IMPACT OF SOCIAL MEDIA
ON NATIONAL SECURITY

By: Capt. CC Alfonso MONTAGNESE

Closed: February 2012
INDEX

IMPACT OF SOCIAL MEDIA ON NATIONAL SECURITY

ABSTRACT pag. 1

- Scope – Sources pag. 2

- Social Media: Definition & Functioning Dynamics pag. 2

- Social Media Users pag. 7

- Social Media and Information Warfare pag. 8

- Social Media Diffusion pag. 13

- Threats to National Security due to the use of Social Media pag. 16
  - Terrorism pag. 16
  - Criminality pag. 18
  - War pag. 19
  - Protest Movements and Revolution pag. 19
  - Incautious use by civil servants pag. 20

- Opportunities for the protection of National Security and Strategic Interests of the State pag. 21
  - Warning and trend prevision tool pag. 21
  - Institutional communication tool pag. 25
  - Influence, Propaganda and Deception tool pag. 26

Conclusions pag. 29

Notes on Ce.Mi.S.S and Author pag. 33
ABSTRACT

Social Media are connection and mass communication tools, characterized by a global diffusion and an ever-growing level of use, considering their handiness and flexibility, as well as their extreme cheapness. Using these media can cause several negative effects for national security and unfavourable consequences for a state’s strategic interests. Nevertheless, their use can also lead to remarkable opportunities for a country in order to reach its strategic relevant goals, foresee how threats will work in the future and figure out how to counter their effects.

Since Social Media are extremely quickly evolving and are facing a many-sided interaction with geo-economic and socio-cultural elements, it is important to constantly monitor how they develop, analyse how they work, and measure their potentialities. This process aims at making the states not be caught by surprise in case of a potential offensive use of Social Media by adversaries and at changing such innovative tools into resources of primary importance, to be ready for all the bodies involved in the protection of the national security. Therefore, a national “Social Media Strategy” added to an in-depth and up-to-date knowledge about Social Media can help developing high capabilities of prevision and analysis (e.g. monitoring conversations and content shared on Social Media), arranging effective methods to counter adversaries’ propaganda and interferences (e.g. releasing certain information and/or multimedia content via Social Media in order to hinder propaganda or disinformation campaigns), improving governmental agencies and institutions’ performances (e.g. more inter-institutional information-sharing and quicker decision-making thanks to the use of customised Social Media), strengthening a state’s geopolitical position and its international credibility (e.g. carrying out influence operations with the integrated use of Social Media and other media).
IMPACT OF SOCIAL MEDIA ON NATIONAL SECURITY

Capt. CC Alfonso Montagnese

“We shape our tools, and thereafter our tools shape us.”

Herbert Marshall McLuhan

SCOPE

The aim of the present paper is to provide an up-to-date picture of the situation concerning the use of Social Media by organized groups (states, movements, terrorist groups, criminal organizations, public institutions, companies, etc.) and to measure its present and future impact on national security, outlining the principal risk scenarios for a state’s interests. In order to reach the pre-arranged goal, it is necessary to sort out what the threats to national security deriving from the use of Social Media are. In addition to this, it is important to know how and how much the use of these tools might help prevent, limit or remove such threats, and help protect a state’s strategic interests.

SOURCES

In order to acquire all the elements necessary to develop the present paper, several documents have been examined. All of them are open source documents by institutional organizations, think tanks, research institutes, scholars, academics, and press bodies of proven and renowned newsworthiness. Since the Italian sources about the subject are really meagre to date, most of the bibliographic sources selected and used for this study are from the United States.

SOCIAL MEDIA: DEFINITION AND FUNCTIONING DYNAMICS

Firstly, a full definition of Social Media needs to be provided, before being able to understand how they can be used and how they function, and, consequently, measure their present and long-term impact of national security. Although a long time passed since they first appeared on the internet (about 10 years), such media are extremely quickly evolving, therefore, at the present time a rather heated debate about the subject is on among scholars, both in Italy and abroad, although there does not seem to be a commonly shared definition of Social Media yet. This is the reason why it is necessary to have a brief look at some of the latest significant definitions within the institutional, academic and press world, in order to outline and...
describe the distinctive characteristics of such media. Bruce Lindsay, analyst of the US Congressional Research Service (CRS) \(^2\), provided the following definition: “The term Social Media refers to Internet based applications that enable people to communicate and share resources and information. Some examples of Social Media include blogs, discussion forums, chat rooms, wikis, YouTube channels, LinkedIn, Facebook, and Twitter. Social Media can be accessed by computer, smart and cellular phones, and mobile phone text messaging (SMS)”\(^3\).

The Chief Information Officer Council (CIO Council) \(^4\), a US governmental body which supports the President and the federal agencies in the field of Information Security, recalling a study carried out by the national Defense University (NDU), defined Social Media as “applications that inherently connect people and information in spontaneous, interactive ways” \(^5\).

Helle Dale, expert on international politics and member of the Heritage Foundation \(^6\), used the expression “social networking” to refer to a phenomenon which “includes sites such as Facebook, Twitter, MySpace and other interactive media tools to communicate with ever-expanding networks of family, friends and colleagues”\(^7\).

Bobbi Lewis, professor at Oklahoma State University and expert on strategic communication, defined Social Media as “Internet tools such as blogs, YouTube, Flickr, MySpace and Facebook [which] allow the average person to create content that can be shared with a worldwide audience. The interactive nature of these tools has transformed media messages from one-way communication to facilitating a dialogue”\(^8\).

She maintains that the expression Social Media “is the new «buzz word» in the communications and marketing industry. It is the current label for digital technologies that allow people to connect, interact, produce and share content. These technologies have donned many labels including: social networking, peer media, new media, digital media, NextGen PR and Web 2.0”\(^9\).

The Financial Services Roundtable \(^10\), an authoritative organization representing US financial, banking and insurance institutions, claimed “Social Media is a term used to define the relatively recent phenomenon of mass personal publishing most often intended for public consumption and typically conducted in an interactive and conversational style. [...] the term Social Media shall include any form of online interaction

\(^2\) http://www.crs.gov
\(^4\) http://www.cio.gov.
\(^5\) CHIEF INFORMATION OFFICERS COUNCIL (CIO), (2009), Guidelines for Secure Use of Social Media by Federal Departments and Agencies, Washington, DC.
\(^6\) http://www.heritage.org. The Foundation is one of the most prestigious and authoritative US think-tank. It was founded in 1973 and its mission is to promote and formulate political strategies based on the principles of free enterprise, limited government, individual freedom and national defence.
\(^7\) DALE H. C., (2009), Public Diplomacy 2.0: Where the U.S. Government Meets “New Media”, Backgrounder n. 2346 – published by The Heritage Foundation, Washington, DC.
\(^8\) LEWIS B. K., (2010), Social Media and Strategic Communication: Attitudes and Perceptions Among College Students, Public Relations Journal vol. 4, New York.
\(^9\) LEWIS B. K., (2010), Social Media and...cit.
\(^10\) http://www.fsround.org.
that allows for the highly scalable publication of user-generated content of any kind (text, audio, video, images) that is meant for general public consumption and uses interactive dialogue with others.11

Andreas Kaplan and Michael Haenlein, professors at Ecole Supérieure de Commerce de Paris – European School of Management (ESCP – Europe), provided the following definition of Social Media: “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content”12.

The Defense Advanced Research Projects Agency (DARPA), the US Department of Defense agency dealing with research and development in the field of new technologies applied to military purposes13, indicates that the expression “Social Media” refers to “blogs, social networking sites, and media sharing technology (such as YouTube)14.”

The US Air Force described Social Media as “tools and platforms people use to publish, converse and share content online. The tools include blogs, wikis, podcasts and sites to share photos and bookmarks”15.

Differently, “social networking”, is referred to as “online places where users can create a profile, and then socialize with others using a range of media tools including blogs, video, images, tags, lists of friends, forums and messages”16.

The Department of Military Sociology of Ce.Mi.S.S. (Military Centre for Strategic Studies17) defined Social Media as new generation mass tools which not only enable people to obtain information but also to share, comment or, more generally, interact with it 18.

According to the Italian section of the Interactive Advertising Bureau, an advertising business organization which represents companies engaged in the sale of interactive advertising and marketing19, Social Media are sites characterized by inherent features which facilitate sharing information among users of a defined network20.

11 BITS – Financial Services Roundtable, (2011), Social Media Risks and Mitigation, Washington, DC. The BITS is the Technology Policy Division of the Financial Services Roundtable. It addresses issues at the intersection of financial services, technology and public policy, where industrial cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services; http://www.bits.org.
12 KAPLAN A., HAENLEIN M., (2010), Users of the World, Unite! The Challenges and Opportunities of Social Media, Business Horizons vol. 53, Paris. Before developing their definition of Social Media, the authors introduce and describe the concepts of Web 2.0 (“a term that was first used in 2004 to describe a new way in which software developers and end-users started to utilize the World Wide Web”) and User Generated Content (“the term, which achieved broad popularity in 2005, is usually applied to describe the various forms of media content that are publicly available and created by end-users”).
14 DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), Social Media in Strategic Communication, DARPA-BAA-11-64, Arlington County, VA.
15 US AIR FORCE – Public Affairs Agency – Emerging Technology Division, (2009), Social Media and the Air Force, Arlington County, VA.
16 US AIR FORCE – Public Affairs Agency – Emerging Technology Division, (2009), Social Media and...cit.
20 INTERACTIVE ADVERTISING BUREAU - ITALIA, (2008), Definizione delle metriche per i Social Media, Milano.
Giuseppe Riva, professor of General Psychology at the Università Cattolica of Milan, claimed that Social Media are platforms based on new media which let the user both handle his/her own social network (organization, extent, exploration and comparison), and his/her own social identity (description and definition)\(^{21}\). Consistently with other authors\(^ {22} \), Riva goes beyond his own definition, maintaining that the use of Social Media aims at building knowledge together\(^ {23} \). Moreover, he claims that Social Media are not just “tools”, but represent proper social contexts where networked flow processes take constantly place\(^ {24} \).

The consultancy firm Burston-Marsteller\(^ {25} \), describes Social Media as “*a shift in how people discover, read and share news, information and content, including writing, video, audio, and photos*”\(^ {26} \).

