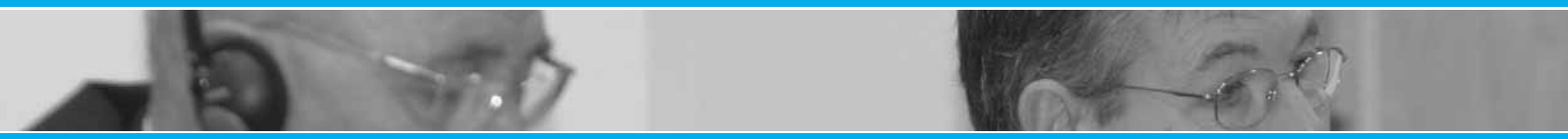
Forum Report on Critical Infrastructure and Continuity of Services in an Increasingly Interdependent World

Compte rendu du Forum sur les infrastructures critiques et la continuité des services dans un monde de plus en plus interdépendant



GCSP

Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

Avenue de la Paix 7bis (WMO/OMM Building)
P.O. Box 1295 . CH-1211 Geneva 1
Tel. +41 22 906 16 00 . Fax +41 22 906 16 49

www.gcsp.ch info@gcsp.ch

FORUM ON CRITICAL INFRASTRUCTURE

FORUM SUR LES INFRA-STRUCTURES CRITIQUES

Conference Report, Geneva, 28 - 29 October 2003

GCSP
Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

Geneva Centre for Security Policy
Centre de Politique de Sécurité,Genève
Genfer Zentrum für Sicherheitspolitik

Designed by Damla Süar, Geneva, info@damlasuear.ch

E

FORUM REPORT ON CRITICAL INFRASTRUCTURE AND CONTINUITY OF SERVICES IN AN INCREASINGLY INTERDEPENDENT WORLD

Geneva, 28 - 29 October 2003

TABLE OF CONTENTS


EADS

1. EXECUTIVE SUMMARY

The Geneva Centre for Security Policy organised a Forum on 28 to 29 October 2003 to address the coordination of planning and security measures in the protection of critical infrastructures across international borders, and between governments and the private sector.

The Forum, the first of its kind, gathered a diverse group of 186 experts from 28 countries representing government and inter-governmental organisations, businesses and academia. The conference was organised by the GCSP with support from several governments and was co-sponsored by Boeing, European Aeronautic Defense and Space Company (EADS), Institut Veolia-Environment, Ilion Security, Société Générale de Surveillance (SGS), Symantec and Thalès.

Concerned about rising threats to essential services, governments and multilateral organisations are proposing new standards, laws and regulations intended to improve infrastructure survivability. The protection of critical services requires coordination across national boundaries and consideration of the potential impact of critical service failures on private industry and the competitive economy. Private corporations have a strong interest in well-designed measures to improve security, because any interruption in service can be financially devastating.

THE TWO-DAY FORUM WAS ORGANIZED INTO THE FOLLOWING PANELS:

1. Risks and Emerging Crises: A Whole New Ball Game
2. What are Global and Regional Organisations doing?
3. What are Governments doing at the International Level?
4. How can Private Companies Interface with Public Sector Policies?
5. Information Network Security
6. Telecommunications Network Security
7. Gas Supply Security
8. Transportation Services Security
9. Security Issues and Nuclear Power Generation
10. Conclusions of the Forum and Plan of Action

Critical infrastructure are key systems and networks the degradation of which would seriously affect the functioning of society. Critical infrastructure is facing ever-increasing and multiple threats. Although there is an awareness of these issues at the national and international level and some important steps have been taken to improve critical infrastructure protection (CIP), much remains to be done. Some critical sectors are better prepared than others.

The Forum reached the following core findings and conclusions:

1. Threats to critical infrastructure are increasing and multiform. They include natural disasters, human errors, and malicious or terrorist acts. Moreover, critical infrastructure is vulnerable due to long supply chains often dependent on transboundary sources; the liberalisation of energy markets; and the instantaneous and direct perception of crisis by the public via media images which amplify the impact. Terrorism is a specific risk.

2. Global and regional organisations are working together in the area of critical infrastructure protection. The ICDO (International Civil Defence Organisation), NATO (North Atlantic Treaty Organisation), the OECD (Organisation for Economic Co-operation and Development), the Council of Europe and the United Nations Economic Commission for Europe are making a considerable effort at conceptual and operational levels.

3. Governments are taking a more proactive approach to CIP. Three examples were discussed in detail: the policies of the European Commission, the United States and the G8. In May 2003, the G8 adopted eleven guiding principles encouraging G8 member countries to create and develop strategies for the protection of their critical information infrastructures.

4. Since 1997, cooperation between public and private sectors has steadily developed through the creation of structures for co-operation by governments by industries and business communities, or jointly. However challenges remain: including the reluctance to share information; a lack of financial incentives; and legal problems.

5. In the area of CIIP (Critical Information Infrastructure Protection) networks, efforts by France, the United Kingdom, the United States, the European Commission and the FIRST (Forum of Incident Response Security) network, which links together 130 computer emergency response teams at the international level, were cited. Since total protection does not exist in information network security, it is important to focus on "resilience" and "robustness."

6. In contrast to the work on information network security, the telecommunications sector appears to be lagging. At the macro level, network security could be improved through placing more importance on international co-operation. At the micro level, network security relies on dialogue and co-operation between the government, the private sector and citizens.

7. The gas sector, which until now has been spared serious problems, will have to tackle challenges linked to Western Europe's increasing energy dependence on outside sources and the liberalisation of the energy market. These factors resulted in more efficiency, but also the separation of supply and transmission activities, thus decentralizing responsibilities.

8. Transportation services security is focusing on reducing vulnerabilities within civil aviation, airports, air traffic, maritime transportation and land transportation. Much remains to be done with regard to maritime control.

9. As regards nuclear power security, terrorist threats include the possible development of nuclear explosives and of radioactive dirty devices, acts of sabotage on power stations and nuclear reactors and on vehicles carrying radioactive material. Vulnerabilities in the information network could be exploited to harm power stations and cause electricity interruptions. The following organisations' efforts were highlighted: IAEA (International Atomic Energy Association); AREVA Group, which operates nuclear power stations in France, UK, and the US; and WANO (World Association of Nuclear Operators), which unites all nuclear electricity operators in the world, public and private (with the exception of North Korea).

10. Despite progress in some areas of CIP, much remains to be done. Public authorities are not always sufficiently open and do not provide adequate information to the private sector; private enterprises do not always have the broader public-interest vision. More research on CIP is needed. Furthermore, it is essential to progress on anti-criminal and anti-terrorist legislation, as well as on the coordination of such legislation at the international level. There is also a need for agreement on which measures to put into place as a priority and how costs could be shared between different parties. International organisations will play an important role in building a consensus on these issues.

11. Finally, protecting critical infrastructure will require a change in perceptions and the creation of a "culture of risk". Civil protection systems should be placed at the same level as traditional defence systems. Authorities should adopt a pro-active approach, capable of "thinking differently" and "thinking the unthinkable". Such a security culture should consider small and medium critical businesses and systems, not just the larger networks. At the micro level, it is important to coach leaders and to encourage individuals to remain vigilant. This should become a "permanent state of mind," especially in the context of daily activities. Finally, it is understood that a zero-risk society is impossible. Therefore, the goal is to make the critical infrastructure system more robust and resilient against attacks and failures which are inevitable.

12. The Forum participants urged the GCSP to build on its first important contribution to the protection of critical infrastructures by organising workshops around specific issues discussed at the Forum.

2. RISKS AND EMERGING CRISES: A WHOLE NEW BALL GAME

The Geneva Centre for Security Policy pursued a double objective with its first Forum on Critical Infrastructure and Continuity of Services in an Increasingly Interdependent World:

- to discuss an important security topic in accordance with its mission; and
- to search for concrete solutions to problems that have practical consequences.

Initial debates in the introductory panel focused on threats to critical infrastructure, national readiness to protect critical infrastructure, and problems which need immediate improvement.

Critical infrastructure faces ever-increasing and multiform threats: natural disasters, the complexity of modern societies, human errors, malicious acts, terrorism and organised crime. In this respect, two examples from the energy sector in particular were highlighted:

a) the unstable nature of oil supply to OECD countries which can be affected by a series of uncontrollable, simultaneous and destabilizing factors, as was demonstrated by the consequences of strikes in Venezuela and Nigeria, harsh winters and war in Iraq. The importance of the role of non-OECD countries in supplying developed countries will increase in the years ahead, making transportation of energy even more crucial and developed societies more vulnerable, especially with regard to terrorist acts; and

b) the liberalisation of the energy market, which has led to the abolishment of monopolies. However, the recent electrical failures which occurred in a number of countries indicated that the market is not the only answer. To succeed in the management of future crises, precise rules of production and transport of energy should be defined as the already difficult process of uncovering new solutions is further complicated by a sociological factor, "not in my backyard".

Public opinion and governments have developed an awareness of the vulnerabilities in critical infrastructure. But results still leave much to be desired.

The United States was one step ahead of Europe as it has developed a central organization for critical infrastructure protection, prompted by the September 11 terrorist attacks. However, work is far from being finished. In Great Britain the government's level of preparedness and capacity of reaction are strong in some parts of the country but uneven in others. In France, considerable progress has been made in intelligence and counter-terrorism, but less so in other sectors.

The main problems in CIP are:

a) lack of international co-operation;

b) lack of comprehensive evaluation of risks at national level where, in addition, some crucial areas remain insufficiently controlled and under-protected;

c) insufficient intergovernmental coordination of funds allocated to these issues and of control mechanisms;

d) insufficient coordination between governments and the private sector, in particular because of the difficulty public decision-makers have in sharing information; not enough resort to incentives;

e) inefficient communication with the public, particularly because governments do not consider the public as mature, even though the public has become more aware of risks, largely due to the media;

f) apprehensive decision-makers, unwilling to address the problems head-on. Their preferred approach is to deny the existence of risks or to look in "the rear-view mirror instead of through the windshield". This attitude, which reflects a refusal to consider what does not fit into the norm, has repercussions when approaching simulation exercises with attempts to avoid "surprises" so as not to scare participants.

3. WHAT ARE GLOBAL AND REGIONAL ORGANISATIONS DOING?

The second panel was composed of representatives of international organizations addressing CIP: the ICDO (International Civil Defense Organisation), NATO, the OECD, the Council of Europe and the Economic Commission for Europe. The panelists provided an overview of their organizations' efforts in CIP. Considerable effort is being expanded on conceptual and operational levels.

a) The ICDO consists of the national civil defence structures of its Member States. It represents a platform for communication, exchange and co-operation. One of its main activities is the standardisation of emergency management procedures. In 2001, the organisation finalised a Framework Convention on Civil Defence. It has been trying for the last thirty years to integrate the private sector into its activities.

b) Two of NATO's divisions are particularly involved in CIP: the Division of Civil Emergency Planning at the operational level and the Committee for the Challenges on Modern Society (CCMS) at the research level. In accordance with its preemptive role, the CCMS addresses problems such as terrorism, the vulnerabilities of interconnected societies, the "prevention and mitigation of societal disruptions" and business and security. NATO countries have established an internal dialogue and reciprocal assistance procedures. In 1998, the Euro-Atlantic Disaster Response Coordination Centre was created, allowing the civilian sector to benefit from NATO's military experience and structures.

c) The OECD's concern with CIP is related to the economic impact of disasters. Japan lost 2% of its GNP because of the Kobe earthquake in 1995; 5% of Turkey's GNP was lost in 1999 with the Marmora earthquake; and because of 9/11, the US lost 1.2% of its GNP. Three of the sectors the OECD addresses were examined: insurance, restoration of telecommunications in countries that are subject to earthquakes, and security in the maritime field. In terms of cross-sectoral issues, the organisation is also concerned with systemic emerging risks, the economic impact of terrorism, and accidents involving chemicals

and their environmental effects. The business community is also involved in these activities.

d) In 1987, the Council of Europe formulated the Partial Open Agreement on major risks. Partial because it is non-compulsory for Member States; open because it is extendable to non-Member States (Morocco, Algeria and Libya have signed). This agreement encourages co-operation in terms of risk management. In this respect, a comparative analysis of legislation is presently being carried out. Furthermore, the Council of Europe is trying to instill a risk culture by promoting academic training in the field, including European Master Degree programmes specialised in training (e.g. disaster-related medicine, science of risk in its legal and social aspects, seismic engineering). It also promotes the notion of risk in civic education in school programmes. Finally, it promotes new technologies that benefit decision-making processes.

e) One of the major activities of the Economic Commission for Europe is to establish infrastructure regulations and standards, and to manage a convention on the transport of dangerous goods as well as a convention on cross-border accidents. In addition, it is actively involved in a project for the development of an early warning system together with the OSCE (Organisation for Security and Co-operation in Europe). It also seeks to involve the business community and society in general into its activities.

Recommendations for better CIP coordination at the international level included:

a) to ensure a better control of existing regulations at national and international levels;

b) to develop a multidisciplinary approach;

c) to work more on textbook cases;

d) to anticipate better;

e) to coordinate better the efforts between international organisations;

f) to comprehend better the differences between countries in terms of culture and approach;

g) to pursue efforts to include the private sector in decision and analysis processes.

4. WHAT ARE GOVERNMENTS DOING AT THE INTERNATIONAL LEVEL?

The third panel considered the role of intergovernmental cooperation on CIP. During the past few years, co-operation between the most developed countries has been reinforced, resulting in an improved political awareness of CIP issues. Work routines are being established, albeit on the basis of different approaches, but focusing on similar issues. Multidisciplinary approaches and the establishment of dialogue between public and private sectors are becoming more common. Moreover, governments are no longer hiding behind a "Maginot line", but are adopting a more pro-active stance based on "communication, coordination and co-operation between all parties" .

The panel highlighted three examples which illustrate these points: the policies of the European Commission, the United States and the G8.

For the past twenty years, the European Commission's policy of coordination and regulatory implementation has been extended in a pragmatic manner. This has occurred: first, in reaction to various crises which took place – the oil crisis of 1974, Chernobyl, Seveso, the Erika and Prestige disasters, 9/11; and second, in reaction to progress in terms of European security construction.

The Commission also sought to reduce risks associated with the opening and liberalising of the energy markets by adopting a series of measures, including the protection of public interest, specific initiatives aimed at small and medium businesses, etc. The Commission has also developed contacts between governments and the private sector as was seen with the organization of Madrid and Rome Forums. Finally, also on the agenda of the Commission is international co-operation, particularly with neighboring countries as Europe remains dependant on them for energy supply.

Taking into account the global interconnection between CIP systems and their security, the United States is encouraging each country to act at a national level, but also to cooperate at an international level. The US is in fact seeking to promote this idea by getting increasingly involved in different structures concerned with the protection of critical infrastructure (G8, the Council of Europe, OECD, APEC (Asia-Pacific Economic Co-operation), OAS (Organisation of American States), UN and WSIS (World Summit on the Information Society). In this respect, the US has pointed to a need for a legal framework on CIP, for national points of contact, for information sharing, for the development of a security culture and for a partnership between public and private sectors.

The G8 has started to address head-on the protection of critical infrastructure. The decision to do so was taken by the G8 Justice and Interior Ministers in Vancouver in May 2002. In March 2003, France and the United States co-sponsored a conference, held in Paris, with the help of G8 groups known as the Rome and Lyon groups which are in charge of the fight against terrorism and organised crime with the support of "cybercriminality" experts. Finally, in

May 2003, the Ministers of Justice and Home Affairs of the G8 adopted eleven guiding Principles (see the attached Annex) encouraging member countries to develop strategies for the protection of their critical information infrastructure at national and international levels. These principles represent the first initiative agreed upon in a multilateral framework for this new area of international security. In accordance with its role as political catalyst, the G8 wishes to encourage the dissemination and implementation of these principles among other multilateral authorities and countries in which infrastructure is less developed and less interconnected, but nevertheless important.

