“The Changing Role of Intelligence Since 9/11: Lessons For Governments, Industry & The Public”

The key element of the theme proposed to me is change and its effects on the necessary adjustment by intelligence services.

The beginning of the change, with the perception of a series of successive alterations to the world order, which we refer generically as the globalization era, lies in the twelve year period from the fall of the Berlin Wall (1989) to the 9/11 terrorist attacks (2001).

In a first phase, the bipolar “Cold War” system was torn down. The system was based on a game of permanent geopolitical and geostrategic checks and balances between two blocs that were presumed rigid and unmoved and where the threats essentially targeted the State and its vital interests. Intelligence activities were focused on espionage, ideological, nationalist and state terrorism and mostly on the tensions that could lead to nuclear holocaust.

Post 9/11 change became astatus quo in itself. The failure of a political, social and ideological model and the multiplicity and speed of transformation, without the construction of new solid world views, popularized different theoretical references, some of them close to the conflict and chaos theories and others which supported the perspective of a supposed perpetual peace.

At the same time, and in our current century, the core idea of change and its speed brought on by new IT and online immediatism, put a special emphasis on a vectorial element for the perception of reality and the future: uncertainty.

The end of this bipolar world, together with a globalizing dynamic, brought with it the dilution of borders and the growing circulation of people and goods. The collapse of the Soviet Union freed the satellite and “sponsored”countries in the so-called third world from political influence that restrained aspirations of real independence. Yet it also had refrained ethnic and religious tensions that maintained an artificial unity, thereby generating conflicts of several types, which led to the setting up of new States, different power relations, a slackening of the control of war arsenals and uncontrolled migration waves. Furthermore, the decline of that which was seen as the “enemy” and the ensuing decrease in the risk of planetary-scale military confrontation led to a weakening of the State and the increase of status of non-state organizations or agents,

which became world players owing to the power of new Information and Communication Technologies.

The threats started to be characterized as asymmetric, diffused, and deterritorialized. And although the so-called "traditional threats" are on the front line of security concerns, such as terrorism, espionage, proliferation and transnational organized crime, these have taken on new transfigurations in their nature, agents, modus operandi and scale; for instance, the fragmented terrorism of Al-Qaida cells, the organized crime clusters that compromise the sovereignty and independence of some States, or the espionage on research, technology and scientific know-how.

All this in the context of the pulverization of the traditional power centers, the emergence of "exiguous" or "failed" States and, on the other side of the coin, the advance of new players with regional or global influence, such as the resurgent and emergent countries, financial operators, multinational corporations, the media, NGOs or knowledge and research centers.

The concept of security also takes on new and various shapes and we talk more and more about human, environmental, international, corporate, or global security and in all these concepts the State loses its core place to the individual, society and citizenship.

New references to the so-called new threats are made, which are uncommon in their nature and scope, namely climate change, pandemics, uncontrolled population movements, humanitarian crises and the scarceness of finite resources, with potential devastating effects on the survival of mankind which go way beyond the geopolitical and geostrategic moves.

Lastly we highlight the emergence of the cyber war and cyber threat concepts, which have become more autonomous, not just with regard to the nature of their threats (in practice they are also attacks between States, terrorist attacks, criminal or sabotage activities) but also because of the technological platform on which they operate, the internet, and their effects, which indelibly mark the security environment.

In a cumulative effect of risk factors associated with the co-existence of the old and new threats and the transformations of those ones, the current insecurity setting also calls for an assessment of more recent trends, namely the radicalization processes in

western societies, social inorganic movements, fragmented violence associated with the so called lone wolves, the tension between the political and the economic and financial powers (with the globalization of operations and growing market sophistication) and the scarceness of world strategic reserves (water, food, energy).

9/11 dramatically confirmed the advent of these new dangers and led to a revision of the security paradigm that had been in force up to then, particularly in terms of a more efficient action by the intelligence services and law enforcement bodies. In fact, the failures that have since then been frequently pointed at the services are mostly due to the incapacity to reproduce in the acting process, i.e. in the intelligence cycle, the adjustments that had to be made when faced with a new threat configuration. And one can also mention a certain neglect of intelligence, given what seemed to be the beginning of the "perpetual peace"period, which started with the imposing of the liberal capitalist model. 9/11 was the strongest denial of this illusion, even though other signs had already been given, such as terrorist acts with special incidence in Africa and the Middle East.

