The concepts of "espionage" and "medium" seem to have nothing in common, but there are numerous and obvious similarities between these two subjects. Firstly, both the espionage and the mass media have always existed. In the first case, espionage as a practice used in gathering information about the opponents, was already used by civilizations as Phoenicians, Assyrians and Romans; but the golden age of espionage and of mass communication, (specifically for the new media) is certainly the century in which we are living. Specifically, in the past fifty years, new media have revolutionized the society, as well as spying, that was forced to become a most evolved form of information gatherer, the Intelligence. Both the new media and the Intelligence have an element in common that in espionage and in mass communication was missing: the bi-directionality and the existence of the feedback. The use of new technologies and social networking is based on sharing information among users, as well as today's Intelligence has not just the purpose of finding information, but also the spread of knowledge. During this evolution, two of the fundamental principles on which it holds the democratic society, have encountered: the privacy and the state secret, two elements protected by the law, but put aside everyday more in the name of progress and security. Communication is the basis of democracy, and today the vehicle of communicative media is almost the only instrument for legitimation of leaders, and then impossible to leave aside. Information services are increasingly needed, not to define a war between nations, but to fight a threat far more current such as terrorism. The political power, alone, cannot guarantee security for citizens; when people do not feel safe, try to defend itself, which may lead to pass of laws and institutions. The Intelligence and New Media are materialized by the figures of the spy and the journalist. Even these figures are facing a series of changes, the first one seems not to have the role of the picking of information: since we are in the era of the internet and the open sources provide us many information and news with an overabundance that the collection itself is no longer the objective of espionage. The spy should, then, become analyst, a person who knows how to assess and rebuild the truth starting from many data to analyze (and also often conflicting). The historical figure of the journalist "above the parties" seems to be too obsolete, thanks to the new phenomena of citizen journalism and user-generated content, bloggers are now getting a foothold in the communications system. Media and Intelligence are two satellites of the same planet, the giant planet of the Communicative Democracy: the first one, born in order to communicate the message of the top leaders towards poorly educated low-class, finds ways to communicate in a horizontal way, while the second, born to protect the common people from the oppression of the high enemy army, tries to defend the higher institutions and the sovereignty of powers, against the low-hidden threat of terrorism. Intelligence and Mass Media are double-edged swords of the globalized world. Information processing such as research, sources and analysis are basic procedures of both activities. The research is carried out analyzing the essential elements of information that come from the analysis of the behavior of the subject studied, usually an opponent. These items will be, then, collected, classified and examined. There are three types of Intelligence's sources: the Human Intelligence (HUMINT) is the kind of espionage perpetrated by human subjects, the Signal Intelligence (SIGINT) that works using technological tools such

as radar and sonar signals, and the Open Source Intelligence, the activity of collecting information through the consultation of publicly available sources. After the Cold War, intelligence's military-type was accompanied by the economic one. Both have the aim to minimize the number of victims, reducing human involvement, especially the first one, and this makes them depending on technology. This dependence has caused a series of failures, for example, 9/11 is frequently ranked as the symbol of the American Intelligence's failure, due to the fact that the Unites States had invested too much on technology but too little on training of competitive analysts. In order to understand the role that the Secret Services perform towards the media industry it is necessary to do an overview of the role of information nowadays. You can give basically two different readings on the relationship between Intelligence and New Media, primarily the manipulation, namely the aspect that deals with the production of Information and how it is manipulated by the Intelligence. The second one is the consume, for example how the Secret Services flow from open sources to build an information network. With regard to decision-making, media and information services appear to be economically dependent on government decision-makers, and then subjected to their power. The forms of government and leaders have therefore influenced the communication and the media during the twentieth century, for example, even today the Anglo-Saxon newspapers are considered a sort of fourth power over the parties, while in Continental Europe (where dictators have taken hold during the first half of the twentieth century) the partisanship is a typical feature of the press. Often the information services act as a filter for the media, for instance when they determine which information must be public and which not. Even journalists are mainly focused on the piece newsworthy, exaggerating as much as possible even what seems obvious for the only