Some speakers highlighted terrorism as one of the major risks for critical infrastructure. A coordinated strategy was needed which would include: seeking to create a global "atmosphere of total rejection" against terrorist attacks, depriving terrorists of their social network, and promoting interdenominational dialogue. The business community could and should contribute to this effort by helping to deprive terrorist organisations from financial resources. Efforts should be made to uncover the underlying motives of terrorist actions and to eliminate root causes.

5. HOW CAN PRIVATE COMPANIES INTERFACE WITH PUBLIC SECTOR POLICIES?

The fourth panel addressed the question of how the private sector could work with the public sector in the field of CIP. The debate on this subject focused on the following points:

1. THE CREATION OF PARTNERSHIPS:

a) During the past few years, the idea of a partnership became obvious for the following reasons: the need for the establishment of responsibilities in the case of an incident; the abolishment of state monopolies; the realisation that security is a concern for the authorities and the private sector; the need to share the limited human resources; and the need for laws and agreements.

b) The US President's Commission for Critical Infrastructure Protection, created in 1996, highlighted in the following months that: information networks represent the foundation of the country's critical infrastructure; the private sector manages 85% of this infrastructure; a dialogue therefore should be established between the authorities and the private sector. To further these goals, a presidential directive called for the creation of government agencies specialised in each CIP sector to ensure co-

operation with the private sector.

c) Since 1997, co-operation between the public and private sectors has developed, with governments and the private sector establishing structures of co-operation at the initiative of one or the other, or jointly.

d) Co-operation between these two sectors becomes somewhat easier when it comes to standardization. This is an area which the public and private sectors are bound to come together and which is of significant importance because it leads to greater security. In addition, ambitious initiatives are currently being taken in this respect (e.g. the United States intends to standardize containers for control and security reasons; the International Labour Organisation's new convention on seafarers' identity documents).

2. DIFFICULTIES ENCOUNTERED IN THE PARTNERSHIP BETWEEN THE PUBLIC AND PRIVATE SECTORS INCLUDE:

a) The private sector is not always aware of their vulnerabilities. They often think that they have taken all the necessary precautions even though this may not be the case.

b) The lack of financial incentives can slow projects as is the case in the United States where security costs cannot be passed on to the consumer.

c) A culture of security has not yet become common practice even when funds are available.

d) Authorities do not always wish to disclose sensitive information even though this would help the private sector orient their efforts in terms of security.

e) Legal problems and disputes can result from information sharing between the public and private sectors (e.g. sensitive information in the trade sector).

f) The legitimate quest for security must not be carried out to the detriment of fundamental freedoms. It is therefore necessary to provide safeguards such as the Commission nationale de l'informatique et des libertés (the National Commission on Information and Civil Rights) in France.

3. RECOMMENDATIONS FOR PROGRESS INCLUDED:

a) With respect to new partnerships, it is necessary to motivate partners, create an atmosphere of trust by sharing non-problematic information, establish rules and criteria, look into the reasons for not wanting to share information, and suggest new models.

b) The authorities must be obligated to ensure the private sector's security at least to a certain level. This approach requires that they place equal importance on civil defence policies as on traditional defence policies. This would require a strategic and cultural revolution. Partnership and co-operation between authorities and busi-

nesses should be established in the financial field for optimal results. Measures which could bring this about include tax incentives, financial backing for research and development, harmonization and sharing on some technical resources (regional centres for electronic surveillance, systematic control of all new employees), debriefing of unusual situations carried out by authorities, common exercises, and the provision of feedback and exchanges between private companies.

c) Even the proponents of the "laissez-faire" approach acknowledged the necessity to rely in some cases on public authorities, for example in order to ensure an adequate stock of critical supplies.

6. INFORMATION NETWORK SECURITY

The fifth panel addressed information network security.

The information sector underpins the whole critical infrastructure. Societies' capacity to respond to crises depends on it. Information network risks are present at both national and international levels. In both cases, those responsible must work together to ensure: early warning in case of a threat; the continuity of services; national security; and proper criminal investigation.

Nevertheless, total protection does not exist. Therefore, instead of "protection" it is preferable to speak of systems' "resilience" and "robustness". The situation improved when CERTs (Computer Emergency Response Teams) were introduced in the 1990s. Also, risk can be diminished by the reduction of "residual" vulnerabilities and an extensive knowledge of computer systems so that the appropriate corrective actions can be carried out in case of virus attacks.

In some countries, considerable effort has been expanded to protect information networks. Great Britain's National Infrastructure Security Coordination Centre addressed the threat to information technology (IT) infrastructure in the context of infrastructure protection which has been considerably developed during the past 30 years in its fight against terrorism. The centre is responsible for investigating threats, preparing responses seeking close co-operation with the private sector, and carrying out research (see http://www.nisc.gov.uk). In the case of IT infrastructure, the Centre's CERT works in coordination with CERTs in other countries.

In the United States, the Homeland Security Department has been set up with an agency responsible for network security similar to the one in the UK (see http://www.cybercrime.gov). Criminal investigation and sentence administration are two other aspects adequately addressed with a good level of coordination between the two sectors. At the instigation of the G8, 34 countries started to reflect on these issues.

The European Commission's Information Society Directorate-General is developing coherent policies in this area. The main initiatives are regulatory framework and research. The Commission is also concerned with external security and will launch a pilot research project in order to improve coordination between different institutions in case of crisis. The European Parliament is considering the creation of a security agency for information networks in order to strengthen good practices, facilitate co-operation between private and public sectors, and to facilitate data and information exchange. In addition, a framework decision on cybercrime is under consideration to provide common definitions which should facilitate the work of the police and judicial authorities.

After the failure of the Eurocert project in 1990, Europe is also seeking to strengthen its coordination at a more technical level. "Task Force CERT", an attempt to ensure a higher level of trust has been developed and a list of incident response teams has been drawn up.

At the international level, a network called "FIRST" (Forum of Incident Response Security) brings together 130 CERTs which includes 59 from the public sector and 69 from the private sector, with 71 located in North America, 48 in Europe, 7 in the Pacific region and 5 in Latin America.

ADDITIONAL EFFORT IS NEEDED, INTER ALIA, IN THE FOLLOWING AREAS:

a) to extend the efforts made in the developed countries to the rest of the world;

b) to maintain safeguards for civil liberties;

c) to modify incident analysis methodology by emphasising trans-sectorial, trans-disciplinary and inter-ministerial approaches (i.e., the Federal Polytechnic Institute in Zurich has developed an inter-disciplinary master's degree specialised in "risk engineering and management");

d) to adopt an innovative way of thinking, learning from past experiences;

e) to develop the structures needed at the international level;

f) to develop a public-private partnership and co-operation with academic and research sectors.

7. TELECOMMUNICATION NETWORK SECURITY

The sixth panel highlighted recent developments in critical telecommunication network protection:

The communication sector has developed rapidly in the past five years in respect to technology and the elaboration of regulations. The network operator's task has become increasingly complex because they have to manage the relationship between several parties: the State, their partners, their clients and the other operators. In addition, companies have become increasingly vulnerable as they are managed via internet. Lastly, there is no overview of the problems. Some assert that many of the

remedial procedures used in the case of the Millennium Bug are still valid. Others argue that it is impossible to apply past solutions to an entirely new set of problems.

One of the main concerns is to provide uninterrupted service or at least to reduce interruptions to the fewest incidents possible. Service must be restored as fast as possible when there has been a disruption. It is necessary in this case to resort to constant monitoring and to back-up plans, an area in which progress is required. In this respect, the relationship with other operators is crucial. Contacts are not always constructive in the strong competitive environment. Coordination with regulators is also essential, yet they are more preoccupied with competition than with security problems. However, following the devastating earthquake in Algeria in 2003, the mobilisation of operators was a success (5 major submarine cables were severed; the whole country, part of the Maghreb and another dozen countries right up to Asia were affected). Some 60% of the services were restored in three days and the cables were repaired in a month.

Network security depends on dialogue and co-operation between the different parties involved: the government, the private sector and the citizens. In this respect, an independent institution in Great Britain, the Information Assurance Advisory Council (IAAC), was presented as a model. This was also the case for the Directors Information Insurance Network which aims to increase the awareness of company decision-makers.

Emphasis was also placed on the importance of international co-operation which was effective at the time of addressing the Millennium Bug. Large regulatory organisations such as ICAO (International Civil Aviation Organisation), ITU (International Telecommunication Union), IAEA and WANO mobilised their resources. The same was the case for large multinationals (Hewlett-Packard, Shell, etc.). For example, governments followed the example of Florida which created its own international network. The idea of creating a specific organisation to address cyber security has been considered unnecessary, except maybe at a technical level. The United Nations General Assembly has adopted several resolutions on the subject, but not much has been done in the establishment of norms. The Summit on the Information Society was expected to address that question.

8. GAS SUPPLY SECURITY

Focusing on the question of gas supply to Western Europe, the seventh session started with a warning. To date, Western Europe has not encountered any problems in this respect. However, there was no guarantee that this would continue in the future. The discussion highlighted the following points:

Gas supply was already complex and the complexity will increase in the future; radical changes were underway due to the liberalisation of the gas market.

Gas resources were plentiful at a global level. They were however restricted to a certain number of countries. In

addition, there were technical rigidities: point-to-point delivery systems without excess capacity; the lack of long term investment planning; and short-term market volatility which could send the wrong signals to investors. Production in Western Europe was limited at best. Europe therefore had to turn more and more towards outside suppliers (Russia, Caspian Sea, Middle-East, Algeria, Nigeria, Latin America). This situation would lead to more expensive investments and increase technical and political risks. The East-West Energy Corridor which crosses the Caucasus via Georgia was reassuring. It was necessary however to go further. The new global landscape created by 9/11 has added to the instability.

The gas market liberalisation in the European Union benefited the consumer and provided more efficiency. It presents, however, a new challenge. Previously, the environment was stable: companies offered integrated services and were responsible for both gas infrastructure and supply; co-operation existed between companies; and long-term contracts provided stability. Since liberalisation, the sector has become complex because of the separation of supply and transmission activities and responsibilities.

SUGGESTIONS TO ENSURE THE SECURITY OF SUPPLIES WERE PUT FORWARD:

a) Forecasting and coordination efforts.

- A global computer model for testing scenarios and directing investments to avoid a possible domino effect does not exist.
- However, the IEA (International Energy Agency) has a global view of the supply and demand of energy and a model to forecast needs. The IEA also has a regional and local view of the specific strengths and weaknesses of the markets. In addition, the IEA has developed forecasting ability for energy investments, particularly for gas and has created a task force on natural gas which brings together all parties involved.
- Other organisations and some countries have developed similar capacities. Every year, the EU asks each member country to review its needs in terms of gas supply and infrastructure. France conducts an identical assessment. diversify supply sources and transportation routes.

b) In security of external supplies, there is a need to:

- encourage investments in infrastructure;
- continue to develop long-term contracts;
- seek to establish stronger links between supply, transit and consumer countries by encouraging risk sharing plans and joint ventures;
- diversify supply sources and transportation routes.

Reorganisation of the internal market, in general, represented viable solutions for the European Union. However, it was especially necessary:

- to secure a clear reallocation of responsibilities between the different actors in the market, such as producers, suppliers/transporters, energy storage companies, and between national authorities;

- to ensure a safe and efficient functioning of the network and its long-term development;

- to take into account the differences between member countries in order to avoid market imbalances;

- to reinforce co-operation between the public and private sectors;

- to maintain and possibly strengthen existing security measures in order to be prepared for technical risks, political risks and also for possible terrorist threats.

9. TRANSPORTATION SERVICES SECURITY

The eighth panel raised the following issues regarding transportation services security:

9.1. VULNERABILITIES:

A) CIVIL AVIATION, AIRPORTS AND AIR TRAFFIC

Commercial aviation is a global and complex system, comprising airports, air traffic, and aircraft. All three must be equally protected. These are highly symbolic targets especially in the case for airports which represent the sovereignty and commercial strength of a country.

- The consequences of an attack or a disaster can affect the economic activities of a country or a region.

- Protection must be ensured domestically and across borders, and must include information technology and telecommunications. In addition, it must be applied to passengers on planes and in airports as well as luggage and containers.

- The 9/11 attacks put all dimensions of air transport security into question, including upstream intelligence, protection of the planes and air traffic control. However, although zero degree risk does not exist, the measures taken over the years have ensured a very high level of security.

B) MARITIME TRANSPORTATION

- The 9/11 attacks also provided cause for concern regarding maritime transportation. Some countries such as France developed protection plans (Vigipirate, Vigimer). This was also the case for the EU. In July 2003, strong US pressure prompted the IMO (International Maritime Organization) in July 2003 to enact measures similar to the ones adopted in the area of civil aviation.

- The measures adopted are global and applicable to both ships and ports. Ships can represent a target as such (e.g. Achille Lauro in 1985). They can also represent a ve-

hicle and a threat as such because of their cargo (transport of noxious goods; spare parts of explosives or a nuclear device used in an attack) or because of their location (a gas tanker explosion near a town, or a ship in the middle of a strait (Ormuz, Pas de Calais).

C) LAND TRANSPORT

➽ The Channel Tunnel was discussed including the different kinds of transport involved (individual transport; freight lorries; public transport including underground and trains).

➽ The Channel Tunnel has various characteristics. First, it has a very strong symbolic value. It also forms an essential physical link between the British Isles and the European continent and between two countries which are subject to internal terrorist threats. Finally, it represents an example of private-public partnership between two governments and a company (Eurotunnel).

➽ The Channel Tunnel also brings together various kinds of traffic which make it a very complex system and which represents a number of risks: TGV "Eurostar"; freight trains (containers), Eurotunnel shuttles (lorries, coaches, cars). Moreover, access to the site represents an additional risk.

➽ Specific measures were agreed upon in the 1986 treaties on security, granting the two governments specific powers with regard to the company (a joint committee on French-British safety was set up). Gradual gaps in security measures were highlighted and corrected.

9.2. POSSIBLE IMPROVEMENTS:

a) Security has to be considered from a global point of view. At the same time, not everything can be fully secured, partly because of technical impossibility and partly because it is not necessarily appropriate. Remedies must be considered based on statistical probability of risk, and choices must be made accordingly. The creation of a "global security fund" should become a priority. It is also essential to determine the response in real time to the impact of an incident.

b) The rationale which underlies terrorist acts is difficult to comprehend as it relates to unfamiliar values. Predicting terrorist acts is also difficult. Greater awareness of signals of terrorist acts should be developed. Financing and resources cannot always be mobilised. The best remedies are prevention (local or international intelligence) and dissuasion.

c) Control of passengers is carried out at several levels: identity check through visas, physical check before boarding, etc. Generally, more significant data banks are available and linked to each other (Schengen II, system for European visas, etc.). However, the terms of reference which govern the transmission of information should be improved. There is also the risk of reaching a saturation point. In addition, since 31 December 2003, some airports are complying with new regulations and have been checking all luggage. However, other airports have not done this yet and have asked for an extension of two years to put the new regulation in effect.

d) With regard to maritime control, much remains to be done. By July 2004, ship operators will have to fulfill many conditions relating to administration (security plans to be established and approved by authorities, etc.), purchase of equipment and personnel recruitment. Constraints will be stronger at port level, but entire port facilities must be secured as well.

9.3. ECONOMIC IMPACT:

a) For civil aviation, the costs resulting from 9/11, Iraq and SARS (Severe Acute Respiratory Syndrome) have been considerable: 30,000 job lay offs in Europe and a loss of 25 billion US dollars in sales. 9/11 cost New York City 140 billion US dollars which is the equivalent of the Homeland Security Department budget for four years, the second largest federal budget in the United States after defence. The global economy also suffered.

b) Security measures at Paris airports cost 230 million euro a year with a 1.5 billion euro turnover. Airport taxes have increased considerably everywhere.

c) Passengers understand the need for the security measures. However, there should be more transparency on the way airport taxes are used with indications on the percentage allocated to security.

d) Security has an impact on competition between airports, ports and between transport modes.

