Sénat de Belgique

international risk governance council

OSCE : SECURITY AND RISK MANAGEMENT IN EUROPE

Hemicycle of the Senate

Brussels, April 18th - 19th 2006

PROGRAMME

Tuesday April 18th 2006

09.30 Registration

10.00 Opening speech by Mrs. Anne-Marie Lizin, President of the Belgian Senate

10.10 **Dr. Patrick Lagadec**, Director of Research, École Polytechnique, Paris : *« Unconventional risks, unthinkable crises : the vital need of paradigm shift, and strategic jump »*

10.45 **Dr. Warner North**, President of NorthWorks Inc., Belmont, USA, Professor in the Department of Management Science and Engineering at Stanford University *: " Energy security for the Baltic region : issues motivating improvement in international cooperation on risk governance "*

11.15 **Dr. Liviu Muresan**, Executive President of EURISC (European Institute for Risk, Security and Communication Management), Bucharest, Romania : *" Reinventing security and discovering risk governance "*

11.45 General discussion

12.30 Walking lunch

14.15 **Prof. Dr. Ortwin Renn**, Professor for Environmental Sociology, University of Stuttgart, Germany :
" Risk governance : concept and policy implications "

14.45 **Prof. Ing. František Božek**, University of Defence, Faculty of Economy and Management, Civil Protection Department, Brno, Czech Republic :
" Protection of critical infrastructure "

15.15 **Mr Bart D'Hooge**, Federal Police, Commissioner General's Office, Directorate Policy International Police Cooperation, Head of Service European Coordination, Belgium :
" Civil crisis management "

15.45 **Mr Askar Nursha**, Head of Department of Foreign Policy Studies, Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan :
" Kazakhstani approach to risk governance in Eurasia "

16.15 **Mr Karl Widmer**, Vice- Director, Federal Office for Civil Protection, Bern, Switzerland :
" Civil emergency management in a federal state : the Swiss solution "

16.45 General discussion

17.30 End

Wednesday April 19th 2006

10.00 **Prof. José Mariano Gago,** Chairman of the IRGC Board :
Presentation of the International Risk Governance Council

10.30 Presentation of the draft joint declaration

12.00 General discussion and adoption of the draft joint declaration

Mrs Lizin, president of the Senate. – Let me welcome you on this Conference on "OSCE: Security and Risk Management", I have the honour to preside over.

Humanity has always been confronted with huge crises and disasters. The threats are the result of forces of nature such as the 2004 Christmas tsunami, technological failures, such as the Chernobyl Accident in 1986, terrorism, such as "9/11", the danger of a possible anthrax contamination in 2003, etc., wars, nuclear, industrial and chemical disasters (we remember us Seveso), the SARS epidemic, etc. All those threats cause unforeseen and unimaginable effects, and contain more widely a large-scale public health risk.

One of those threats is the risk of a nuclear disaster. Mentioning the danger of nuclear accidents, we all think immediately about what happened in Chernobyl. On April 26th, 1986, the world's worst nuclear power accident occurred at Chernobyl in the former USSR, now Ukraine.

The Chernobyl nuclear power plant located 80 miles north of Kiev had 4 reactors and whilst testing number 4, numerous safety procedures were disregarded. The chain reaction in the reactor became out of control creating explosions and a fireball which blew off the reactor's heavy steel and concrete lid. The out-of-control reaction blew off the roof of the steel building and spewed tons of radioactive material into the air, releasing 30 to 40 times as much radioactivity as the Hiroshima and Nagasaki atomic bombs combined in 1945.

Immediately after the explosion, 203 people were hospitalized, of whom more than 30 dies from accute radiation exposure. Most of these were fire and rescue workers, trying to bring the accident under control, who were not fully aware of how dangerous the radiation exposure was. 135 000 peopole were evacuated from the area, including 50 000 from the nearby town of Pripyat.

This apocalyptic nuclear accident has still consequences more than 20 years later: health problems, economic ans social consequences, etc. Health officials have predicted that over the next 70 years, there wille be a 2% increase in cancer rates in much of the population which was exposed to 5 à 12 EBq of radioactive contamination released from the reactor. The issue of long-term effects of the Chernobyl disaster is inevitably controversial.

Anyway, in September 2005, a report by the Chernobyl Forum, comprising a nomber of agencies including the International Atomic Energy Agency, the World Health Organisation, other UN bodies and the governments of Belarus, the Russian Federation and Ukraine, put the total predicted number of deaths at 4 000. Children died from thyroid cancer.

The Chernobyl accident was a unique event, on a scale by itself. It was the first time in the history of commercial nuclear electricity generation that radiation-related occurred. For the occasion of the 20th anniversary of the Chernobyl accident, an international conference "Comchernobyl", which starts this week in Minsk, has the main objective to analyse the accumulated Chernobyl disaster relief experience and develop recommandations to define the strategy of action in this field for the next decade.

Other "industrial" accidents were responsible for a lot of killed people. Well known cases are the Bhopal disaster (in 1984, a Union Carbid plant in Bhopal, India, leaked 40 tons of a very toxic gas, which killed at least 15 000 people; the Seveso disaster (in 1976: a valve broke at a chemical plant in northern Italy, releasing a cloud of chemicals containing dioxine that wafted an estimated 50 meters into the sky; carried southeast by the wind, the toxic cloud enshrouded the municipality of Seveso and communities in the area).

Le sujet est difficile et inquiétant. La gouvernance peut être en péril. Seveso, Bhopal, le sang contaminé, l'amiante, la vache folle, Erika, AZF-Toulouse, le Prestige.

Les tempêtes de 1999 et la canicule en 2004 en France, le changement climatique, les vulnérabilités informatiques. Les attaques du 11 septembre, les attaques ou alertes à l'anthrax, le spectre de la variole, ….

Nombre de disciplines ont été mobilisées bien au-delà des sciences de l'ingénieur. Des avancées, en termes d'outils et de pratiques de sécurité, de débats, de dispositifs institutionnels, ont été acquises sur le terrain. D'indéniables progrès ont été faits dans la matière des risques. Cependant, les défis ne cessent de sortir des cadres établis, de déborder les terrains que l'on vient de conquérir.

Het verheugt me ten zeerste vandaag en morgen de grootste deskundigen inzake risicodetectering en –beheer te kunnen aanhoren. Het is een uitdaging voor de OVSE op dit terrein een stap vooruit te zetten. Het is bovendien een goede oefening om deskundigen en parlementairen van meer dan 55 staten samen te laten debatteren.

Today we have the big pleasure to receive all these distinguished researchers who will speak about all facets of security and risk government. Special thanks to Prof. Gago, President of the IRGC, to Prof. Contzen, member of the Scientific Board and Mister Christopher Bunting, secretary general of the International Risk Governance Council, for the constructive collaboration in the organisation of this colloquium.

Mr Patrick Lagadec. – Risks and crisis are becoming more and more crucial and vital for our countries. For decades risks and crisis have been seen as something of a second order of importance, something which is left to the firemen, the army, or some specialist. Risk was not thought of as a question of strategy.

Why is the challenge of risk so difficult and so important? What are the key traps present when confronted with these unconventional events and more importantly what can be done to avoid them? These questions have to be handled strategically.

Take for example Hurricane Katrina in New Orleans. Why was this such a catastrophe? During Hurricane Katrina people were confronted with off-scale complexities, they had to face the hurricane itself, huge floods, toxic swamps, riots and many, many other problems all at the same time.

If the tactical plan is to only address something specific and no preparations have been made in case of many problems occurring at the same time in the same place then the first problem which arises when an unexpected event occurs is how to handle it.

Secondly, even before it is known what to do you are confronted with 'globalisation in speed'. You realise that if you lose this harbour you lose something very strategic for the whole country.

You realise if you don't repair the pipeline New York will be cut off from oil within two days leading to world-wide consequences. Dealing with a problem locally is very difficult but it is not enough. Problems have to be dealt with on both a global and local level at the same time.

The 'texture dimension' is another dimension people are not used to. Each person, each director, is shocked by what he/she has to leave behind during unexpected events or catastrophes. All the families, all the people, all the employees left without houses, all ask themselves where their families are, where their customers/suppliers are and so on.

There are many organisations given immediate mutual aid, for example the airport of New Orleans was supported by the fireman but the question here is what do the people do when the firemen leave the airport? The support is of an immediate nature and not an ongoing nature. The whole global texture was completely struck by Hurricane Katrina. The inconceivable question emanating from Hurricane Katrina was 'in one minute did we lose a town'?

The second question; New Orleans is important but what if it were a hub-city like Houston? Hurricane Rita occurred near Houston just after Hurricane Katrina. What would it mean to lose a hub-city today? The same challenges are present globally, the first problem is going from local to global.

Secondly there are network problems. IAJC worked on the network, critical infrastructure problem. It is like a skeleton, in one moment there is very high speed domino effects throughout the whole systems, across borders, again 'globalisation in speed'. In a few days it is possible to go from Hong Kong to Toronto at very high speeds. We are not used to this. We are used to speed for emergency. We are prepared for one accident but when it is a whole country and all citizens are effected by a problem it tends to be many days before organisations are able to step in. This was seen during the heat waves in France, Italy, Chicago and so on.

There are many problems today which seem to be out of our control: 9/11, Anthrax, pandemic problems. The problem which exists is that all of our tools, our managerial computers are for something specific, something stabilised, something marginal. The current paradigms do not fit with these problems.

As soon as these problems occur the immediate reaction is a sort of 'bunker effect', we don't know what to do. Why are we trapped in our vision and what happens when we are confronted with crisis?

Every country in the world seems to be preparing to fight the last war. We are not only confronted with one specific event but something very complicated.

We are prepared for single events. But if there are exceptions, irregularities, or disorders, globally we are not prepared for this. This leads to chaos when something unexpected happens. What do we do? Wait.

Where are the wounded people? Everywhere, perhaps, we don't know, what do we do? How do we clarify the problem? Let's wait for a few years and then clarify it.

The belief we have is it is not possible, it is not my duty, it is not my responsibility, see the firemen, see anybody, but I am not in charge. This is the normal way these sort of challenges are answered and naturally it takes time to react to something you are not used to or are not prepared for. There is a tendency for teams to become completely disrupted by these unexpected events. Teams like to follow a script. If there is no script anymore, and you are trained just to follow a script, there will be a fiasco.

When these unthinkable crises occur the first thing that happens is to divide all institutions, between the private and public sectors, between ministries, even in the same building. It is not strange, it is a result of the 'stun effect' originating from these new crises. People lose their temper, lose their way of doing things. People on the ground like those in New Orleans felt that they were totally abandoned, there was no communication, nobody came to help them, they had to wait, to wait and to wait.

The problem which then arises, and this is a real political problem, is to avoid a certain disarray of people in charge, and to avoid a loss of confidence in the people for the people in charge. The disconnecting process which arises between the people and people in charge needs to be avoided.

9/11, was called a 'failure of imagination', and Hurricance Katrina was called a 'failure of initiative'. The key element here is to really understand why there are so many difficulties. The problem is if no paradigm exists to confront these crises we will be lost in any circumstances.

How can this challenge be met? Firstly, do not fight the last war. Be prepared to look ahead, this is the first paradigm of shift. The key notion of discontinuity must be worked on. Rather than working on something which is very far away we must work on something which is at the heart of our systems and work on this from a discontinuity point of view. In New Orleans, for example, the coast guards did in three weeks what they did in 10 years in the whole country, to save people during Hurricane Katrina. This is something which is not in our Gaussian approach of statistics.

Secondly, which is very important is to shift the thinking from 'let the fireman do that' to 'make the people in charge, at the highest level, really be in charge'. Empowerment, you have to work with people and not against them or without them. This is what was discovered in New Orleans. The teams which worked the best where the teams where the team leader used his people. If employees are lost, or confidence is lost then everything is lost. Team work is vital, we must think of others, their family is my problem too. I have to work with the whole texture of my system, my environment, this means confidence, trust, working with, preparing with and not I have a plan, I will be in charge. No, I work with people.

The quote from Giuliani, the mayor of New York, about 9/11 demonstrates this: 'He had more faith in us than we had in ourselves'. This is something to work on now, how to develop faith, confidence and working together.

Concerning innovative policies, it is usual to have drills but much more must be done now to have 'outside the box' initiatives, either for debriefings, simulations, partnerships with people from different countries, between public and private sectors and so on. Regarding Strategic Intelligence, fast response teams are in place ready to act but no strategic thinking exists to be used whenever something new arises.

There are four points which need to be addressed in a crisis situation. Firstly, what is it about? When a crisis occurs nowadays it is not exactly known what it is about. Secondly, what are the key traps that need to be avoided? Thirdly, who are the stakeholders? This is going to change very rapidly during a crisis. Finally, and this is very important, what initiatives can be taken in order to possess the capability to do something and to be in a position of confidence?