Considering the characteristic elements pointed out in the above-mentioned definitions, an attempt to give a general and complete definition of Social media is due. In short, Social Media can be said to be connection and communication tools, exclusively available in the cyber-space\(^ {27} \), whose operative functioning is based on technologic hardware (Internet and mobile networks, pc, etc.) and software (Facebook, Twitter, MySpace, LinkedIn, YouTube, etc.) platforms. Thanks to these tools all users can:

- communicate with each other;
- share different kinds of content (videos, photos, images, texts, sounds, etc.);
- build/strengthen networks in one or more fields (professional, familiar, social, cultural, religious, political, etc.);
- develop and define their social identity.

Social Media are found to have an extremely high level of interaction among the users, differently from traditional media, which are characterized by a one-way communication flow. Indeed, Social Media users can be at the same time both senders and recipients of information, and creators, and users of content\(^ {28} \).


\(^{22}\) Luca Milani is a researcher in Education and Development Psychology at Università Cattolica, Milan; Andrea Gaggioli is professor of Cognitive Empowerment and Psychology and New Communication Technologies at Università Cattolica, Milan.


\(^{24}\) RIVA G., MILANI L., GAGGIOLI A., (2010), *Networked...*cit. The Networked Flow is a process that allows users to get particularly high results in the fields of innovation and creativity. Such results would have never been reached by individuals, and their value is considerably higher than the mere sum of the single contributions of the users. The Networked Flow is based on the theory that creation and innovation processes frequently come from the net, even before a single user makes his/her own contribution, and evolve in the net.


\(^{26}\) BURSON-MARSTELLER, (2010), *Social Media Check-up: a Burson-Marsteller Evidence-Based Tool*, New York.

\(^{27}\) US DEPARTMENT OF DEFENSE, (2011), *Department of Defense Strategy for Operating in Cyberspace*, Arlington County, VA. “*Cyberspace has become an incubator for new forms of [...] new social networks*”.

In 2008, in the specific memorandum entitled *The Definition of Cyberspace*, the US Under-Secretary of Defense maintained that cyberspace is “*a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers*”.

LIBICKI M. C., (2009), *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, CA. “*Cyberspace is a virtual medium, one far less tangible than ground, water, air, or even space and the RF spectrum*”.

\(^{28}\) RIVA G., MILANI L., GAGGIOLI A., (2010), *Networked Flow...*cit. The authors affirm that we are moving from the typical asymmetry of traditional mass media communication (radio, TV) based on the one-to-many model where the
Comparing traditional and Social Media, the last ones appear to have reached the participation element: "the communication tends to be more dynamic, personal and interactive." and the users do not simply receive information and content passively, instead, they have the opportunity to take part into the process of information and content creation and distribution.

Another element which characterizes Social Media is their being “viral”, referred to as the power to make all multimedia information and content immediately available all over the world, removing time and space issues, and to circulate them to a huge catchment area whose extent increases exponentially as biological viruses do.

Moreover, user-friendliness and cheapness distinguish Social Media from other media (especially for the so-called “digital natives”) In fact almost all Social Media:

- have intuitive features and simple graphics, which allows immediate use; in-depth computing experience is not required;
- are virtually free: the price of the hardware terminal (pc, smart phone, etc.) and the service provider costs are the only costs to incur. Besides, a periodic fee is requested by some Social Media in order to provide supplementary services, in addition to basic ones (e.g. LinkedIn).

Three elements characterize the use of Social Media:

- a virtual space where the user can activate and set his/her own profile (account); this space basically dovetails with the application that offers the “social networking” service (Facebook, Twitter, LinkedIn, YouTube, etc.);
- the opportunity to make such profile public (in part or totally), linking it with other profiles and, then, placing it in a network; in doing so, the user can communicate with the other profiles linked to his/her network. Besides making his/her own profile public, the user can decide if and to what extent he wants to make his network public, too;
- the opportunity to handle one’s own network, developing and updating it constantly.

Although Social Media are extremely simple to use, they are true to traditional social networks and boost their articulated dynamics thanks to the quick sharing of content, the volume of the information exchanged, the multidirectional communication flows and the ability to aggregate even people who are far away from one another geographically. Traditional social networks represent complex systems, and their inner dynamics cannot be easily told in advance: “social networking is more than simply the sum of the

“many” have few possibilities to influence the messages, to the many-to-many model, with more opportunities and symmetries, typical of the communication via computer.

29 BITS – Financial Services Roundtable, (2011), Social...cit.
30 INTERACTIVE ADVERTISING BUREAU - ITALIA, (2008), Definizione delle...cit.
31 LOMBARDI F., (2011), I social...cit.
34 according to Giuseppe Riva, the difference between Social Media and traditional media is the capacity to make someone’s own social networks visible and usable. Therefore, thanks to Social Media it is possible to figure out personal, relational and professional opportunities, not clearly visible otherwise.
attitudes or activities of its members. The system’s complexity creates outcomes that are different than the sum of the group\textsuperscript{35}.

Consequently, Social Media follow the complexity of traditional social networking, too, and prove to be an heterogeneous reality as well, whose dynamics are hard to anticipate, since they are influenced by several factors.

Lastly, Social Media are connection and communication tools, and just because of their being “tools”, they can represent either a threat or an opportunity for national security according to the way they are used, by who are used and for what reason. Therefore, it is not Social Media to represent a potential threat to national security or a resource for the protection of a state’s strategic interests. Instead, the purposes Social Media are used for by certain categories of users, and particularly organized groups of users, represent a potential threat or opportunity for a state. The US 2010 National Security Strategy goes in this direction when it refers to new technologies in general (and so to Social Media, too) and claims: “the very technologies that empower us to lead and create also empower those who would disrupt and destroy”\textsuperscript{36}. Every tool can be a threat and an opportunity at the same time.

### SOCIAL MEDIA USERS

Social Media users are firstly, single individuals, who, as above-mentioned, use such tools to communicate, share information and content, interact with other people, develop their personality\textsuperscript{37} and strengthen their social identity\textsuperscript{38}. Single individuals are able to satisfy all their basic needs (except for physiological needs such as drinking, eating or sleeping)\textsuperscript{39} using Social Media. When he talks about it, Riva claims that Social Media can help their users satisfy the following categories of needs\textsuperscript{40}:

- security needs: the user interacts and communicates mainly with the contacts of his own network, who are not supposed to be unknown, instead they should be already part of his/her network because of previous relations (social, professional, cultural, etc.); it is the user who decides what contact to have in his/her network, and who are those who might be eliminated, in case they are no more welcome. In so doing, the user acts in a well-known and defined social context;
- membership needs: the user has the opportunity to communicate and share content, having constant confrontations with the contacts of his/her network; the need to create or be part of a group is strictly linked to the following categories of needs;
- appreciation/esteem needs: apart from choosing the contacts to include in his/her own network, the user can be chosen in turn by other users, as well. Such a process can boost one’s self-esteem, since he/she can also measure his/her social consideration on the basis of the number of invitations he receives from new contacts;


\textsuperscript{36} US GOVERNMENT, (2010), National Security Strategy 2010, Washington, DC.

\textsuperscript{37} ZINZOCCHI R., (2009), Da Facebook a Twitter vogliamo lasciare tracce, Il Tempo. According to Maurizio Ferraris, professor of Theoretical Philosophy at Università di Torino, interviewed by the author of the article, for many people Social Media create a personality as if a rich digital identity, connected with endless other digital identities was the condition for a complete real identity.

\textsuperscript{38} RIVA G., MILANI L, GAGGIOLI A., (2010), Networked...cit.

\textsuperscript{39} RIVA G., (2010), I social ...cit.

\textsuperscript{40} RIVA G., (2010), I social ...cit.
• self-fulfilment needs: the user can describe himself/herself on the profile he/she creates on his/her network. He/she can provide information of different kind about his/her physical aspect, age, profession, studies, interests, etc. Since the user makes his/her qualities and abilities public, he/she can become the recipient of several requests of advice, opinions, information or help by his/her contacts. This process can help boost one’s self-perception, especially about his/her perceived usefulness toward the network of his/her contacts.

Single individuals can use Social Media not only for strictly personal purposes, but also for the interests and/or purposes of the organized group they are part of. Hence, although the use of Social Media is necessarily linked to the interaction between a person and the information medium, organized groups (in the broadest meaning of the term: states, public agencies, companies, movements, terrorist groups, etc.) are potential Social Media users, too. In this case, the single members (in terms of affiliation, association, etc.) of these organized bodies are to manage the “institutional” accounts and become the factual users of Social Media on behalf of the entire group, pursuing the purposes and protecting the interests of the group itself.

**SOCIAL MEDIA AND INFORMATION WARFARE**

Information Warfare (IW)\(^{41}\)/Information Operations (IO)\(^{42}\) activities occur when Social Media are used by organized groups with a precise strategy in order to obtain a competitive advantage toward their competitors. As for this kind of activities, the dimension of the conflict (economic, political, etc.) among two or more organized groups shifts from the merely military one, strictly and traditionally speaking, to a multi-dimensional one, less palpable and concrete, and characterized by a never-ending “battlefield” and an asymmetric conduct\(^{43}\). According to Carlo Jean and Paolo Savona, professors of Geopolitics and experts on intelligence and strategic studies, IW/IO activities are spreading remarkably, especially thanks to the fast and wide spread of new media and new communication and information technologies. In particular, the two scholars claim that communication is used to manipulate perceptions and, consequently, the adversary’s, competitor’s or the market behaviour\(^{44}\). They add that the ability to manipulate will increase along with the spread of interactive media\(^{45}\), and that IW/IO activities consist of propaganda, counter-

---

\(^{41}\) US DEPARTMENT OF DEFENSE, (1995), *Joint Publication 1-02: Dictionary of Military and Associated Terms*, Arlington County, VA. Until 1998, the US Department of Defense defined *Information Warfare* as the “actions taken to preserve the integrity of one’s own information system from exploitation, corruption, or disruption, while at the same time exploiting, corrupting, or destroying an adversary’s information system and the process achieving an information advantage in the application of force”.


