (2005). Cited in Zanasi (2014) [44].

[12] – –. (2014). Rapporto Clusit 2014 sulla sicurezza ICT in Italia, Italy.

[13] Colella A. (2014). *Armi cibernetiche e strategie di difesa: Importanza della Societal Digital Security Culture*, in Cyber Warfare 2014. Armi cibernetiche, sicurezza nazionale e difesa del business, cur. Gori U., Lisi S. Franco Angeli Editore, Milano.

[14] Consiglio dell'Unione Europea 12109/13 (2013). *Strategia dell'Unione europea per la cybersicurezza: un ciberspazio aperto e sicuro*, UE.

[15] COPASIR [Comitato Parlamentare per la Sicurezza della Repubblica] (2010). *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, Italy.

[16] Decreto Legislativo del 11 Aprile 2011, 61. *Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione*.

[17] Denning D.E. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy*, in Networks and netwars: the Future of Terror, Arquilla J. e Ronfeldt D. (2001). Crime and Militancy, RAND Publications, Santa Monica. Available at: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

[18] Edwards M. (2014). Critical infrastructure protection, in NATO science for peace and security. E., Human and Societal dynamics, vol. 116. IOS Press, Amsterdam.

[19] Enisa [European Network and Information Security Agency] (2012). *National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace*, UE.

[20] – –. (2010). Cyber Europe 2010 – Evaluation Report, UE.

[21] European Commission COM 702 (2004). *La protezione delle infrastrutture critiche nella lotta contro il terrorismo*, UE.

[22] Gori U. (2014). *L'inarrestabile sviluppo delle armi cibernetiche*, in Cyber Warfare 2014. Armi cibernetiche, sicurezza nazionale e difesa del business, cur. Gori U., Lisi S. Franco Angeli Editore, Milano.

[23] Geers K. (2011). *Strategic Cyber Security*, CCD COE Publications, Tallinn.

[24] Green J. (2002). *The Myth of Cyberterrorism*. Available at: http://www.washingtonmonthly.com/features/2001/0211.green.html

[25] ISCOM [Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione], (2004). *La Sicurezza delle reti nelle Infrastrutture Critiche*, Italy.

[26] Kagan F.W., Stiansen T. (2015). *The growing Cyberthreat from Iran. The Initial report of project Pistachio Harvest*, American Enterprise Institute Critical Threats Project and Norse Corporation, USA.

[27] Kekovic Z., Kesetovic Z. (2013). *National Critical Infrastructure Protection. Regional Perspective*. ICS, Belgrade.

[28] Lachow I. (2009). *Cyber Terrorism: Menace or Mith?*, in *Cyberpower and National Security*, Kramer F.D., et.al (2009). Potomac Books, Inc, Washington D.C.

[29] Lazari A. (2014). *European Critical Infrastructure Protection*, Springer.

[30] Libicki M.C. (2013). *Brandishing Cyberattack Capabilities*. Rand for National Defense Research Institute.

[31] Maggioni M., Magri P. (2015). Twitter and Jihad: the communication strategy of ISIS, ISPI. Italy.

[32] Manzoni Zapparoli A. (2010). Sicurezza 2.0: è tempo di convergenza tra sicurezza fisica e logica, available at: http://www.secsolution.com/articolo.asp?id=24

[33] Mele S. (2014). La cooperazione tra pubblico e privato nella cybersecurity. Punti di forza e criticità per la sicurezza nazionale. Available at: http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/la-cooperazione-pubblico-privato-nella-cyber-security.html

[34] Panzieri S., Setola R. (2004). *Vulnerabilità indotte dal Cyberspace sui sistemi di monitoraggio e controllo*, Convegno Scientifico Nazionale ENERSIS, Italy.

[35] Presidenza del Consiglio dei Ministri (2004). *Protezione delle infrastrutture critiche informatizzate, la realtà italiana. Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate*, Italy.

[36] *Public Law 107-56, 26 October 2001* available at: https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

[37] Report Tenace (2014). *Critical Infrastructure Protection: Threats, Attacks and Countermeasures*. Italy.

[38] Setola R. (2011). *La strategia globale di protezione delle infrastrutture e risorse critiche contro gli attacchi terroristici*. CeMISS, Italy.

[39] Tabansky L. (2013). *Critical Infrastructure Protection Policy: the Israeli Experience in The Journal of Information Warfare*, vol. 13, Issue no. 3.

[40] – –. (2012). *International Cooperation in Critical Infrastructure Protection Against Cyber Threats*, Atlantic Voices vol. 2, no. 9, 6-9.

[41] – –. (2011). *Critical Infrastructure Protection against Cyber threats*, in Military and Strategic Affairs, vol 3, no.2, 61-78.

[42] – –. (2011). *Basic Concepts in Cyber Warfare in Military and Strategic Affairs*, vol 3, no.1, 75-92.

[43] Cur. di Théron P. (2013). *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, IGI Global.

[44] Zanasi A. (2014). *Cultural e Cyber Intelligence: la Nuova alleanza?*, in *Cyber Warfare 2014. Armi cibernetiche, sicurezza nazionale e difesa del business*, cur. Gori U., Lisi S. Franco Angeli Editore, Milano.

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

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

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

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

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-6780-958-5

Euro 20,00