What is the impact of these changes on intelligence services?

The impact occurred on several levels, namely on its structure, operating methodology, relationship with law enforcement and security services, involvement with the civil society and foreign relations.

Please allow me to make a brief reference to what happened in my country, as this shows in some way the transformations which took place.

The present Portuguese Intelligence System was created only in 1984 following a complex trauma that resulted from the dictatorship period, which lasted until 1974, whereby intelligence services were confused with political police. In such an abnormal context, the system imposed onuses and restrictions based on the following:

- Strict control of its activities;

- Airtight partition of the competence on producing intelligence between an internal service (SIS - Security Intelligence Service) and an external service (SIED, at the time SIEDM - Strategic Intelligence Service for Defence and the Military);

- A radical separation between the intelligence production and police activities. Police bodies were strictly forbidden from engaging in intelligence actions and intelligence services forbidden of undertaking any law enforcement acts.

With the emergence of new threats, we quickly realised that this two-faced model, each side looking in a different direction, ran the risk of a limited and static perspective of an essentially dynamic reality, hindering the capability to globally assess phenomena that were increasingly global. In fact, the classic distinction between internal and external security became diluted with the emergence of global actors, as for example Jihadi terrorism or the most virulent forms of transnational organized crime.

9/11 was what set the debate on the intelligence system model, which in Portugal would be changed in November 2004, also as a result of the 3/11 that year in Madrid.

In Portugal there began a period of reflection – widely debated and based on the general principles of better coordination and access to information – on the need to reform the intelligence system. The idea of merging the two services into one was discussed, taking on from similar models, such as the one of our neighbour Spain.

However, this was not the path chosen. Instead, the option came upon an intermediate solution which, for some, offered greater guarantees in protecting citizen's civil and political rights.

The model adopted was conceived with the idea of a merger at the top level of the services, through the Secretary-General, who would coordinate the system. He enjoys leadership powers over the intelligence services' activities and also inspection, supervision and coordination powers. This solution enabled SIED and SIS to run within a framework of a true system, sharing information and avoiding overlapping of their respective activities. They combined their capabilities to face up to foreign threats with an impact on internal security allowing for a coherent and combined effort in foreign relations, directly dependent on the Secretary-General.

The revision of the model under the regulations of the Framework Law enabled also both services to share common departments in the support areas. Accordingly, the internal and external services dedicated themselves entirely to operational activity, i.e.

intelligence gathering, processing and producing. The infrastructure for finances and administration, security, recruitment and training, and IT are shared by both.

The efforts for coordination within the national intelligence system also had implications in the field of cooperation with other bodies domestically, namely through the creation of an anti-terrorist coordination unit, a cooperative structure for the intelligence services and law enforcement.

There was an effort to optimize and rationalize the activities undertaken by SIED and SIS, where they act in a complementary and participatory manner without prejudice to the dynamics of each of them. At the same time, the intelligence services and law enforcement bodies became closer, which also meant an increase in information sharing.

These changes to the general threat framework and the role that 9/11 imposed on the services also implied a new way of relating with civil society.

Even in democratic countries it is traditional for citizens to mistrust the intelligence services, namely when the threat level makes it hard for the average citizen to understand the real utility of intelligence. The Portuguese example also shows this quite well. In Portugal we were only able to reach political consensus to create the services in the 1980's, when we witnessed a round of terrorist attacks of both domestic and international origin. Until then terrorism had been seen as a distant threat because common opinion does not differentiate between field distance itself and the actual proximity of a threat; people find it difficult to perceive the consequences of a failed State to collective security; they do not ponder the effects of a defeat in a faraway land, and when their own country is involved in distant combats, they ask themselves in the name of what are people and resources sacrificed for.

Such an attitude meant that services had to come closer to society in order to provide a better understanding of their tasks and the relevance of their acts. It also implied fine-tuning the supervision and control mechanisms and a closer connection to the media and academia.