\(^{42}\) US DEPARTMENT OF DEFENSE, (2006), *Joint Publication 3-13.4: Doctrine for Military Deception*, Arlington County, VA. Since 1998 the US Department of Defense has removed the expression «Information Warfare» and updated it substituting the former expression with the new «Information Operations», defined as “the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military reception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own”.


propaganda and influence operations, emergency communication management, disinformation, and erosion of the adversary’s reputation and credibility.\footnote{JEAN C., SAVONA P., (2011), Intelligence…cit.}

Social Media can prove to be effective IW/IO tools since they enable their users to:

- obtain considerable results, both in the strategic and tactical field, even though they act:
  - in a domain (cyber space) which is different from traditional military ones (ground, sea, air space);
  - on dimensions which are different from war, strictly speaking (e.g. psychological, anthropological, cultural, media, perceptive dimension);
  - not only against military targets, but also against social society (as a whole or referring to specific ethnic, religious, cultural or professional communities) and a state’s critical infrastructures (strategic-relevant companies, telecommunication networks, banking systems, etc.);

- reach considerable results without investing a lot of means (their handiness and cheapness have been mentioned above); for example, using such tools it is possible to rapidly share an extremely high number of content and information with a huge number of addressees at a ridiculous cost: “information is being [...] turned from an expensive commodity into an inexpensive one; and being free from the control of a few to make it almost universally accessible”\footnote{HIMANEN P., (2001), L’etica Hacker e lo spirito dell’informazione, Feltrinelli, Milano.};

- stand an asymmetric conflict: a small/medium-sized organized group (e.g. a terrorist group) can carry out offensive operations against a more resourceful and powerful competitor (e.g. a state), managing to effectively reach the set goals and cause severe damage to the competitor.

IW/IO activities through Social Media can have different hallmarks, according to the nature of the organized group (state, company, terrorist group, criminal organization, cracker group, etc.) and, consequently, to the set objectives of the group itself. IW/IO activities can be divided as follows:

- \textit{cyber war}: conflict among nations, fought systematically pulling down an adversary’s critical protection barriers of security, that is disturbing or “switching off” strategic communication networks, and complementing these activities with merely war operations\footnote{COPASIR, (2010), Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall’utilizzo dello spazio cibernetico, Stabilimenti tipografici Carlo Colombo, Roma.}. Richard Clarke, USA national security expert, defines cyber war as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption”\footnote{CLARKE R. A., (2010), Cyber War: The Next Threat to National security and What to Do About It, Harper Collins, New York.}. In short, cyber war is to be referred to as the ensemble of offensive activities carried out in the cyber space by one or more states against another state or another non-state entity possessing international subjectivity.

- \textit{cyber terrorism} (or \textit{counter-cyber terrorism}): cyber terrorism is referred to as the use of the net by terrorist organizations for propaganda, detraction, or affiliation purposes\footnote{COPASIR, (2010), Relazione…cit.} or to put out of order critical transmission points of structures or processes related to national security\footnote{COPASIR, (2010), Relazione…cit.}. Therefore,
cyber terrorism is an offensive activity\textsuperscript{52}, carried out in the \textit{cyber space} by a terrorist group to cause damage to a state or another non-state entity possessing international subjectivity, which, besides causing physical damage, can cause negative psychological effects\textsuperscript{53};

- \textit{cyber crime} (or \textit{counter-cyber crime}): the expression “cyber crime” is used to refer to the ensemble of the threats by criminal or transnational organizations, which take advantage of the cyber-space for offences such as fraud, identity theft, embezzlement of information, creations or intellectual property\textsuperscript{54}. Cyber crime activities are offensive operations, and are carried out in the cyber space to the detriment of single individuals or an organized group (state, company, etc.). The foremost purpose in cyber crime activities is to obtain an economic advantage.

In order to simplify the analysis, it is possible to map the organized groups which could be potential users of Social Media as IW/IO tools categorising them according to the dimension (inland or international) they act in, and measuring the potential level of threat for national security. As for a state’s inland dimension (referred to as a space delimited by the territorial boundaries a state exercises its sovereignty within), the following organized groups can be classified, in descending order according to their potential threat level:

- national subversive groups (Marxist-Leninist groups, anarchist-insurrectionalist groups) \textsuperscript{55};
- national criminal organizations (mafia, ‘ndrangheta, camorra, sacra corona unita) \textsuperscript{56};
- opposing movements/extra-parliamentary forces (no global movement, environmental associations, anti-nuclear groups, xenophobic groups, extremist supporters, far right groups) \textsuperscript{57};
- cracker groups (predominantly acting within a state) \textsuperscript{58};
- religious sects\textsuperscript{59};
- companies (with national capital stock);
- hacker groups;
- associations/foundations/ non profit organizations;
- political parties/labor unions;
- public institutions (national security agencies included)\textsuperscript{60}.

\textsuperscript{52} The use of \textit{Social Media} can also consist in activities aimed at carrying out offensive operations (i.e. it can even limit to the recruitment and/or organization of an activity).

\textsuperscript{53} THEOHARY C. A., ROLLINS J., (2011), \textit{Terrorist...}cit. The authors stress that some consider the expression “cyber terrorism” inappropriate since carrying out offensive operations in the \textit{cyber space} can cause only unease and not dread, while others maintain that such combined actions, can cause so much unpredictability, economic damage and fear that can be considered terrorist activities. "Cyber terrorism exists when unlawful, politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage".

\textsuperscript{54} COPASIR, (2010), \textit{Relazione...}cit.

\textsuperscript{55} PRESIDENZA DEL CONSIGLIO DEI MINISTRI – SISR, (2011), \textit{Relazione sulla politica dell’informazione per la sicurezza}, Roma.

\textsuperscript{56} PRESIDENZA DEL CONSIGLIO DEI MINISTRI – SISR, (2011), \textit{Relazione...}cit.

\textsuperscript{57} PRESIDENZA DEL CONSIGLIO DEI MINISTRI – SISR, (2011), \textit{Relazione...}cit.

\textsuperscript{58} HIMANEN P., (2001), \textit{L’etica...}cit. The author of the book is Professor at Helsinki and Berkley Universities. He refers to \textit{crackers} as to individuals who destroy the security of a system, create malwares and enter informatics/informative systems thus causing damage. The term was invented around 1985 by the hackers who wanted to defend themselves against the journalistic use of the term \textit{hacker} and in order to avoid being confused with computer criminals.


\textsuperscript{60} Armed Forces, Police Forces, intelligence agencies.
Expanding the analysis to the international dimension (referred to as the ensemble of the space other states exercise their sovereignty above and the space subject to the rules of international customary and treaty law), the following organized groups are identified as follows, starting from the one which can represent the more likely potential threat to national security:

- international terrorist groups (al-Qaeda, jihad-inspired groups, separatist organizations, pan-Albanian extremism)\(^61\);
- transnational criminal organizations (Chinese, African, Balkan and South American)\(^62\);
- non allied foreign states or non political-military and/or economic-financial partner states (security services related included);
- multinational corporations;
- cracker groups (mostly in foreign states);
- companies (with foreign capital stock);
- religious sects (spread transnationally)\(^63\);
- hacker groups;
- NGO;
- international organizations;
- allied foreign states or states with a political-military and/or an economic-financial partnership.

As Social Media are evolving very rapidly and they are soaring worldwide, the above-mentioned mapping cannot be considered comprehensive and/or definitive since:

- in the future, new organized groups might appear, as new Social Media users;
- several groups act simultaneously both in the inland and in the international dimension; for this reason their precise and unchanging placement in one of the two dimensional areas is quite difficult to achieve, hence, some overlapping areas arise\(^64\);

Despite its limits, the map traced above (figure n.1) can provide a useful tool for an overall view of those who use Social Media for IW/IO activities by means of their own agents. Therefore, the map shows how certain groups can prove to be either a threat to national security or to have the power to counter threats and protect a state’s strategic interests.

\(^64\) JEAN C., SAVONA P., (2011), *Intelligence...*cit. The authors emphasize how difficult it is to trace the boundaries between the domestic dimension and the external dimension especially referring to economic and financial aspects: they affirm that at the time of the Westphalian states the governments used to prioritise national economic, technologic, financial and commercial policies, which take origin from major interests rooted in geographical, physical and human realities of their countries. As a matter of fact there was a strong link among state, territory and wealth, while today companies do not act on a territory and in close and preserved markets but in a world without borders.
Fig. no. 1

(source: Alfonso Montagnese)
Social Media were born at the beginning of the XXI century in the US and, since that date they have been growing and spreading exponentially, especially in the last two years. It took a relatively short time for Social Media to change from “an interesting emerging communications trend to a critical part of the media landscape”\textsuperscript{65}. According to some 2010 estimates, all Social Media users add up to over two billion people\textsuperscript{66}.

In their early stage (2000-2005), Social Media started to spread chiefly in the more developed countries, with a high technological power (broadband speed, number of per capita computers, etc.) and whose governments guarantees complete freedom of expression and communication. In this very stage Social Media took root especially in North America, Europe, Russia, Japan, South Korea and Australia \textsuperscript{67}. Nevertheless, since 2005 they have started to catch on in less developed (both technologically and economically), non democratic countries, too. Thus, new media started to spread in Northern Africa, Middle East, China, Southeast Asia, in the Persian Gulf states, in Southern and Central America \textsuperscript{68}. According to Emanuela Del Re, professor at Università La Sapienza, Rome, differently from other communication revolutions where the diffusion of media happened before in the developed states and only after in less developed states, Social Media are spreading everywhere contemporaneously. In fact, today some areas of the World are no more marginalized, instead they become aware of their freedom of expression, share thoughts and customs and endorse them. The only discrimination left is maybe about social classes and genre\textsuperscript{69}.

According to the \textit{Hague Centre for Strategic Studies} \textsuperscript{70} the level of penetration of Social Media into everyday life is soaring and it is expected to see a marked increase not only in the near future, but also in the long run\textsuperscript{71}. The level of social penetration for these media is strictly dependent on several factors, the most important of which are: “accessibility, bandwidth and trust, where trust is akin to a belief in the benignity of, and a level of familiarity with, social networks”\textsuperscript{72}. Since these factors are expected to grow considerably, Social Media diffusion will presumably increase, too\textsuperscript{73}.