Strategic Intelligence bodies have to be established. Generally, when there is crisis people think they must act first and then think. However, in the type of crisis situations which are occurring nowadays it is essential to think, and to ask what the crisis is about and what the key traps are. Bodies and groups of people have to be trained to work on asking these questions before any event occurs.

This can be worked on together in advance. People in charge must be educated, not to have all the answers or the ready-made scripts, but to confront the unknown together instead. This is something which is not known and probably is not liked because it is so comfortable to have scripts for everything and to say if it doesn't go to script then I'm not in charge. No, if it doesn't go to the script I am in charge and I have to be prepared to do this. New answers to new problems must be searched for and found. They will not simply fall like a gentle rain from the sky.

Mr Warner North. – Security of energy supply was a major concern for political leaders in the 20th century, and it promises to be an even more important issue for political leaders in the 21st century. Energy security deserves very high priority in an agenda for risk management in Europe, and as an area for deliberation and leadership from the OSCE.

The Baltic States of Lithuania, Latvia, and Estonia were part of the Soviet Union until the end of the Cold War. These newly independent states are now part of the European Union, but their electric power systems and natural gas supply are a legacy from Soviet times, closely integrated with Russia, rather than with the European Union. The recent Green Paper refers to the Baltic States as an "'energy island,' largely cut off from the rest of the [EU] Community."

The government of Lithuania agreed as a condition for its membership in the European Union to shut down the Ignalina Nuclear Power Plant (NPP) [2]. This plant has two 1500 MW nuclear generating units of the graphite channel (RBMK-2) type, the same design as for the Chernobyl NPP in the Ukraine. Ignalina NPP was built during the time of the Soviet Union to provide electricity for the Baltic region, and it became a part of Lithuania when Lithuania became an independent country. Its 3000 MW generation capacity has allowed Lithuania to meet most of its own needs for electricity from this NPP and also to export large amounts of electricity to Latvia, Estonia, Belarus, and the Russian Federation. The first unit was shut down at the end of 2004. The second unit is scheduled to be shut down in 2009. Shutting down these two nuclear units will require that this electric generation be replaced by other energy sources, such as natural gas from Russia or a heavy oil/water mixture called “orimulsion” from Venezuela.

Increased reliance by European countries on natural gas from Russia has positive features for these countries and also for Russia. Russia has extremely large natural gas resources that can be developed and transported to European countries for costs that should be competitive with other energy sources. Natural gas does not contain sulfur, nitrogen, metals, or complex hydrocarbons, so control of air pollutants is inherently much more easily accomplished than for oil or coal. The low carbon content of natural gas compared to oil and coal implies lower levels of carbon dioxide emissions into the atmosphere. More use of natural gas, instead of coal or oil, therefore will reduce the potential for global climate alteration. For these reasons natural gas will increasingly be viewed as a premium fuel, for which customers are willing to pay a higher price.

Production areas of natural gas in Western Europe, such as in the North Sea, are depleting, and large new gas resources are unlikely to be discovered. Russia is known to have very large gas resources in the Arctic that are only now beginning to be developed, such as the Shtokman field. These resources could provide ample supplies for European consumers, including the Baltic States, for much of the 21st century.

Development of Russian natural gas for export to European countries will require considerable capital expenditure, including the construction of new pipelines and development of gas fields in the Arctic region. While agreement was reached between GAZPROM and German companies last year to construct a new gas pipeline to provide Russian gas to Germany, the Baltic countries and Poland expressed concern that this pipeline would bypass them and leave them dependent on single pipelines from Russia. The countries would have preferred an alternative overland route. The 2004 interruption of gas supply to Belarus, the New Year’s Day 2006 interruption of gas supply to the Ukraine, and the recent terrorist attacks on the pipelines to Georgia have increased concerns among Europeans that the supply of gas from Russia may not be reliable. Events such as equipment breakdowns and extreme weather can lead to supply interruptions. The planning of the multibillion dollar investments in gas field development and pipeline construction will depend on perceptions that (1) the price of the natural gas to customers will be competitive with other energy sources, and (2) that supplies will be reliable. Strengthened institutions and investments are needed to reduce risks that politically motivated shutdowns, equipment failures, extreme weather, or acts of terrorism will disrupt the transport of gas essential for heating and continued function of the economy in countries depending on natural gas imports. Alternative supplies of energy are available to Europe through North Africa, the Middle East, and possibly from Central Asia, especially as new pipelines or LNG facilities are constructed. The Baltic States are in an unfavorable position to receive natural gas or electricity from their EU neighbors, because their existing infrastructure connects eastward to the Russian Federation.

Analysis using probabilistic risk methods and economics can address (1) the competition in price between gas from Russia and other energy materials for meeting the needs of European Countries, looking forward for decades (2) the uncertainties arising from weather, equipment failures, and political events, so as to plan for adequate redundancy in the energy supply system, so that the probability of significant supply interruption can be made acceptably low. Multiple natural gas pipelines connecting gas fields to customers, underground gas storage located in customer countries, and provision to obtain and use other supplies under upset conditions may be needed to assure adequate supply reliability. The cost of these facilities needed for adequate supply reliability should be included in calculating what it will cost to provide gas from Russia to serve export markets in Europe. Understanding how the European energy system may evolve over a period from now to the middle of the twenty-first century can be greatly aided by the use of advanced energy modeling tools. Energy models are particularly useful for projecting changes as energy prices and the availability and cost of energy technologies change over time. The models can also be used to analyze upset conditions, such as those that occurred in the United States following the hurricane damage in 2005.

The author has presented papers at recent conferences for the European Commission SEIF-IV meeting in 2005, and risk management meetings in early 2006 for VNIIGAZ/GAZPROM and for RAO-”United Energy Systems” in Moscow, with details on analysis methodologies appropriate for this problem. At this meeting, for an audience of political leaders from the 55 countries that are members of the OSCE and from the host organization, the Belgian Senate, the presentation focuses on motivating such analysis as a basis for planning the energy future of the Baltic States – where a substantial transition must be made, and where large investments in expanding the energy infrastructure will be needed. Such an effort can be a demonstration of methods not only for analysis, but also of collective international decision making using advanced concepts of risk management and risk governance described in recent reports of the International Risk Governance Council and the US National Academy of Sciences.

In planning Europe's energy future, the leadership in energy companies and governments need to work effectively together, and to overcome legacies of mistrust and misunderstanding that come from historical events and from differences in institutions and cultures. Effective planning and decision making require not only the mastery of analytical methods for dealing with the complexity and uncertainty of energy markets and technological development, but also learning how effective governance can be achieved among a multiplicity of stakeholders – national governments, the European Union and the G-8, energy companies, and concerned citizens in many countries. It is not just a technical problem – it is also an extreme social and political challenge! Meeting this challenge for the Baltic Region may help develop methods and procedures for more difficult, worldwide energy policy problems: (1) risks of oil supply interruption from the Middle East, (2) increases in oil and gas prices from the rapid industrialization occurring in China, India, and elsewhere, and (3) risks of alteration in the earth's climate because of the increasing atmospheric loading of carbon dioxide from combustion of fossil fuels.

The Baltic Countries, especially Lithuania, need assistance in implementing the agreement to phase out nuclear generation from the Ignalina nuclear power plant. Reliable natural gas supply from Russia could be one important source of replacement energy within the next four years. Other energy sources, including increased efficiency, biomass, and new nuclear plants, could be important on a longer time scale. The other nations of Europe, including Russia, should support the use of advanced analysis and dialog in support of decisions that must be taken soon to assure energy security for the Baltic Region. OSCE's leadership in this process will be most welcome.

Mr Liviu Muresan. – The Parliamentary Assembly of the OSCE was set up in the early 90's. At this time stability and security were discussed in different terms than in 2006. Take Romania for example, it is continually under threat of heavy flooding. In 2005 Romania experienced six waves of flooding, these were the heaviest recorded in the recent history of Romania. In 2006, the risk seems to be of a different kind. The politicians of Romania do not only need to fight against flooding, but they also need to fight landslides, as well as preparing for possible earthquakes in the future.

It is important for Europe to discuss the topic of risk. 9/11 is usually discussed when talking about the subject of security. But Europe has also experienced tragic events like the terrorist attacks which took place in Madrid and London as well as black-outs, not only in the States but also here in Europe. These events are becoming reference points in benchmarking and for identifying new and agreed needs to understand the priority to reforming the whole security concept. A much wider concept of security is needed.

Ralph Stacey had a vision over 10 years ago to speak about the need to stabilise instability. After so-called stability during the cold-war period we jumped to a profound and generalised instability. We have to be realistic and accept that the stability experienced before 1989 will never be seen again. What can be done is to find solutions on how to stabilise instability during periods of instability.

Security in the 21rst Century needs to be seen in a much wider sense. It is related to and pivotal for sustainable development on a local, regional and global level.

More and more it is the citizen who comes under huge threat, it is the citizen who suffers directly and who pays the cost as a citizen and as a taxpayer. Managing this security from the level of the individual to that of the international environment is important but not easy to do. A new approach is needed. New questions must be raised and new answers must be found.

Initially there was a preoccupation with the military domain. There is still a very poor cooperation between the military and civilians. They have to work closer and closer together and to transfer the expertise in order to find solutions to these problems.

Security now tends to be a common good, with specific market associated standards, ratings, in turn as a result of a future complex process of reform. This is a basic idea which has been developed. This is being pushed by the present political and economical interests, globalisation and market de-regulation in different parts of the world.

After 9/11 we started to think, together with colleagues from the United States and Western Europe; what would be the next 9/11? What needs to be changed immediately in terms of thinking and working together? We started to look at the way in which the private sector is ready to give answers to the problem of terror. Their answer is to simply say that terror is a part of the problems we have to face and we just have to accept this.

A study ‘Investing Against Terror: How vulnerable is Corporate America?’ published in The Financial Times found that people in charge of security are not trained for the new types of security companies have to face. At the same time it was discovered that many chief executives are looking mainly to the ‘physical security’ and have never ever held discussions with the people in charge of security in their own company. This lack of dialogue is a risk in itself.

One of the subjects of real concern in this study, was that this poor experience of the new non-military security is a real problem which has to be addressed. The knowledge which has already been received in different parts of our activities must be transferred to the private sector.

Sooner or later chief executives resorting to the crises committee, scenarios, risk mapping, early warning systems, will have to see these not only as challenges for the company but also as new business opportunities. We have to be optimistic, the more risk there is the more work there is and the more we have to do. We have to find solutions for this kind of new risk and new tools need to be found to tackle these new risks.

These new security solutions will lead to good governance, and will be crucial for better quality of life for citizens in the decades to come. It is necessary to look at these topics as part of the good governance and will be crucial for better quality of life of the citizens.

Global governance is a broad concept. The sum of the many ways, individuals and institutions, public and private, manage their common affairs and at the same time the neighbourhood. Never before have so many people had so much in common but never before have the things that divide them been so obvious. How can these kind of issues be dealt with?

At the beginning of the 21rst Century the international community has to cope with new emerging systemic risks which will co-exist with the old ones. New solutions have to be imagined and discussed. How does a parliament deal with such issues? How do they control them, approve them, discuss them? There are very specific committees, there are problems which are so complex which are part of different committees or are part of committees which are not yet organised.

The poor cross-fertilisation among professional communities puts the debate on 9/11 under a parochial perspective and not as a link between risk-security-communication-governance. Communication is very important. At the same time there is an urgent need to redesign the very concept of security, up to the level of ‘reinventing’ security in an era of profound economic, political, environmental, scientific, and religious challenges and changes.

Today security is perceived as the intervention of authorities into citizens’ life. Laws to improve security in our countries must be approved and introduced. How far, as a citizen, does intervention in our private lives have to be accepted in order to have more security?

Security should be thought of as a ‘common good concept’. It should also have a price associated to it. Security is a commodity which should be properly marketed, e.g. security marketing, and made available from the level of the citizen to higher levels of the society organisation.

In re-analysing the security concept one has to introduce and operate with so called operators such as ‘dynamism, complexity, the reduced importance of geographical sectors’. What is extremely important to understand is that geography is relevant. A tsunami in Asia is something we should look at carefully, not only because some of our people are there on holidays but because we have to learn. In Romania a possible risk was discovered which must be looked at and this is the risk of a tsunami in the Black Sea for which a solution must be found.

Security has a multi-dimensional descriptor indicator set: political, social, health, terrorism, extremism, crime related, religion, etc. and this must be worked on. The technologies and the scientific support are available to work on these issues.