purpose of attracting the attention of public opinion. The media control over the public opinion comes in part from state control over the media, creating a sort of chain that the latest technologies are questioning. The Citizen Journalism, in the case of the Syrian Revolt but in general in the whole context of the Arab Spring, has questioned the role of the medium of journalism, no longer so necessary, creating unrest in the world of Intelligence who finds difficult to control the information conveyed from the search engines or simply by the citizens themselves through the Social Networks. Open Sources began to be used as an indispensable source only in the years of the Cold War. Later in the 90s the OSINT increased its success thanks to economic globalization and political integration but also thanks to the marginalization of the origin military espionage. Internet, as a communication medium, which is made available to the entire western population, allowing access to a database containing an infinite number of database with an infinite amount of relevant data, has enabled Open Source Intelligence to gain in those years always more relevance. Open sources are easily accessible and requires very little time, it is a useful and flexible resource to which the intelligence services cannot give up. New technologies have also upset the concepts of security and war. Those technologies are now adding a new threat because of the terrorism: the cyberwarfare. It is a politically motivated hacking to conduct sabotage and espionage, a form of information warfare sometimes seen as analogous to conventional warfare. The Cyberwar is becoming increasingly important because if, as we have said, communication is the basis of our society, paralyzing or destroying the media is the easiest, less bloody and less expensive way to harm a nation's heart. The methodologies of cyberattacks ranging from simple vandalism on the web, the collection of data

otherwise secrets, destruction of equipment, servers or software, and finally even the essential services provided by the nations through the most advanced technologies. Cyberterrorism is an “anonymous” weapon, on which the law still has not established a sufficient number of limitations and which requires fewer economic resources. Two examples of cyberterrorism attacks are the Americans “Titan Rain” and “Moonlight Maze”, attributed to Chinese and Russian hackers. In addition, there had been identified several cyber-espionage campaigns such as “Flame”, “Gauss”, “Traveler” and “Icefog”, the highly-evolved malware “Red October”, responsible for having struck many embassies, the operation “Winnti” perpetrated against Gaming Companies, and a number of other viruses and trojans directed against various computer systems, including the one of the nuclear industry, the military one, maritime sector’s one. To defeat these new threats, without override the sovereignty of the people and to create a common definition of what are the new forms of terrorism, intelligence services should spread all the relevant information to the citizenry, rather than hide it. Social networks and web journalism no longer allow people to be excluded from knowledge, in particular, repression leads anyone with sufficient computer skills to bypass the institutions and reach an understanding which would be, otherwise, excluded. Every day more people are claiming the right to be involved in decision-making and political phenomena. International organizations, in this context, should develop a closer partnership than we have now. With regard to the European Union in 2010 was approved the "Internal Security Strategy for the European Union", a document that describes the threats against the security of the continent and established a defense system throughout Europe. Probably the cyberattacks that occurred in Estonia in 2007 and in Georgia in 2008 created the necessity to include cyberterrorism among the most dangerous threats to the nations of the UE, and with it, the importance of raising a barrier of defense in computing. We often talk about intelligence failures, two of the most discussed case studies are most definitely the WikiLeaks case and DataGate one. Activists of WikiLeaks want to establish themselves as propellers of a greater democracy and social transparency, but they have violated numerous laws and this has created a major conflict of ideals: on the one hand, the charges of treason and espionage, on the other hand the contribution to freedom of information. The “DataGate Scandal”, however, has reopened the debate on wiretapping, and the eternal struggle between privacy rights and security rights. Made these assumptions, it is clear that the international community, despite the numerous alliances and the apparent peace, still needs espionage. Every nation needs to defend its interests, but they must work hard to adapt the Intelligence Services to the digital age, and to the globalized world. The first step could be the use of the new channel of “Information Peacekeeping”, a new way to achieve the objectives of national policy without using violence. For what concerns civilians, to have a key to understanding the changes that global society is facing, the use of passive media must give way to public knowledge, and to a global transparency. The Intelligence is evolving day by day along with the role of communication in our society. That’s why it seems necessary for the information to be shared publicly, in order to educate the population and avoid the need to bypass the institutions. In addition, nation-states must adapt to these changes are learning to combat the new threats to national interests with the technologies, without resorting to the use of force.