The new threat configuration has also been reflected, as I said before, on doctrine, methodology, structure, human resources, priorities, boundaries and exclusivity.

We can highlight the following as essential changes:

Doctrine: an apparent inadequacy of the traditional intelligence cycle, its circular formation and somewhat rigid connection between collection-analysis-dissemination does not respond to the diversification of sources and methods for intelligence collection. There was a search for other solutions, more flexible, in view of the changes in reality, such as the target-centred approach;

Methodology: the use of new communication technologies and an increase in new intelligence analysis methods, such as the competing hypotheses, opportunity and analogy analysis and also the growth of inter-peer control techniques and brainstorming sessions in everyday work;

Structure: the notions of flexibility, resilience, synergy, objective-based work, excellence teams, complementary work, efficacy and efficiency, which have influenced civil service and the economic organizations have also been adopted by the intelligence services, making them less rigid and complex and more adaptable to change;

Human resources: when it comes to recruiting and managing human resources, other concerns have come about in addition to the growing demands from the point of view of formal and academic skills, which are increasingly diversified, the need for ongoing training and the preparation for the use of new IT. These new concerns are emotional, psychological and character traits;

Priorities: the inputs for the development of intelligence activity tend to not come exclusively from the political sphere, which is exposed to growing pressure by the media, public opinion and other institutional partners;

Boundaries: services are increasingly questioned, scrutinized and supervised. Transparency and accountability are imperative in the context of citizens' rights, as well as the growing demands of an open public administration, which places fundamental questions regarding the dividing line between what is restricted and what is public, namely concerning State secret;

Exclusivity: services'openness to the outside in a mutual relation with research centres, universities, industry and citizens has been a slow and sometimes controversial process. Yet it is an inevitable one, with mutual advantages. The

“appropriation”of the intelligence analysis methods by the economic and business circles – we are referring to the expansion of business and competitive intelligence – is an example of this.

Lastly, changes and uncertainty, which should increase, are a fundamental challenge for intelligence, which will be forced to strengthen its prospective side. This will imply a great investment in its capabilities to prevision and scenario planning. Here intelligence shall be judge by the public assessment on its efficacy, credibility and thus its usefulness.

The impacts on its foreign relations context were no lesser.

International cooperation in the field of intelligence is an important part of the response to the new typology of threats and the unpredictability of the international system. The democratic intelligence community understood that the solution to transnational issues calls for an answer on the same level, one that can and must be found in international cooperation, i.e. by sharing intelligence and data, creating relations based on trust and the coordination of efforts, whether at analytical or operational level.

This is seen in the growing number of multilateral fora, the role which intelligence plays in the European Union today or in the reform of NATO’s intelligence system, but particularly in the bilateral relations between services. Even with regard to intelligence structures in countries which in the current strategic panorama are deemed hostile, it is difficult not to find specific areas in which we can or may wish to cooperate, such as terrorism or organized crime.

With regard to the relations at domestic and also at international level it is often said that we are now evolving from a “need to know” stance to a less rigid one, based on the“need to share”. The traditional stance was based on the need to protect the services, which were foremost geared to espionage and counter-espionage activities given the risks of infiltration by the enemy through the nets that had been set up. However, bear in mind that underlying the principle of need to know, there was already a need to share with those who needed to know. The shift in paradigm therefore does not represent an inversion. Rather it means a more open attitude, essential in facing common threats, i.e. the need to know must never overlook the need

to share or knowledge will be an object on itself and will no longer be instrumental in terms of policy requirements.

This need is increasingly felt in an open world where even the individual, due to the endless possibilities offered by the internet, becomes a global player and change adopts a progressively faster pace.

The vastness of the knowledge required in a framework as dilated as this, and where events occur at the speed enabled by new technologies does not allow any organisation, regardless of size or resources, to forego cooperation. The volume of information, the diversity of risks and threats, the variety of contexts, languages and dialects used, the technological capabilities required mean that cooperation among allied services is indispensible for joint action, sharing sources, sharing technical or human resources in specific knowledge fields or even in specialized areas, differentiated so that this know-how can then be exchanged.