\textsuperscript{65} BURSON-MARSTELLER, (2011), \textit{The Global Social Media Check-up 2011}, New York.
\textsuperscript{66} LOMBARDI F., (2011), \textit{I social...cit}.
\textsuperscript{67} \url{http://www.vincos.it/world-map-of-social-networks/}.
\textsuperscript{68} BURSON-MARSTELLER, (2010), \textit{Social Media...cit}.
\textsuperscript{70} \url{http://www.hcss.nl/about-hcss/}.
\textsuperscript{72} THE HAGUE CENTRE FOR STRATEGIC STUDIES, (2011), \textit{Social...cit}.
\textsuperscript{73} THE HAGUE CENTRE FOR STRATEGIC STUDIES, (2011), \textit{Social...cit}. 
Burston-Marsteller analysed the presence of companies on Social Media calculating the percentage of companies which are using Social Media, both in 2009 and in 2010 and the results are the following:

- the most used digital media - considering the number of registered profiles and the volume of content published or shared - are Facebook (with more than 3 hundred million users), Twitter (with 75 million users), YouTube (91 million users only in the US), and the blogs (surveyed in 2002, they turn out to be more than 133 million);
- the Social Media which is spreading more rapidly than others, especially in the corporations, is Twitter, with an 18% increase in companies using it only in 2010, thanks to the ever-growing use of functions such as “retweet” or “@mention”, to direct tweets to other Twitter accounts;
- during the period analysed, while the level of “digital presence” and the number of companies present on Social Media platforms remained unchanged in North America and Europe, it grew considerably in the rest of the world. According to this study, it is Asia the area with the highest Social Media growth trend. In fact, in 2010 Asian companies, arose their “digital presence” of about 34% on at least one of the four most widespread platforms.

Incite, a Nielsen-McKinsey company specialized in marketing advice with the aid of new Social Media, published a report with an up-to-date map of Social Media users in the US, the UK, Australia, Brazil, France, Germany, Italy, Japan, Spain and Switzerland. This study was conducted during the first semester of 2011, and showed that in the surveyed countries:

- more than 75% of Internet users has at least an active profile on a Social Media;
- about 40% of Social Media users enters their own profile via their mobile phone;
- people older than 55 are particularly active using Social media via mobile phone service;
- women are primary Social Media users;
- most of the users are between 18 and 34 years old.

Vincenzo Cosenza, in marketing and communication, and head of the Digital PR Rome office, adapted Geoffrey Moore’s diffusion of innovations model to Social Media diffusion, with the aim of plotting their actual growth level and understanding their future development trends. According to this abstract model, Social Media diffusion, as well as new technology diffusion, follows a classic normal distribution (fig. n.2) or “bell curve” divided in 5 stages. Each stage of the curve has its own corresponding category of Social Media users:

- The study is limited to the 100 more prestigious and influential global companies, as they have been chosen by the business newspaper Fortune.
- BURSON-MARSTELLER, (2010), Social Media..cit.
- BURSON-MARSTELLER, (2011), The Global Social...cit.
- According to more recent estimates dating back to June 2011, Facebook users have become more than 700 million.
- The efficiency level has been measured according to the volume of the material published, the number of «followers» (Twitter), «fans» (Facebook), and of those who join thematic channels (YouTube), of comments and posts (blogs).
- It is an agency of the Hill & Knowlton group, specialized in studying and using new forms of digital communication.
- The curve is used in order to represent casual variables to true values which tend to concentrate around a single mean value.
Media potential adopters, based on the relative adoption and use level: innovators (2.5% of the potential population of adopters), early adopters (12.5%), early majority (34%), late majority (34%), laggards (16%). In its ascending stage, the curve is characterized by a gap the author calls “chasm”, which has to be crossed in order for a Social Media to have a large scale diffusion. The “chasm” is located between the second and the third adopter group and indicates the threshold beyond which a Social Media reaches global diffusion, moving from early adopters to early majority stage. On the contrary, in the case diffusion does not go beyond the second stage (early adopters), a certain Social Media does not become globally adopted, instead it might stop at regional level, and might be limited to a certain geographic area (e.g. One\textsuperscript{85}, VKontakte\textsuperscript{86}, Hi5\textsuperscript{87}, Orkut\textsuperscript{88}, QZone\textsuperscript{89}, Mixi\textsuperscript{90}, etc.), or a certain category of users, linked to a specific area: professional (e.g. LinkedIn), artistic (e.g. MySpace), or a certain age range\textsuperscript{91}.

![Social Networks Adoption Lifecycle](http://vincos.it/social-media-statistics/)

Fig. no. 2

(source: [http://vincos.it/social-media-statistics/](http://vincos.it/social-media-statistics/))

\textsuperscript{85} Widespread in Central Europe.
\textsuperscript{86} Russia’s most used Social Media.
\textsuperscript{87} Particularly popular in Central and South America.
\textsuperscript{88} Very popular in Paraguay and India.
\textsuperscript{89} PRC’s most used Social Media.
\textsuperscript{90} Japan’s most used Social Media.
\textsuperscript{91} INCITE, (2011), State...cit.
Gianni De Gennaro, Director General of the DIS – Dipartimento Informazioni per la Sicurezza (Security Intelligence Department), recently interviewed by a cultural magazine about cyber-space threats, claimed that the higher the informatization level of a certain country’s population, the more widespread the use of IT devices by its citizens, companies and public agencies, the more frequent the use of web for information sharing, acquiring or transfer, the higher that state’s vulnerability is. Consequently, threats for national security and unfavourable consequences for a state’s strategic interests may arise from the very use of Social Media, which are main information sharing and transfer tools on the net. Such negative effects for a state can be caused by the use of Social Media, both by competitors (states or non-state actors), and by that very state’s apparatuses, but in an unsupervised way, especially referring to those related to security and sensitive areas (diplomacy, bench, strategically relevant companies, etc.).

- TERRORISM

Social Media are more and more used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training. In addition to this, terrorist groups take advantage of Social Media to communicate with cyber-crime organizations and to coordinate along with them fund-raising activities (from illicit activities) carried out in part (drug smuggling, gunrunning) or completely (e.g. phishing) on the Internet. The link between organized crime and terrorist organizations is increasing considerably in the cyber-world, and this coalition will be able to produce new offensive technologies.

To date the terrorist groups which make the most substantial use of Social Media for their own purposes are the Islamic-jihadist ones. Facebook and YouTube channels are often used by al-Qaeda with the aim of recruiting and increasing the number of sympathizers and jihad-supporters, especially in the West (e.g. spreading photos and videos of successful terrorist attacks, publishing lists and biographies of the martyrs, preaching or ideological texts). Lorraine Bowman-Grieve, researcher at Leeds Trinity University College, and specialized in terrorism and political violence, pointed out that Social Media “play an important role in influencing the behaviour of the individual and their readiness to take part in collective action because of

---

93 UN COUNTER-TERRORISM IMPLEMENTATION TASK FORCE, (2011), Use of the Internet to Counter the Appeal of Extremist Violence, Conference Summary, Riyadh.
95 It is a computer fraud carried out sending counterfeit messages via e-mail or Social Media, and it is aimed at acquiring classified information for illegal purposes.
97 The term «jihadism» is used to refer to the instrumental use terrorist and religious extremism leaders make of jihad (which literally translates as «struggle» and which, from a juridical point of view, consists of war activities aimed at defending Islam, advancing it and repelling evil from Muslims); the term «Islamism», instead, is used to refer to the phenomenon of Islamic radicalization, that is following extremist ideas and being closed to any kind of ideological, cultural and religious contamination.
their inherent socialising, recruitment and decision shaping functions”\textsuperscript{99}, besides, they “facilitate social interaction and the formation of social bonds, which in turn can lead to changes in attitudes and behaviour over time. These changes in attitude might include adopting the most prevalent ideology expressed within the community”\textsuperscript{100}. Social Media, and, more generally speaking, the Internet allow the publication and diffusion of “extremist ideas and material that may lead a vulnerable individual to recruit himself, sometimes unaided by any intermediary”\textsuperscript{101}. Apart from being used for proselytism purposes, Social Media are used by Islamist groups for propaganda activities aimed at making public successful terrorist attacks, and, consequently, at throwing civil population into a panic. Since spreading news and content on Social Media can be considered “viral”, this kind of propaganda can be able to considerably overdraw the media effect already produced by traditional means of information and communication (satellite TV, newspapers, radio) and cause consequences even more dangerous than those caused by the terrorist attacks themselves (e.g. circulating the news of an attack to communication and connection infrastructures used by the stock market might throw investors into a panic, and, consequently, lead small money-savers to behave irrationally; in so doing, it could cause even more severe economic damage than the damage itself to the very material infrastructure). As before-mentioned\textsuperscript{102}, the US Congressional Research Service conjectured that some organized groups, mainly terrorist groups, could use Social Media with the aim of knowingly spreading false information (in part or in full) during a disastrous event (e.g. an earthquake, a flood, the accidental blast of a nuclear reactor, a pandemic, etc.) or immediately after it ends, in order to overdraw their damaging effects, mystifying the people and delaying emergency operations and the response of a country.

According to a report by the US Army\textsuperscript{103}, Social Media can also be used as a vehicle for malwares so as to cause damage to computers or other mobile terminals (smart phones, tablets, etc.). The report chiefly stresses that “Social Media tools such Twitter and Facebook can be used by terrorist groups to expand networks and not only to spread propaganda, but can also host embedded malicious software in links and applications that can corrupt an unsuspecting user’s electronic device”.\textsuperscript{104}

Seth Jones, expert in foreign policy and terrorism at Rand Corporation and professor at Georgetown University, argues that al-Qaeda developed a well-framed strategy committed to using Social media in order to achieve their own goals. According to Jones, Anwar al-Awlaki\textsuperscript{105} was one of the major promoters of such strategy. He was a leading figure of al-Qaeda organization and was killed in Yemen on 30\textsuperscript{th} September 2011 by the CIA in collaboration with the Joint Special Operations Command, a special command of the US Department of Defense\textsuperscript{106}. To be precise, al-Awlaki took cleverly advantage of Social Media potentialities: he worked actively on most of social networking sites, and used them to spread a huge amount of propaganda material specially addressed to members scattered all over the world in order


\textsuperscript{100} BOWMAN-GRIEVE L., (2010), A psychological...cit.

\textsuperscript{101} UN COUNTER-TERRORISM IMPLEMENTATION TASK FORCE, (2011), Use of...cit.

\textsuperscript{102} LINDSAY B. R., (2011), Social...cit.

\textsuperscript{103} US ARMY, 304th Military Intelligence Battalion, (2008), Sample Overview: al Qaida-Like Mobile Discussions & Potential Creative Uses, Fort Huachuca, Arizona.

\textsuperscript{104} US ARMY, 304th Military Intelligence Battalion, (2008), Sample...cit.

