GLOBAL SECURITY

AN ONGOING CHALLENGE

The purpose of this programme is to contribute to a better control of State security through a thorough knowledge of all the issues to be identified, analysed and managed over time, enabling the appropriate response to be implemented.

It is necessary to be aware of the potential risks and to control the elements enabling their assessment in order to anticipate, or even prevent them, and to better manage every possible type of crisis.

This training is divided into ***three two-day sessions***, depending on the participants' areas of interest and/or required expertise.

1. **GLOBAL SECURITY, RISKS AND THEIR ASSESSMENT**
2. **MANAGING THE CRISIS**
3. **INTELLIGENCE AND PROTECTIVE TOOLS**

It addresses all the issues enabling participants to adapt the lessons learned to the situations they are in, or may be confronted with, in their natural environment.

Beyond the importance of discussions organised with the Institute's Experts, the group of Participants itself, all experienced professionals from multiple horizons and various countries, represents an exceptional source of interactivity, exchanges and creation of the networks necessary for the implementation of international cooperation, fundamental for effectiveness in the protection of global security.

THIS TRAINING CAN BE TAILORED TO SUIT THE NEEDS OF A STATE AND ITS ADMINISTRATIONS

TRAINING OBJECTIVES

- Improve the strategic design and outlook for global security at a time when the recent phenomenon of migration, the disintegration of certain social frameworks, terrorism and technological risks are disrupting our conceptions, already shaken up by globalisation
- Acquire a theoretical understanding of security issues from a dynamic and potentially operational perspective
- Broaden knowledge and management of risks and dangers, especially the most recent such as cyber-attacks
- Learn to anticipate risks and threats
- Encourage a spirit of international cooperation
- Develop proficiency in communication and information technologies to better assess their impact on global security

SESSION No.1

GLOBAL SECURITY, RISKS AND THEIR ASSESSMENT

Any occurrence of a risk in terms of global security implies that the decision-maker of the response must evaluate the situation very quickly, put it into perspective and then arbitrate, make difficult or even painful choices.

At all times, he/she must be able to weigh each element of the situation in a balanced manner.

This first two-day module allows participants, in a deliberately interactive framework rich with shared experiences, in the presence of recognised experts, to review the different aspects of global security, the multiple risks they could face in the exercise of their duties and to be prepared to choose the right response based on a preliminary assessment weighing the various factors involved.

Security is indeed a complex and interactive world in which a clear grasp of the multiple facets is essential to understanding a problem and providing the appropriate response. Most of the recent failures have been due to a lack of understanding of the type of situation in progress and its direct and indirect consequences.

In modern competition, it is necessary to be able to identify the main types of risks, their interactions and to act quickly by determining the priorities and methods of intervention required.

1
In search of the endogenous and exogenous parameters of global security

This module provides a general overview of the theme of global security within its environment. It forces us to move away from the accepted reality, which is often a mixture of angelism and naivety, to examine the true reality with which the participant will be confronted. It raises awareness of the perception of internal and external risks by comparing countries and areas, referring to the past and present, and integrating the cultural and sociological dimension.

Using international examples, it teaches us how to differentiate between the different types of attacks according to their origin, objectives and methods and how to break down their mechanisms.

It heightens awareness of the globalisation of attacks that are rarely carried out on a single level and encourages reasoning outside any ideology to seek maximum effectiveness in the responses provided.

- Definition of safety and global security
- The direct and indirect cost of security
- Key security risks
- The impact of culture and environment
- Internal and external risks
- Direct or indirect risks
- Criminal attacks

- State attacks
- Pressure from multinational companies
- Pressure from NGOs
- Media attacks

2

The types of risks and their diversity are an additional challenge for global security managers

The risks faced by decision-makers are varied but often closely interrelated. Media, public or political pressure often interpret and orient them while frequently losing sight of their origin, purpose and modus operandi. From recent examples, the participant will discover the fundamentals of each one, and what to expect from them, knowing that war is no longer the continuation of politics by other means because today the Economy is more important.

Special emphasis will be put on the devastating chain of events that occur as a result of a destabilisation strategy or a rupture of equilibrium. The legal or ethical risk will be examined in greater detail in view of its systematic use by certain powers and large companies.