9.4. SECURITY POLICIES:

a) The state evaluates threats and advises the private sector on measures to adopt, especially in the case of companies providing public services. The private sector implements these measures without knowing exactly the threat. The gap between those who evaluate and those who implement should be bridged. For this, the available information should be shared and an efficient strategy developed.

b) Security is one of the state's sovereign duties. Therefore, it would be fair to assume that it could bear the associated costs, at least in part. It would also be useful to reflect upon associated security measures to be disseminated among different parties concerned instead of being centralised.

10. SECURITY ISSUES AND NUCLEAR POWER GENERATION

The ninth panel, consisting of an equal number of nuclear power regulators and operators, focused on the following points: the effects of the terrorist threat on risk management, the resources available for security reinforcement, the importance of trust in risk management and the development of co-operation at the international level.

The terrorist threat could take on various forums: development of nuclear explosives and of radioactive dirty devices, acts of sabotage on power stations and nuclear reactors or on vehicles carrying radioactive material. Three major challenges were identified: proliferation, theft and sabotage. More than ever, the production of nuclear energy required the establishment of international safeguards and robust security.

In this respect, the IAEA has launched a global programme which aimed to address nuclear security issues for both energy supply and infrastructure. It covered the following points in particular: appropriate physical protection of nuclear products and installations including their transport; inspection of radioactive products; detection and prevention of illicit traffic; integration of security systems for maximum benefit; and implementation of emergency response plans. Whereas these principles were shared, there was not yet a global solution applicable to each country. Within a state, the responsibilities were specified as follows: the authorities establish the requirements and monitor their implementation; operators were responsible for security and safety.

Two other types of risk were noted: IT risks for power stations which were more important in the United States than in Europe where access to the Internet was more limited, and the risk of electricity interruptions which should be better examined at the international level.

In terms of the physical protection of nuclear power stations, Switzerland's example was highlighted. Nuclear power security was reassessed after 9/11 to take into account the risk of blackmail or attacks by suicide planes. The result of this reevaluation was presented to the mass media in April 2003.

The AREVA Group offered a particularly interesting example in which security and safety were integrated and taken into account at all levels as both types of management are in fact similar. Safety relates to the containment of radioactive material in case of an accident, fire, radioactive leaks and earthquakes. Security relates to physical protection, nuclear power plant layout and on the control processes at an operational level.

As the operator of nuclear power stations in France, Great-Britain and the United States, AREVA also controlled the entire nuclear fuel cycle through its subsidiary Cogema. With its subsidiary Framatome, it was also providing nuclear power plant design. The management of security and safety for power stations also had to include the management of the human factor, which presented the most uncertainty. In general, resources devoted to security were inferior to the ones devoted to safety. This was quite natural: the nuclear industry remained a high-risk industry despite the progress made. Nonetheless, the sector's security record was superior to others, such as the chemical industry or the transport sector. Finally, the distribution of security and safety costs between operators and authorities should be considered further.

Good risk management also requires constructive and transparent dialogue between operators and regulators.

Operators needed regulators to define risks and threats in a plausible manner in order to determine measures to be established. What could reasonably be done by operators and what should rest within the competence of the authorities, at the financial, legal and technical levels, must be established.

Operators always work within a statutory framework. For this to be possible, however, the system must be stable and implementable. Operators must be part of the decision process when the authorities identify risks and define remedies. Operators have a culture of security. They represent therefore good interlocutors for the authorities with whom a constructive dialogue could be established.

The role of international co-operation in the reinforcement of security for nuclear installations was crucial. Three points were highlighted in this respect:

a) The concerns of the international community and IAEA in terms of security in the nuclear area had gone through several phases: in the 1960s there was a need to counter the danger of nuclear arms proliferation; in the 1980s and 1990s, risks related to traffic, blackmail and attacks; after 9/11, the emphasis was on the risk of sabotage.

b) Developments started in 1999 when the IAEA debated the issue, leading to recommendations to include in the 1980 Convention on the physical protection of nuclear material the resources necessary for tackling the problem. At the same time, a group of five countries (France, Great-Britain, Belgium, Sweden and Germany) was formed in order to exert a decisive influence on this question and to press for a revision of the activities of international agencies in terms of protection and assistance. Later, three other countries joined the group (Switzerland, Spain and Finland) which became the group of "eight". A series of twelve principles aiming to govern the protection of installations and nuclear material was finally put together and is still to be adopted as an amendment to the 1980 Convention.

c) International co-operation is needed for assistance in the security of nuclear installations. This concern appeared in 1998. Large countries provided assistance at a bilateral level or through conferences and international workshops. This concept is however encountering certain difficulties: the threat to the environment varies from one country to another; the confidentiality necessary for avoiding information leaks does not go hand in hand with the transparency always required for the transmission of knowledge and the willingness to impose standards at the international level.

International co-operation in terms of safety led to the creation of WANO (World Association of Nuclear Operators) in 1989 following the Chernobyl accident. This organisation is independent of governments and regulators. It unites all nuclear electricity operators in the world, public or private, with the exception of North Korea. It aims to reduce risks in the nuclear industry by encouraging information exchange, communication, comparison and emulation between members. Real improvement in terms of safety has been made on all fronts during the past few years. However it is important to continue to develop a "culture" in this area as accidents are not due to

inevitable circumstances, but are due to gaps in the safety culture. The events of 9/11 had an impact on the WANO Paris Center: in the autumn of 2002 the Governing Board held a session, without keeping minutes, on studies performed and measures taken to further improve plant security, already extremely high; the organisation was looking into establishing common lists of experts with the IAEA, so that visas and access to power stations, more difficult to obtain in some countries since 9/11, can be facilitated for WANO experts.

11. CONCLUSIONS OF THE FORUM AND PLAN OF ACTION

1. The following general trends in the area of CIP were noted:

a) A growing number of risks had increased the "uncertainty threshold" in our societies.

b) As these risks, threats and targets were all interconnected, a strong interdependence was created at a global level.

c) Universal requirements for security emerged as public opinion had become more aware of the situation.

d) Terrorism gained prominence because of its significant effects and mass impact, "wrestling" with modern society.

e) A significant role could be played by cultural features and organisational practices, i.e. the human factor, when past achievements were relied upon instead of the necessary tests being undertaken to understand what went wrong; when the existence of organisational barriers would prevent information from circulating as it should; when a management team was incapable of integrating and controlling each of the overall elements; when informal chains of command operating outside the normal organisational rules would appear and further complicate the whole process.

f) Considerable progress had been made in the protection of information infrastructure at the G8 level and also at national levels in France, the US and the UK. Undoubtedly much still remained to be done, but as these sectors were well defined, the task was easier than in others. However, in all areas considered together, international co-operation remained largely insufficient. This also applied to dialog between authorities and the private sector where respective responsibilities were often not well defined. Considerable effort was also needed in research. Progress was needed on anti-criminal and anti-terrorist legislation, as well as on the coordination of these legislations. Also, measures required and allocation of costs between different parties should be addressed.

2. Some incorrect approaches were highlighted:

a) Continuing to spend time on definitions and theoretical research projects.

b) Getting caught up in tactical considerations rather than establishing a strategic direction in the first instance.

c) Circulating the problem yet again between "37 new bureaucracies and 37 coordination bodies".

d) Giving more importance to technology and overlooking the human factor.

e) Promoting answers for "public relations" rather than for substance.

f) Giving in to paranoia after having denied the problem.

3. Bearing in mind that extraordinary issues call for extraordinary solutions and require a global approach, the following initiatives were suggested: "a change of mentality", "thinking differently" and "thinking the unthinkable." Therefore, it was necessary:

a) At a general level,

- to place CIP on the agenda. A "World Economic Forum" exists. Why could there not be a "World Resilience Forum" which would bring together director-generals, give authorities as well as the private sector an equal voice and which would include NGOs? This would provide an opportunity to explore new ideas, particularly through experience sharing;
- to focus on subjects that could mobilize public opinion: i.e the protection of major cities, channels of communication, etc.;
- to remember to take into account small and medium-size businesses, as only larger networks tend to be considered.

b) At an individual level,

- to press leaders (especially ministers and director-gen erals) to face the real issues;
- to encourage immediate debriefing after a disaster;
- to encourage people to remain vigilant. This should become a permanent state of mind, especially in the context of daily business activities;
- to carry out unconventional simulation exercises;
- to encourage think-tanks to work together on practical issues (e.g. crisis management in real time) rather than on theoretical questions.

4. The Forum participants urged the Geneva Centre for Security Policy to build on its first important contribution on the protection of critical infrastructure by organising workshops around specific issues.

ANNEXE I

FORUM ON CRITICAL INFRASTRUCTURE AND CONTINUITY OF SERVICES IN AN INCREASINGLY INTERDEPENDENT WORLD

PROGRAMME

TUESDAY, 28 OCTOBER 2003

08:00 - 09:00 REGISTRATION AND COFFEE

09:00 - 09:15 WELCOME & OPENING

- **Ambassador Gérard Stoudmann**, Director, Geneva Centre for Security Policy
- **Senator Paul Girod**, Chairman, Haut Comité pour la Défense Civile, Paris
- **Prof. François Heisbourg**, Director, Fondation pour la Recherche Stratégique, Paris, Chairman of the Foundation Council, Geneva Centre for Security Policy, Chairman of the Council of the International Institute for Strategic Studies, London

09:15 - 09:30 OPENING KEYNOTE ADDRESS:

Mr. Claude Mandil, Executive Director, International Energy Agency, Paris

PLENARY SESSIONS

09:30 - 11:00 RISKS AND EMERGING CRISES: A WHOLE NEW BALL GAME

Moderator: Dr. John Gault, President, John Gault S.A, Geneva and Associate Member of the Faculty, Geneva Centre for Security Policy

Panelists:

- **Mr. Alain Bauer**, Criminologist and Consultant, AB Associates, Paris
- **Mr. Mike Granatt**, General Director, Government Information and Communication Service (GICS), Cabinet Office, Former Head, Civil Contingency Secretariat, London
- **Mr. Jean-Philippe Grelot**, Groupe d'experts du G8 , Chargé de mission « Protection et Sécurité de l'Etat », Secrétariat Général de la Défense Nationale, Paris
- **Dr. Patrick Lagadec**, Director of Research, Ecole Polytechnique, Paris
- **Dr. Erwann Michel-Kerjan**, Center for Risk Management, The Wharton School, Philadelphia
- **Mr. Daniel B. Prieto**, Fellow, Council on Foreign Relations and Professional Staff, Select Committee on Homeland Security, U.S. House of Representatives, Washington D.C.

11:00 - 11:15 COFFEE BREAK

11:15 - 12:45 **WHAT ARE THE GLOBAL AND REGIONAL ORGANIZATIONS DOING?**

Moderator: Dr. Terrence Kelly, Senior Operations Researcher, Rand Corporation, Pittsburgh

Sub-panel # 1: INTERNATIONAL CO-OPERATION

- **Mr. Pascal Gondrand**, Private Secretary, Head of the Information Department, International Civil Defence Organisation - ICDO, Geneva
- **Mr. Jean Fournet**, Assistant Secretary-General for Public Diplomacy, NATO, Brussels
- **Mr. Barrie Stevens**, Deputy Director of the Advisory Unit to the OECD Secretary-General, OECD, Paris

Sub-panel # 2: REGIONAL CO-OPERATION: ONE EXAMPLE - EUROPE

- **Mr. Jean-Pierre Massué**, Executive Secretary, EUR-OPA Major Hazards, Council of Europe, Strasbourg
- **Mr. Geoffrey Hamilton**, Regional Advisor, United Nations Economic Commission for Europe, Geneva
- **Col. Giuliano Porcelli**, Expert, Department of Civil Protection, Italian Presidency of the Council of Ministers, Rome

12:45 - 14:15 WORKING LUNCH

Mr. Pierre Maciejowski, CEO and Managing Director Thales Security Systems, **"From Biometry to NBC detection: key technologies in a system for critical infrastructures protection"**, Thales International, Paris

14:15 - 15:30 **WHAT ARE THE GOVERNMENTS DOING AT THE INTERNATIONAL LEVEL?**

Moderator: Ambassador André Lewin, First Vice-president, Académie Diplomatique Internationale, Paris; former French Ambassador to Guinea - Conakry, India, Austria, Senegal-Gambia; Spokesman for Mr. Kurt Waldheim, former Secretary-General of the United Nations, New York

Panelists:

- **Mr. Philippe Meunier**, Sous-Directeur de la Sécurité, Direction des Affaires Stratégiques, de Sécurité et du Désarmement, Ministère des Affaires Etrangères, Paris
- **Mr. Christopher Painter**, Chair, High Tech Crime Subgroup of the G8 (Lyon Group), and Deputy Chief, Section on Computer Crime and Intellectual Property, U.S. Department of Justice, Washington D.C.
- **Mr. Joseph P. Richardson**, Senior Foreign Affairs Advisor, International Critical Infrastructure Protection, US Department of State, Washington D.C.
- **Mr. Helmut Schmitt von Sydow**, Director, Conventional Energies, European Commission, Brussels
- **Mr. Alexander Zmeevsky**, Director, Department on New Challenges & Threats, Ministry of Foreign Affairs, Moscow

15:30 - 15:45 COFFEE BREAK

15:45 - 17:15 HOW CAN PRIVATE COMPANIES INTERFACE WITH PUBLIC SECTOR POLICIES?

Moderator: Mr. Howard A. Schmidt, Vice-president, Chief Information Security Officer, eBay Inc., Campbell, California; Former Chief Security Officer, Microsoft Corp., Chairman of the U.S. President's Critical Infrastructure Protection Board; Former Special Adviser, Cyber space Security at the White House, Washington

Panelists:

- **Mr. Daniel Bircher**, Head, Process and Information Security, Ernst Basler + Partner AG, Zollikon/Zurich
- **Mr. Aled Miles**, Vice-president and Managing Director, Symantec Northern Europe, UK
- **Mr. Kyle Olson**, President, Community Research Associates, Inc., Alexandria, Virginia
- **Mr. Michael Stepek**, Attorney at Law, Solicitor to the Supreme Court of England and Wales, Winston & Strawn, Partner, Geneva
- **Mr. Christian Sommade**, Development Director, Defence & Security, Cegelec Group; Member of the Security Commission of GITEP-EDS (French defence and security industries association - telecommunication and electronics systems); Secretary General of the French High Committee for Civil Defence & Domestic Preparedness, Paris

19:30 - 22:30 DINNER & ADDRESS AT THE ARIANA MUSEUM

Rt. Hon. Mike Moore, member of the Board of Directors, Société Générale de Surveillance Holding S.A., Geneva; former Prime Minister of New Zealand; former Director General of the World Trade Organisation, Geneva

WEDNESDAY, 29 OCTOBER 2003

08:15 - 08:45 SIDE EVENT

"Current risks and threats of computer hacking and innovative long term solutions for large organizations and governments" by **Mr. Marco Ricca**, Partner, ILION Security SA, Geneva; Researcher at Hewlett Packard Trusted Systems Lab, Bristol; Researcher at Security and Cryptography Laboratory, Ecole Polytechnique Fédérale de Lausanne (EPFL)

09:00 - 09:15 OFFICIAL SESSIONS

"Supply-Chain Security Issues" by **Mr. Sten Bertelsen**, Vice-President, Trade Assurance Services, Société Générale de Surveillance Holding S.A., Geneva

09:15 - 10:30 PLENARY SESSION

INFORMATION NETWORK SECURITY

Moderator: Mr. Christopher Painter, Chair, High Tech Crime Subgroup of the G8 (Lyon Group); and Deputy Chief, Section on Computer Crime and Intellectual Property, U.S. Department of Justice, Washington D.C.