\textsuperscript{105} JONES S. G., (2011), Awlaki’s Death Hits al-Qaeda’s Social Media Strategy, RAND Corporation, Santa Monica, CA.

\textsuperscript{106} http://www.guardian.co.uk/world/2011/sep/30/anwar-al-awlaki-yemen.
to push them into committing terrorist acts\(^{107}\) (as for the case of US Army major Nadil Hasan, who committed a terrorist act in the US, killing 13 people and wounding 43\(^{108}\), after being influenced by al-Awlaki via Social Media, too).

Since al-Qaeda has a “net-like” decentralized structure, Facebook and Twitter can be effectively used as platforms to organize and connect the single groups linked to al-Qaeda, and also the “lone wolves”\(^{109}\) and the leadership\(^{110}\). Furthermore, Social Media are used to communicate coded messages\(^{111}\), to arrange plans for terrorist acts\(^{112}\), to manage the training of new terrorists, and provide logistical support and operative assistance (i.e. giving advice about how to go through a roadblock\(^{113}\), build themselves and handle arms and explosives\(^{114}\), find and use cyber weapons\(^{115}\), dodge and counter investigation by security agencies\(^{116}\)).

**- CRIMINALITY**

Criminal organizations use Social Media as support, communication and coordination tools to conduct their illicit activities. This kind of illicit activities can be either purely information ones (i.e. spreading child pornography with fee, “virtual” identity thefts, phishing, spread of viruses, trojans, worms, etc.), or “traditional” ones (i.e. drug smuggling, human trafficking, money-laundering, transfer of documents from industrial espionage\(^{117}\)).

Criminal groups which use Social Media are made of people coming from the same geographic area and who know each other personally, but also of people scattered all over the world who are linked exclusively by “virtual” relations. These “criminal communities” are generally coordinated by one or more moderators who have the power to remove the members who do not provide high-quality information or tools and to assign an increasing level of reliability to those who make more contribution than others\(^{118}\).

The use of Social Media and, in general, of IT technology for criminal purposes is dramatically expanding, not only because they are spreading increasingly, but also because the individuals perceive the actions they commit as less serious if compared to what happened in the past. The same happens for the extent of the damage caused by their behaviour, and the risk of being found\(^{119}\).

---

\(^{107}\) JONES S. G., (2011), Awlaki’s...cit.
\(^{108}\) http://www.bbc.co.uk/2/hi/8345944.stm.
\(^{109}\) Referred to as isolated subjects who, despite not organically joining a terrorist group, are always ready to act in favour of the terrorist ideology and the religion and to carry out terrorist attacks.
\(^{112}\) THEOHARY C. A., ROLLINS J., (2011), Terrorist...cit.
\(^{114}\) ROLLINS J., (2011), Al Qaeda...cit.
\(^{115}\) THEOHARY C. A., ROLLINS J., (2011), Terrorist...cit.
\(^{117}\) INTELLIGENCE AND NATIONAL SECURITY ALLIANCE, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA.
- WAR

According to a recent NATO provisional study\textsuperscript{120}, future conflicts will occur in more and more connected environments, which will be characterized by the use of new communication and information technologies, Social Media included. It is a few years since Social Media have been employed by the Armed Forces in several countries, and now they are ready to be employed more and more frequently to accompany traditional offensive means. In particular, the use of Social Media during a conflict adds to the employment of other mass media (newspapers, TV, radio, etc.) for propaganda, influence and deception activities, as better explained in the following section. Since in the last decade the number of wars between entities with international subjectivity has been very low\textsuperscript{121}, and that open-source material is sparse, it is not possible to investigate cases of military campaigns conducted with an actual employment of Social Media in support of military operations. Nevertheless, at this regard it can be useful to briefly mention the two latest conflicts between Israel and Lebanon.

During the second Israeli-Lebanese war in 2006, Hezbollah carried out several IW activities thanks to the use of Social Media. To be precise, during all the conflict they published several videos and photos on blogs, social networking sites and YouTube so as to foster their own image and decry Israel’s one and their security services. Further to this activity, Hezbollah managed to instil a “perception of failure” in the Israeli political-military establishment which conditioned the course of the conflict\textsuperscript{122}. During the following war (2008-2009), instead, Israel showed a much effective management of Social Media, employing them in information and counter-information campaigns\textsuperscript{123}.

- PROTEST MOVEMENTS AND REVOLUTION

New technologies and in particular Social Media constitute an asset of great importance both for protest movements and for revolutions\textsuperscript{124}. Rebels and revolutionary groups turn to such tools to better organize and spur masses to action, to arrange protest or struggle activities and manage their tactical and operational aspects.

Since Social Media are gaining a great deal of clout in determining the conclusion of protests and revolutions, their employment is likely to increase remarkably in the immediate future. According to Marco Papic and Sean Noonan, analysts at STRATFOR, Social Media are tools which enable revolutionary groups to lower the costs of participation, organization, recruitment and training\textsuperscript{125}.

\textsuperscript{120} NATO Allied Command Transformation, (2009), \textit{Multiple Futures Project – Navigating Towards 2030}, Norfolk

\textsuperscript{121} Which, as above-mentioned, corresponds to the times of Social Media affirmation and diffusion.


\textsuperscript{123} MAYFIELD T. D., (2011), \textit{A Commander’s...cit.}

\textsuperscript{124} PEDDE N., (2011), \textit{La crisi libica, e le differenze con le rivolte in Tunisia ed Egitto}, Informazioni della Difesa – SMD, n.2/2011, Roma. The author makes a distinction between revolutions and revolts; a revolution is a rare phenomenon which provokes a radical and often irreversible change when compared to the past, since it aims at deeply and violently breaking with the political and social reality it takes place in. A revolt, instead, is only partially similar to a revolution. In fact it lacks two fundamental elements (if compared to a revolution): the capability to cause subversion in the pre-existing political and social order and a sound and resolute leadership, characterized by a clear ideology and an assertive rhetoric.

\textsuperscript{125} PAPIC M., NOONAN S., (2011), \textit{Social Media as a Tool for Protest}, STRATFOR, Austin, TX.
The two experts studied the recent protest movements in Tunisia and Egypt, and discovered that:

- there is a noticeable increase in the use of Social Media by revolutionary groups, especially to spur civil disobedience and manage protest and struggle actions;
- together with mobile phones, Social Media guarantee rapidity in spreading information and spurring masses to action: “protest movements can reach hundreds of thousands of adherents with a single Facebook post or Twitter feed, launching a massive call to action in seconds”\(^\text{126}\);
- thanks to their being extremely cheap (as above-mentioned), Social Media allow revolutionary movements to be more autonomous and, therefore, less easily influenced by people not involved in the organization and less dependent on external financing.

General Francesco Lombardi, assistant director and head of the Military Sociology Department at Ce.Mi.S.S. (Military Centre for Strategic Studies), examined the role of Social Media in the latest protest movements and/or revolutions and affirmed that in the future such movements will not be different as for the procedure (conflicts, occupations, manifestations, civil disorders, etc.) and the purposes (improvements of social and economic conditions, change of the political system, etc.), but will surely be different for what concerns the interactions among the protesters themselves, among them and the power they want to counter, and among them and the external world\(^\text{127}\). Lombardi adds that Social Media let their users “bypass” the censorship and the control the government usually makes on the media, creating an alternative channel to spread (true) news\(^\text{128}\). Emanuela Del Re agrees on this very observation, and talks about the role of Social Media in the course of the recent protests in Libya, Tunisia, Egypt and Syria, claiming that the regimes have lost the absolute control on the information, gradually losing power while the population has acquired the power to handle and spread the information, in turn\(^\text{129}\). The Algerian writer and journalist Amara Lakhous also points out how Social Media and the Internet make information censorship and manipulation almost impossible\(^\text{130}\). Similarly, Marco Hamam, freelancer for the cultural magazine Limes, studied the recent protests in Egypt and noticed that in societies where traditional public media are controlled by the government and private ones are censored by the companies they work for, Social Media represent a unique opportunity for civil population to counter the regime and enhance their freedom of speech and communication\(^\text{131}\).

- **INCAUTIOUS USE BY CIVIL SERVANTS**

Turning to Social Media enables the diffusion of confidential or job-related news whose subsequent use or possible manipulation cannot be predicted and circumscribed. Cases of non-authorized and uncontrolled publication of classified or sensitive information or content (audio, video, photo, etc.) through Social Media are more and more frequent. In these cases national security can be severely compromised by the use of Social Media. Freedom of expression and communication has to stop where the need to protect the confidentiality and integrity of sensitive data starts, that is to fulfil the general duty of confidentiality at work. Since the civil service is making more and more use of Social Media for their institutional purposes, as well as civil servants are doing for personal interests, a series of information campaigns should be launched.

\(^{126}\) PAPIC M., NOONAN S., (2011), Social...cit.
\(^{127}\) LOMBARDI F., (2011), I social..cit..
\(^{128}\) LOMBARDI F., (2011), I social..cit..
\(^{129}\) DEL RE E. C., (2011) La Rete...cit.
\(^{131}\) HAMAM M., (2011) La Rete...cit.
so as to increase the level of civil servants’ awareness about the Social Media risks for personal and national security. In order to mitigate the risks for national security coming from the improper use of Social Media, a specific national policy is desirable, on whose basis all the institutions can elaborate their own guidelines for their staff, according to their area of expertise. The US government followed this direction, in fact in 2009 the above-mentioned Chief Information Officers Council adopted a series of guidelines to assist federal departments and agencies in developing a strategy to enable the safe use of Social Media\textsuperscript{132}. In brief, the document supplies federal agencies with a special policy, and stresses that policies should not be adopted on the basis of technology itself, instead, they should focus on public servants’ behaviour, whose professional knowledge cannot be lacking of an appropriate security culture, and whose use of Social Media needs to be responsible. On the basis of the government guidelines, the US Air Force adopted a specific document\textsuperscript{133} aimed at keeping under control the use of Social Media by the Air Force employees.