There is a need for security standards. This was discovered, mainly after 9/11, when the accent was put on the need of a public-private partnership in security methods.

But how is it possible to work with private security when the same standards are not being used? How can on private security companies be relied on if they do not have the same language or are not using the same code of conduct?

The UN and other international institutions are supporting this relation between good governance and private security. The rating for security is needed to create a real market for security based on public-private partnership. These indicators are being worked on.

A sustainable security system is needed. To elaborate and to implement a security system only and not to check if it is sustainable will lead to problems all of the time from outside. Security must also be tangible for citizens. Everybody is looking for a new normality which is so difficult to obtain. The State is not only in charge of this. This instability must be stabilised and also some problems which are related to security as a common good.

Who are the actors or the stakeholders? We have actors which are becoming more and more active and are part of everyday life. In a center for combating organised crime in Romania a meeting with people participating on fighting terror and organised crime coming from about 20 countries was held. One of the conclusions was that it is no longer possible to think in a narrow view on organised crime or in a narrow view on terrorism because in practice there is a combination of terrorism and organised crime and these issues need to be tackled.

What is important is the proposal to think about risk governance. It is a solution introducing the concept of governance. The security sector reform in the countries in transformation but also in the other countries must look to the new agenda of security. This transformation of reform in relation to the new agenda of security has to be made.

Concerning security sector governance this concept of reform of the whole security sector must be analysed, not only from the point of view of reform in the defence but also reform in the field of police, and coast-guards and also reform in the area of intelligence.

More and more intelligence services are ready to open their minds to these kind of topics. Last year the German Intelligence Service, the Bundeskriminalamt in Wiesbaden held an international session to discuss the need of new alliances for the Intelligence Services.

The first alliance needed is alliance with Intelligence Services and the army, because usually these two bodies do not cooperate. The second alliance needed is between Intelligence services and Academic communities, alliance of Intelligence Services with foundations and civil society and the private and business sector. It is no longer possible to work together, to be part of the globalization, if you are not thinking together of the challenges which must be faced around the world.

It is very important to look at the critical infrastructures. In 1996, President Clinton launched an invitation to the American Business and Academic community to draft a report on Critical Infrastructures.

In 1997 the first document on Critical Infrastructures was introduced. In Europe the potential of the Critical Infrastructures was discovered after some years. Why is this so important? After 9/11 it was discovered that when speaking about vulnerabilities and protection of critical infrastructures it has to be accepted that, in countries like the UK for example, that 80% of the critical infrastructures are private. This is a new way of thinking and of acting of authorities and of private sectors on this issue. Critical infrastructures must be looked at from the perspective of business continuity which is so important.

What is interesting is that around the world there are several discussions about this kind of risk governance, new security agenda and so on.

In Brussels the first European Public-Private Security forum was held at the end of 2005. More than 350 people from all around Europe attended it to find out what were the markets, how to find solutions, how to cooperate and what the chances would be of surviving in an extremely competitive market in this field of security from both a public and private perspective.

The first European Conference on Security Research was organised for the first time in March this year in Vienna. The very broad programme of financing the research on security matters was launched.

In Prague in February there was a conference on Energy-Security. The Representative of NATO discussed possible tasks of NATO in the future. These tasks included protecting critical infrastructures and assuring the security of energy for Europe and the other countries. The way to deal with these new tasks must be thought about and could be a reality in some years. During a NATO advanced research workshop at the Black Sea the ports and the containers, which are the possible next 9/11, were discussed. If there was an attack how would it be dealt with? For example, how would a terrorist attack, or a criminal one in a port like Constanta which is the biggest in the Black Sea area be managed.

All topics must be discussed to attempt to make this cross-fertilisation. In the framework of the World Security Forum, based in Switzerland, a security time horizon of 2020, is being developed. Work can no longer be carried out in a parochial way. What is important now is to network ourselves.

It is important to realise that we are already a community, a community which must cooperate, which must transfer the expertise from countries with experience to countries in transformation.

The fact that the OSCE and the Parliamentary Assembly of OSCE and the Belgium Senate established this initiative for the 55 members of the OSCE to start to think of organising a committee to transfer this expertise and to enrich the debate in the field of risk security and good governance, is extremely commendable.

Mr Andronius Azubalis. – The output of electrical power in the Baltic states will significantly decline in the near future. By the year 2016, Baltic states will face deficits of electrical power generation due to the fact that the second unit of their nuclear power station will be closed down in 2009. At the same time Estonia is also planning to shut down its outdated blocks of its thermal power plant in Narva in 2016. In Mr. North's report he underlined that the only two options for Lithuania is to replace the closed nuclear power stations with 1. Natural gas from Russia or 2. A heavy oil/water mixture called a orimulsion from Venezuela.

At the same time the Baltic States are looking for another way to resolve this problem. On 27th February 2006 the Prime Ministers of the three Baltic States signed a joint communication agreeing to prepare a Common Baltic Energy Strategy this year, and to support the initiative to construct a new nuclear power plant in Lithuania and invited the energy enterprises of the Baltic States to invest in the project and the construction of the new nuclear plant in Lithuania. The Heads of the States also agreed to investigate the possibility for the development of a liquid-gas terminal and storage facility in one of the Baltic States, probably in Latvia.

If the Russian-Germany gas pipeline is to bypass the Baltic countries then they would be dependent on single pipelines from Russia which means gas for the Baltic countries would become more and more expensive. Recent experience shows that Russia uses its gas supply as a political tool and that it may not be too reliable. Examples of the unreliability of the Russian gas supply were seen in Ukraine, in Belarus, and in Georgia. This is a challenge not just for Baltic states but for all European communities.

The Russia-Germany pipeline construction under the Baltic Sea project costs twice as much if you compare it with a ground pipeline from Russia, via Poland or Baltic States to Germany. This project started without pre-consultation with the States concerned. This project will be looked at from an environmental-security point of view rather than from a cost point of view.

In 1947/48 according to an order issued by Soviet Union Military Administration in Germany about 40,000 extremely dangerous explosive bombs were sank in the Baltic Sea. The biggest part of these bombs were filled with yperite. From an environmental-security standpoint it is important for the OSCE to carefully examine or to create a special commission to investigate the possible effects of these gas pipelines on these explosives.

Mr Oleh Bilorus *(in Russian)*. – We have underscored here with a special political and humanitarian accent that the global catastrophe that Chernobyl – the twentieth anniversary of which all of humankind will sadly be commemorating – brought to bear on civilisation has not been erased, but continues to exist and carries the risk of being repeated in the future. That is why today's conference is a very important event, one that forces us to think about the fact that the overall prospect of civilisation's survival in the 21st century is the highest imperative of the development and, obviously, safe development is the most important resource and reserve for the progressive development of all humankind.

As today's experts pointed out, on completely justified grounds, it is necessary to organise controls for all high-risk production sites and industrial facilities by both the OSCE and the IAEA. It is clear that the very lack of such oversight led to the Chernobyl disaster, which became a planetary disaster, and not just a disaster confined to countries belonging to the former USSR (Belarus, Ukraine, and neighbouring states). Logically, we cannot escape such constant, daily inspections of operations, all the more so as everywhere we feel the shortfall of electric energy and, in this century, atomic energy will reach a critical mass.

The time has clearly come to create a security network, one that could take the form of an electricity network. Moreover, European solidarity has become a reality today. And Ukraine is thankful to all the donor countries that are investing huge sums of money through the European Bank for Reconstruction and Development to build a new, more secure, shield ("the sarcophagus") around the Chernobyl reactor.

I believe that this century will build a road not only to pan-European solidarity, but to global democratic solidarity as well, and, thanks to well-devised risk management and crisis-prevention systems, the threat about which the experts have spoken so convincingly here will be prevented. Moreover, in my view, scientists bear particular responsibility in this matter.

Each country must work to avert and cope with disasters and crises. Unfortunately, starting with the United States of America and ending with any other place on this planet, the record shows that such readiness does not yet exist. Not long ago we participated in a conference on developing the Barents Sea's resources. If one approaches the development of such resources from the position of traditionally conservative industrialism and the race for profit, then a planetary disaster could also come from the Arctic, meaning the disaster of global warming and other grave consequences for Europe.

We must think about these problems together. Moreover, I think that NATO can also play a role in organizing a warning and control system for risk situations. Ukraine is doing its utmost to develop new concepts, a new doctrine, and approaches to solving these problems. On the occasion of our conference, I brought my new book, published in Ukraine. As it happens, it is called "The Global Perspective and Sustainable Development". I understand that it is necessary to move forward today. Sustainable development must in future go hand in hand with development on a planetary basis, that is, on the basis of general human reason. The world has only one alternative: either to live reasonably as one family, or to die foolishly before this century ends. So, it is better to live and work on the future together.

Mr Ihor Ostash *(in Russian)*. – First of all I should like to thank the president of the Belgian Senate, Anne-Marie Lizin, for her wonderful opening speech, in which she especially highlighted the problem of Chernobyl, and our Belgian colleagues for this conference's brilliant organisation and the wonderful opportunity to exchange opinions on a very important topic that worries us all.

Indeed, this year marks the 20th anniversary of the Chernobyl disaster. While masses of various technological disasters have occurred, few of them have had consequences that we shall continue to feel for more than a century. The Chernobyl accident is just such a disaster. It is quite fitting that Chernobyl, when translated from Ukrainian, means "bitter grass". It was indeed a bitter experience for all humankind. This disaster also contributed to the collapse of the former Soviet Union and formation of new states on the territory of the USSR.

After this collapse, Ukraine found itself dealing with its very serious problem practically "one on one". I should like to remind you that today Chernobyl is surrounded by a thirty kilometre zone where there is no life. Yet "voluntary returnees" who wish to die where they were born are going back there. In addition, some unique monuments to Ukrainian culture remain in this zone.

Ukraine took an unprecedented step. Although it had no real substitutes, it closed Chernobyl Nuclear Power Plant, the future status of which can today be compared to that of Ignalina Nuclear Power Plant. However, the question of a credit line to make up for Chernobyl NPP's power showed that, unfortunately, humankind has a very short memory. In addition, I should like to stress in particular that this really is our common tragedy and no one here can brandish the well-known Ukrainian saying, "*моя хата краю*" (moya khata krayu), which means "It isn't my business", for here we are all in the middle of the problem.

So, building a new sarcophagus is indeed a challenge for the entire European community, since our safety for many, many years to come will depend on what kind of sarcophagus we build.

Let me add that a special session of the Ukrainian Parliament devoted to the twentieth anniversary of this terrible tragedy will be held in Kiev on April 26. We of course invite all who want to take part in this session to come to our country's capital, which, by the way, is located all of ninety kilometres from Chernobyl Nuclear Power Plant.

We hope that this twenty year experience will help us find new mechanisms and instruments so that we will be able to say that we did everything possible, so that in the future we can feel safe and no one will suffer any more from the consequences of the Chernobyl tragedy.

Mr Ali Berchiche. – Notre délégation remercie vivement la Présidente du Sénat de Belgique pour son aimable invitation à ce séminaire de haut niveau qui réunit d'éminents professeurs et collègues.

Mon pays est, comme vous le savez, confronté de façon cyclique à des catastrophes naturelles, telles que des séismes ou des inondations, et il est toujours sous la menace terroriste, même si on constate une nette amélioration grâce à la Charte sur la réconciliation nationale mise sur pied à l'initiative de notre Président de la République. C'est pourquoi nous souhaitons être associés plus étroitement aux travaux de groupe des spécialistes en gestion du risque et ce, malgré notre statut d'observateur au sein de l'OSCE. Cela nous permettrait de bénéficier de votre expérience en matière de gouvernance du risque.

Permettez-moi également de vous rappeler que notre pays s'est retrouvé, à un certain moment, isolé sur la scène internationale dans la lutte contre le terrorisme. Il a malheureusement fallu les événements du 11 septembre 2001 à New York, puis, les attentats de Madrid et de Londres après ceux de Paris, pour que l'on prenne enfin conscience d'un danger qui est universel. Nous vous avons écouté avec intérêt parler des risques industriels, évoquant le cas de Tchernobyl, car nous avons également des complexes industriels en matière de pétrochimie. C'est pourquoi nous souhaitons être associés aux travaux du groupe de travail, malgré notre statut d'observateur.

Mr Lahcen Daoudi. – On parle beaucoup de la sécurité en Europe et de la mondialisation de la sécurité. Je voudrais pour ma part évoquer la sécurité sur le plan politique. Il vaut mieux prévenir que guérir. Or bon nombre de problèmes de sécurité trouvent leur origine dans des situations politiques. Je pense à l'Irak ou à la Palestine. Les politiques ont une grande responsabilité en ce qui concerne la sécurité internationale et lorsqu'ils prennent des décisions, c'est la population qui en subit les conséquences.