Panelists:

- **Mr. Ted Barry**, Manager, Private Sector Outreach, UK National Infrastructure Security Coordination Centre (NISCC), London; G8 "CIIP Experts Group"
- **Mr. Michel Dupuy**, Groupe d'experts du G8; Head, Computer Emergency Responses Team/Administration, Secrétariat Général de la Défense Nationale, Paris
- **Mr. Jan Lundberg**, Strategic Analyst, The Swedish Emergency Management Agency (SEMA), Stockholm
- **Dr. Jan Metzger**, Senior Researcher, Center for Security Studies, ETH Zurich, Zurich
- **Mr. Andrea Servida**, Head of Sector, Directorate General Information Society, Trust and Security, European Commission, Brussels

10:30 - 10:45 COFFEE BREAK

10:45 - 12:30 PARALLEL SESSIONS

Session I: TELECOMMUNICATION NETWORK SECURITY

Moderator: Mr. Eduardo Gelbstein, Independent Advisor, Senior Special Fellow, United Nations Institute for Training and Research, Geneva

Panelists:

- **Mr. Jean-Louis Blanot**, Deputy Director for Administration, Directorate of Security and Information, France Télécom, Paris
- **Ms. Olivia Bosch**, Senior Research Fellow, New Security Issues Programme, Royal Institute of International Affairs (Chatham House), London
- **Mr. Neil Fisher**, Vice Chair, Information Assurance Advisory Council (IAAC); Macro Security Capabilities Leader, QinetiQ, Malvern, UK
- **Mr. Hugo Straumann**, Security Manager, Swisscom Innovations, Swisscom AG, Bern

Session II: GAS SUPPLY SECURITY

Moderator: Mr. Nordine Ait-Laoussine, President, Nalcosa; former Minister of Oil, Algeria

Panelists:

- **Mr. Giorgi Vashakmadze**, Chairman, Sub-committee of Eurasian Corridor, Parliament of Georgia; former General Director, Georgian International Oil Corporation, Tbilisi
- **Ms. Sylvie Cornot-Gandolphe**, Principal Administrator, Gas Expert, International Energy Agency, Paris
- **Mr. Philippe Mannoni**, Executive Secretary, Gas Transmission Europe, Brussels

12:30 - 14:00 WORKING LUNCH

Mr. Roger Naff, Director of Marketing, "The Protection of Critical Infrastructure and Multi-modal Transportation", Boeing Homeland Security & Services, California

14:00 - 15:30 PARALLEL SESSIONS

Session I: TRANSPORTATION SERVICES SECURITY

Mr. Michel Quatre, Ingénieur Général des Ponts et Chaussées; Haut Fonctionnaire de Défense, Ministère de l'Equipement, des Transports, du Logement, du Tourisme et de la Mer ; Commissaire Général aux Transports, Paris

Panelists:

- **Mr. Jean-Louis Blanchou**, Vice-president, Airport Security, Aéroports de Paris (ADP), Paris
- **Mr. Michel Babkine**, Administrateur en chef des Affaires maritimes et chargé de mission "Sûreté maritime", Secrétariat général de la mer, Services du Premier Ministre, Paris
- **Mr. Andrew Charlton**, Director of Industry and Government Affairs, Société Internationale de Télécommunications Aéronautiques (SITA), Geneva
- **Mr. Bruno Masnou**, Vice-President, Systems & Defence Electronics, Homeland Security Unit, European Aeronautic Defence and Space Company (EADS), Paris
- **Mr. Pierre Perrod**, President, Security Committee, Commission du Tunnel sous la Manche, Paris

Session II: SECURITY ISSUES AND NUCLEAR POWER GENERATION

Moderator: Ms. Anita Nilsson, Head of Office, Nuclear Security; Coordinator, Nuclear Security, Department of Safety and Security, International Atomic Energy Agency, Vienna

Panelists:

- **Mr. Denis Flory**, Head, Radioactive Materials Security Department, Nuclear Protection and Safety Institute IRSN, France
- **M. Christian Gobert**, Senior Executive Vice-president, Cogema, Areva Group, Paris
- **Mr. Ramon Revuelta**, Deputy Director, World Association of Nuclear Operators, Paris Center
- **Dr. Beat Wieland**, Head of Nuclear Energy Section, Swiss Federal Office of Energy, Bern

15:30 - 16:15 PLENARY SESSION: **CONCLUSIONS OF THE FORUM AND PLAN OF ACTION**

Chairmen: Mr. Jean-François Daguzan, Maître de Recherche, Fondation pour la Recherche Stratégique, Paris; **Dr. Patrick Lagadec**, Director of Research, Ecole Polytechnique, Paris; **Dr. John Gault**, President, John Gault S.A, Geneva; Associate Member of the Faculty, Geneva Centre for Security Policy

ANNEX II

MEETING OF THE MINISTERS OF JUSTICE AND HOME AFFAIRS

Paris – 5 May 2003

G8 PRINCIPLES FOR PROTECTING CRITICAL INFORMATION INFRASTRUCTURES

(Adopted by the G8 Ministers of Justice & Home Affairs, May 2003)

Information infrastructures form an essential part of critical infrastructures. In order effectively to protect critical infrastructures, therefore, countries must protect critical information infrastructures from damage and secure them against attack. Effective critical infrastructure protection includes identifying threats to and reducing the vulnerability of such infrastructures to damage or attack, minimizing damage and recovery time in the event that damage or attack occurs, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement. Effective protection also requires communication, coordination, and co-operation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies. Such efforts should be undertaken with due regard for the security of information and applicable law concerning mutual legal assistance and privacy protection.

To further these goals, we adopt the following PRINCIPLES and encourage countries to consider them in developing a strategy for reducing risks to critical information infrastructures:

I. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

II. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

III. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.

IV. Countries should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.

V. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

VI. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

VII. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

VIII. Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

IX. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.

X. Countries should engage in international co-operation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analyzing information regarding vulnerabilities, threats, and incidents, and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

XI. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

F

COMPTE RENDU DU FORUM SUR LES INFRASTRUCTURES CRITIQUES ET LA CONTINUITÉ DES SERVICES DANS UN MONDE DE PLUS EN PLUS INTERDÉPENDANT

Genève, 28 - 29 octobre 2003

TABLE DES MATIÈRES


EADS

1. RÉSUMÉ DES TRAVAUX

Les 28 et 29 octobre 2003, le Centre de politique de sécurité de Genève a organisé un Forum sur le thème de la coordination en matière de protection des infrastructures critiques au niveau international ainsi qu'entre les gouvernements et le secteur privé.

Ce Forum, le premier du genre, a regroupé 186 experts en provenance de 28 pays parmi lesquels des représentants d'organisations gouvernementales et intergouvernementales, de sociétés privées ainsi que d'universités et centres de recherche. Organisée par le GCSP avec le soutien de plusieurs gouvernements, la rencontre a bénéficié de l'appui financier de Boeing, d'EADS (European Aeronautic Defense and Space Consortium), de l'Institut Veolia-Environment, d'Ilion Security, de la Société Générale de Surveillance (SGS), de Symantec et de Thalès.

Préoccupés par l'accroissement de la menace à laquelle sont confrontés les services essentiels, les gouvernements et les organisations multilatérales mettent en avant de nouvelles normes, lois et règlements destinés à améliorer la protection des infrastructures. Cette protection nécessite une coordination au niveau transfrontalier et la prise en compte de l'impact potentiel que peuvent avoir les défaillances des services critiques sur l'industrie et l'ensemble du secteur privé. Les entreprises privées ont fortement intérêt à ce que les mesures prises pour l'amélioration de la sécurité soient bien conçues puisque toute interruption dans la continuité des services peut entraîner des conséquences financières désastreuses.

D'UNE DURÉE DE DEUX JOURS, LE FORUM A ÉTÉ ORGANISÉ AUTOUR DES THÈMES SUIVANTS :

1. Risques et crises émergentes: une nouvelle donne
2. Que font les organisations internationales et régionales?
3. Que font les gouvernements au niveau international ?
4. Comment le secteur privé peut-il assurer l'interface avec le secteur public?
5. Sécurité des réseaux d'information
6. Sécurité des réseaux de télécommunications
7. Sécurité des fournitures de gaz
8. Sécurité des moyens de transport
9. Sécurité et production d'énergie nucléaire
10. Conclusions du Forum et plan d'action

Les infrastructures critiques constituent des systèmes vitaux et des réseaux, dont la dégradation porterait sérieusement atteinte au bon fonctionnement de la société. Elles sont confrontées à de multiples menaces qui vont toujours croissant. Bien qu'une prise de conscience des enjeux se soit opérée aux niveaux national et international et que d'importantes mesures aient été prises dans le but d'améliorer la protection des infrastructures critiques, beaucoup reste à faire. Certains secteurs critiques sont mieux préparés que d'autres.

Le Forum a permis de parvenir aux constats et aux conclusions suivantes :

1. La menace à laquelle sont confrontées les infrastructures critiques présente un caractère multiforme et toujours croissant : catastrophes naturelles, erreurs humaines, actes malveillants ou terroristes. De plus, les infrastructures critiques sont vulnérables car les chaînes d'approvisionnement, de plus en plus longues, dépendent souvent de sources extérieures ; en raison aussi de la libéralisation des marchés de l'énergie ; et, enfin, de la perception instantanée et directe par l'opinion publique de situations de crise, à travers l'image, ce qui a pour effet d'en amplifier la portée. Le terrorisme représente un risque spécifique.

2. Les organisations globales et régionales travaillent ensemble en matière de protection des infrastructures critiques. L'OIPC (Organisation internationale pour la protection civile), l'OTAN (Organisation du Traité de l'Atlantique Nord), l'OCDE (Organisation de coopération et de développement économiques), le Conseil de l'Europe ainsi que la Commission économique des Nations Unies pour l'Europe accomplissent un effort considérable tant sur le plan opérationnel que conceptuel.

3. Les gouvernements aussi deviennent plus actifs. Trois exemples ont été cités : l'action de la Commission européenne, celle des Etats-Unis et celle du G8. En mai 2003, le G8 a adopté 11 principes directeurs incitant les pays membres du G8 à créer ou à développer des stratégies de protection de leurs infrastructures critiques en matière d'information.

4. Depuis 1997, la coopération entre les secteurs public et privé s'est développée de façon régulière avec l'établissement de structures de coopération soit à l'initiative des gouvernements, soit des représentants de l'industrie et de la communauté d'affaires, soit encore, de façon conjointe. Toutefois, des blocages subsistent : réticence à partager l'information, absence d'incitations financières ou problèmes juridiques.

5. Dans le secteur de la protection des réseaux d'information, les efforts de la France, du Royaume-Uni, de la Commission européenne et du réseau FIRST (Forum of Incident Response and Security Teams) ont été mentionnés. Ce dernier regroupe 130 CERT (Computer Emergency Response Team) au niveau international. Etant donné que la notion de protection totale n'existe pas en matière de sécurité des réseaux d'information, il a été souligné qu'il valait mieux parler de « résilience » et de « robustesse ».

6. Par opposition aux travaux effectués en matière de sécurité des réseaux d'information, le secteur des télécommunications apparaît en pleine période de tâtonnements. De manière générale, la sécurité des réseaux pourrait bénéficier d'une plus grande coopération au niveau international. Plus précisément, elle passe par le dialogue et la coopération entre le gouvernement, le secteur privé et les citoyens.

7. Le secteur du gaz, qui jusqu'ici n'a pas été confronté à de sérieux problèmes, va devoir répondre à des défis liés à l'approvisionnement de l'Europe Occidentale qui deviendra de plus en plus dépendante de sources extérieures et à la libéralisation du marché de l'énergie. On

assiste, par conséquent, à une plus grande efficacité mais aussi à une séparation entre les activités d'approvisionnement et de transmission ce qui entraîne une décentralisation des responsabilités.

8. Des efforts sont entrepris pour améliorer les faiblesses en matière de sécurité au sein de l'aviation civile, du trafic aérien, du transport maritime et terrestre. Beaucoup reste à faire dans le domaine du contrôle maritime.

9. Quant à la sécurité de la production d'énergie nucléaire, les menaces terroristes peuvent revêtir plusieurs aspects : mise au point éventuelle d'explosifs nucléaires et de bombes « sales », actes de sabotage sur les centrales et les réacteurs nucléaires ainsi que sur les véhicules de transport de matériel radioactif. Les réseaux informatiques des centrales nucléaires sont également vulnérables avec un risque d'interruption dans la fourniture d'électricité. Les efforts des organisations suivantes ont été soulignés : l'AIEA (Agence internationale de l'énergie atomique) ; le groupe AREVA qui gère des centrales nucléaires en France, au Royaume-Uni et aux Etats-Unis ; et WANO (World Association of Nuclear Operators) qui regroupe toutes les centrales nucléaires dans le monde, qu'elles soient publiques ou privées, à l'exception de la Corée du Nord.

10. Malgré les progrès effectués dans certains secteurs en matière de protection des infrastructures critiques, beaucoup reste encore à faire. Les pouvoirs publics ne font pas toujours preuve de suffisamment d'ouverture et ne transmettent pas les informations adéquates au secteur privé ; les entreprises privées n'ont pas toujours à cœur les intérêts de l'ensemble du public. La recherche reste insuffisante. De plus, il est indispensable de progresser en matière de législation anti-criminelle et anti-terroriste mais aussi en matière d'harmonisation de ces législations au niveau international. Il convient également de parvenir à un accord sur les moyens à mettre en œuvre en priorité et sur la question de la répartition des coûts entre les différents acteurs. Le rôle des organisations internationales sera déterminant dans l'établissement d'un consensus sur ces questions.

11. Enfin, la protection des infrastructures critiques nécessitera un changement de perception et la création d'une « culture du risque ». Les systèmes de protection civile devraient être placés au même niveau que les systèmes de défense traditionnels. Les autorités devraient adopter une attitude dynamique, être capables de « penser de façon différente » et de « penser même l'impensable ». Cette culture de sécurité devrait prendre en compte non seulement les plus grands réseaux mais aussi les petites et moyennes entreprises. Sur le plan particulier, il est important de former les hauts responsables et d'encourager les individus à faire preuve de vigilance. Ceci devrait devenir un « état d'esprit permanent », dans le cadre du quotidien. Enfin, il est reconnu que le « risque zéro » dans une société n'existe pas. De manière générale, les infrastructures critiques doivent être mieux protégées face à des attaques et à des défaillances qui sont inévitables.

12. Les participants du Forum ont invité le GCSP (Centre de Politique de Sécurité de Genève) à continuer à apporter sa contribution en matière de protection des infra-

structures critiques en organisant des ateliers centrés sur des thèmes spécifiques évoqués pendant ces deux jours.

2. RISQUES ET CRISES ÉMERGENTES : UNE NOUVELLE DONNE

En organisant ce premier Forum sur les infrastructures critiques et la continuité des services dans un monde de plus en plus interdépendant, le Centre de Politique de Sécurité de Genève a poursuivi un double but :

- traiter un thème important en matière de sécurité conformément à sa vocation ; et
- adopter une approche concrète face à des problèmes aux retombées pratiques.

Les débats introductifs ont porté sur la menace à laquelle sont confrontées les infrastructures critiques, sur le degré de préparation et la capacité de réaction des gouvernements pour leur protection ainsi que sur les domaines où des améliorations immédiates sont nécessaires.

La menace à laquelle sont confrontées ces infrastructures est multiforme et va croissant : catastrophes naturelles, complexité de nos sociétés modernes, erreurs humaines, actes malveillants, terrorisme et crime organisé.

A cet égard, deux exemples dans le domaine spécifique de l'énergie ont été cités :

a) l'approvisionnement en matière de pétrole des pays de l'OCDE qui peut être soumis à une série de facteurs incontrôlables, simultanés et déstabilisants comme cela a été montré par les retombées des grèves au Venezuela et au Nigéria, les hivers rigoureux et la guerre en Irak. L'importance croissante que prendra dans les prochaines années la part des pays non membres de l'OCDE dans l'approvisionnement des pays développés rendra le transport énergétique encore plus critique et nos sociétés développées plus vulnérables, particulièrement en ce qui concerne les actes terroristes ;

b) la libéralisation du marché de l'énergie dont la conséquence a été la disparition des monopoles. Toutefois, le marché ne règle pas tout comme on a pu le constater lors des pannes électriques survenues récemment dans une série de pays. Pour mieux gérer les crises à venir, il faut donc que des règles précises de production et de transport soient mises au point étant donné que la recherche de nouvelles solutions, déjà très difficile, est compliquée par un facteur sociologique, le NIMBY (« not in my backyard »).