- National and international
- Political
- Economic
- Financial
- Military
- Social
- Environmental
- Technical
- Legal
- Ethical

3

Accurate risk assessment is the essential element in determining the effectiveness of the response

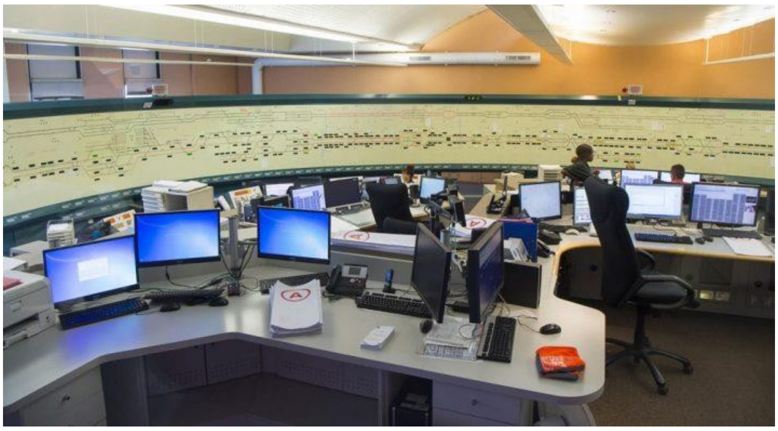
Global security involves identifying a risk in reality or by anticipation. The difficulty for the decision-maker lies in imagining its extent and evolution over time, in assessing its impact at the sectoral or global level, its economic or socio-cultural impact and other interactions.

The participant will be made aware of the positive and negative consequences of the emergence of risks at a local, national or international level.

Through the use of analysis grids and summary charts, he/she will learn to methodically reflect on the consequences and evolution of each risk selected as a problematic. He/she will work on their prioritisation and the different responses to be introduced over time within the framework of the country's or company's policy.

- Assessment of the real risk
- Assessment of potential risk
- Evaluation over time
- The cost of direct and indirect risk
- The media impact of risk
- The political and economic impact
- The international impact
- Risk prioritisation
- The level of response required

SESSION No.2



MANAGING THE CRISIS

The collapse of some State apparatuses in the face of a security crisis is due, for the most part, to the huge gap that exists between its very serious but totally theoretical preparation and drills and the immediate, brutal and often bloody reality of the sudden and unexpected events to be faced.

This second module assumes that the participant has acquired the basic knowledge required to go into detail on the steps and techniques necessary to ensure overall safety at all times.

A first step will be to study the key management principles based on examples from real events around the world.

An in-depth analysis will outline best practices in crisis management at each step of the process and the mistakes to be avoided.

Finally, the participant will be prepared for what is an essential element of crisis management in the modern world: communication in the face of media coverage. Experience shows that in many cases, it is the errors or omissions at this stage that cause the greatest problems individually or collectively.

1

Management of security risks

Once the major risks have been identified, it is crucial that we learn how to imagine their most probable evolution in order to develop a capacity for prospective anticipation.

The secret to combating risks lies in the ability to prepare for them beforehand. This allows us to prepare and organise ourselves in advance by drawing on the modelling of the problem with the input of other experiences and an analysis of our real capacities.

Training can only be carried out in relation to an objective which integrates the present level and that to be achieved. Full-scale exercises are necessary to avoid unpleasant surprises and technical oversights when in the midst of the crisis.

And all professionals know that a crisis is not over when it stops. This is why it is essential to share feedback with all participants in order to analyse its operation, any mistakes made and possible improvements in the event that it should happen again.

- Identification of emerging and potential permanent risks
- National and international development and monitoring
- Anticipation
- The modelling process
- The preparation
- The training
- The organisation
- The action
- The communication
- The analysis and review
- The update

2
Crisis management

The crisis management unit is the place where all the decisions will be made. In this operational centre, the manager plays a vital role that has been fully defined and approved by the appropriate authorities in the confidential crisis plan. Faced with the complexity and multiplicity of issues, he/she cannot address them all and manage them alone.

Each of his/her assistants must properly fulfil their assignment as everything depends on the expertise of specialists in each field. Much is entrusted to these assistants, which implies a clear definition of everyone's role and ongoing direct coordination or through secure means of communication.

The quest for maximum efficiency by first testing the entire process through full-scale exercises. As in military art, strategy is implemented throughout the crisis, but changing circumstances can lead to tactical changes at any time that require the ability to define and manage.

- The management or crisis unit
- The organisation and modus operandi
- Each individual's role
- Assessment tools
- The use of experts
- The use of emergency response forces
- The training
- Transmission security
- Backup of information
- Internal and external coordination
- Responsiveness and constant adaptation
- Ability to react over time

3
Crisis communication

The modern world has become the world of information through the sheer volume available and the speed at which it circulates. Doing well and making it well known has become the key to a positive image, while destroying or damaging that image has become the objective of pressure groups from various backgrounds.