Mr Gennady Novitsky *(in Russian)*. – Today, Mrs Lizin dwelt at length in her opening remarks on the problem of the Chernobyl disaster. I am very pleased that this conference, taking place on such a representative level, is discussing this problem. Of course, this problem, which will have taken place twenty years ago come April, has many facets. Without a doubt, this conference must set itself the goal of learning from this disaster, so that it becomes possible to create the conditions under which such disasters would not be possible and if – God forbid! – one did occur, we would be able to counter it actively and reduce the consequences of this type of technological disaster.

I think that one of the problems of this disaster is the fact that the Chernobyl power plant continues to exist on the territory of Ukraine and requires serious measures and major financial expenditures to make Europe and the world safe from the possible risk linked to the preservation of the station's reactor.

I think that the huge number of inhabitants of Ukraine, Russia, and Belarus who suffered as a result of the disaster is no less important a problem. Moreover, according to the IAEA's conclusions, more than eighty percent of the radioactive fallout came down on Belarussian territory.

According to experts, including the IAEA's specialists, the damages sustained by Belarus alone amount to roughly US$235 billion. In comparison, Byelorussia's budget the year that the accident occurred was such, that it would have taken the country about thirty-five years to eliminate the consequences of the accident. So, coping with such a problem alone would have been impossible for Byelorussia. Nevertheless, a huge amount of work was done: some 150,000 people were moved out of the contaminated areas, which required the construction of not only new homes, but of the corresponding infrastructure. And today Belarus spends more than US$80 billion to eliminate the accident's consequences.

The local population's main task is to create normal conditions of development on the contaminated territories. Moreover, the topicality of this issue stretches from the density of humanitarian aid that is given to the density of the creation of economic and social conditions allowing the people who live there to develop independently and live normally within the existing limitations. So, the world and Europe should turn their attention, in this connection, to the need for mutually beneficial co-operation to attract investments to these territories in parallel with conducting research and developing warning mechanisms for such accidents and, if they should occur, the ability to counteract them actively.

The second aspect that resonated loudly throughout the conference is linked to the issue of energy risk management in Europe. For this reason let me mention briefly that Belarus, which is essentially located in the centre of Europe, has mutual interests and great possibilities in the energy sector. More than a quarter of Russia's gas and more than forty percent of all oil products are transported to Western Europe across Belarus.

When it comes to the very serious subject of the transit of narcotics through our state, as well as human trafficking, I think that it is practically impossible for one state, even a powerful one, to solve such a global problem alone, without joint actions. We must inform you that we and our active and responsible partners are working to take the corresponding decisions, building the legal basis for, and organising practical actions in the area of the fight against this evil and with the support of the OSCE. So, our country has done considerable – in our view – work to create national legislation in the area of controlling human trafficking, in compliance with international legal standards. Last year Belarus's parliament made changes in and additions to various national legal codes with the aim of increasing amenability for trafficking in human beings and other collateral violations of the law. In addition, right now a state programme of measures to combat human trafficking and the spread of prostitution is being implemented. Five international co-operation projects are being conducted in this direction.

Dear conference attendees, in our view, the organisation of work to ensure security and co-operation in Europe has had considerable success in combating the challenges of the 21st century. I have touched upon only some of the aspects and problems that are most acute for Belarus at the current time. It goes without saying that we realise that we must doggedly continue our work to mobilise domestic resources as well as getting the entire European community to draft international legislation and ensure that it is enforced. Through joint efforts we shall be able to create the necessary legislative conditions and minimise existing risks and problems that, unfortunately, have become topical not only for a few countries, but for Europe as a whole.

For our part, I should like to underscore that Belarus has always been and will continue to be a reliable partner of the European states, acting to guarantee security in crisis situations. Allow me to take this opportunity to wish the conference participants a fruitful discussion and constructive resolutions.

Mr Jean-Pierre Contzen. – There are lessons to be learned from the speeches. The first lesson is that there is a great convergence of the preoccupation of the political decision makers and of the experts. It is important to underline, taking the speech of the Lithuanian delegate as an example, that there is a huge need for an enlarged dialogue between all the people who could possibly be involved. The question of dealing with security is not only a question of dealing with security but also security linked to environmental security. A holistic approach should be applied where all aspects are taken into account. It is very important and essential to work on new concepts and new doctrines and to work on these together.

The speech from Ukraine shows that risk prevention is very important but it is clear that when the catastrophe has occurred there is also a very important aspect which is remediation. Even in remediation there are some risk aspects. If you take the problem of the remediation of Chernobyl it is clear that there are also some risks involved. If you go to control room of the reactors in Chernobyl it is clear from the level of radiation that there is still some risk even during the remediation phase. These aspects should also be looked at.

To respond to the speech of the Algerian delegate it is evident that all types of risks should be looked at, those induced by natural posers, terrorism and security aspects and also industrial risk. This should be looked at altogether.

It is clear that the expert can give their scientific expertise, their scientific knowledge in order to help the decision maker to make the deliberation themselves and to take actions. But some of the risk is also created by a lack of good political governance, this needs to be dealt with. The political aspect in risk governance is certainly something which should not be ignored.

Finally the speech of Mr Novitsky once again shows the need for a wider collaboration not only between the political decision maker but also between the scientific community. It is surprising that there is not much emphasis on the health aspect of risk. The globalized world is under threat in this area. This is one of the aspects which OSCE should also consider.

Mr Ortwin Renn. **–** The International Risk Government Council (IRGC) has developed a risk governance framework. Policy makers are facing a specific challenge. Policy making bodies need to look into risk management, risk appraisal and risk regulation.

The main problem that policy makers face is that if they make policies according to what people like them to do, to the perceptions and desires of the public they actually may tolerate more sacrifices than necessary because perception does not reflect the actual risk numbers. If policy makers follow the advice of all the good experts they may lose public support. The issue is how to ensure that whenever a specific risk is addressed, a risk of transportation, an energy risk, a risk like Chernobyl, that you are not always torn between the public perceptions on the one hand who would like to do one thing and the scientific assessment on the other hand who would like to do something else. A framework is needed that addresses both, the perception side that concerns society as well as the assessment, the scientific analysis of what kind of risk we are faced with.

What was the main purpose of developing the IRGC framework? Why is it important? One reason is because we are in an age of confusion. This is absolutely true when we talk about risk. There are so many definitions about what risk is, about what risk assessment is, what risk management means, what risk regulation means, what concern means. There are so many fuzzy words but most of time the meanings of the word are not known or they mean different things in different contexts. So the first thing was to facilitate understanding. What we really wanted to do was to make sure that when we talk about specific terms in risk assessment management we mean the same thing, in order to avoid confusion.

The second thing was to ensure that this terminology or this concept could be applied to a whole set of different risk classes. Why is this important? Very often trade-offs between one risk and another are made. For example, a technological risk is increased by building large dams for reducing the natural risk. Or we re-navigate, re-naturalise some of our natural environment and then have a higher impact on natural disaster for some other risk we would like to reduce. In order to achieve a good balance between different risks, different opportunities, it is important to apply the same concept from one risk area to the other because otherwise tradeoffs between environmental risk against health risk, natural risk against technological risk, habitual risk against lifestyle risks may occur.

The second point was to ensure that there is a comparative approach that helps us to look at risks in different contexts.

The third goal was to make it economically feasible, it should be legally and ethically justifiable, it should be politically acceptable and it should certainly be scientifically sound. Those were the goals we had by developing this specific framework.

When the IRGC said it wanted to have a comparative approach it looked at a whole set of risks. The IRGC decided to look at the risks that have some kind of physical primary impact. Examples of these are physical agents, chemical agents, biological agents, natural forces and social communicative hazards. Social communicative hazards are hazards that come through the social process of communicating diseases or other things from one group to another.

Communication can be a very important hazard. In Iraq, a rumour that there was a bomb killed more people than the actual bomb would have killed. The panic alone killed 85 people in that incident. It is interesting that even though there was no physical risk present just the communication that there could be one resulted in more victims than was actually calculated by a bomb of the size that was allegedly being detonated.

There are also combined hazards. All of these things are being looked at to ensure that there is a comparative approach.

When looking at risk it is not just what happens to whom at what time but how the organisations cope with this? How are the actors involved in all of this? What is the social climate in the country? Is there trustworthy relationships between the government and the different constituencies or not? All of these issues need to be considered because they have a direct impact on what happens in the inner cycle as well as a political and regulatory culture that has an impact on the way that risks are being governed. When looking into the inner cycle, and this is the one which really pins down what needs to be done in risk assessment and in risk management, it can be seen that there are four major stations. The risk management literature only lists two, assessment which indicates how big the risk is and management which determines what to do with this risk.

We believe that this is not sufficient so we have added two other major assessments. The first one is called pre-assessment. This is the stage where the problem is determined, maybe it is not a risk problem, maybe it is an innovation problem, maybe it is a problem of putting the right opportunities together, maybe it is a problem of political will but it is been framed as a risk problem. It is very important to think about this because in the case of nanotechnology some countries frame it as a risk issue and then everybody immediately associates it with biotechnology. Others frame it as a new innovation cycle. The framing is extremely important in the beginning. It is also important to set the priorities, where the resources are to be used.

The second stage is the risk assessment stage. This assessment stage is the one where the scientists are being asked to make sure that whatever can be known about the impact of that specific technology or that specific event on human health, environment and other things that we value is known. In addition to just knowing what the physical impacts are an assessment on the concerns of people associating this specific activity with other types of impacts needs to be carried out. Neglecting these concerns has been a major problem in the past, think of nuclear waste, of genetically modified organisms, of some of the new applications of nanotechnolgy. It is vitally important to investigate what people are afraid otherwise half of the picture is missing.

Within the IRGC framework two types of assessments are needed. Assessment number 1 is the real physical impact, we need to know what is going to happen. Secondly; the concerns of all the important people in society, in different constituencies, and in various stakeholders groups should be known. What do they think about it, why are they worried? It may be found that they are not worried about something which is risk associated. Maybe they are worried that they will lose control.

It was found from a survey on mothers in Southern Italy that they hate genetically modified organisms because they feel that they are losing control over their family. An Italian mother’s stability and prestige in the family is to know what to cook for their husbands and family. With genetically modified organisms they don’t know this anymore so competence is lost and that’s what Italian mothers don’t like. It was not a health risk issue.

It is very important to see what the concerns are because this not only aids decisions on the best way of managing the concerns but also how to address these concerns in different ways.

The third stage is a risk-evaluation stage. Risk-evaluation involves making a judgement as to whether the risk is acceptable or tolerable. Acceptable means it is ok, that the benefits outweigh the risks by far. Tolerable means it still is necessary to do that but the risks have to be reduced to make it acceptable or it is intolerable and this is a value judgement, it is not something that scientists can do.

Very often in the past this task was given to the science field but scientists are no better than anyone else to make value judgements. This is a political task. We need to say if this is tolerable or not and this requires leadership, this requires sovereignty and we have to make good arguments for doing that. You have to have the courage to make judgements and you cannot avoid this. And if it is judged as not tolerable or it is even unacceptable then something has to be done in terms of management and management means introducing measures and options that reduce the risks to a degree that is acceptable to society. The impacts are then monitored and the cycle starts all over again, a reframing is done again to ensure that whatever happens afterwards will be one that is desired in terms of risk reduction.

There are three elements that are important here, the first one is when looking at the risk-appraisal side which includes the assessment and the concerned side the three major aspects of risk are addressed. The first aspect is complexity meaning what is the causal connection between an agent and a result: if it is simple like falling from a bicycle then it is no problem. But very often it is more complex, it is not known where the cancer is coming from, it is not known how the pollution is being caused. A lot of modelling is needed to determine the cause, for example in climate change.

The second aspect is uncertainty. Very often the risk fields, and that is why it is called risk, is that there is no definite answer, it is not possible to say that A causes B. It is only possible to say that A causes B with a specific probability, there is even some uncertainty about it so there is always alternate explanations.

And the last aspect is ambiguity which means there are always different interpretations possible. Many interpretations are possible which leads to competing claims.

The reason why risk is such a difficult subject to deal with is because of these three elements combined, complexity, uncertainty, and ambiguity. When making risk judgements, there are three choices, acceptable, tolerable or intolerable. In addition to these three elements there are different levels, high complexity, low complexity, high uncertainty, low uncertainty, high ambiguity, low ambiguity. There are different ways of managing risk. There are guidelines on how to manage risk depending on the composition of complexity, uncertainty and ambiguity.

This is the risk-evaluation, this is the second step after the assessment. There are three elements here, green means acceptable, yellow means the risk has to be reduced and red means this is not tolerable.