Une prise de conscience des vulnérabilités des infrastructures critiques s'est opérée au niveau des opinions publiques et des gouvernements. Les résultats laissent toutefois encore largement à désirer.

Les Etats-Unis ont une longueur d'avance sur l'Europe depuis qu'ils se sont organisés au niveau central pour la pro-

tection des infrastructures critiques en réaction aux attentats du 11 septembre. Le chantier ouvert est en revanche loin d'être terminé. En Grande-Bretagne, le degré de préparation et la capacité de réaction des pouvoirs publics sont plus élevés dans certaines régions que dans d'autres. En France, des progrès considérables ont été réalisés en matière de renseignement et de contre-terrorisme par opposition à d'autres domaines.

Les problèmes principaux rencontrés en matière de protection des infrastructures critiques sont :

a) la faiblesse de la coopération internationale ;

b) l'absence d'une évaluation compréhensive de la menace au niveau national où, en outre, certains espaces vitaux sont encore insuffisamment contrôlés ou protégés ;

c) l'insuffisance de la coordination intergouvernementale, des crédits alloués à ces questions ainsi que des mécanismes de contrôle ;

d) l'insuffisance de la coordination entre les pouvoirs publics et le secteur privé, en particulier en raison de la difficulté qu'ont les décideurs publics à procéder à une mise en commun de l'information ; et un recours encore très limité aux méthodes incitatives ;

e) l'inefficacité des systèmes de communication avec le public, notamment parce que les gouvernements n'osent pas traiter les populations en « adultes » même si la prise de conscience des risques par ces dernières s'est accrue en raison principalement de l'action de diffusion des media ;

f) l'appréhension des décideurs à aborder les problèmes de front. On préfère nier l'existence de risques ou encore « regarder dans le rétroviseur plutôt qu'à travers le pare-brise ». Cette attitude, qui reflète un refus d'envisager ce qui ne rentre pas dans la norme, se répercute dans la manière d'aborder les exercices de simulation où l'on cherche à éviter les « surprises » afin de ne pas effrayer les participants.

3. QUE FONT LES ORGANISATIONS INTERNATIONALES ET RÉGIONALES ?

Cette deuxième session était composée de représentants d'organisations internationales qui traitent de la protection des infrastructures critiques : l'OIPC (Organisation internationale pour la protection civile), l'OTAN, le Conseil de l'Europe et la Commission économique pour l'Europe. Les intervenants ont fourni une vue d'ensemble des efforts de leurs organisations en la matière. D'importants efforts ont été faits tant sur le plan opérationnel que conceptuel.

a) L'OIPC est une fédération des structures nationales de protection civile de ses Etats membres. Elle constitue une

plateforme de communication, d'échanges et de coopération. L'une de ses responsabilités principales est la standardisation des procédures d'urgence. En 2001, elle a mis au point une convention-cadre en matière de protection civile. Enfin, elle s'efforce depuis une trentaine d'années déjà d'intégrer le secteur privé dans ses activités.

b) Deux divisions de l'OTAN sont particulièrement impliquées dans la problématique de la protection des infrastructures critiques : la division des plans civils d'urgence au niveau opérationnel et le Comité pour les défis de la société moderne (CDSM) au niveau prospectif. Conformément à son rôle de prévention, le CDSM se penche sur des questions telles que le terrorisme, les vulnérabilités des sociétés interconnectées, les ruptures sociétales, le monde des affaires et la sécurité. Les pays de l'OTAN ont instauré un dialogue interne et mis en place des procédures d'assistance réciproques. En 1998, le Euro-Atlantic Disaster Response Coordination Centre (Centre euro-atlantique de coordination des réactions en cas de catastrophe) a été créé permettant ainsi au domaine civil de profiter de l'expérience militaire et des structures dont dispose l'OTAN.

c) L'OCDE s'intéresse à la question sous l'angle des incidences économiques des catastrophes. En 1995, le Japon a perdu 2% de son PNB à cause du tremblement de terre de Kobé; et la Turquie 5% en 1999 suite au tremblement de terre de Marmara ; les attentats du 11 septembre ont fait perdre aux Etats-Unis 1,2% de son PNB. Trois des secteurs étudiés par l'OCDE ont été présentés : les assurances, le rétablissement des télécommunications dans les pays sujets à des tremblements de terre et la sécurité dans le domaine maritime. Au niveau transsectoriel, l'organisation se penche aussi sur des sujets tels que les risques systémiques émergents, les effets économiques du terrorisme et les accidents chimiques et leurs effets sur l'environnement. La communauté d'affaires est également impliquée dans ces activités.

d) En 1987, le Conseil de l'Europe a créé l'accord "partiel ouvert sur les risques majeurs". Partiel, car non obligatoire pour les pays membres et ouvert, car extensible à des pays non-membres (le Maroc, l'Algérie et le Liban en font partie). Cet accord a pour but de favoriser la coopération en matière de gestion des risques. A cet égard, il est actuellement procédé à une analyse comparative des législations en la matière. De plus, le Conseil de l'Europe s'efforce d'inculquer une culture du risque en créant des formations universitaires dans le domaine, telles que des mastères européens spécialisés dans ce domaine (médecine des catastrophes, science du risque pour ses aspects juridiques et sociaux, ingénierie sismique, etc.). Il encourage également l'inclusion de la notion de risque dans les programmes scolaires d'éducation civique. Enfin, il se préoccupe de l'aide à la décision que les nouvelles technologies peuvent apporter.

e) L'une des activités principales de la Commission économique pour l'Europe est d'établir des normes et des standards en matière d'infrastructures et de gérer que la convention sur le transport des produits dangereux ainsi convention sur les accidents transfrontaliers. Par ailleurs, elle est engagée dans un projet de développement d'un système d'alerte rapprochée (« early warning ») avec l'OSCE (Organisation pour la sécurité et la coopération en Eu-

rope). Elle s'efforce enfin d'associer à ses travaux la communauté d'affaires et la société civile en général.

Pour améliorer la coordination de la protection des infrastructures critiques au niveau international, les recommandations ci-dessous ont été faites :

a) mieux assurer au niveau national et international le contrôle des réglementations existantes ;

b) développer une approche pluridisciplinaire ;

c) travailler davantage sur des cas d'école ;

d) mieux anticiper ;

e) coordonner davantage les efforts entre les organisations internationales ;

f) mieux appréhender les différences de culture et d'approche entre nations ;

g) poursuivre les efforts pour inclure le secteur privé dans les processus de décision et de réflexion.

4. QUE FONT LES GOUVERNEMENTS AU NIVEAU INTERNATIONAL ?

La troisième session s'est penchée sur le rôle de la coopération intergouvernementale en matière de protection des infrastructures critiques. La coopération internationale entre les pays les plus développés s'est renforcée au cours des dernières années avec, comme conséquence, une meilleure prise de conscience de ces questions au niveau politique. Des habitudes de travail commencent à s'établir à partir d'approches différentes certes mais sur des problèmes similaires. Le traitement de ces problèmes dans une perspective multidisciplinaire est de plus en plus privilégié comme l'est également le dialogue entre le secteur public et privé. En outre, les gouvernements ne se réfugient plus derrière une « ligne Maginot » mais passent à une posture plus offensive basée sur la « communication, la coordination et la coopération entre tous les acteurs ».

Le groupe a cité trois exemples qui illustrent ces points : l'action de la Commission européenne, celle des Etats-Unis et, enfin, celle du G8.

Durant les vingt dernières années, la Commission européenne a vu son action de coordination et d'exécution réglementaire s'étendre de façon pragmatique. Ceci s'est passé d'abord en réaction aux différentes crises survenues

(choc pétrolier de 1974, catastrophes de Tchernobyl, de Seveso, de l'Erika et du Prestige, attentats du 11 septembre, etc.) et ensuite aux progrès de la construction européenne en matière de sécurité.

La Commission a par ailleurs cherché à éviter l'augmentation des risques liés au mouvement d'ouverture et de libéralisation des marchés de l'énergie par l'adoption d'un certain nombre de mesures telles que la sauvegarde des intérêts publics, des actions spécifiques envers les petites et moyennes entreprises, etc. Elle a également développé les contacts entre les pouvoirs publics et le secteur privé comme en témoigne la tenue des Forums de Madrid et de Rome. Enfin, la coopération internationale, notamment avec l'étranger proche, est également à son ordre du jour de la Commission car l'Europe reste très dépendante de celui-ci pour son approvisionnement en énergie.

Les Etats-Unis, qui prennent en compte l'interconnexion globale des systèmes de protection des infrastructures critiques et la nécessité d'assurer la sécurité de ces derniers, encouragent chaque pays à agir au plan national mais aussi à coopérer au plan international. Ils cherchent au demeurant à promouvoir cette idée en s'impliquant de plus en plus dans les différentes enceintes qui traitent de la protection des infrastructures critiques (G8, Conseil de l'Europe, OCDE, APEC (Asia-Pacific Economic Co-operation), OEA (Organisation des Etats Américains), ONU et Sommet mondial sur la société de l'information. Ils insistent, à cet égard, sur la nécessité d'une infrastructure juridique, de points de contact nationaux, d'un partage de l'information, du développement d'une culture de sécurité et d'un partenariat entre les secteurs public et privé.

Le G8 vient de se saisir à bras le corps de la question de la protection des infrastructures critiques. La décision de le faire avait été prise à Vancouver en mai 2002 par les Ministres du G8 de l'Intérieur et de la Justice. Une conférence co-parrainée par la France et les Etats-Unis s'est tenue à Paris en mars 2003 avec l'aide des groupes du G8, dits de Rome et de Lyon, en charge de la lutte contre le terrorisme et la criminalité organisée appuyés par les experts en « cybercriminalité ». Enfin, en mai 2003, les Ministres de l'Intérieur et de la Justice du G8 ont adopté un texte comprenant onze principes directeurs (voir annexe ci-joint) incitant les pays du G8 à développer des stratégies de protection de leurs infrastructures critiques en matière d'information aux niveaux national et international. Ces principes constituent la première démarche agréée dans un cadre multilatéral pour ce nouveau domaine de sécurité internationale. Conformément au rôle d'impulsion politique qui est le sien, le G8 souhaite par ailleurs encourager la diffusion et l'application de ces principes auprès d'autres instances multilatérales et pays où les infrastructures sont moins développées et moins interconnectées mais néanmoins importantes.

Certains intervenants ont souligné que le terrorisme représentait l'un des risques majeurs pour les infrastructures critiques. Il était nécessaire de définir une stratégie coordonnée qui comprendrait plusieurs actions telles que : chercher à créer une « atmosphère de rejet total » face aux attentats terroristes, priver les terroristes de leur support social, et promouvoir le dialogue interconfessionnel. La communauté d'affaires peut et se doit de contribuer à

cet effort en aidant à couper les organisations terroristes des circuits financiers. Il fallait aussi rechercher les motivations de ces actions et tenter d'en éliminer les causes.

5. COMMENT LE SECTEUR PRIVÉ PEUT-IL ASSURER L'INTERFACE AVEC LE SECTEUR PUBLIC ?

Les participants de la quatrième session se sont penchés sur la question de savoir comment le secteur privé pourrait collaborer avec le secteur public en matière de protection des infrastructures critiques. Les débats sur ce sujet se sont concentrés sur les points suivants :

1. LES DÉBUTS DU PARTENARIAT :

a) Au cours des dernières années, l'idée de partenariat s'est imposée pour les raisons suivantes : nécessité d'établir les responsabilités en cas d'incident ; disparition des monopoles d'Etat ; prise de conscience du fait que la sécurité est un souci partagé par les pouvoirs publics et le secteur privé ; nécessité de mettre en commun les rares ressources humaines nécessaires à cet effet ; et aussi de mettre en place des lois et des accords.

b) Créée en 1996 aux Etats-Unis, la President's Commission on Critical Infrastructure Protection a souligné dans les mois qui ont suivi ces points: les réseaux d'information constituent le soubassement des infrastructures critiques du pays ; 85% des infrastructures sont gérées par le secteur privé ; un dialogue doit par conséquent s'instaurer entre les pouvoirs publics et le secteur privé. A cette fin, une directive présidentielle prévoit la création d'agences gouvernementales spécialisées dans chaque secteur concerné pour assurer l'interface avec le secteur privé.

c) A partir de 1997, cette idée de coopération entre les secteurs public et privé s'est développée : les gouvernements et le secteur privé ont établi des structures de coopération de façon conjointe ou à l'initiative des uns ou des autres.

d) La coopération entre ces deux secteurs se développe plus aisément en matière de standardisation où public et privé se retrouvent forcément. Il s'agit là d'un domaine de la plus haute importance pour l'obtention d'une plus grande sécurité. Des initiatives ambitieuses sont par ailleurs actuellement prises à ce niveau (volonté des Etats-Unis de standardiser les containers à des fins de contrôle et de sécurité ; nouvelle convention du BIT sur les pièces d'identité des marins).

2. LES DIFFICULTÉS DU PARTENARIAT :

a) Le secteur privé n'a pas toujours conscience de ses vulnérabilités. Il vit souvent dans l'idée qu'il a pris toutes les précautions nécessaires alors que ce n'est pas toujours le cas.

b) Il peut être freiné dans ses projets en raison de l'ab-

sence d'incitations financières comme c'est le cas aux Etats-Unis où les coûts liés à la sécurité ne peuvent être répercutés sur le consommateur.

c) Une culture sécuritaire n'est pas encore entrée dans les mœurs alors que les fonds nécessaires sont disponibles.

d) Les pouvoirs publics ne souhaitent pas toujours divulguer les informations sensibles qu'ils détiennent alors que cela permettrait au secteur privé de mieux orienter ses efforts en matière de sécurité.

e) Le partage de l'information entre pouvoirs publics et secteur privé peut créer des problèmes juridiques et entraîner des litiges (p.ex. informations commerciales sensibles).

f) La recherche légitime de la sécurité ne doit pas se faire au détriment des libertés fondamentales. D'où la nécessité de prévoir des garde-fous tels que la CNIL (Commission nationale de l'informatique et des libertés) en France.

3. RECOMMANDATIONS POUR ALLER PLUS LOIN :

a) Dans le cas de la mise sur pied de nouveaux partenariats, il est recommandé de motiver les partenaires, de créer un climat de confiance en limitant le partage de l'information à des questions non critiques, d'établir des règles et des critères, de chercher à connaître les causes d'une volonté de demeurer en-dehors du processus et, enfin, de proposer de nouveaux modèles.

b) Les pouvoirs publics doivent avoir l'obligation d'assurer la sécurité du secteur privé, au moins à partir d'un certain niveau. Cette approche exige que les pouvoirs publics mettent en place des politiques de défense civile de même importance que les politiques de défense traditionnelles. Ceci passerait par une révolution au niveau stratégique et culturel. Le partenariat et la coopération entre les pouvoirs publics et les entreprises devraient se faire par filières économiques de manière à obtenir un résultat optimal. Parmi les mesures qui permettraient d'accéder à cela, on trouve les incitations fiscales, l'aide à la recherche-développement, l'harmonisation et la mise en commun de certains moyens techniques (centres régionaux de télésurveillance régionaux, le contrôle systématique de nouveaux employés), les debriefings de situations anormales par les pouvoirs publics, les exercices communs, les retours d'expérience et échanges entre entreprises privées.

c) Même les partisans de l'approche du « laissez faire » ont reconnu qu'il fallait pouvoir compter sur les pouvoirs publics dans certaines situations comme lorsqu'il s'agissait de constituer un stock adéquat de fournitures vitales.

6. SÉCURITÉ DES RÉSEAUX D'INFORMATION

La cinquième session a traité de la question de la sécurité des réseaux d'information.

Le secteur de l'information sous-tend l'ensemble des infrastructures critiques. Notre capacité de réaction en cas de crise en dépend. Les risques liés aux réseaux d'information existent tant au niveau national qu'international. Dans les deux cas, les responsables doivent travailler ensemble pour assurer : une alerte avancée en cas de menace ; la continuité des services ; la sécurité nationale ; et une investigation criminelle appropriée.