It is well known that intelligence sharing is still restricted to the so-called conventional threats and that the scope of international cooperation is always limited by the strategic nature of some threats and need to disrupt these in the name of specific national interests, always involving dynamics that many times dictate that the threats against some States are opportunities for others.

The obstacles cannot be ignored. These range from the level of trust, differences in terms of capabilities of the various agencies and their strategic goals, the diversity in terms of competences and organization models, as well as the participation in regional blocs or the tendency to preserve influence in different regional settings within the framework of protection of strategic interests.

In any case, as I have mentioned, there is a wide field of cooperation which entails or may entail improving secure communications channels, creating early warning systems, intensifying working groups on specific geopolitical and geo-economic issues, acknowledging and sharing best practices, setting up common knowledge parameters, creating fora for discussion among services, creating teams of experts or centres of excellence in the different fields and subjects that the services monitor.

Modern technology of communication make this cooperation a lot easier and naturally it requires the prior definition of areas of common interest, namely on a bilateral level.

The new threat panorama and the new perspective on the nature and evolution of the intelligence services' mission concept imposes that we use specific tools and technologies, whose development will be undertaken by the scientific and industrial research sectors.

The growing need for more security and in more areas has led to a progressive sharing of responsibilities in security matters, the guarantee of which does not fall solely on the State as it used to, yet the State still plays a central role in this. We have been witnessing the transfer of tasks and services that fell to the State before, to private sector entities, including in the field of critical infrastructures. Sometimes these actors have technical and technological knowledge which, due to the level of expertise or high costs is not accessible to the intelligence services. This calls for the setting up of communication channels for fostering cooperation, that must be backed by constant training of intelligence human resources, which will enable an advantageous and secure cooperation to take place.

In the current context, where the strong and global competitiveness requires constant redefinition of plans and strategies, the continued focus on innovation and development, the ability to anticipate changes and the need for permanent identification and response to threats and risks, it is the persistent access to intelligence that can make the difference.

Moreover, the fact that the majority of the activities, whether public or private, rely on technological systems, in most cases connected and interdependent without delimited frontiers and exposed virtually to the same threats and vulnerabilities, requires a joint effort of close cooperation.

Within this framework, it is imperative to conclude that it is proper combination of the two premises –access to knowledge and cooperation – that will allow us to meet the challenges of the future.

The emergence of this reality was in fact strongly reinforced by NATO, following the Lisbon Summit, that created the Working Group IRCSG – Industrial Resources and Communications Services Group – in which the exchange of experiences and sharing of best practices are already a reality, though only aimed at the issues related with the protection of critical infrastructures. We believe that it is precisely this way of close connection that industry followed in the military field –with initiatives like "Pooling &

Sharing" and "Smart Defence", two of the known examples – that industry has also to pursue within the intelligence system.

First off, in matters of cyberspace. Nowadays, the internet is everywhere and present in all our simple, everyday tasks. The web has become a utility whose regulation and control are extremely difficult.

The fact that many socioeconomic activities have become permanently fixed in the virtual realm led individuals and groups taking advantage of the internet to commit illicit acts.

Preventing and combating this type of threat has become a priority for the intelligence services within the scope of State organisation, as cyber threats are one of the main vectors of its activity.

Yet the difficulties are manifold and unparalleled when compared with the so-called traditional threats, namely because the acts carried out on the internet are done so in private property, using an active and passive infrastructure that is mostly held by private entities based in different countries and ruled by different legal frameworks.

Furthermore, the volume and scale of data on the internet make the task of monitoring it in search of early warnings for illicit acts unbearable, not to mention the legal constrains that this would place on most western countries.

In addition, the intelligence services are not strictly technological entities with sufficient technical and human resources to monitor in a satisfying manner all the relevant events on the internet, opening the industry the possibility to act as a platform for the early detection and warning of illicit acts.

This role is of extreme importance in the case of telecommunications industry in general, which includes carriers, telecommunications operators, software suppliers, as well as web active and passive equipment and sector regulators.