Today, any crisis is first and foremost a media crisis, with everyone exploiting it to serve their own interests. This is why crisis communication has become so important, and it cannot be improvised, whether in terms of objectives and targets or the means to be implemented.

Here again, there is a need for a plan and experts working with a specific goal at the highest level. Analyses of successful or failed communication operations in different types of situations will help to identify the key points to be addressed.

- Formal and informal communication
- Media communication and social networks
- Global and sectoral communication
- Responsibility for communication
- The definition of a single objective
- The strategic communication plan
- The choice of media and social media
- Tactical adaptation of the plan
- Communication organisation
- Defining the role of the participants
- The secure communication link between participants

SESSION No.3

INTELLIGENCE AND PROTECTIVE TOOLS

In the 21st century, Intelligence is the key to global security and its continuous improvement, justified by the relentless evolution of threats.

Effective global security requires a thorough knowledge of all the stakeholders and their environment beforehand. This implies comprehensive knowledge of this operational tool and the ability to use its information and intelligence as quickly as possible.

Security requires the implementation of protection systems downstream to minimise risk by using all the available information. This requires the deployment of sensors for each of the risks identified and an organisation capable of responding in advance or immediately to threats of any kind.

The recent advent of the cyberworld has revolutionised attack techniques and their financial costs. It has multiplied the capacity for data acquisition and storage, which reinforces means of intrusion and diversion, as well as means of defence by using significantly more efficient tools.

This is an area that will become increasingly important in the future. This is why participants will be made aware of the offensive and defensive field of action that cyberspace provides.

1

Intelligence

Intelligence is the major key to strategy. It makes it possible to identify risk factors and then anticipate their evolution based on the internal and external situation.

Its practice and use in understanding the environment and its potential evolution is therefore essential for global security. Acquiring it involves method, leaving nothing to improvisation.

This requires knowledge of the full range of research and analysis capacity for a given issue across public and private services and organisations. Unlike journalism, intelligence is built up over time from sources and cross-referenced information to avoid fake news and misinterpretation.

The use of high-performance tools and the technical skills of analysts make it possible to produce objective summaries that satisfy the expectations of decision-makers. However, they need to be provided as quickly as possible to allow for immediate exploitation.

- State intelligence
- Economic intelligence
- Research objectives
- Research framework
- Research and types of sources
- Networking

- Cross-checking and fake news
- Analysis
- Additional research
- The Summary Report
- Diffusion of information

2
Protection

In the face of adversaries whose objective is to destroy or incapacitate you, knowledge of the enemy or the competitor is not enough.

Protection barriers that are adapted to each problematic must be set up in order to identify, filter or prohibit their attacks. This means keeping up to date with the methods used, which are constantly being revised as a result of technological progress and the inventiveness of public, private or criminal aggressors, and selecting the best defence tools to deal with them.

The protection plan, which is deployed by a coordination centre working directly with all the services and divisions concerned, must ensure that the degree of alert and response capacity is maintained at the optimal level.

- Constant monitoring of attacks around the world
- Analysis and definition of the protection required
- The protection plan and its security level
- The selection of tools and their level of risk
- The set up of a global coordination centre
- The creation of complementary services or divisions
- Identification of the services and divisions that may be used
- The implementation of the protection required
- The training of the various services and units
- Individual and collective training of services and units

3
Cyber security

Today, all States and companies are faced with cyber security issues.
It has become an unavoidable problem that can ruin or destroy a state's computer networks, a company, an image or a policy through ever improved techniques.

The problem is all the more complex because many attacks are not carried out by criminal groups but by States for various but rarely recognised reasons or by companies that do not abide by the law.

The objective of this module is to show participants that the capacity to resist is primordial and is based on a clear definition of the levels of protection and the means to be implemented.

The implementation of these protection systems requires a specific organisation and specialists capable of responding in real time, but the basic principles and capacities of these systems must be known.

Experience shows that the level of security depends on the highest levels of authority because they are costly systems, which must be regularly renewed and are only rarely used: but once is enough to jeopardise everything.

- The use and security of digital technology
- The information risk
- Security of intangible assets
- The different types of attacks
- The cost of attacks
- Resilience
- IT systems protection
- Levels of protection
- Means of protection
- The organisation of cyber security
- The implementation of cyber security