Toutefois, une protection totale n'existe pas. Il est donc préférable de parler de « résilience » ou de « robustesse » des systèmes au lieu de « protection ». L'introduction des CERT (Computer Emergency Response Team) dans les années 90 a contribué à améliorer la situation. De plus, on peut diminuer le risque en limitant les vulnérabilités résiduelles et en connaissant parfaitement son parc informatique afin d'appliquer les correctifs nécessaires en cas d'attaques de virus.

Dans certains pays, d'importants efforts ont déjà été entrepris afin de protéger les réseaux d'information. La Grande-Bretagne a créé le National Infrastructure Security Coordination Centre qui traite de la menace sur les infrastructures informatiques dans le cadre de la protection de toutes les infrastructures. Ce domaine s'est considérablement développé depuis une trentaine d'années à travers la lutte contre le terrorisme au niveau national. Ce Centre est chargé d'enquêter sur les menaces, de préparer la réponse en recherchant une étroite collaboration avec le secteur privé et d'entreprendre des recherches (cf. http://www.nisc.gov.uk). Dans le cas des infrastructures informatiques, le CERT du Centre fonctionne en coordination avec les CERT des autres pays.

Aux Etats-Unis, le Homeland Security Department a été créé. Il comprend une agence chargée de la sécurité des réseaux semblable à celle qui se trouve en Grande-Bretagne (cf. http://www.cybercrime.gov). L'investigation criminelle et l'application des peines représentent deux autres secteurs qui sont pris en compte de manière adéquate aux Etats-Unis et qui bénéficient d'une bonne coordination. Sous l'impulsion du G8, 34 pays ont commencé à réfléchir à ces questions.

La Direction générale de la Société de l'information, qui fait partie de la Commission Européenne, a lancé également des initiatives cohérentes dans le domaine des infrastructures critiques. Les plus importantes se situent au niveau d'un cadre régulateur et à celui de la recherche. La Commission se préoccupe aussi de sécurité externe et doit lancer un projet-pilote de recherche en vue d'améliorer la coordination des différentes institutions en cas de crise. Le Parlement européen envisage de créer une agence de sécurité pour les réseaux d'information afin de renforcer les bonnes pratiques, de faciliter la coopération entre secteur privé et secteur public ainsi que les

échanges de données et d'information. En outre, une décision-cadre sur le cybercrime, actuellement à l'étude, devrait fournir des définitions communes susceptibles de faciliter le travail de la police et des autorités judiciaires.

Suite à l'échec du projet Eurocert en 1990, l'Europe cherche elle aussi à renforcer sa coordination sur un plan plus technique. Le projet « Task Force CERT » a été mis sur pied pour tenter d'assurer un niveau de confiance plus élevé et une liste de responsables de la sécurité (incident response teams) a été établie.

Au niveau international, un réseau intitulé « FIRST » (Forum of Incident Response and Security Teams) regroupe 130 CERT dont 59 en provenance du secteur public et 69 du secteur privé, répartis pour 71 en Amérique du Nord, 48 en Europe, 7 dans le Pacifique et 5 en Amérique Latine.

UN PLUS GROS EFFORT DOIT ÊTRE CONSENTI, ENTRE AUTRES, DANS LES DOMAINES SUIVANTS :

a) étendre l'effort accompli dans les pays développés à l'échelle du globe ;

b) préserver des garde-fous pour les libertés fondamentales ;

c) modifier la méthodologie utilisée pour analyser les phénomènes en mettant l'accent sur une approche transsectorielle, transdisciplinaire et interministérielle (l'Ecole polytechnique fédérale de Zürich a ainsi développé un mastère interdisciplinaire en « risk engineering and management »).

d) avoir une pensée innovante tout en continuant à tirer des leçons du passé ;

e) développer les structures requises au niveau international ;

f) développer le partenariat public-privé et la coopération avec les milieux universitaires et de recherche.

7. SÉCURITÉ DES RÉSEAUX DE TÉLÉCOMMUNICATIONS

La sixième session a mis l'accent sur les évolutions qui se sont produites dans le domaine de protection des réseaux critiques de télécommunication.

Au cours des cinq dernières années, le secteur de la communication a été en effet soumis à d'importants changements tant au niveau technique qu'en matière d'élaboration de réglementations. La tâche de l'opérateur de réseau est devenue de plus en plus complexe étant donné qu'il gère les relations entre plusieurs parties prenantes : l'Etat, ses partenaires, la clientèle et les autres opérateurs.

En outre, les entreprises sont devenues de plus en plus vulnérables étant donné que leur management passe désormais par internet. Enfin, on manque de vue générale des problèmes. Pour certains, un grand nombre de procédés correctifs utilisés dans le cadre du Bug de l'an 2000 restent toujours valides. Pour d'autres, il n'est pas possible d'appliquer des solutions du passé à une problématique entièrement nouvelle.

L'une des préoccupations principales est de pouvoir assurer un service continu, ou, tout au moins, de faire en sorte qu'il y ait le moins d'interruptions possibles. En cas d'interruption, le service doit être rétabli aussi rapidement que possible. Le cas échéant, il faut pouvoir compter sur une veille permanente et sur des plans de secours, domaine où des progrès sont encore à faire. A cet égard, la relation avec les autres opérateurs est fort importante. Au sein du contexte de forte compétition qui existe à ce niveau, les contacts ne sont pas toujours constructifs. La coordination avec les régulateurs est également essentielle. Or, ceux-ci semblent plus préoccupés par l'organisation de la concurrence que par les problèmes de sécurité. Il convient de noter toutefois que la mobilisation des opérateurs s'est effectuée avec succès en Algérie en 2003 lors du tremblement de terre dont les effets ont été dévastateurs (5 câbles sous-marins majeurs ont été sectionnés ; le pays entier, une partie du Maghreb et une quinzaine d'autres pays jusqu'en Asie ont été affectés). Les services ont été rétablis à 60% en trois jours et les câbles réparés en un mois.

La sécurité des réseaux passe par le dialogue et la coopération entre les différentes parties prenantes : le gouvernement, le secteur privé et les citoyens. A cet égard, l'Information Assurance Advisory Council (IAAC), une institution indépendante située en Grande-Bretagne, a été présentée comme un modèle. Il en a été de même pour le Directors Information Insurance Network, toujours en Grande-Bretagne, dont l'objectif est de sensibiliser les décideurs dans les entreprises à la problématique.

L'importance de la coopération internationale, qui avait bien fonctionné lors du Bug de l'an 2000, a également été soulignée. De grandes organisations régulatrices, comme l'OACI (Organisation de l'aviation civile internationale), l'UIT (Union internationale des télécommunications), l'AIEA et WANO, s'étaient mobilisées. Il en avait été de même pour les grandes multinationales (Hewlett Packard, Shell, etc.). Les gouvernements, quant à eux, ont suivi l'exemple de la Floride qui avait créé son propre réseau international. L'idée de créer une organisation spécifique pour traiter de la cybersécurité a par ailleurs été jugée inutile sauf peut-être au niveau technique. L'Assemblée générale des Nations Unies a voté plusieurs résolutions concernant ce problème mais peu a été entrepris en ce qui concerne l'établissement de normes. Le Sommet mondial sur la société de l'information prévu fin 2003 devait aborder cette question.

8. SÉCURITÉ DES FOURNITURES DE GAZ

Essentiellement consacrée à la question de l'approvisionnement en gaz de l'Europe Occidentale, la septième session a débuté par une mise en garde. Jusqu'ici, L'Europe Occidentale n'avait pas eu de problèmes à cet égard. Il n'existait, cependant, plusieurs aucune garantie pour le futur. Au cours de la discussion, les points suivants ont été soulignés.

L'approvisionnement en gaz était déjà complexe et ceci allait s'accroître à l'avenir ; la libéralisation du marché du gaz allait complètement modifier la donne.

Les ressources en gaz étaient abondantes au niveau mondial. Elles étaient cependant limitées à un certain nombre de pays. En outre, il fallait tenir compte d'un certain nombre de rigidités techniques : systèmes de livraison point à point et sans capacités en excès ; absence de planification des investissements à long terme ; volatilité du marché à court terme qui pouvait envoyer des signaux erronés aux investisseurs. La production en Europe Occidentale était au mieux limitée. L'Europe devait donc s'adresser de plus en plus à l'extérieur (Russie, Mer Caspienne, Moyen-Orient, Algérie, Nigeria, Amérique Latine, etc.). Cette situation entraînerait des investissements plus coûteux et un accroissement des risques techniques et politiques. L'existence du couloir énergétique Est-Ouest qui traversait le Caucase et particulièrement la Géorgie était pourtant un élément rassurant. Mais on ne pouvait s'arrêter là. Le nouveau panorama mondial créé par les attentats du 11 septembre avait ajouté à l'instabilité.

La libéralisation du marché du gaz au sein de l'Union Européenne était bénéfique pour le consommateur et apportait plus d'efficacité. Toutefois, elle constituait un nouveau défi. Auparavant, l'environnement était stable : les entreprises offraient des services intégrés et se chargeaient à la fois des infrastructures de gaz et de sa fourniture ; les compagnies coopéraient entre elles ; et les contrats étaient à long terme. Désormais, le secteur était devenu complexe à cause de la séparation entre les activités de fourniture et de transmission et de la fragmentation des responsabilités.

DES PISTES DESTINÉES À ASSURER LA SÉCURITÉ DES APPROVISIONNEMENTS ONT ÉTÉ MISES EN AVANT :

a) Efforts de prospective et de coordination.

- Il n'existait pas de modèle informatique global destiné à tester des scénarios et susceptible d'orienter les investissements de manière à éviter un éventuel effet de domino.

- Toutefois, l'IEA (International Energy Agency) possède une vue globale de l'offre et de la demande d'énergie dans le monde ainsi qu'un modèle de prévision des besoins. Elle dispose aussi d'une vue régionale et locale des

forces et faiblesses spécifiques des marchés. De plus, l'IEA a développé des prévisions en matière d'investissement dans le secteur de l'énergie, en particulier pour le gaz, et a créé une task force sur le gaz naturel qui regroupe toutes les parties prenantes.

➤ D'autres organisations et certains pays ont développé des ressources semblables. L'Union Européenne demande annuellement à chaque pays membre d'évaluer ses besoins en gaz et en infrastructures. La France effectue un bilan identique.

b) En matière de la sécurité des approvisionnements extérieurs, il fallait :

➤ favoriser l'investissement dans les infrastructures ;

➤ continuer à développer les contrats à long terme ;

➤ chercher à mieux lier entre eux les pays fournisseurs, de transit et de consommation en favorisant les formules de partage des risques et les joint-ventures ;

➤ diversifier les sources d'approvisionnement ainsi que les routes d'acheminement.

De manière générale, la réorganisation du marché intérieur comportait des solutions viables pour l'Union européenne. Il convenait toutefois à ce niveau :

➤ d'obtenir une claire redistribution des responsabilités entre les différents acteurs du marché tels que les producteurs, les fournisseurs/transporteurs et les entreprises chargées du stockage ainsi qu'entre les autorités nationales ;

➤ d'assurer un fonctionnement efficace et sûr du réseau ainsi que son développement à long terme ;

➤ de prendre en compte les différences entre les Etats membres de manière à éviter les distorsions au niveau du marché ;

➤ de renforcer la coopération entre les différents intervenants des secteurs public et privé ;

➤ de maintenir et éventuellement de renforcer les mesures de sécurité existantes pour parer aux risques techniques et politiques mais aussi à un éventuel risque terroriste.

9. SÉCURITÉ DES MOYENS DE TRANSPORT

Les questions suivantes, relatives à la sécurité des moyens de transport, ont été soulevées par le huitième groupe :

9.1 VULNÉRABILITÉS :

A) AVIATION CIVILE, AÉROPORTS ET TRAFIC AÉRIEN.

- L'aviation commerciale est un système global et complexe qui comprend les aéroports, le trafic aérien et, enfin, l'aéronef. Ces trois éléments doivent être protégés au même titre. Ils représentent des cibles à forte charge symbolique, et en particulier les aéroports qui constituent un symbole de souveraineté et de force économique pour un pays.

- Les conséquences d'un attentat ou d'une catastrophe peuvent porter atteinte à l'activité économique d'un pays ou d'une région.

- La protection doit se faire de manière interne et transfrontalière et doit intégrer la dimension informatique et les télécommunications. Par ailleurs, elle doit porter sur les passagers dans les avions et dans les aéroports ainsi que sur les bagages et les conteneurs.

- Après les attentats du 11 septembre, tous les domaines de la sécurité du transport aérien ont été remis en question : les renseignements en amont, la protection des avions et le contrôle aérien. Pourtant, même si le degré « 0 » n'existe pas, les mesures prises au fil des années avaient permis d'atteindre un très haut degré de sécurité.

B) TRANSPORTS MARITIMES

- Les attentats du 11 septembre ont aussi engendré des préoccupations sur les risques que présentent les transports maritimes. Certains pays, comme la France, ont lancé des plans de protection (Vigipirate, Vigimer). Il en a été de même pour l'Union Européenne. En juillet 2003, sous une forte pression américaine, l'OMI (Organisation maritime internationale) a édicté des mesures semblables à celles adoptées en matière d'aviation civile.

- Les mesures adoptées sont globales et applicables tant aux navires qu'aux ports. Le navire peut être une cible en soi (ex. l'Achille Lauro en 1985). Il peut aussi être un vecteur et une menace en lui-même de par sa cargaison (transport de marchandises nocives ; explosifs ou engin nucléaire en pièces détachées en vue d'un attentat) ou de par sa situation (un tanker gazier qui exploserait à proximité d'une ville, ou un navire en plein milieu d'un détroit (Ormuz, Pas-de-Calais)).

C) TRANSPORTS TERRESTRES.

- Parmi les différents types de transports dans cette catégorie (transports individuels ; camions de marchandises ; transports en commun dont les métros et les chemins de

fer), c'est le Tunnel sous la Manche qui a été choisi pour le débat.

➽ Le Tunnel présente plusieurs caractéristiques. Il représente, tout d'abord, une symbolique très forte. Il constitue également un lien physique vital entre les îles britanniques et le continent européen et entre deux pays soumis à des menaces terroristes internes. Enfin, il est un exemple de partenariat public-privé entre deux gouvernements et une société (Eurotunnel).

➽ Le Tunnel réunit également plusieurs types de trafic qui en font un système intermodal très complexe et qui représentent autant de risques : TGV « Eurostar » ; trains de marchandises classiques (conteneurs) ; navettes d'Eurotunnel (camions, autocars, voitures). En outre, l'accès au site lui-même constitue un risque supplémentaire.

➽ Des dispositions précises ont été prises dans les Traités de 1986 en matière de sécurité. Celles-ci ont donné aux deux gouvernements des pouvoirs spécifiques vis-à-vis de l'entreprise (création d'un comité mixte de sécurité franco-britannique). Progressivement, certaines lacunes du dispositif de sécurité ont été mises en lumière et corrigées.