The cooperation by industry is pertinent in situations where the monitoring of networks by companies reveal indications of acts being prepared, acts that may endanger our societies' safety and security.

In this field it is necessary to come up with solutions in the near future that involve the intelligence services and industry representatives, in an agile way in order to obstruct such illicit acts and build a free internet, one that is open yet also secure.

At the same time the software industry has an essential role in containing and controlling the growing quantity of data available – in open and semi-open sources – which the intelligence officers are faced with in their day-to-day analytical processes.

The growing use of data structuring as a way of overcoming the analytical burden of huge amounts of data, and the qualitative selection of such data is a challenge that must be dealt with by the specialised industry, which may seek solutions adapted to the specific intelligence needs.

At the same time, over the last few decades States have been obtaining technological instruments, such as satellite technology, spatial applications and nanotechnology, thereby making the most of the innovation and development in the industry.

In this sense, research and development are part of a value chain which, in many cases, leads to innovative programmes such as Galileo, which has enabled the development in the EU of security and humanitarian assistance programmes through cartography (e.g. de-mining, crisis management and planning, ocean monitoring, especially regarding sea transport, coast surveillance, etc).

Technology's contribution enables us to improve on and prevent conflicts and maintain strict surveillance of the potential threats to security in the physical and virtual worlds. Most States tend to develop policies which, using technologies, infrastructure and industrial and technological services foster economic growth, job creation, industrial competition and a strengthening of security beyond the traditional tasks of border control, surveillance of critical locations and facilities and the prevision and following up of crisis management.

Lastly, addressing nanotechnologies is unavoidable (known as horizontal sciences), such as molecular or bimolecular nanotechnology and quantum computing, which may surpass current technological platforms and become a key factor in security and improving quality of life for people, thus becoming one of the States' main priorities.

In this matter of industry, as in others in the past, intelligence services have tried to set up communication channels that enable mutual knowledge, based on institutional respect and mutual assistance, always working towards cooperation for a better fulfilment of their missions. The challenge here is to dare the "common use of capabilities" in areas that may begin by the fruitful sharing of best practices, for example: the use of mutual resources for training and education, the anticipation of new vulnerabilities and threats (where cybercrime is "only" one of the new realities), the identification of new needs and the respective solutions and also participation in the test and validation of new products –all examples of the kind of cooperation that the future will require from us.

The highly technological environment we live in, the swift changes we see, the gigantic mass of information and data we operate with, the lethal aspect, amplitude and versatility of the threats we are faced with, all call for an increasingly greater investment in technological tools and collaboration, and in some cases even association, between the intelligence services and industry, namely with regard to sources of information and analytical processing. In intelligence, the human factor is ultimately the deciding factor. However, without ample use of technological tools, the analyst runs the risk of becoming lost amidst the array of information and its volatility, thereby increasing rather than decreasing uncertainty. All this calls for the need to create communication channels that foster cooperation because in modern societies, exposed to the risks I have mentioned so far, enabled by the infrastructure that makes our life easier, yet also makes us potential targets of threat agents, security itself has become a vulnerable asset. It is many times a scarce one, which cannot be fully guaranteed by the State, which is why all of us, individuals, organisations, corporations, must take on the role of active security agents.

As a conclusion, I feel it is safe to claim that the intelligence services have been an important assistant in decision-making at government level, for the guarantee of States'internal security or foreign defence and notwithstanding some mistakes or bad performances, the success stories – which are kept in the need to know category – are much greater.

Intelligence services, more or less readily, due to their preventive and prospective nature, have been able to monitor the development of the threats, as will be shown clearly in any list of priorities drawn for 2012, or in the diverse nature of

qualifications of the intelligence officers recruited in the last few years, or even in the most used technical resources available to the services.

In these times that we describe as marked by uncertainty, together with practical constraints such as scarceness of resources, there is one certainty that shines through: cooperation, be it national, bilateral or multilateral, with academia and/or industry has become an essential working tool for intelligence services and it is part of our standardmodus operandi.

Júlio Pereira, Secretary-General of the Portuguese Republic Intelligence System.

AFCEA Conference - Brussels – 21 September 2012