**OPPORTUNITIES FOR THE PROTECTION OF NATIONAL SECURITY AND STRATEGIC INTERESTS OF THE STATE**

Apart from being potential threat tools, Social Media can represent an effective opportunity to preserve national security and/or reach the strategic interests of a state if used properly by civil institutions and, in particular, by security services and/or information security services. In this respect, the before-mentioned Stratfor analysts Papic and Noonan stressed that if Social Media “are presenting a demonstrable threat to governments, it could be vital for security services to continually refine and update plans for disrupting new Internet technology”\textsuperscript{134}. Besides, these tools “can be used by governments for content creation, external collaboration, community building, and other applications”\textsuperscript{135} and that “failure to adopt these tools may reduce an organization’s relative capabilities over time”\textsuperscript{136}.

Social Media can also be employed at the same time both for defence activities (prevention, warning, prevision, institutional communication, crisis management, counter-propaganda) and for offensive actions (influence, propaganda, deception).

- **WARNING AND TREND PREVISION TOOL**

The ability to forestall future strategic and tactical contexts is of paramount importance in order to reduce the possibilities to be caught by surprise by threats and increase the resilience to them. In this regard, General Nicola Gelao - Chief of the Information and Security branch of the Italian Defense General Staff - affirmed that the ability to “hypothesize” the future is not an exact science, and it is very hard to foresee in advance and accurately how, when and where a threat will materialize\textsuperscript{137}. From this perspective Social Media can become an invaluable resource for the benefit of security services, both military and civil, since

\textsuperscript{132} CHIEF INFORMATION OFFICERS COUNCIL (CIO), (2009), Guidelines...cit.
\textsuperscript{133} US AIR FORCE – Public Affairs Agency – Emerging Technology Division, (2009), Social Media and...cit.
\textsuperscript{134} PAPIC M., NOONAN S., (2011), Social...cit.
\textsuperscript{136} DRAPEAU M, WELLS L., (2009), Social...cit.
they “can quickly turn into a valuable intelligence-collection tool” 138, as all Social Media users leave marks about their identity, abilities, predilections, movements, contacts, etc. 139, which can be easily collected and analysed, even though they have a no more updated or active profile.

A continuous and deep monitoring of these media can be carried out as a warning tool in case of present and future threats to national security, since the use of Social Media by criminal organizations, terrorist groups, adversary states and other competitors is more and more increasing. For this reason a continuous analysis of Social Media by Intelligence can serve as:

✓ early warning: monitoring Social Media in order to recognize the first signs of an hostile or potentially dangerous activity for a state’s security (i.e. collecting and analysing messages by opposing movements sent via social network sites for the organization of a violent protest can be useful in order to forestall a rebellion or to mitigate its negative consequences 140; studying the information shared by crackers in specialized blogs in order to launch an information attack to a critical infrastructure can concur in adopting suitable protection counter-measures; tracking teaching videos for military recruitment, spread via YouTube by an al-Qaedaist group can help find the users who make use of them, understand the attack methods and techniques and devise effective methods to react and counter the terrorist threat; the continuous control of a Facebook profile updates and a careful exam of the photos published on that very profile can allow to trace the movements and the activities of the members of a criminal group and mapping their connections, etc.);

✓ strategic warning and horizon scanning 141 aimed at outlining the long- and medium-term trend of threats, at identifying the orientation of the opposing groups and forecasting their choices (i.e. collecting signs of protest from young people through the monitoring of the principal social networking sites can help forecast and maybe nip in the bud a dissent which could change into an organized protest movement or even in a revolutionary group; analysing the discussions on blogs specialized in international politics and strategic studies (often held by the leading experts or by the representatives of the major think tanks) can be useful to understand the possible long-term evolutions of foreign policy and of the strategic thinking of a state’s leadership; studying the discussions of blogs specialized in science and technology can help measure the possible long-term development of scientific and technological expertise in a certain place; mapping the relational networks developed on Social Media by members of subversive groups and analysing their evolution can allow to forecast the possible development of the group itself, etc.).

---

139 RIVA G., (2010), I social...cit. The author defines such a consequence as the «second paradox of social networks» and stresses how the users uploading content (photos, videos, texts, etc.) on their personal profiles of a social networking site, involve the construction of a «historical memory» of the users themselves, which will stay public for many years, until that profile is active, even if no more updated. In addition to what Riva maintains, in some cases, the above-mentioned «historical memory» will prove to be available and even after the account deactivation (i.e.: by the company which is the proprietor of the social networking site, by the Law Enforcement, intelligence agents, crackers, etc.).
140 PAPIC M., NOONAN S., (2011), Social...cit. “In Egypt, almost 40 leaders of the April 6 Movement were arrested early on in the protests, and this may have been possible by identifying them through their Internet activities, particularly trough their various Facebook pages”.
141 The expression horizon scanning is used to refer to a methodology for the analysis and prevision of possible future long-term scenarios.
The Intelligence Advanced Research Projects Activity (IARPA), a research institute of the US Office of the Director of National Intelligence (ODNI), has recently launched a project aimed at developing innovative methods to support intelligence analysts in their previsions of future social events. The research program, called Open Source Indicators (OSI), means to actively involve the academic world and the technologic industries with the aim of developing automatic systems for provisional analysis applied to forestalling national security related events: political crises, migrations, epidemics, humanitarian emergencies, protests, periods of economic instability, etc. In particular, OSI is based on the principle that relevant social events are always anticipated by changes of behaviour through the population (increase/reduction of communication, consumes, movements, etc.). Plotting and studying such behaviours can, in fact, be useful to anticipate the events themselves. The observance and measure of such changes can be carried out through monitoring data publicly available and coming from different sources, among which Social Media are placed first.

The Center for Collective Intelligence (CCI) of the Massachussets Institute of Technology, is part of the IARPA’s OSI program and developed a specific software for a dynamic and computerised analysis of Social Media, and, more generally speaking, of the Internet. The computer program, called Condor, aims at providing careful previsions on the behaviour of people and organized groups, and even anticipate future trends, thanks to the combining of connection networks and advanced semantic analysis techniques. Thomas Malone, Director of CCI, in an interview to the New York Times, stressed the great potentialities of the project, and affirmed this: “we have vastly more detailed and richer kinds of data available as well as predictive algorithms to use, and that makes possible a kind of prediction that would have never been possible before.”

IARPA’s OSI program is not the first attempt made by the Office of the Director of National Intelligence to use Social Media for warning or provisional analysis. Also the Open Source Center (OSC), an ODNI specialized centre for open source intelligence (OSINT) activities, started paying attention at Social Media for a while, analysing the content shared and studying users’ dynamics of behaviour. OSC is an agency which deals chiefly with analyses, and its staff is specialized in media-monitoring. Many of the people who work there are experts in several languages (Arab dialects, Pashtun, Chinese dialects, etc.), and have been recruited since 2005 to increase the ability to comprehend and analyse information and content found on Social Media about ethnic-linguistic communities belonging to various areas of the World. Both in its central office in Virginia and in the US foreign services abroad, OSC analysts explore social networks, from Facebook to Twitter, in search of information and sensations; they try to catch the mood of young people, to understand either if somewhere in China a protest is going to break out or if the turmoil in the city of a given country is the sign of a rebellion which will set an entire area on fire; they collect pieces, file

146 http://cci.mit.edu/
148 http://www.opensource.gov. The centre executes the tasks of the CIA Foreign Broadcast Information Service (FBIS).
them, and compare them with other “signs” coming from field sources\textsuperscript{151}. Apart from obtaining information from Social Media in order to forecast future trends, OSC deals with monitoring diffusion, use and impact of Social Media in some countries, too.

Using Social Media to obtain and analyse data for info-prevision and tactic-strategic warning purposes is of great interest to the US DoD, too, which is developing a specific program called “Social Media in Strategic Communication” (SMISC)\textsuperscript{152} through DARPA, with the aim of monitoring such media so as to obtain a better knowledge of the environment some units deployed abroad work into, and collect useful information to support military missions. Therefore, using Social Media this way can help the commanders of the US deployed locations to better understand the socio-politic, religious, economic and cultural characteristics of the area they work in and detect emerging threats\textsuperscript{153}. At this regard Thomas Mayfield, a US army colonel, claimed that “

\textit{maintaining a Social Media presence in deployed locations [...] allows commanders to understand potential threats and emerging trends [...]. The online community can provide a good indicator of prevailing moods and emerging issues\textsuperscript{154}}. The DARPA affirmed that the general purpose of the 42 million dollar SMISC program is “to develop a new science of social networks built on emerging technology base [...] including, but not limited to, information theory, massive-scale graph analytics and natural language processing\textsuperscript{155}”, to be achieved creating automated and semi-automated support techniques and tools for analysts who systematically use Social Media for military purposes. In detail, the use of such techniques and tools aims at\textsuperscript{156}:

- detecting, classifying, measuring and tracking the formation, development, and diffusion of ideas and opinions, and deceptive messaging or misinformation;
- recognizing persuasion campaigns and influence operations carried out by the adversaries through Social Media;
- identifying the participants to such activities and discovering their activities.

The actual functionality of the SMISC program and of other similar activities is linked to the implementation and inclusion of specific parallel projects launched in order to devise systems for extraction, capture, classification and transposition of information (rare languages, idiomatic expressions, dialects, slang, etc.), such as IARPA’s Babel\textsuperscript{157} and Metaphor\textsuperscript{158} programs.

In recent years several partnerships between Western intelligence agencies and private firms began and strengthened for the study and analysis of Social Media for national security purposes\textsuperscript{159}. A CIA venture capital called In-Q-Tel\textsuperscript{160}, has recently funded Visible Technologies\textsuperscript{161}, a software developer company specialized in Social Media monitoring\textsuperscript{162}.