9.2 COMMENT AMÉLIORER LES CHOSES ?

a) La sécurité doit être prise de manière globale. En même temps, on ne peut pas tout protéger, en partie parce que cela est techniquement impossible et en partie parce que cela n'est pas forcément opportun. Les actions correctives doivent être basées sur la probabilité statistique des risques et il convient d'opérer les choix qui s'imposent. Priorité doit être donnée à la création d'un « fonds global de sécurité ». Par ailleurs, il est également essentiel de chercher à déterminer la réactivité en temps réel à l'impact d'un accident.

b) Il est difficile d'appréhender la rationalité des actions terroristes puisqu'elle renvoie à des valeurs qui ne sont pas les nôtres. Il n'est non plus pas évident de prévoir ces actions. Il faut devenir plus attentif aux signaux. Il n'est pas toujours possible de mobiliser le financement et les ressources nécessaires. Les meilleures parades sont la prévention (intelligence locale ou internationale) et la dissuasion.

c) Le contrôle aérien des passagers s'effectue à plusieurs niveaux : identité par les visas, contrôle physique avant l'embarquement, etc. De manière générale, de plus en plus de banques de données significatives sont disponibles et reliées entre elles (Schengen II, système de visas européen, etc.). Il convient toutefois d'améliorer les modalités de transmission de l'information. Il y a aussi un risque de saturation. De plus, depuis le 31 décembre 2002, certains aéroports se conforment aux nouveaux règlements et contrôlent l'ensemble des bagages. Ce n'est pas le cas cependant pour d'autres aéroports qui demandent des délais de deux ans pour la mise en application du nouveau règlement.

d) En ce qui concerne le contrôle maritime, il reste encore beaucoup de chemin à parcourir. D'ici juillet 2004, les opérateurs des navires devront remplir plusieurs conditions administratives (établissement de plans de sûreté et homologation de ceux-ci par les autorités, etc.), acheter

du matériel et recruter du personnel. La contrainte sera plus forte encore du côté portuaire mais il est nécessaire de sécuriser également l'ensemble des installations portuaires.

9.3 QUEL EST L'IMPACT ÉCONOMIQUE ?

a) Les coûts liés aux attentats du 11 septembre, au conflit en Irak et à la crise du SRAS ont été énormes pour l'aviation civile : 30 000 postes de travail perdus en Europe et 25 milliards de dollars de chiffre d'affaires en moins. Les attentats du 11 septembre ont coûté 140 milliards de dollars à la ville de New York, soit l'équivalent de quatre années du budget du « Homeland Security Department » qui est le deuxième budget fédéral aux Etats-Unis après celui de la défense. La croissance économique mondiale a aussi été affectée.

b) Les mesures de sécurité prises dans les aéroports de Paris coûtent 230 millions d'euro par an sur un chiffre d'affaires de 1,5 milliards d'euros. Partout, les taxes d'aéroport ont considérablement augmenté.

c) Les passagers comprennent la nécessité de ces mesures. Il faudrait toutefois créer davantage de transparence quant à l'utilisation des taxes d'aéroport et indiquer quel pourcentage est consacré à la sécurité.

d) La sécurité modifie les conditions de la concurrence entre les aéroports, les ports et les modes de transport.

9.4 LES POLITIQUES DE SÉCURITÉ :

a) L'Etat évalue les menaces et oriente le secteur privé sur les mesures à prendre, en particulier lorsqu'il s'agit de sociétés qui offrent des services publics. Le secteur privé prend ces mesures sans connaître la nature précise de la menace. La dichotomie entre ceux qui évaluent et ceux qui mettent en œuvre doit cesser. Pour cela, les données disponibles doivent être mises en commun et une stratégie efficace doit être développée.

b) La sécurité constitue l'une des missions régaliennes de l'Etat. Il serait donc normal que celui-ci prenne en charge les coûts dans ce domaine, du moins en partie. Il serait également utile de réfléchir à un ensemble de mesures de sûreté qui serait disséminé entre les différents acteurs au lieu d'être centralisé.

10. SÉCURITÉ ET PRODUCTION D'ÉNERGIE NUCLÉAIRE

La neuvième session, à laquelle participait un nombre égal de régulateurs et d'opérateurs, s'est concentrée sur les points suivants : les effets de la menace terroriste sur la gestion du risque, les moyens nécessaires au renforcement de la sécurité, l'importance de la notion de confiance pour la gestion de risque et l'évolution de la coopération au niveau international.

La menace terroriste pouvait revêtir plusieurs aspects : mise au point d'explosifs nucléaires et de bombes « sales », actes de sabotage sur les centrales et les réacteurs nucléaires ou sur les véhicules de transport de matériel radioactif. Trois défis majeurs ont été relevés : prolifération, vol et sabotage. Plus que jamais, la production d'énergie nucléaire ne pouvait se passer de garanties internationales et d'une sécurité robuste.

L'AIEA a lancé à cet égard un programme global dont l'objectif est de traiter les questions de sécurité nucléaire tant dans le cas de la fourniture d'énergie que dans celui des infrastructures. Il couvrait notamment les points suivants : la protection physique adéquate des produits et des installations nucléaires ainsi que leur transport ; le contrôle de produits radioactifs ; la détection et la prévention du trafic illicite ; l'intégration des systèmes de sécurité de façon à en retirer un bénéfice maximum ; et la mise en œuvre de plans réactifs d'urgence. Si ces principes étaient communs, il n'y avait en revanche pas encore de solution globale applicable à chaque pays. Les responsabilités à l'intérieur d'un Etat étaient définies de la manière suivante : les pouvoirs publics établissaient les exigences et supervisaient leur mise en œuvre ; la sécurité et la sûreté étaient du ressort des opérateurs.

Deux autres types de risques ont été relevés : le risque informatique pour les centrales qui était plus important aux Etats-Unis qu'en Europe où l'accès à l'Internet était plus limité, et le risque d'interruption dans la fourniture d'électricité qui méritait d'être mieux étudié au niveau international.

L'exemple de la Confédération Helvétique en matière de protection physique des centrales nucléaires a été mis en avant. La sécurité liée à l'énergie nucléaire avait été réévaluée au lendemain du 11 septembre afin de tenir compte des risques de chantage ou d'attaque par des avions-suicides. Les résultats de cette réévaluation avaient été présentés à la presse en avril 2003.

Le groupe AREVA offrait pour sa part un exemple particulièrement intéressant où sécurité et sûreté étaient intégrées et prises en compte à tous les niveaux, les deux types de gestion présentant en fait beaucoup de similitudes. La sûreté vise à contenir la dispersion de matériel radioactif en cas d'un accident, d'un incendie, de fuites radioactives ou encore de tremblements de terre. La sécurité reposait sur la protection physique, la conception de la centrale ainsi que sur les processus de contrôle au niveau opérationnel.

Opérateur de centrales nucléaires en France, en Grande-Bretagne et aux Etats-Unis, AREVA maîtrisait également tout le cycle nucléaire à travers sa filiale Cogema. Grâce à sa filiale Framatome, il s'occupait aussi de la conception des centrales nucléaires. Le facteur humain, qui présente le plus d'incertitude, devait également être intégré dans la gestion de la sécurité et de la sûreté. Cela était naturel : l'industrie nucléaire demeurait une industrie à hauts risques malgré les progrès réalisés. Néanmoins, le secteur pouvait se targuer d'une tradition de sécurité supérieure à d'autres tels que l'industrie chimique ou les transports. Enfin, la répartition des coûts entre les opérateurs et les pouvoirs publics devrait être examinée davantage.

Une bonne gestion du risque passe également par un dialogue constructif et transparent entre opérateurs et régulateurs.

Pour les opérateurs, les risques et les menaces devaient être définis par les régulateurs de façon plausible afin de déterminer quelles sont les mesures à prendre. Il fallait également que soit établi ce que les opérateurs avaient raisonnablement les moyens de faire et ce qui devait relever des pouvoirs publics aux niveaux financier, légal et technique.

Les opérateurs travaillent toujours dans le cadre des limites réglementaires. Toutefois, pour cela, le système doit être stable et praticable. Lorsque les pouvoirs publics identifient des risques et déterminent la manière d'y remédier, il faut que les opérateurs fassent partie du processus de décision. Les opérateurs possèdent une culture de sécurité. Dès lors, ils représentent de bons interlocuteurs pour les pouvoirs publics avec lesquels ces derniers pourraient développer un dialogue constructif.

La coopération internationale joue un rôle déterminant dans le renforcement de la sécurité des installations nucléaires. A cet égard, trois points ont été soulignés :

a) En matière de sécurité dans le domaine nucléaire, les préoccupations de la communauté internationale et de l'AIEA étaient passées par plusieurs phases : nécessité de contrer le danger de prolifération d'armes nucléaires dans les années 60 ; risques de trafic, de chantage et d'attentats dans les années 80 et 90 ; après le 11 septembre, l'accent a été mis sur le risque de sabotage.

b) Cette évolution avait débuté en 1999 lorsque des discussions au sein de l'AIEA s'étaient tenues sur la question. Celles-ci avaient abouti à la recommandation d'inclure les moyens d'y faire face dans la Convention de 1980 sur la protection physique des matières nucléaires. Parallèlement à cela, un groupe de cinq pays (la France, la Grande-Bretagne, la Belgique, la Suède et l'Allemagne) a été constitué pour peser dans ce sens et demander une révision des activités des agences internationales en matière de protection et d'assistance. Ce groupe s'est ensuite élargi à trois autres pays (la Suisse, l'Espagne et la Finlande) pour devenir le groupe des « 8 ». Une série de douze principes destinés à régir la protection des installations et des matières nucléaires a été finalement mise au point et attend d'être adoptée sous forme d'un amendement à la convention de 1980.

c) La coopération internationale doit de plus en plus faire place à l'assistance dans la sécurité des installations nucléaires. Cette préoccupation est apparue en 1998. Les grands pays fournissent une assistance à un niveau bilatéral ou à travers des conférences ou des ateliers internationaux. L'assistance se heurte toutefois à quelques difficultés : les menaces sur l'environnement varient d'un pays à l'autre ; la confidentialité requise pour éviter les fuites d'information ne fait pas bon ménage avec la transparence qu'imposent toute transmission de savoir et la volonté d'imposer des standards au niveau international.

La coopération internationale en matière de sûreté a entraîné la création de WANO (World Association of Nuclear Operators) en 1989 à la suite de l'accident de Tchernobyl. Cette organisation est indépendante des

gouvernements et des régulateurs. Elle regroupe à l'heure actuelle toutes les centrales nucléaires dans le monde, qu'elles soient publiques ou privées, à l'exception de la Corée du Nord. Elle a pour mission de réduire les risques dans l'industrie nucléaire en encourageant les échanges d'information, la communication, la comparaison et l'émulation parmi ses membres. Des progrès sensibles en matière de sûreté ont été réalisés sur tous les fronts au cours des dernières années. Il est important cependant de continuer à développer une « culture » dans ce domaine étant donné que les accidents ne sont pas dus à des circonstances fatales mais représentent des lacunes dans la culture de la sûreté. Les événements du 11 septembre ont eu un double impact sur les activités de WANO Paris-Centre. D'une part, en automne 2002, aucun procès-verbal n'a été pris lors de la réunion du Conseil d'Administration qui a porté sur les études effectuées et les mesures destinées à améliorer la sûreté des centrales, déjà très élevée. D'autre part, l'organisation s'est orientée vers l'établissement de listes communes d'experts avec l'AIEA afin que l'obtention de visas et l'accès aux centrales, plus difficiles dans certains pays depuis les événements du 11 septembre, soient rendus plus faciles pour les experts de WANO.

11. CONCLUSIONS DU FORUM ET PLAN D'ACTION

1. En matière de protection des infrastructures critiques, les tendances générales ci-dessous ont été relevées :

a) Le « seuil d'incertitude » pour nos sociétés s'est accru de manière générale en raison de la multiplication des risques de toute nature.

b) L'imbrication de ces risques, des menaces et des cibles crée une forte interdépendance au niveau planétaire.

c) Une exigence universelle de sécurité est apparue. L'opinion publique est en effet devenue plus consciente de la situation.

d) Le terrorisme conserve une place à part en raison des effets importants et de son impact de masse. (Il « pratiquait le judo » avec les sociétés modernes.)

e) Les traits culturels et les pratiques organisationnelles, à savoir le facteur humain, peuvent jouer un rôle non négligeable quand on se repose sur les succès passés au lieu de se livrer aux tests nécessaires pour comprendre ce qui ne fonctionne pas ; lorsque des cloisonnements en matière d'organisation empêchent la circulation nécessaire de l'information ; quand une équipe de direction est incapable d'intégrer et de contrôler tous les éléments de l'en-

semble ; quand encore des chaînes informelles de commandement fonctionnant en-dehors des règles organisationnelles normales apparaissent, venant ainsi compliquer le processus.

f) Des progrès considérables ont été réalisés dans la protection des infrastructures en matière d'information au niveau du G8 et aussi au plan national en France, aux Etats-Unis et au Royaume-Uni. Il reste certes encore beaucoup à faire mais la tâche est plus aisée dans ce secteur que dans d'autres car il est bien circonscrit. La coopération internationale reste cependant largement insuffisante tous domaines confondus. Tel est également le cas pour le dialogue entre les pouvoirs publics et le secteur privé où, souvent, les responsabilités respectives ne sont pas clairement fixées. Un gros effort est également à faire en matière de recherche. Des progrès sont indispensables en matière de législation anti-criminelle et anti-terroriste et d'harmonisation de ces législations. La question des moyens à mettre en œuvre et celle de la répartition des coûts entre les différents acteurs doivent également être posées.

2. Certaines fausses solutions ont été dénoncées :

a) Continuer à se pencher sur les définitions et les projets de recherche théorique.

b) S'enliser dans des considérations tactiques plutôt que de définir une direction stratégique avant tout.

c) Répartir à nouveau le problème entre "37 nouvelles bureaucraties et 37 organes de coordination".

d) Privilégier la piste technologique et négliger le facteur humain.

e) Promouvoir des réponses attractives au niveau des « relations publiques » mais qui sont finalement creuses.

f) Céder à la paranoïa après avoir nié le problème.

3. Etant entendu que les problèmes sont hors normes, les solutions doivent l'être aussi et l'approche doit être globale. « Changer de mentalité », « penser différemment » et « penser l'impensable » : voilà la voie à suivre. Il convenait donc :

a) Sur le plan général,

- d'inscrire la question de la protection des infrastructures critiques à l'ordre du jour. Il existe un « Forum économique mondial ». Pourquoi ne pas avoir un « Forum mondial de la résilience » qui regrouperait des PDG, donnerait une même voix aux pouvoirs publics et au secteur privé, et inclurait les ONG? On tenterait ainsi d'explorer de nouvelles voies notamment à travers l'échange d'expériences ;

- de se concentrer sur les thèmes pouvant mobiliser l'opinion publique : par exemple la protection des principales grandes villes, les voies de communication, etc. ;

- de ne pas oublier les petites et moyennes entreprises car on a tendance à ne penser qu'aux grands réseaux.

b) Sur le plan particulier,

- de pousser les leaders (surtout les Ministres et les PDG) à affronter les vraies questions ;

- d'encourager les « debriefings » instantanés après une catastrophe ;

- d'encourager la vigilance qui devrait devenir un état d'esprit permanent, surtout dans le fonctionnement quotidien d'une entreprise ;

- d'effectuer des simulations non conventionnelles ;

- d'encourager les « think tanks » à travailler ensemble, davantage sur des problématiques concrètes (p.ex. gestion d'une crise en temps réel) plutôt que sur des questions théoriques.

4. Les participants du Forum ont invité le Centre de Politique de Sécurité de Genève à continuer d'apporter sa contribution en matière de protection des infrastructures critiques en organisant des ateliers centrés sur des questions spécifiques.

ANNEXE I

FORUM SUR LES INFRASTRUCTURES CRITIQUES ET LA CONTINUITE DES SERVICES DANS UN MONDE DE PLUS EN PLUS INTERDEPENDANT

PROGRAMME

MARDI 28 OCTOBRE 2003

08:00 - 09:00	INSCRIPTION ET CAFÉ
09:00 - 09:15	OUVERTURE ET PAROLES DE BIENVENUE

- **Ambassadeur Gérard Stoudmann**, Directeur, Centre de Politique de Sécurité, Genève
- **Sénateur Paul Girod**, Président, Haut Comité pour la Défense Civile, Paris
- **Prof. François Heisbourg**, Directeur, Fondation pour la Recherche Stratégique, Paris ; Président du Conseil de Fondation, Centre de Politique de Sécurité, Genève ; Président, Conseil de l'Institut International d'Études Stratégiques, Londres

09:15 - 09:30 ALLOCUTION D'OUVERTURE :

M. Claude Mandil, Directeur Exécutif, Agence Internationale de l'Energie, Paris

REUNIONS PLENIERES

09:30 - 11:00 RISQUES ET CRISES ÉMERGENTES : UNE NOUVELLE DONNE

Modérateur : **Dr. John Gault**, Président , John Gault S.A., Genève ; Membre Associé de la Faculté, Centre de Politique de Sécurité, Genève

Intervenants :

- **M. Alain Bauer**, Criminologue et Consultant, AB Associates, Paris
- **M. Mike Granatt**, Cabinet Office, Londres, Directeur général, Government Information and Communication Service (GICS) ; précédemment : Chef du Civil Contingency Secretariat
- **M. Jean-Philippe Grelot**, Groupe d'experts du G8 ; Chargé de mission « Protection et Sécurité de l'Etat », Secrétariat Général de la Défense Nationale, Paris
- **Dr. Patrick Lagadec**, Directeur de recherche, Ecole Polytechnique, Paris
- **Dr. Erwann Michel-Kerjan**, Chercheur, Center for Risk Management, The Wharton School, Philadelphia
- **M. Daniel B. Prieto**, International Affairs Fellow, Council on Foreign Relations ; Professional Staff, Select Committee on Homeland Security, U.S. House of Representatives, Washington D.C.