The most difficult thing here is to find out where the demarcation lines need to be made. Where is the limit between yellow and red and green and yellow? This is the tolerability or excitability judgement and both knowledge which is combined to risk characterisation and the evaluation itself which is based on political judgement are needed.

In terms of risk management it can be seen if this framework helps do a better job in risk management. It can be seen if it is really of assistance and if it facilitates this process.

The first element of a good risk management structure is to see a decision as an eluded process and this process includes looking at the options available, sometimes there are standards or economic incentives, labels can be put on products, people can be educated. There are a whole set of options, some are very expensive, some very inexpensive, some are very effective, some very ineffective.

First the options that help to deal with a problem need to be generated, then the impact of these options need to be assessed, whether they do the job or not. The comparative review of these options is then examined, then a selection is made, it is implemented and then monitored. Beyond this structural form it is important to see that there are different management strategies, these strategies again relate to the three major elements of risk: complexity, uncertainty, and ambiguity.

There are four types of management strategies, the first deals with routine or mundane risks, like falling off a bicycle or similar small accidents, this involves little complexity, there is not much uncertainty and no ambiguity so this is not so important.

The other three are the more important ones. The first is risk-informed/robustness-focussed: this involves highly complex and sophisticated risks where a lot of scientific modelling is needed but at the end the uncertainty has been reduced and there is very little ambiguity. It is very clear what has to be done.

The second is precaution-based/resilience-focussed: this involves highly uncertain risks where it is still unknown how exactly the risk is being played out in society and where there are a lot of competing claims from the scientists.

And thirdly discourse-based: maybe it is certain or not certain but it is contested. People will say it is good or it is bad, gmo and stem-cell research would be good cases, where there are many different judgements about whether it is acceptable or not or whether it is tolerable or not and how you deal with this kind of concerned dissent in society.

A taxonomy has been developed that looks at the diagnostics of risks. If there are ‘simple risks’ then basically you do the routine things that normally we all do when we look into either personal risks or other types of risk. These things include risk-benefit analysis, technical standards, economic incentives, education, labelling and information. These are the elements that are the normal reservoir of risk-reduction methods.

When looking at step number 2, risks which are being characterised by very high complexity it is important to distinguish things that can be done about the risk source, the agent, the agent, for example a food item or a building and the ones who are being effected by it, which records the risk-absorbing system which means people, buildings and environments.

Regarding the agent it is important to be able to characterise the evidence as precisely as possible.

The absorbing system should be robust so that even if science is not completely correct that the person or environment can cope even if there are some surprises.

There is a dual strategy here. The first step is to try to define what is the main problem with that agent, with some complexity behind it and secondly to ensure that if this complexity turns out to be more problematic than first thought that the system which absorbs this type of risk is able to cope. The robustness was not adhered to in the case of Hurricane Katrina.

Examples of complexity induced risks are; industrial plants with hazardous material, large dams, bridges and highways, LNG terminals, weapon complexes, dense settlements, classic infectious diseases and deterministic health risks with thresholds. These are all very complex risks.

We are not saying these are physical hazards, chemical hazards, natural hazards but we have a different ordering system. The ordering system means these are hazards that if characterised correctly have little uncertainty and little ambiguity. Everybody agrees that these risks should be controlled and that there are real benefits behind them. But the system must be robust enough even to withhold surprises which were not anticipated.

If you go one step further you have the uncertainty induced risks. Uncertainty induced risks are risks that still have uncertainty attached to them, even after all the risks have been characeterised as precisely as possible scientifically. In this case it is very difficult to make a judgement because what you have to say is how much uncertainty am I willing to trade-off against some maybe certain or uncertain benefits. The danger of over-regulating is always there. Being too cautious may stifle innovation. Or not being cautious enough, this can put a whole set of your population at risk.

How can the trade-off between too much precaution and not enough precaution be made? In Europe this is normally looked at from a precautionary position meaning when in doubt be a little more cautious rather than being too innovative. In other countries there is a reversal in this depending on the preferences. This is a judgement call.

If the distinction between risk agent and the risk absorbing system is made, and the risk agent is looked at then the main thing that needs to be ensured is that there are no irreversible consequences. Irreversible consequences mean that if the uncertainty turns out to be more negative than anticipated it still must be possible to withdraw from that decision. So the more persistent, the more ubiquitous, the more bio-accumulating the risk is the more sensitive we should be if we have high uncertainties. In this sense there are different sets of hazardous criteria and the tools that should be used here are basically containment of time and space as low as reasonably achievable, so trying to minimise the impacts. All of this helps to avoid irreversibility and this is part of a very prudent way of judgement to ensure that we are not declining or reducing the amount of freedom we have to respond to unexpected or surprising results.

In terms of the risk-absorbing system a resilience approach is needed. Resilience means trying to avoid vulnerabilities. Vulnerabilities mean that the system is more apt to react to uncertain events than other systems that have this ability either through passive structures or to active safety issues.

There are a whole set of instruments that can lead to more resilience, to avoid high vulnerability, to allow flexible responses and to be prepared for adaptation. This is a more evolutionary approach. It is very important that within the uncertainty field that there are two strategies in place, 1. The precaution base which means trying to reduce irreversibility, this is how we translate precaution and 2. The resilience focus approach which looks at the risk-absorbing system, for example improving the immune systems of people, having good and resilient building codes in natural disaster areas. All of this would help improve the resilience and to cope with uncertainty.

A few examples selected from very different backgrounds of precaution and resilience-based management are ‘green’ biotechnology, internet sabotage, new epidemics, BSE, endoctrine disruptors and extreme weather events due to global climate change. In terms of precipitation on the one hand and the sea-level on the other hand these are getting worse than anyone had expected. This is one of those uncertainty cases which we need to be aware of. We need to have these two things, firstly containment, ensuring that what we are doing is reversible and secondly making our system resilient.

The third and last case is discourse-based management where these various types of ambiguities are looked at. There are different types of interpretation of whether that is good or bad, of whether it is ethically acceptable or not, whether different people have associations with it that links them to distributional injustice. All of these values associated with different risk sources give rise to societal conflict.

What is needed here is to have a discourse with these different people because it is not just the physical impact that they are concerned about but what is meant by these physical impacts and what is associated with them. We have to integrate the stakeholder, we have to emphasise communication and social discourse as a part of this resolution.

This is not recommended if it is a simple risk issue, it is even not recommended if it is a complex risk issue. Having people participate is a scarce resource. Time is a scarce resource, not everybody wants to participate. We should use this for those purposes where there is real controversy. This is not always easily detectable but if this is detected then this is the place where this type of discourse has to take place. A very good example where discourse-based management can be used are ‘red’ biotechnology, cloning or stem-cell research. This is not about uncertainty, this is not about complexity, this is not about risk, it is about whether stem-cells are part of a human being or whether they are just biological entities. This is the question and there are different connotations depending on how you answer the question.

‘Industrial food production’ is another one, this is not about risk, it is really about how we would like to live. Biochips for human implementation, this is a big exercise which will last for two years having a lot of citizen panels on how we do brain research, should this be regulated or not? Electromagnetic fields is another area where the physical impacts are probably low but people feel that there is a high concern for them. Other examples are globalisation of consumer technologies or in the climatic field, projects of grand geo-engineering.

This is again not so much a risk issue, but an issue of whether this is acceptable for society or not. This is where these discoursive methods need to be employed. This can all be brought into one major scheme called ‘The Risk Management Escalator’. The Management Escalator tells us how much input in terms of policy energy, in terms of participation, in terms of involvement of different groups, is necessary depending on the characteristics of the risk issue that is being looked at.

It starts with a simple type of risk. These simple risks are the usual accidents, small things that you deal with. These are not trivial but they can be handled within the staff that you have if you have the organisation capacity.

If it is much more complex than this then you have an issue where you need better knowledge, better information. This is where you really want external experts to come in and make sure this modelling effort is done and to make sure you invest in the robustness of your systems.

The third step is where there is a lot of uncertainty. In this case what is needed in addition to good Probabilistic Risk Modelling, is to balance the risks and the benefits under the condition of uncertainty and this means negotiations. There is no scientific means of balancing costs and benefits if you are uncertain about them. Very often economists say they can do this but they cannot. If you are uncertain then you are in trouble and you need to negotiate. Negotiations have to be carried out between those who will benefit from the risk source and those who will suffer and an agreement has to be found on what is a good level of protection or what is a good level of insurance, what is a good level of ensuring that if the worse happens the victims are compensated. This is where stakeholder participation is needed, this is called ‘reflective discourse’ and this is really about dealing with uncertainties.

The last step in the stakeholder participation ladder is if there are high ambiguities. In this case it is not enough just to have the stakeholders who will either benefit or will take the risk, a larger societal discourse is necessary which is called ‘participative discourse’ which looks at normative questions, how do we want to live in the future.

In terms of all the risk issues we are dealing with around 20% in the lowest risk level, around 20% in the second level, 30% in the third level because we are dealing with risk uncertainties and around 30% in the final level so we are not always dealing with the highest risk level.

When talking about risks a specific set of problems have to be dealt with that are typical for risks and maybe not as typical for other policy issues. Firstly, risks are being characterised as we have plural values and knowledge claims. Because risk deals, by definition, with uncertain events it has to be dealt with in terms of A could happen but also B and this makes it more difficult to handle.

Secondly we have expert dissent on many risks and benefits. There is not one dogmatic answer to how high is the risk and how high is the benefit, there is a choir of different answers, it is not arbitrary. Demarcation between nonsense and sense can be made but the sense is a variety of different things and plurality needs be thought about as an answer to a definite question.

Thirdly, risk transcends boundaries. It cannot be limited to just one country, one risk may have an impact on several countries, when thinking about global change and greenhouse gases this is very obvious. These risks have triggered social concerns because of their social amplifications. There is a lot of pressure from globalised economy to look into risks and either to manage them or to really reap the benefits. There is a lack of organisational capacity in many countries to deal with it and of course connected to this a lack of effective governance structures. A framework is needed that addresses these various problems and we believe the IRGC framework could help to actually do this.

The IRGC believes that four risk-management regimes are the best way of dealing with these various problems. These risk regimes are based on a diagnostic of the risk in question, in terms of how complex it is, how uncertain is it and how ambiguous is it.

Then there are three major strategies. The first is if it is highly complex, if it takes a lot of scientific modelling we are looking into a risk informed management strategy with expanded risk-assessment seeking expert consensus, seeking clarification on the issue while at the same time making sure that our absorbing systems are robust enough to withstand all the pressure.

Secondly if the uncertainty is very high and it is not known exactly what is happening, if there are many dissent competing claims in the scientific community then a precaution and resilience based management is needed. This means negotiating a safety level under uncertainty between the stakeholders who will benefit from it and those who will suffer. A consensus is needed on this and we want to rely in terms of resilience on containing that risk so that if things become worse we can still reduce the risk and to make sure we have flexible approaches.

Finally if the risk is characterised by high ambiguity, different types of interpretation then a much more value-based approach is needed, more public input and stakeholder involvement is needed to ensure that all interpretations are taken into account and to be in line with the preferences of society.

Bertrand Russel once said ‘What man desires is not knowledge but certainty’. Although policy makers may not be able to produce certainty they can help people to develop coping mechanisms to deal prudently with the necessary uncertainty that is required for societies to progress in a world where uncertainty remains.

Mr Frantisek Bozek. – Changes in civilization are accelerating enormously at present. The pursuit of higher standards of living alters economic aspects, principally maximalization of profit. On the other hand the environmental and social components are underestimated and this leads to complexity in dealing with the problem.

Globalization is seen not only in the economy, but it also includes other spheres of life. There are implicit advantages connected with the cumulation of the potential for solving existing problems, economic growth, better flow of information and communication, and the breakdown of barriers, etc. Besides the above mentioned advantages there are also numerous risks caused by the process of globalization, e.g. terrorist actions, environmental burden, the cumulation and anonymity of power, endangered democracy, elimination of competition, media manipulation, loss of identity and cultural traditions, expanding uniformity, including the loss of control over most processes.

Changes cause some risks to disappear or decline, others are more intensive and become global. At the same time entirely new risks arise. The following risks have been recently discussed: disturbances, damage or destruction of critical infrastructure caused by deliberate terrorist attacks, industrial breakdowns, negligence, computer hackers, criminality, and illegal acts. Explosions in Madrid and London have highlighted the risk of terrorist attacks against European infrastructure. The EU’s response must be swift, coordinated and efficient.

The USA and Australia were the first countries to perceive the problem of critical infrastructure in its complexity. These countries opened a dialogue on the vulnerability of vital infrastructure, later called critical infrastructure.