\textsuperscript{151} OLIMPIO G., (2011), Twitter...cit.
\textsuperscript{152} DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), Social Media...cit.
\textsuperscript{153} MAYFIELD T. D., (2011), A Commander’s...cit.
\textsuperscript{154} MAYFIELD T. D., (2011), A Commander’s...cit.
\textsuperscript{155} DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), Social Media...cit.
\textsuperscript{156} DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), Social Media...cit.
\textsuperscript{157} This program was launched by IARPA in January 2011, in order to develop a speech recognition technology able to process - in a short time and with a high level of accuracy - huge amounts of texts written in different languages.
\textsuperscript{158} This program was launched by IARPA in April 2011, in order to develop computerized tools able to detect, categorize and comprehend «linguistic metaphors» used in several languages and all over the world.
\textsuperscript{159} PAPIC M., NOONAN S., (2011), Social...cit.
\textsuperscript{160} http://www.wired.com/dangerroom/tag/in-q-tel.
Three successful projects in different fields need mentioning in order to understand the actual prevision-oriented potentialities of Social Media and to catch their flexibility in use:

- thanks to its own research and development group HP Labs\textsuperscript{163}, Hewlett Packard managed to accurately foresee box-office revenues for newly-released movies in US cinemas, using advanced algorithms to process and analyse data previously extracted by Twitter\textsuperscript{164};
- in September 2011 the National Science Foundation’s Division of Information & Intelligent Systems\textsuperscript{165} allocated funds to advance a research called RAPID – Earthquake Assessment for Social Media, aimed at evaluating in real-time or in a very short time the extent of the damage caused by earthquakes thanks to the data collected from Social Media\textsuperscript{166};
- researchers from the Indiana University’s School of Informatics and Computing and the University of Manchester’s School of Computer Science carried out a research\textsuperscript{167} aimed at verifying whether or not and at what level of accuracy Twitter can be used to forecast Dow Jones trend\textsuperscript{168}, which is the main means to measure the US economic growth rate.

- INSTITUTIONAL COMMUNICATION TOOL

All the states have to reach the Information Superiority, referred to as an advantage on the adversary in IT and decision-making, if they really want to guarantee high competitiveness and efficiency standards, protect their own strategic interests and effectively counter threats to national security. Social Media can help reach this kind of competitive advantage since they increase the agility and flexibility of the information sharing procedures and accelerate the decision-making process.

The use of Social Media can, in fact, contribute considerably to rapid information sharing within each single government agency and to increase inter-institutional communication flow. Social Media can thus guarantee an effective information and content interchange among offices of the same agency or among different agencies and concur in improving public agencies performances.

With a particular reference to national security agencies, the use of Social Media (potentially projected and/or modified for this very field) represents an important opportunity to complete their functional and organizational evolution, gradually moving from the “need-to-know” to the “need-to-share”. This kind of change makes information available not only to those who actually need it, but also to those who might need it\textsuperscript{169}. Obviously, such organizational and functional evolution needs to go with a correct risk-analysis and a following adoption of safety measures fit to avoid sensitive information to leak from security agencies knowledge\textsuperscript{170} (as noted above).

With a particular reference to Armed Forces and intelligence agencies, Social Media can become a truly effective communication and information sharing tool, if appropriately used, especially in operative settings.

\textsuperscript{161} [http://www.visibletechnologies.com].
\textsuperscript{162} PAPIC M., NOONAN S., (2011), Social...cit.
\textsuperscript{163} [http://www.hpl.hp.com].
\textsuperscript{164} MARKOFF J., (2011), Government...cit.
\textsuperscript{165} [http://www.nsf.gov].
\textsuperscript{166} MARKOFF J., (2011), Government...cit.
\textsuperscript{168} KELLER J., (2011), How the CIA Uses Social Media to Track How People Feel, The Atlantic, Boston.
\textsuperscript{169} RAMACCIOTTI S., (2011), La sicurezza...cit.
\textsuperscript{170} RAMACCIOTTI S., (2011), La sicurezza...cit.
characterized by the presence of different institutions of the same country and/or contingents form different countries, where the mechanics of coordination and information sharing is very prompt. From this perspective colonel Mayfield maintained that “a proactive and innovative Social Media strategy using social networking, blogs, and Twitter-like capabilities can aid commanders in ensuring all concerned entities in the theatre of operations are sharing the necessary information to work toward a common goal” 171.

In addition to this, the use of Social Media by a state’s agencies can help incisively and transparently interact with the public opinion and shorten the gap between institutions and citizens. Civil society can, therefore, become acquainted with the purposes pursued by each public agency, and can be involved in institutional activities, when possible. In particular, Social Media can constitute valid support tools in emergency management (disasters, calamities, pandemics, etc.)172 or to obtain useful prominent information from the on-line community in order to counter crime, illegal behaviour or threats to national security (i.e. locating wanted people, identifying a person with certain characteristics, finding the witnesses for a certain situation, detecting behaviours potentially dangerous for national security, etc.) 173.

- INFLUENCE, PROPAGANDA AND DECEPTION TOOL

The use of Social Media allows not only to communicate, share or capture information, analyse socio-political dynamics and anticipate economic-financial trend, but also to describe events, model reality, influence the perception of a certain situation, a specific issue or a person 174, and influence choices and behaviours. Therefore, Social Media can strongly affect institutional, business or team strategic decision-making, as well as formation and development of the public opinion’s collective awareness. These tools can be employed to interfere with the adversaries’ decision-making process, both directly, that is manipulating their information and analysis framework or influencing their close collaborators, and indirectly: influencing groups of people (i.e. political parties, trade unions, public opinion, etc.) whose reactions affect the very choices of a country’s leadership.

Since they have very distinctive characteristics (as above-mentioned), Social Media can act as effective tools for influence 175, propaganda 176, and deception 177 activities.

174 RIVA G., (2010), I social ...cit. According to the author the «first paradox of social networks» is their ability to allow every single user not only to “mould” their “social identity” creating their own profile, but also to modify the way other users’«social identity» is perceived by other people (i.e.: through the tagging).
175 LARSON E. V., DARILEK R. E., GIBRAN D., NICHIPORUK B., RICHARDSON A., SCHWARTZ L. H., THURSTON C.Q., (2009), Foundations of Effective Influence Operations, RAND Corporation, Santa Monica, CA. The authors define influence operations as the coordinated, integrated and synchronized application of a state’s diplomatic, military, informatic and economic apparatuses so as to induce the adversaries to behave or decide in a certain way. This kind of operations are arranged in order to obtain a competitive advantage toward the adversary; they are carried out using mass media and are addressed against determined subjects: single individuals (i.e.: public agents, military commanders, political leaders, etc.) or small groups of limited dimensions (i.e.: military units, trade unions, a political party leadership, the management of a firm, etc.).
176 ELLUL J., (1983), Storia della propaganda, Edizioni Scientifiche Italiane, Napoli. According to the sociologist propaganda is the ensemble of the methods used by an organized group in order to make people join actively and
The US DoD has already launched several projects providing for the employment of Social Media in influence, propaganda (and counter-propaganda) and deception activities. The following are particularly significant:

- the DARPA undertook a project, called STORyNET\(^{178}\), in order to measure the power of influence stories exert on human behaviour, judgement, and decisions, to study the interaction between narrative and ideological, political or religious radicalization, which result in violent mobilization, insurgency and terrorism. The DARPA research context identifies Social Media and other communication and information media as suitable tools to analyse the stories spread by certain subjects for proselytism and propaganda purposes (i.e. jihadist terrorist leaders), and to understand how and how much the stories narrated and spread in the cyber-space can influence human cognitive mechanisms;

- in addition to developing advanced data analysis power, the above-mentioned DARPA’s Social Media in Strategic Communication (SMISC) program\(^{179}\) aims at detecting deception and influence activities carried out by the opponents\(^{180}\), as well as carrying out appropriate counter activities\(^{181}\) (counter-deception and counter-influence);

- in 2010 the US Air Force 6\(^{th}\) Contracting Squadron commissioned the so-called Persona Management System (PMS) (developed by HBGary\(^{182}\)), for the purpose of creating and managing in an automated way fake profiles on Social Media in order to direct conversations toward certain topics\(^{183}\), stress information favourable to US image and interests, and hide information which could be dangerous for national security, with a special reference to the security of military contingents abroad. Some of the software characteristics follow: the possibility for each user to control up to 10 separate identities, all with a sound and convincing background (ethnically, geographically, culturally and technically consistent\(^{184}\)), and all protected thanks to advanced systems which prevent both the operator from being geo-localized and his/her real identity from being discovered. In reference to the project, US Central Command (CentCom) spokesman Bill Speaks claimed that “the technology supports classified blogging activities on foreign-language websites to enable CentCom to counter violent extremism and enemy propaganda outside the US”\(^{185}\). PMS software is part of a wider framework called Operation Earnest Voice (OEV), firstly developed in Iraq as an Information Warfare tool against the online presence of al-Qaeda and al-

---

177 WHALEY B., (1982), Toward a General Theory of Deception, The Journal of Strategic Studies, vol. 5, Routledge, Taylor & Francis Group, London. The author defines deception as information designed to manipulate the behavior of others by inducing them to accept a false or distorted presentation of the environment. Deception operations differentiate from influence and propaganda activities basically because these latter provide deceiving information (false or partially false) to the subjects they are addressed, in order to cause their mis-perception and cognitive dissonance.


179 DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), (2011), Social…cit.


182 WEBSTER S. C., Revealed: Air Force ordered software to manage army of fake virtual people, The Raw Story.


184 WEBSTER S. C., Revealed…cit.

Qaeda supporters, then expanded into a program against proselytism and propaganda by Afghani, Pakistani and Middle-Eastern Islamist groups. The present CIA Director and former CentCom Commander General David Petraeus referred to OEV program as to a useful tool to “counter extremist ideology and propaganda and to ensure that credible voices in the region are heard” 186;

- the Sentient World Simulation (SWS) 187 project, firstly developed by Purdue University 188 and then adopted by the US DoD 189, consists of a model of the real world translated to a virtual model provided with very many social, economic, climatic, political and geographic variables that allow to forecast and estimate future events. Some virtual models have been developed in the SWS system to be used in order to test propaganda and measure its anticipated effects on a target population 190.

US diplomacy actively uses Social Media for influence and propaganda activities, too. In fact, in 2008, the program Public Diplomacy 2.0 was developed and officially presented by the then Undersecretary of State for Public Diplomacy James Glassman during an event specially organized 191 at the New America Foundation. Public Diplomacy 2.0 has been defined by Glassman himself as a new communication process which takes advantage of Social Media potentialities and credits the diplomatic corps with a significant competitive advantage, both in the relationships with other states in the economic, scientific, technologic and geo-strategic fields and with regard to soft power activities aimed at countering radicalized ideologies, religious extremism, and politic violence. Public Diplomacy 2.0 activities must be based on specific central strategic planning, coordinated with all the institutions involved in diplomatic activities, and well-integrated with the military apparatus. Talking about Public Diplomacy 2.0, Helle Dale argued that Social Media can become a primary vehicle with which the US government addresses public opinion around the world, in addition to traditional means such as radio, TV, libraries, student exchange programs, etc. 192. She further claims that “public diplomacy and strategic communications experts within the US government are exploring the potential of the new social media in the effort to win hearts and minds abroad, especially in the Muslim world where today war of ideas is being fought. Enemies of the United States are already expert in using these low-cost outreach tools that can connect thousands, potentially even millions, at the touch of a computer key or cell phone button” 193. In order to better understand how important Social Media are for the US Department of State it can be useful to briefly cite a cablegram 194, released by the site Wikileaks 195, thanks to which on February 2010 the US embassy in Jakarta required immediate additional funding to use new media and social networking tools so as to support the visit of President Obama in Indonesia, scheduled for the following March.