11:00 - 11:15 PAUSE CAFÉ

11:15 - 12:45 **QUE FONT LES ORGANISATIONS INTERNATIONALES ET RÉGIONALES ?**

Modérateur : Dr. Terrence Kelly, Directeur de recherche, Rand Corporation, Pittsburgh

Sous-groupe 1 : COOPÉRATION INTERNATIONALE

- **M. Pascal Gondrand**, Directeur de Cabinet, Chargé de l'Information, Organisation Internationale de la Protection Civile - OIPC, Genève
- **M. Jean Fournet**, Secrétaire général adjoint pour la diplomatie publique, OTAN, Bruxelles
- **M. Barrie Stevens**, Directeur-adjoint, Unité Consultative auprès du Secrétaire général, OCDE, Paris

Sous-groupe 2 : COOPÉRATION RÉGIONALE : UN EXEMPLE, L'EUROPE

- **M. Jean-Pierre Massué**, Secrétaire Exécutif de l'Accord EUR-OPA-Risques Majeurs, Conseil de l'Europe, Strasbourg
- **M. Geoffrey Hamilton**, Conseiller régional, Commission Économique des Nations Unies pour l'Europe, Genève
- **Col. Giuliano Porcelli**, Expert, Département de la Protection Civile, Présidence du Conseil des Ministres, Rome

12:45 - 14:15 DEJEUNER DE TRAVAIL

M. Pierre Maciejowski, Directeur général Thalès Security Systems : « **De la biométrie à la détection NBC : les technologies clés dans un système de protection d'infrastructures critiques** », Thalès International, Paris

14:15 - 15:30 **QUE FONT LES GOUVERNEMENTS AU NIVEAU INTERNATIONAL ?**

Modérateur : Ambassadeur André Lewin, Premier Vice-président de l'Académie Diplomatique Internationale, Paris ; ancien Ambassadeur de France en Guinée-Conakry, Inde, Autriche, Sénégal-Gambie ; porte-parole de M. Kurt Waldheim, ancien Secrétaire général des Nations Unies, New York

Intervenants :

- **M. Philippe Meunier**, Sous-Directeur de la Sécurité, Direction des Affaires Stratégiques, de Sécurité et du Désarmement, Ministère des Affaires Etrangères, Paris
- **M. Christopher Painter**, Président, Sous-groupe du G8 sur le crime en matière de haute technologie (Groupe de Lyon) ; Chef-adjoint, Section chargée du Cybercrime et de la Propriété Intellectuelle, Département de la Justice, Washington D.C..
- **M. Joseph P. Richardson**, Senior Foreign Affairs Advisor, International Critical Infrastructure Protection, US Department of State, Washington DC
- **M. Helmut Schmitt von Sydow**, Directeur, Energies Conventionnelles, Commission Européenne, Bruxelles
- **M. Alexander Zmeevsky**, Directeur du département en charge des nouveaux défis et des nouvelles menaces, Ministère des Affaires Étrangères, Moscou

15:30 - 15:45 PAUSE CAFÉ

15:45 - 17:15 COMMENT LES SOCIÉTÉS PRIVÉES PEUVENT-T-ELLES ASSURER L'INTERFACE AVEC LES POLITIQUES DU SECTEUR PUBLIC ?

Modérateur : M. Howard A. Schmidt, Vice-président, Chef de la Sécurité en matière d'information, e-Bay Inc, Campbell, Californie ; précédemment : Chef de la Sécurité, Microsoft Corp, Californie ; Président, US President's Critical Infrastructure Protection Board ; Conseiller Spécial pour la Cyber-Sécurité à la Maison Blanche, Washington

Intervenants :

- **M. Daniel Bircher**, Chef de la sécurité informatique, Ernst Basler Partner AG, Zollikon/Zurich
- **M. Aled Miles**, Vice-président et Directeur exécutif, Symantec Northern Europe, UK
- **M. Kyle Olson**, President, Community Research Associates, Inc., Alexandria, Virginia
- **M. Michael Stepek**, Avocat, Solicitor to the Supreme Court of England and Wales, Winston & Strawn, Genève
- **M. Christian Sommade**, Directeur du développement, Défense et Sécurité, Groupe Cegelec ; Membre de la Commission de Sécurité du GITEP (Association des Industries de Sécurité et de Défense) ; Secrétaire général, Haut Comité Français pour la Défense Civile, Paris

19:30 - 22:30 DINER ET ALLOCUTION AU MUSEE ARIANA

Rt. Hon. Mike Moore, Membre du Conseil de Direction, Société Générale de Surveillance S.A., Genève ; précédemment : Premier Ministre de Nouvelle-Zélande ; Directeur Général, Organisation Mondiale du Commerce, Genève

MERCREDI 29 OCTOBRE 2003

08:15 - 08:45 EVENEMENT PARALLELE

« Risques et menaces actuels de piratage informatique et solutions novatrices et durables pour les multinationales, les organisations et les administrations gouvernementales » par **M. Marco Ricca**, Associé, ILION Security SA, Genève ; Chercheur à Hewlett Packard Trusted Systems Lab, Bristol et au Laboratoire de Sécurité et Cryptographie, Ecole Polytechnique Fédérale de Lausanne (EPFL)

09:00 - 09:15 REUNIONS OFFICIELLES

« Questions relatives à la chaîne de sécurité en matière d'approvisionnement » par **M. Sten Bertelsen**, Vice-président, Département des assurances commerciales, Société Générale de Surveillance Holding S.A., Genève

09:15 - 10:30 SESSION PLENIERE

SÉCURITÉ DU RÉSEAU D'INFORMATION

Modérateur : M. Christopher Painter, Président, Sous-groupe du G8 sur le crime en matière de haute technologie (Groupe de Lyon); Chef-adjoint, Section chargée du Cybercrime et de la Propriété Intellectuelle, Département de la Justice, Washington D.C.

Intervenants :

- **M. Ted Barry**, Manager, Private Sector Outreach, UK National Infrastructure Security Coordination Centre (NISCC), Londres et G8 "CIIP Experts Group"
- **M. Michel Dupuy**, Groupe d'experts du G8 ; Chef du CERT / Administration, Secrétariat Général de la Défense Nationale, Paris
- **M. Jan Lundberg**, Spécialiste en questions stratégiques, Agence Suédoise de Gestion des Crises, Stockholm
- **Dr. Jan Metzger**, Directeur de Recherche, Centre pour les Études de Sécurité, ETH Zurich, Zurich
- **M. Andrea Servida**, Chef de secteur, Commission Européenne, Direction Générale Société de l'Information, « Confiance et Sécurité », Bruxelles

10:30 - 10:45 PAUSE CAFE

10:45 - 12:30 SESSIONS PARALLÈLES

Session I : SÉCURITÉ DU RÉSEAU DE TÉLÉCOMMUNICATIONS

Modérateur : M. Eduardo Gelbstein, Independent Advisor, Senior Special Fellow, United Nations Institute for Training and Research, Geneva

Intervenants :

- **M. Jean-Louis Blanot**, Directeur délégué pour le domaine gouvernemental, Direction de la Sécurité et de l'Information, France Télécom, Paris
- **Mme. Olivia Bosch**, Directrice de Recherche, Programme sur les nouveaux défis en matière de sécurité, Royal Institute of International Affairs, Londres
- **M. Neil Fisher**, Vice-président, Information Assurance Advisory Council (IAAC) and Macro Security Capabilities Leader, QinetiQ, Malvern, UK
- **M. Hugo Straumann**, Responsable de la Sécurité, Swisscom Innovations, Swisscom AG, Berne

Session II : SÉCURITÉ DES FOURNITURES DE GAZ

Modérateur : M. Nordine Ait-Laoussine, President, Nalcosa ; précédemment : Minister of Oil, Algeria

Intervenants :

- **M. Giorgi Vashakmadze**, Président du Sous-Comité du « couloir eurasien », Parlement de Géorgie ; précédemment : Directeur général, Georgian International Oil Corporation, Tbilisi
- **Mme. Sylvie Cornot-Gandolphe**, Administrateur Principal, Expert Gaz, Agence Internationale de l'Energie, Paris
- **M. Philippe Mannoni**, Secrétaire exécutif , Gas Transmission Europe, Bruxelles

12:30 - 14:00 DEJEUNER DE TRAVAIL

M. Roger Naff, Directeur Marketing, **"Protection des infrastructures critiques et transport mullti-modal"**, Boeing Homeland Security & Services, Californie

14:00 - 15:30 SESSIONS PARALLÈLES

Session I : SÉCURITÉ DES MOYENS DE TRANSPORT

M. Michel Quatre, Ingénieur Général des Ponts et Chaussées; Haut Fonctionnaire de Défense, Ministère de l'Equipement, des Transports, du Logement, du Tourisme et de la Mer ; Commissaire Général aux Transports, Paris

Intervenants :

- **M. Jean-Louis Blanchou**, , Directeur de la Sûreté, Aéroports de Paris (ADP), Paris
- **M. Michel Babkine**, Administrateur en chef des Affaires maritimes et chargé de mission "Sûreté maritime", Secrétariat général de la mer, Services du Premier Ministre, Paris
- **M. Andrew Charlton**, Director of Industry and Government Affairs, Société Internationale de Télécommunications Aéronautiques (SITA), Genève
- **M. Bruno Masnou**, Vice-président, Systems & Defence Electronics, Homeland Security Unit, European Aeronautic Defence and Space Company (EADS), Paris
- **M. Pierre Perrod**, Président du Comité de Sûreté, Commission du Tunnel sous la Manche, Paris

Session II : QUESTIONS DE SÉCURITÉ ET PRODUCTION D'ÉNERGIE NUCLÉAIRE

Moderator : Mme. Anita Nilsson, Chef du Bureau de la sûreté nucléaire et Coordinateur de la sûreté nucléaire, Département de la sécurité nucléaire et de la sûreté, Agence Internationale de l'Energie Atomique, Vienne

Intervenants :

- **M. Denis Flory**, Chef du Département de sécurité des matières radioactives, Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France
- **M. Christian Gobert**, Directeur général adjoint, Cogema, Groupe Areva, Paris
- **M. Ramon Revuelta**, Directeur adjoint, World Association of Nuclear Operators, Paris Center
- **Dr. Beat Wieland**, Chef de la section Energie Nucléaire, Office Fédéral de l'Énergie, Berne

15:30 - 16:15 SEANCE PLENIERE : **CONCLUSIONS DU FORUM ET PLAN D'ACTION**

Président : M. Jean-François Daguzan, Maître de recherche, Fondation pour la Recherche Stratégique, Paris ; **Dr. Patrick Lagadec**, Directeur de recherche, Ecole Polytechnique (Laboratoire d'Économétrie), Paris ; **Dr. John Gault**, Président , John Gault S.A., Genève ; Membre Associé de la Faculté, Centre de Politique de Sécurité, Genève

ANNEXE II

REUNION MINISTERIELLE JUSTICE/AFFAIRES INTERIEURES

5 mai 2003, Paris

LES PRINCIPES DU G8 POUR LA PROTECTION DES INFRASTRUCTURES VITALES D'INFORMATION ET DE COMMUNICATION

(Adopté par les Ministres de la Justice et de l'Intérieur du G8, mai 2003)

Les infrastructures d'information et de communication constituent une part essentielle des infrastructures vitales. En conséquence, afin de protéger efficacement leurs infrastructures vitales, les Etats doivent protéger leurs infrastructures vitales d'information et de communication d'éventuels dégâts et les sécuriser face aux risques d'agression. Une protection efficace des infrastructures vitales comprend l'identification des menaces contre ces infrastructures, la réduction de leurs vulnérabilités aux dommages et aux attaques, la minimisation des dégâts et de temps de restauration en cas de dommages ou d'attaque, et l'identification de l'origine des dégâts ou de la source de l'attaque en vue de leur analyse par des experts et / ou de leur investigation par les services judiciaires. Une protection efficace exige aussi communication, coordination et coopération, nationales et internationales, entre toutes les parties prenantes -industriels, universitaires, secteur privé et structures administratives, mais aussi services de protection des infrastructures et services de police. De tels efforts doivent être entrepris avec un respect évident de la sécurité des informations et de la législation relative à l'assistance mutuelle et à la protection de la confidentialité.

En vue de ces objectifs, nous adoptons les PRINCIPES suivants et encourageons les Etats à les prendre en compte pour développer une stratégie de réduction des risques encourus par les infrastructures vitales d'information et de communication.

I. Les Etats devraient constituer des réseaux d'alerte et d'urgence face aux vulnérabilités, aux menaces et incidents affectant les systèmes d'information et de communication.

II. Les Etats devraient renforcer la sensibilisation des parties prenantes pour faciliter leur compréhension de la nature et de l'importance de leurs infrastructures vitales d'information et de communication, ainsi que du rôle que chacun doit jouer dans leur protection.

III. Les Etats devraient examiner leurs infrastructures et identifier leurs interdépendances afin de renforcer leur protection.

IV. Les Etats devraient promouvoir le partenariat entre les parties prenantes, qu'elles soient publiques ou privées, afin qu'elles partagent et analysent leurs informations sur

les infrastructures vitales en vue de la prévention des dégâts et des attaques à l'encontre de ces infrastructures, de leur enquête et de leur parade.

V. Les Etats devraient créer et entretenir des réseaux de communication de crise, et les tester afin de garantir leur bon fonctionnement, leur sécurisation et leur stabilité en cas de crise.

VI. Les Etats devraient s'assurer que les règles d'accès à l'information ne nuisent pas au besoin de protection des infrastructures vitales.

VII. Les Etats devraient faciliter le traçage des attaques contre les infrastructures vitales d'information et de communication et, selon l'opportunité, la divulgation des données de traçage aux pays étrangers.

VIII. Les Etats devraient assurer des actions de formation et mener des exercices pour améliorer leur capacité de riposte et tester leurs plans de continuité et de secours face aux attaques contre les infrastructures d'information et de communication, et devraient encourager les opérateurs à faire de même.

IX. Les Etats devraient s'assurer que leurs dispositions législatives pénales et procédurales, à l'instar de celles de la Convention du 23 novembre 2001 du Conseil de l'Europe relative à la cybercriminalité, et que leur personnel formé leur permettent d'enquêter sur les actes de malveillance contre des infrastructures vitales d'information et de communication et de les poursuivre, et de coordonner, en tant que de besoin, de telles investigations avec des pays étrangers.

X. Les Etats devraient s'engager dans une coopération internationale, selon les opportunités, pour sécuriser les infrastructures vitales d'information et de communication, comprenant, dans le respect des lois nationales, le développement et la coordination des systèmes d'alerte et d'urgence, l'échange et l'analyse d'informations relatives aux vulnérabilités, aux menaces et aux incidents, et la coordination des enquêtes sur les attaques contre de telles infrastructures.

XI. Les Etats devraient promouvoir la recherche et le développement nationaux et internationaux et encourager l'application de techniques de sécurité certifiées au regard de normes internationales.