A White Paper was the first document addressing the issues of the protection of critical infrastructure. It was Presidential Decision Directive No 63 issued in 1998 in the U.S. [4]. The White Paper describes critical infrastructure as the primary systems of material and cybernetic platforms having influence on the operation of the economy and the state. The primary systems include the areas of telecommunication, energy, bank and financial sectors, transport, water supply and rescue services. The Directive was aimed at adopting necessary measures, which could quickly eliminate significant vulnerability to material and cybernetic attacks on critical infrastructure. Higher stress was laid on possible attacks on cybernetic systems at that time.

The policy of the protection of critical infrastructure and its dissemination to all interested subjects both in the civil and public sectors is an important requirement of the White Paper. A critical infrastructure protection policy determined objectives, provided concept and resources and classified critical infrastructure as being part of national vital interests.

European countries administration also dealt with the issues of critical infrastructure [5]. At first the National Infrastructure Security Coordination Centre was established in Great Britain at the end of 1999. Its task was to develop and coordinate activities for the protection of critical national infrastructure and to identify relevant subsystems the continuity of which is important for the functioning of the state. The loss or disturbance of these subsystems would endanger lives and have negative economic and social impacts on the society or a major part of it.

Material dealing with the threats to key infrastructures was also discussed in Germany in December 1999. Measures were also taken on a national level in the Netherlands. Protection of critical infrastructure had a common attribute at that time – a focus on the protection of information and communication technologies, often connected with transition to the new millennium and protection against the Y2K.

The USA intensified the protection of critical infrastructure after September 2001. The issue gained new content and dimension. The National Strategy for Homeland Security and then National Strategy were adopted in July 2002. It is required to interconnect the above mentioned documents and to implement the approach to all the levels of state administration in cooperation with the private production sector, institutions and American citizens.

By adopting a strategy for the protection of critical infrastructure and the strategy for the cybernetic security the critical infrastructure have been divided and specified for physical and cybernetic infrastructures. The task is to secure and protect cybernetic operations under US ownership, control and inspection. The task in the area of material assets is to physically protect critical infrastructure and key facilities.

The significance of globalization as well as diversification and the continuously increasing probability that critical infrastructure could be disturbed, damaged or destroyed is highly topical even in the EU. In June 2004 The European Council asked the Commission of the European Communities to prepare an overall strategy to protect critical infrastructure. The Council conclusions endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the set-up of the Commission of a Critical Infrastructure Warning Information Network (CIWIN).

The Commission organized two key seminars in response to the appeals and put forward clear suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures. To begin with, green paper outlining the options for EPCIP has been put forward. During this year specific proposals of measures should be developed and taken in individual sectors of critical infrastructure.

Critical infrastructure includes those physical resources, services, and information technology facilities, network and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments. The list of critical infrastructure sectors is presented in table No 1.

Sector	Product or service
Energy	oil and gas production, refining, treatment and storage including pipelines; electricity generation; transmission and distribution of electricity, gas and oil.
Information and Communication Technologies	information system and network protection; instrumentation automation and control systems; internet; provision of fixed and mobile telecommunications; radio communication and navigation and satellite communication; broadcasting.
Water	provision of drinking water; control of water quality; stemming and water quantity control.
Food	provision of food and safeguarding food safety and security.
Health	medical and hospital care; medicines, serums, vaccines, pharmaceuticals; bio-laboratories and bio-agents.
Financial	payment services, and payment structures (state and private); government financial assignment.
Public & legal order and safety	maintaining public & legal order, safety and security; administration of justice and detention.
Civil administration	armed forces and government function;

	civil administration, postal and courier services; emergency services.
Transport	road, rail, and inland waterways transport, ocean and short-sea shopping and air traffic.
Chemical and nuclear industry	production, storage and processing of chemical and nuclear substances pipelines for dangerous goods (chemical substances).
Space and research	space research.

Table 1 Indicative list of critical infrastructure sectors

There are three types of infrastructure assets:

public, private and governmental infrastructure key assets (e.g. nuclear power plants, dams, significant commercial centres) and interdependent cyber & physical networks;

procedures and places where individuals exert control over critical infrastructure function.

facilities having cultural or political significance as well as “soft targets” which include mass events (i.e. sports, leisure and cultural events).

Protection of critical infrastructure requires an integrated approach, team and interdisciplinary co-operation of experts and all stakeholders, carried out on a sophisticated theoretical-methodological basis. At the same time it is sensible to apply the basic principles such as preliminary precaution, subsidiarity, complementarity, confidentiality and proportionality. A successfully implemented process leads to increased environmental security, citizen satisfaction and cost reductions.

It can be stated that the protection of European critical infrastructure arising from the principle of subsidiarity is based on providing protection on regional or national levels. Effective protection of regional critical infrastructure should follow an analytical process the content of which is the following:

a) Critical infrastructure and identification of its sectors, elements (products, services) and possible risks;

b) Vulnerability analysis of particular sectors of the critical infrastructure on the basis of criticality and sensitivity of its elements to each threat;

c) Analysis of threats resulting from their level of danger, access to individual sectors (elements) and motivation, i.e. the wish to initiate the threat;

d) Qualitative, semi-quantitative or quantitative risk assessment of disturbance, damage or destruction of individual sectors (elements) of critical infrastructure in consequence of carried out threats. The quantitative risk assessment can be made according to formula (1), where the level of risk is a function of P probability, that the threat and I impact of undesirable event will take place in relation to t time.

$R = \int P_{(t)}.\ D_{(t)}.\ dt$ (1)

Index assessment is used for semiquantitative risk assessment, while a verbal assessment is used for quantitative assessment and is based on the probability of occurrence and impact of undesirable event;

e) Risk acceptance analysis based on adopted standards and decisions leads to conclusion, whether it is efficient either to carry out measures for a particular sector (element) of critical infrastructure or just to monitor the risk and focus on operative management;

f) Proposal of organizational or physical protective measures and choice of optimal measures while considering economic, environmental, technical, social, political and other possible factors. It is recommended to use some of the invention methods, e.g. ideas generation brainstorming leading to possible measures, while some of the methods of operation analysis, e.g. multicriterial analysis, is used for choosing an optimal option;

g) Implementation of sufficient measures for individual sectors (elements) of critical infrastructure;

h) Monitoring and operative risk management in individual sectors (elements) of critical infrastructure.

Acceptable risk to critical infrastructure should be provided by building a warning information network enabling not only the exchange of information and best available practices and technologies, but also particular coordinated and effective response in case of threat.

Security of critical infrastructure in a region can be effective through the risk assessment of individual sectors and elements including particular products and services. While accepting the existing security measures it is possible to identify the spheres of critical infrastructure requiring priority solution. We can agree that security support is a permanent and gradual process and there will not be enough financial, material and personnel resources for immediate and complex solution. At the same it is necessary to accept the principle of proportionality, which respects socially acceptable level of risk.

The index method developed at our institution, which was originally designed for risk prioritization in a region with the aim to ensure sustainable development and stability of the region [13], can be used for the purpose of setting priority measures and comparing the security levels of critical infrastructure in individual regions.

Let us assume that there were n sectors of critical infrastructure identified in a region. The sectors require risk assessment from with respect to their damage or destruction. Then n_i represents i-sector, where $i \in \langle 1; n \rangle \wedge i \in N$ and N is a symbol for the set of natural numbers.

Each i-sector includes s (i) identified elements, i.e. the products and services of critical infrastructure, which can be endangered. It is clear that $s_{i, j}$ symbol, where $j \in \langle 1; s(i) \rangle \wedge j \in N$, represents j-element of i-sector. Let us assume that $s_{i, j}$ element can be endangered by h(i, j) number of threats, then $h_{i, j, k}$ symbol represents k-threat in i-sector for j-element and $k \in \langle 1; h(i, j) \rangle \wedge k \in N$.

If we are able to assess the degree of vulnerability and the level of k-threat to $s_{i, j}$ element and probability of damage or destruction of $s_{i, j}$ element resulting from it and eventually also the level of impact of the threat, we can assess the $R_{i, j, k}$ risk resulting from k-threat to $s_{i, j}$ element with the help of relation (2) as it follows:

$$R_{i, j, k} = P_{i, j, k} . D_{i, j, k} \quad (2)$$

where $P_{i, j, k}$ is the probability, and $D_{i, j, k}$ is the impact of $h_{i, j, k}$ threat to $s_{i, j}$ element. It should be remarked that relation (2) is a simplified modification of relation (1) with the absence of time relation between probability and impact.

Quantitative risk assessment cannot often be applied according to formula (2) due to the lack of input data. In such a case we recommend to use a qualified expert risk assessment in the form of indexes in order to assess probability and impact of an undesirable event. It is recommended to use the indexation in the field of real numbers being in an interval $\langle 0; 5 \rangle$, where the indexes represent the following:

0 – risk is negligible;

1 – risk is marginal;

2 – risk is acceptable, below the level of valid standards, if they were developed and adopted;

3 – risk is tolerable, but should be reduced;

4 – risk is significant, above the current standards and should be minimized immediately;

5 – risk is absolutely unacceptable.

$I_{i, j}$ risk index for i-sector and j-element of critical infrastructure can be determined as a weighted mean of individual indexes of $I_{i, j, k}$ threats according to the following relation (3):

$$I_{i, j} = \sum_{k = 1}^{h(i, j)} w_{i, j, k} . I_{i, j, k} \cap \sum_{k = 1}^{h(i, j)} w_{i, j, k} = 1 \quad (3)$$

where $w_{i, j, k}$ represents the risk index weight of k-threat to j-element of i-sector of critical infrastructure.

Risk index value I_i representing the threat to critical infrastructure for the sectors under consideration can be obtained in the similar way by using relation (4). Requirements for increased security in such sectors are necessary to be solved as a matter of priority.

$$I_i = \sum_{j=1}^{s(i)} w_{i, j} . I_{i, j} \cap \sum_{j=1}^{s(i)} w_{i, j} = 1 \ (4)$$

where $w_{i, j}$ represents the weight of significance of j-element in i-sector.

Finally indexes can be set for the threats to critical infrastructure of a monitored region according to formula (5). Index value enables regions to be compared among themselves and be identified on a national level in order to pay extra attention to their protection and financial support.

$$I = \sum_{i=1}^{n} w_i . I_i \cap \sum_{i=1}^{n} w_i = 1 \ (5)$$

where w_i symbol represents the weight of significance of i-sector.

The values of individual weights $w_{i, j, k}$, $w_{i, j}$, a w_i, represent significance of indexes and they can be determined with the help of expert methods or in an analytical way.

It is clear from the above mentioned procedure, that risk indexes represent non-dimensional quantity, which is derived from the risk assessment of a particular threat to individual elements of critical infrastructure. Risk assessment, or the assessment of indexes, must use the latest scientific findings, measurements, calculations, statistical data, sociological researches and expert assessments. It is required to know the assessed area and the risk assessment methods precisely. It is also required to have a wide range of identification data available for the assessment of administrative unit or territory.

Range and multidisciplinary character of the security assessment of individual sectors, their products and services require co-operation of expert teams from individual areas and cannot be an outcome of an individual. Determination of critical values and safe standards (limit values) has to be carried out by experts on the basis of international and national comparisons. Valid standards and local conditions have to be accepted while assessing whether the risk is tolerable. Qualified assessments are used for the assessing of risk acceptance in case there is not enough data available.

Column and star charts marked in colours are recommended for showing the threats to individual sectors, or elements of critical infrastructure. Structure of charts enables the teams to analyze the efficiency of each measure having been implemented.

Globalization, diversification of risks and a reduced security of critical infrastructure both on national and international levels require co-ordinated and complex approach and a team co-operation during problem solving. The paper has been focused on history and current tendencies in the protection of critical infrastructure, the sectors and elements, i.e. products and services, of which have been classified in compliance with the current EU concept.

Protection of critical infrastructure of a region has been drafted on the basis of current findings. The procedure is based on the risk assessment that individual elements and then sectors of critical infrastructure could be disturbed, damaged, or destroyed. The risk assessment results from the assessment of vulnerability and threats to individual elements of critical infrastructure and the possible impact of threats on a monitored region. The proposed risk assessment index method locates the elements and sectors of critical infrastructure requiring priority solution. In this way investments can be rationalized and implemented measures made more effective. Protection of critical infrastructure in a region is a prerequisite of national and European security.

Immanent development of scientific branches and methodology in relation to security, requirements of practice and the security research are the main reasons for establishing a scientific branch „Environmental Security”.

Mr Bart D’Hooge. – First of all I would like to thank the Belgian Senate for inviting me at this Colloquium “OSCE: Security and Risk management in Europe”. Actually, I am representing the Minister of Internal Affairs, Mr. Dewael who was unable to attend. Having spent 10 years in international missions for the United Nations, OSCE and the European Union, I am currently in charge of coordinating European Affairs for the Belgian Federal Police, in the department dealing with the Policy for International Police Cooperation.