---

186 FIELDING N., COBAIN I., (2011), Revealed...cit.
187 http://www.theregister.co.uk/2007/06/23/sentient_worlds/
188 http://www.purdue.edu/.
189 The US Department of Homeland Security adopted the system, too.
190 TAYLOR D., (2011), Social...cit.
191 http://www.newamerica.net/events/2008/public_diplomacy_2_0.
192 DALE H. C., (2009), Public...cit.
193 DALE H. C., (2009), Public...cit.
The analysis of the cablegram addressed to the Department of State confirms that:

- a new media team is present within the US Embassy in Jakarta, made up of 4 people assisted by short-term experts (i.e. marketing and communication advisors), and in exclusive charge of propaganda and influence activities carried out through Social Media; therefore, such a specialized body is very likely to be present in every US foreign service;
- US diplomacy actively uses Facebook, Twitter and YouTube, and engages leading local bloggers to promote the image of the US government and of its representatives;
- Public diplomacy operations are even more effective when the use of Social Media is integrated with that of SMS.

In addition to the US, other countries have already developed the skills to use Social Media for propaganda and influence purposes, as it has been noticed by the ODNI Open Source Center (OSC). In particular, the Open Source Center has published several non classified reports about the operations carried out through these media, such as the one about Social Media in India\textsuperscript{196}, the one about the use of Social Media by North Korea for propaganda purposes toward South Korea\textsuperscript{197}, and the one about the use of Social Media by the Israeli government against the media dissent raised by the free gaza flotilla case\textsuperscript{198}.

CONCLUSIONS

Considering their “tool” nature, Social Media can constitute either a threat to national security or a resource for the protection of a state’s vital interests, according to the people who use them, the way Social Media are used and what the pursued purposes are, as in figure 3. Therefore, in the last analysis, it is not Social Media to be a potential threat to national security or a resource for the protection of a state’s strategic interests, instead, the purposes these tools are employed for by certain categories of users, and, particularly, by organized groups of users can represent a potential threat, indeed.

\textsuperscript{196} OPEN SOURCE CENTER, (2010), Overview of Leading Indian Social Media, McLean, Virginia.
\textsuperscript{197} OPEN SOURCE CENTER, (2010), North Korea - Using Social media in Long-Standing Propaganda Effort Targeting South, McLean, Virginia.
\textsuperscript{198} OPEN SOURCE CENTER, (2010), Israeli Government Uses Social Media To Counter Flotilla Criticism, McLean, Virginia.
Fig. n. 3

(source: Alfonso Montagnese)
Since Social Media are quickly evolving and spreading globally as a very highly elaborate phenomenon, a national Social Media Strategy is desirable as soon as possible in order to effectively counter the negative involvements deriving from the use of such tools, and, at the same time, completely take advantage of the opportunities for the protection of a state’s national strategic interests. Stressing the importance of a strategic approach to the use of Social Media, the US Undersecretary of State for Public Diplomacy and Public Affairs Judith McHale argued that “these new tools must be carefully tailored to particular circumstances and always used in the service of a larger strategy”\(^{199}\). Such national strategy should be centrally developed and approved\(^{200}\), should determine general policies, the basic purposes to pursue, the lines of action to adopt, with a particular reference to the use of Social Media by the civil service, especially for the organizations more or less directly assigned to national security (i.e. intelligence community, Armed Forces, diplomatic corps, police, strategic-relevant companies, etc.).

The adoption of a Social Media Strategy by the political leadership in the wider framework of a national security strategy would mean choosing a specific approach toward Social Media, as the result of a balanced choice between two diametrically opposite lines of action:

- the “aggressive option” would mean investing huge resources, both people and means, in offensive (influence, deception, propaganda, etc.) and defensive (counter-propaganda, counter-insurgency, early warning, etc.) activities carried out thanks to the direct or indirect use of Social Media. Such approach would imply a very high intrusiveness in personal privacy, freedom of expression, connection and communication through the Internet;
- the “passive option” would mean precluding every possibility to employ Social Media for national security purposes and would limit to merely monitoring what happens on such media, and defensively responding, should seriously prejudicial events for a state’s national security occur.

On the basis of the above-mentioned considerations, and with reference to the mid- and long-term risks and opportunities deriving from the use of Social Media, it is possible to outline three possible future scenarios. The scenarios’ contingencies are inseparably linked to the political leadership’s choices taken while developing the national Social Media Strategy and to the subsequent level of implementation by the complex apparatus involved in the protection of national security.

---

\(^{199}\) DALE H. C., (2009), *Public…cit.*

\(^{200}\) Bearing in mind the present structure of the Italian security system, this kind of strategic document could be developed within the Presidency of the Council of Ministers, with the involvement of CISR, Comitato Interministeriale per la Sicurezza della Repubblica (Interministerial Committee for the Security of the Republic) and DIS, Dipartimento delle Informazioni per la Sicurezza (Security Intelligence Department), according to what is provided for by L. no. 124/2007.
scenario no. 1

The first scenario is characterized by a huge employment of Social Media by public agencies for national security purposes, with a particular reference to propaganda, monitoring and censoring activities, and interception of communication and of the content spread by such media. When the activities to counter threats and to avert illicit actions in cyber space prove not to be effective, a temporary Social Media disruption or interruption of the Internet service might be exceptionally implemented. Intelligence agencies’ analytical capabilities are jeopardized by an overload of information due to the high volume of the content acquired through Social Media and the excessive attention paid to monitoring such media, which is the cause of strategic distraction. Individual freedom of expression and communication and the right to information, as well as the self-ruling capabilities of the net are considerably compressed.

scenario no. 2

The second scenario is characterized by a proactive use of Social Media by public agencies. These latter have developed very high offensive (influence, disinformation, perception management and deception operations, etc.) and defensive (counter-propaganda, warning, etc.) capabilities, contemporaneously succeeding in both guaranteeing the confidentiality and privacy of the individuals, and limiting to the bare minimum the compression of individual liberty. The effect on the entire nation is positive since an effective use of Social Media guarantees the improvement of provisional analysis techniques in support of the leadership, of patterns of threats interpretation and threats countermeasures. The employment of Social Media favourably affects civil service’s performances, making the decision-making process quicker and increasing intra-institutional and inter-institutional information-sharing. With regard to the risks for personal and national security deriving from an improper use of Social Media, knowing who the users of Social Media are is of considerable importance, thus it concurs in considerably reducing negative effects for a state’s interests.

scenario no. 3

The third scenario is characterized by a complete absence of any national Social Media strategy, as the potentialities of such tools for national security related purposes are given little thought. A non-coordinated, non-planned and non-optimal use of these tools by national security related organizations follows. Such organizations just cannot see the opportunity side of Social Media, despite carrying out several activities thanks to them. The Internet is absolutely free from every kind of monitoring, control or filter activity, and becomes a place where opponents (adversary states, terrorist groups, criminal organizations, etc.) develop great information warfare capabilities especially aimed at Social Media and can get the best of it.
Ce.Mi.S.S.\textsuperscript{201}

The Military Centre for Strategic Studies (Ce.Mi.SS)\textsuperscript{202} is the body that manages, within and for the Italian Ministry of Defence, the research on issues of strategic nature.

Founded in 1987 by Decree of the Minister of Defence, the Ce.Mi.SS carries out its work by availing itself of civilian and military experts, both Italian and foreign, who are left completely free to express their thoughts on the topics covered.

The content in the studies published thus reflects only the opinion of the researcher and not of the Italian Ministry of Defence.

\textbf{Cap. CC Alfonso MONTAGNESE}

Alfonso MONTAGNESE serves as officer of the Carabinieri corps since 2003. He currently holds the office of Head of the Administrative Unit at 6° Battaglione Carabinieri “Toscana”, Florence. He is a graduated of the University of Rome “La Sapienza” (July 2002), faculty of Political Science, with a political and international course of studies, where he defended a thesis in aerospace law on “Satellite communications interceptions and the Echelon case”.

In December 2010 he obtained a master’s degree in “Intelligence and National Security” at Link Campus University of Malta, Rome, with a thesis on “Intelligence and Strategic Deception, techniques and methods of information manipulation”. He has a good knowledge of English language and basic knowledge of Arabic.

\textsuperscript{201}http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Pagine/default.aspx
\textsuperscript{202}http://en.wikipedia.org/wiki/Italian_Military_Centre_for_Strategic_Studies
Ce.Mi.S. S.

Il Centro Militare di Studi Strategici (Ce.Mi.S.S.)\textsuperscript{203} è l'Organismo che gestisce, nell'ambito e per conto del Ministero della Difesa, la ricerca su temi di carattere strategico.

Fondato nel 1987 con Decreto del Ministro della Difesa, il Ce.Mi.S.S. svolge la propria opera avvalendosi si esperti civili e militari, italiani ed esteri, che sono lasciati completamente liberi di esprimere il proprio pensiero sugli argomenti trattati.

Quanto contenuto negli studi pubblicati riflette quindi esclusivamente l'opinione del Ricercatore e non quella del Ministero della Difesa.

Cap. CC Alfonso MONTAGNESE


Ha conseguito nel dicembre 2010 il Master di II livello in “Intelligence e Sicurezza Nazionale”, presso la Link Campus University of Malta – sede di Roma\textsuperscript{206}, con una tesi sull’ “Intelligence e la deception strategica: tecniche e metodi della manipolazione informativa”. Ha una buona conoscenza della lingua inglese e una conoscenza di base della lingua araba.

\textsuperscript{203} http://it.wikipedia.org/wiki/Centro_Militare_di_Studi_Strategici
\textsuperscript{204} http://it.wikipedia.org/wiki/6%20%C2%B9_Battaglione_carabinieri_%22Toscana%22
\textsuperscript{205} http://w3.uniroma1.it/scpol/default.asp?sec=1
\textsuperscript{206} http://www.unilink.it/