My presentation will be rather practice oriented in nature and will cover the Belgian experience with regards to threat assessment and our National Security Plan, a short overview of international police cooperation and our strategic approach, OSCE and risk assessments, EUROPOL and the Organized Crime Threat Assessment and finally a word on the new European Architecture for internal security.

Security is the condition in which one’s values and interests are protected from or not exposed to danger, i.e. risks and threats. A security policy aims to keep one’s values and interests safe and makes use of several practices and instruments selected from the available ones, according to one’s security culture.

Security practices and instruments change over time. New ones are invented, experimented and added to the existing ones, according to one's danger, risk and threat perceptions and security culture. The multidimensional or comprehensive notion of security has been developed in contemporary times from the interdependence between all dimensions of security, i.e. the political, socio-economic, ecologic, cultural and military dimension.

In 2004, the Belgian Council of Ministers approved a framework memorandum on Integral Security from the Ministry of Internal Affairs and Justice. This memorandum was the framework for our federal integral and integrated security policy. The fact that this memorandum was jointly drafted by both Ministries implies that the necessity of an integrated approach is not limited to the conceptual phase but has implications for the implementation phase. The National Security Plan for the police has a validity cycle of 4 years, which is equal to the parliamentary legislation.

The memorandum consists of three parts:

a conceptual framework that outlines the integral and integrated security policy

the prioritization of the criminal phenomena

the implications for the policy and the management of the plan

Security is a necessary condition for the good functioning of our society and has become one of the most important measures for quality of life. It is expected from the government that it provides answers to the need for safety and security and the protection of life, health and commodities against threats and risks, since it is its core business. Integral security means that crime will be looked upon in a very broad context. Integrated refers to the conceptual approach that guides all the actors in the field and harmonizes their approach.

As stated earlier, the National Security Plan contains a number of priorities for action by the Federal Police. The Government has defined, based on assessments and analysis, a number of specific criminal phenomena and safety problems as policy priorities:

– Terrorism

– Organized Crime (mobile criminal groups; criminal activities in Belgium committed by foreign criminal networks trafficking in drugs and illegal weapons, trafficking in human beings and smuggling and illegal migration)

– White collar crime

The trans-national or cross border character of a number of phenomena that have an impact on safety and security is steadily increasing. This is the case for most of the prioritized phenomena listed earlier. For Belgium and more specifically the Ministry of Internal Affairs and the Federal Police, it is important to actively participate in and contribute to the cross border and European approach to the fight against these types of crime.

The Belgian government has therefore decided to enhance and increase participation with our neighbouring countries in the fight against crime, asylum and migration and other areas where a national approach is too limited to be efficient. This increase in police and justice cooperation has taken place with Luxemburg and the Netherlands – our Benelux partners – and with France, Germany and the UK.

Additionally, a number of initiatives will be taken to increase police cooperation with so called key countries. These are the countries that are frequently involved in the prioritized criminal phenomena. Conventions for Police Cooperation are signed with these countries and depending on their ratification, action plans are developed to address specific areas or criminal phenomena.

International Police Cooperation remains high on the agenda for the Ministry of Internal Affairs and the Federal Police because of the international aspects of modern crime and their complexity. The Department for International Police Cooperation operates on the strategic level and closely follows and coordinates evolutions in this area. We try to strive for a balance between political and geographical opportunities on the one side and knowledge, expertise and capacity in terms of resources on the other side. It is important to stress the major role that the European Union and its partners will play in this domain because European decision making will more and more define the territory for cross border policing.

The topics with regards to international police cooperation, our department is actively dealing with are:

follow up and preparation of the Schengen Information System second generation (SIS II)

closely following of the activities of Frontex, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States. This agency, based in Warsaw, has a mission statement that includes among other things the coordination of the collaboration between Member States on border control, assistance in the training of border guards, the promotion of research projects and technological developments that are relevant to border surveillance and the support of Member States in the organisation of joint return operations.

Actively participate in relevant EU bodies to influence the decision making and work towards strengthening the European Union as an area of freedom, security and justice and more operational cooperation between member states.

We also actively participate in CFSP and more specifically in ESDP missions for civilian crisis management.

The rationalization and enhancement of existing structures for police cooperation (joint use of Benelux police liaison officers, geographical and functional evaluation of our network of police liaison officers in foreign countries with specific attention to the key countries and tailor made action plans).

Continued cooperation with the international organizations that play a key role in international police cooperation such as Europol and Interpol. Interpol remains an important partner in the area of International Police Cooperation. The different working groups within Interpol continue to work on a solid judicial foundation for the exchange of information. I will elaborate on Europol in a while.

Active participation in the framework of the London Group with the goal of developing with our European Partners an "information led policing".

Before I continue with the topic of Threat Assessment, I would like to draw your attention to a new body for Threat Assessment in Belgium. Dr. Javier Solana in his speech "A secure Europe in a better world" at the European Council in Thessaloniki on June 20th 2003, defined terrorism as one of the strategic threats for Europe, being both a basis and a target for terrorist. He also pleaded for a better exchange of information, because a joint threat assessment is the best foundation for joint action. Belgium has followed this initiative and has created a Coordinating body for threat analysis because cooperation between all involved partners, the efficient exchange of information and punctual and strategic risk assessments will lead to an accurate image of threats and risks and thus will be the cornerstone of an efficient security policy.

Risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack. Risk management principles acknowledge, that while a risk generally cannot be completely eliminated, enhancing the protection from known or potential threats can reduce it, in other words it allows for preventive action. Crime proofing is applied to the legislation making process and is the testing of legislative proposals as regards the crime opportunities they might create or the scanning of loopholes and crime facilitating opportunities. A good risk management approach includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment. Threat assessments are important decision support tools that can assist organizations in security-program planning and key efforts.

A threat assessment identifies and evaluates threats based on various factors, including capability and intentions as well as the potential lethality of an attack. The assessment is a tool to improve the perception and strategy-setting for example in the fight against OC. Such risk/threat assessments aim to point to concrete risks and threats and the identifying and examining vulnerable areas of the society that are, or could be exploited (by criminals) (Europol Analytical Guidelines) on the basis of an analysis and include a forward-looking component. This approach is based on a methodology that is multidisciplinary in nature, includes input from services other than traditional law enforcement agencies and also pays attention to the vulnerabilities of the legal economy.

There is thus a need for a methodology to:

define opportunities and vulnerabilities (future oriented)

measure and rank the opportunities and vulnerabilities (defining priorities)

be used for preventing (organised) crime

We will never know whether we have identified every threat, nor will we have complete information about the threats that we have identified. Consequently, the two other elements of the approach are essential. A vulnerability assessment is a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses. A criticality assessment is a process designed to systematically identify and evaluate an organization’s assets based on the importance of its mission or function, the group of people at risk, or the significance of a structure. Criticality assessments are important because they provide a basis for prioritizing which assets and structures require higher or special protection from an attack.

One of the priorities for the Belgian Government as Chairman in Office for OSCE in 2006 is the fight against Organized Crime. A number of aspects will be covered during the Presidency. Let me just briefly stop at one of them, namely organized crime and risk and threat assessments.

There is growing international consensus on the increasing importance of the threat of trans-national Organized Crime and Terrorism as being the most important new threats to our society. In many instances, organized crime is both cause and effect of the inadequate functioning of national institutions and a severe impediment to effective development. The threat posed by organized crime has been acknowledged in OSCE’s basic documents since at least 1999. This has also been recognized by the Heads of State and Governments during the UN Summit in 2005, and was also covered in the European Security Strategy.

These phenomena are a threat to all countries within the OSCE sphere, both east and west. The fight against organized crime is not a new theme for the OSCE and a lot has been done already. You can find this in the Action Plans in the fight against Trafficking in Human Beings and Illegal Migration, Trafficking in weapons and drugs, money laundering and in the OSCE efforts with regards to Border Management, Border Control, Rule of Law and other.

The Belgian Presidency wants to continue to build on these achievements, on this *acquis* and wants to give some new impulses, for example by introducing the topic of “*risk and threat assessments”*, in which Belgium has a vast experience. This initiative is a joint venture of the Federal Police with the University of Ghent, the academic market leader in this area, under the umbrella of the Chairmanship Task Force. We see this as a very valuable tool in the fight against international crime and we would like to introduce and promote the methodology needed to pinpoint concrete risks and threats based on the analysis of data provided by different services. Our approach will be multi-disciplinary and not only based on the input of the traditional law enforcement agencies, but will also concentrate on the economic vulnerabilities of legal economies, therefore making it a useful topic for OSCE.

A workshop for the experts of the 55 participating states of the OSCE will be held on April 26th in Vienna. The Workshop on Tools for Assessing the Threat of Organized Crime to be held in Vienna in the "Neuer Saal" in the Hofburg Congress Centre on Heldenplatz. This workshop will be the basis for further activities during the next years, such as increasing the capacity of States for this type of analysis through technical assistance and training.

We believe that it is evenly important, apart from having an accurate picture or image of crime, to have the appropriate judicial instruments. The Chairmanship will therefore in parallel continue to promote the ratification and implementation of the Palermo Convention, this in cooperation with the UN. A number of efforts will be directed to enhance the effectiveness of the criminal justice system such as a methodology on how to assess the criminal justice system and the development of OSCE norms and standards/common approaches/best practices regarding the organization and functioning of the criminal justice system

The following assumptions are at the basis of this approach:

an effective and efficient fight against organized crime requires that the basics of the criminal justice system function properly;

the criminal justice system is a chain, only as strong as its weakest link; it comprises law enforcement (policing), prosecution, judiciary and execution of sentences (including prison systems);

we should be guided by the principle of the rule of law (*état de droit*), one of the main building blocks of good governance and crucial in ensuring the respect of human rights.

When talking about international organizations that play a key role in International Police Cooperation, I need to stop a moment with EUROPOL and the active role Belgium is playing. The Europol Vision document within the framework of the EU Security Plan will continue to be the focus of our attention as well as the Organised Crime Threat Assessment. We will also continue to improve the flow of relevant information towards Europol and continue to play an active role in the development of the Europol Information System. I have also mentioned before, our efforts to contribute to the development of an information led policing within the European context.

Intelligence-led law enforcement consists of the following four steps:

(1) It requires that a sound threat assessment is available, indicating which are the major causes of harm faced.

(2) On that basis, political priorities should be set, defining those threats which should be addressed.

(3) To implement those priorities, resources have to be allocated, projects set up and appropriate action taken.

(4) The evaluation and results of these projects and actions shall, in addition to other sources, feed into the intelligence cycle and provide input for the following threat assessment, which are better informed.

Before continuing with OCTA I would like to mention some other existing Threat and Risk assessments. Protecting the EU internal security requires a good knowledge and a helicopter view of the threats to this security. One major component thereof is the OCTA but other threat and risk assessments are also being drawn up: the threat assessments of EU Joint SitCen on various aspects of terrorism and its forthcoming assessment on organised crime in the Balkans, the risk assessments of Frontex (e.g. on illegal immigration in the Mediterranean area), etc. The Terrorism Situation and Trend Report (TE-SAT) is according to the ENFOPOL 41 REV 2 (8466/2/01), intended to inform the European Parliament on the phenomenon of terrorism in the Member States. The Presidency is responsible for drafting the TE-SAT based on a file and analyses supplied by Europol. Europol has recently made some proposals on a new version of the TE-SAT when developing policies on counter terrorism.

I want to briefly mention where we stand in this area since a lot of work has been done within the different EU bodies and institutions, such as the Multidisciplinary group on organised crime (MDG), the Article 36 Committee (CATS) and Coreper. I am mentioning these, because the Federal Police is or playing an active role or playing an advisory role.

The the Hague Programme (section 2.3) called upon Europol to replace its Crime Situation Reports by threat assessments on serious forms of organised crime with effect from 1 January 2006. This will support the further development of a common intelligence model, by Europol and the Member States. The action plan to implement the Hague Programme was agreed by the JHA Council on 3 June 2005.

Europol will produce the OCTA using the information and criminal intelligence it receives from Member States, from EU agencies and bodies, particularly Eurojust, from third countries and agencies with which Europol has co-operation agreements, from information and analysis drawn from the Analysis Work Files (AWF) held at Europol and from any other information that is available to Europol, that is pertinent and may assist with the identification of threats from organised crime to the Member States of the European Union. As far as possible, Europol will make use of relevant comparable national statistical data in drawing up the OCTA. Europol will therefore have to issue to Member States, an Intelligence Requirement which will give Member States a clear indication of what information and criminal intelligence Europol needs. The findings presented in the OCTA will be and will remain Europol’s independent assessment of the nature of the organised crime threats facing the Union.

The OCTA and the strategic priorities adopted by the Council will be used by Europol to guide the definition of Europol’s work programme and strategic planning for Europol. The OCTA will also be used as a tool by the Council to adopt the strategic priorities that other appropriate agencies and bodies at EU level engaged in the fight against crime, in particular the Police Chiefs Task, will take forward. As appropriate the OCTA may also inform the Council’s wider work on the fight against terrorism, in particular the links between organised crime and terrorism.

The OCTA and the strategic priorities adopted by the Council will guide the Police Chiefs’ Task Force to assist with planning its priorities and operational activity for the COSPOL strategy or any other operational strategy the Police Chiefs’ Task Force may take forward. Member States should, alongside other national considerations, take account of the OCTA and the strategic priorities adopted by the Council in planning their individual and joint responses to the threats they face from organised crime.

This process should contribute to the goal of setting up and implementing a methodology for intelligence-led law enforcement at EU level. The goal of setting up and implementing a widely used and common methodology for intelligence-led law enforcement at EU level must be further enhanced through concerted and co-ordinated action by all bodies and agencies of the European Union involved in these efforts, as well as the Member States.

The creation of a European Crime picture could be the first attempt to an overall strategic vision. For the moment Europol’s mandate covers a wide range of criminal phenomena. However, it is impossible for Europol to address all those phenomena. Until this moment Europol’s work has been prioritised on the basis of an Organised Crime Situation Report (OCSR). This report has always been mainly a “cut and paste” version of the member states’ contributions that are often politically cleaned versions due to the reluctance to show the real situation within a country and was not at all future-oriented. Already during the Belgian presidency it was agreed that this report had to evolve to a threat analysis.

The future oriented threat assessment, together with the Intelligence Led Policing concept, introduced during the past British presidency, could constitute a major breakthrough for Europol. A word of caution is needed since all depends on the willingness of the member states. The introduction of OCTA and ILP implies not only the acceptance of a new policing methodology, but also a drastic change in the way countries look upon the problems of criminality. When there is a cross border aspect to a certain criminal phenomenon, most member states until now have always perceived this phenomenon to be a national problem and not a European problem. If co-operation with other countries is needed, it is for the moment mostly done via bilateral co-operation.

Using the above-mentioned methodology means the acceptance of a European criminality picture and the acceptance that there are criminal phenomena that can only be tackled efficiently through a European co-operation. And above all, it means that countries must be willing to really invest in capacity to deal with the problems that are not primarily defined as a national problem.

Because my time is limited, I cannot go into detail on the internal security architecture of the European Union and on how to reinforce the operational co-operation and horizontal coordination within the European Union. Nevertheless, there will be a need to establish a coherent policy and operational cycle with the following elements: OCTA – European Safety Plan – Operational phenomenon orientated plans (COSPOL projects – TFCP) – AWF's (target groups) and JIT's.

One of the fundamental objectives of the European Union is to offer its citizens an area of freedom, security and justice without internal borders and protecting EU citizens against crime. People have the right to expect the Union to address the threat to their freedom and legal rights posed by serious crime. To counter these threats, a common effort is needed to prevent and fight crime and criminal organisations throughout the Union. The joint mobilisation of police and judicial resources is needed to guarantee that there is no hiding place for criminals or the proceeds of crime within the Union.

The Treaty of Amsterdam on the European Union (EU) which came into force on 1 May 1999 states that the EU:

must be maintained and developed as an area of freedom, security and justice;

that the EU is an area in which the free movement of persons is assured;

this in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime.

In November 2004, the European Council adopted the Hague programme which set the objectives to be implemented in the area of freedom, security and justice in the period 2005-2010. Having recognised the need for greater coordination of the operational cooperation in matters of EU internal security, the European Convention proposed including in the Constitutional Treaty the set-up of a "Committee on Internal Security" (COSI).

Delays in the entry into force of the Constitutional Treaty means that it is not considered appropriate to set up such a committee at present. Nonetheless, the Justice and Home Affairs Ministers at their informal meeting in Vienna on 13 and 14 January 2006 called for greater coordination and requested that arrangements to improve coordination be examined.

The The Hague Programme has – in anticipation of the new European Constitution -attempted to restructure and reinforce the European police and judicial cooperation landscape and aims at reinforcing the position and role of Europol within the new internal security strategy and at the same time tries to anchor Europol within the co-operation structures existing within the European Union.

The creation of new structures seems to lead to divergence and does not lead to synergy. There is still a lack of coherence as the relations between those organisations/institutions are not sufficiently clear. In reality we fear that we will see discussions about the competences and responsibilities of these organisations. This proliferation has consequences with regards to the development of expertise within the organisations, because fragmentation of tasks usually means fragmentation of expertise.

So far my presentation. It is clear that threat assessment is a relatively new concept that is slowly finding its way in international organizations. The threat of terrorism has actually accelerated this process but much more needs to be done in terms of policy making, institution and capacity building and coordination in order face the modern threats in an efficient and effective manner.

Mr Askar Nursha *(in Russian)*. – In step with the growing scale of globalisation, many threats and challenges to national security with which states formerly grappled are taking on a cross-border nature and require corresponding cross-border co-operation to prevent and neutralise them. Interdependency is currently deepening in the current global economy, specifically in the spheres of trade, transport, and financial and monetary policies, and states are also in no position to manage security risks alone. Under these conditions, the co-ordinating and integrative roles of regional security institutes are increasing significantly. In Eurasia, the OSCE occupies a particular position among such institutes.

Kazakhstan’s major foreign policy orientations recognise the development of co-operation with the OSCE in the sphere of security. This strategic task meets the republic’s national interests. It is included in the number of its long-term national priorities. Kazakhstan’s geographic situation in Central Asia, at the crossroads of Europe and Asia, and its multitude of cultures, religions and regional security systems make the republic especially susceptible to threats and risks in this area. Its active participation in the activities of the OSCE, which is one of the few structures where the EU Member States, post-Soviet republics, and leading North American states are represented concurrently, is definitely an important complement to the measures that the Central Asian states are taking to ensure national and regional security within the CSTO and SCO.

It was very important for the republic, as of the very first days of its independence, that the states that joined the OSCE should undertake to abide by this authoritative international organisation’s founding principles, *i.e.*, respect for the sovereignty, territorial integrity, and inviolability of the states’ internationally recognised borders. Kazakhstan took its first steps in the international arena and its participation in the pan-European process that was launched in Helsinki in 1975 was considered to be an important step on the way to its full integration in the community of independent nations, as well as a factor bolstering peace and security in the post-Soviet space.

The situation in the republic today is very different from the one that prevailed in the first half of the 1990s. Kazakhstan has achieved serious economic success. Positive changes have come about in the socio-economic and political spheres. The standard of living and well-being of the republic’s inhabitants have risen. Kazakhstan is generally recognised to be a regional leader in carrying out market reforms and democratic transition. It has fully settled its territorial issues with neighbouring states and demarcated the state’s borders.

Relations between Kazakhstan and the OSCE are on a qualitatively new level. Kazakhstan has applied to fill the presidency of the OSCE in 2009. In so doing, the republic is ready to take on serious obligations in the framework of the leading directions of activity and priorities of the organisation. Their stepwise accomplishment can become a catalyst for the development of the political modernisation and democratic institutions not only of Kazakhstan but of the entire Central Asian region. Using the experience of democratisation in Kazakhstan to instil democratic values in Central Asia is a vast and promising field of activity for co-operation between Kazakhstan and the OSCE.

The OSCE’s efforts to defend human rights, fundamental freedoms, and the principles of civil society are welcomed in Kazakhstan. Progress in the area of democracy is considered by right to be a key prerequisite and basic condition for sustainable development and regional security in today’s world. At the same time, it is necessary to take note of the topicality of a series of extremely significant risks that, if they increase, could have negative impacts on the political and economic situations in Europe and call for no less fixed attention on the part of the OSCE.

First we must point to the risk of a legal vacuum’s developing in the security area. The world powers have resorted increasingly to military force instead of using political and diplomatic means to settle international problems. There is currently a tendency to deal with security problems based on the formula of “right makes might” rather than on the basis of a brief from an international body that has been reached by consensus.

In eroding the legal foundations on which the entire system of militaro-political and diplomatic relations between states is based, we run the risk of undermining confidence in this system, of casting doubt on the legitimacy of the actions of the basic international bodies and regional institutes, as well as causing states to forsake dialogue and negotiations for the use of force. And the deeper the crisis of international law becomes, the more widespread force will be in the political climate in Europe and Eurasia. And then, neither the OSCE nor the Council of Europe, nor even the UN, as has happened before, will be able to control the situation.

In the current situation, the OSCE, in its capacity as a regional security structure, might be able to play an important role as an intermediary, after equipping the mechanisms of politico-military and humanitarian baskets that have withstood the test of time. If, in the opinion of the OSCE Member States, there are gaps in international law that prevent the effective settlement of existing problems on the continent, then the OSCE might be able to initiate and become the co-ordinator of a legal reform in order to take balanced, agreed actions and add to or perfect clauses that do not match realities in the field or were nor elucidated earlier. Respecting national sovereignty and reinforcing international legal standards by all means will play a very important role in reducing security risks not only in the territory of the OSCE, but also in the entire world.

There remains the current problem of preventing and settling local and regional conflicts in Southern Europe, Central Asia, and the Caucasus. The OSCE played an important role in normalising the situation in the Balkans. However, much remains to be done, given the differences that continue to divide the Serbian government and ethnic Albanians of Kosovo. The organisation is faced with similar problems in South Ossetia and Abkhazia. Unfortunately, the OSCE Member States' approaches to these problems are diametrically opposed to each other. A weighted solution must be taken and preventive mechanisms for the future worked out. Ethnic minorities must be protected from the possible tyranny of a government formed by an ethnic majority, without, however, encouraging ethnic separatism, which would only bolster the erosion of states along ethnic lines and lead to an escalation of violence.

The next key question is that of the duplication of functions and limited institutional capacities of the OSCE. In current politics, the OSCE's role is much more limited than it was in the early 1990s. When the OSCE is criticised in the post-Soviet space for concentrating too much on democracy issues to the detriment of security, it would be much more logical to ask whether the OSCE's powers to resolve security issues are sufficient and its functions are duplicated by other organisations acting in Europe, such as the Council of Europe, PACE, and NATO, or not. For the OSCE to regain its past authority and, most importantly, effectiveness as a security organisation, it is necessary to formulate its priorities and missions in a swiftly changing world more clearly and to set the limits of its powers in relation to other regional co-operation and security structures.

The risks that are linked to migration and demographic processes on the European continent are very significant. Over the second half of the 20th century and the first years of the 21st century Europe has been a traditional destination of migratory flows from developing countries. However, European governments worried little about this, given the falling birth rates in Europe, and believed that these new influxes of migrants would shore up their workforces. Moreover, to date, the conviction remains that the migrants who have become full-fledged citizens of European countries inevitably blend into their cultural and linguistic environments, if not in the first generation, then at least in the second and third generations.

However, we see that this process is not taking place as quickly as the European governments had hoped. Migrants are conserving their religious and cultural traditions and customs. What is more, today we observe non-European ethnic groups' unwillingness to be integrated in European society. They live in closed communities according to their own informal laws and do not assimilate with the mainstream population. This generates tensions in society. For example, a discussion about the Muslim women's wearing of the Islamic headscarf, the *hidjab*, flared up in France, and the upshot was that the public demonstration of religious symbols was banned by law in that country. On 2 November 2004, a religious fanatic assassinated filmmaker Theo Van Gogh in the Netherlands.

The local population's worry is leading to [the rise of] conservative movements and nationalistic circles that are expressing the questions linked to the problems of racial and religious intolerance and xenophobia. In the USA, the famous political scientist Samuel Huntington writes about the issue of the mass immigration of Latin Americans ("Latinos" or "Hispanics") and threat of the undermining of America's WASP identity in his polemical book "Who Are We? The Challenges to America's National Identity (2004)". This is by no means an ordinary event in a country that was formed as a country of immigrants.

A menacing new trend took shape in 2005: Having reached a certain number, immigrants have started to insist more adamantly on their rights and the extraterritoriality of their cultural preferences. In November 2005 pogroms against immigrants from the East swept across the towns of France and a series of other European countries. Pogroms in which emigrants from Arab countries took part were observed in Australia in December 2005. Since 26 March of this year demonstrations involving thousands of opponents of a toughening of [US] immigration laws have taken place in the streets of the American cities of Los Angeles, Washington, New York, Chicago, Atlanta, Dallas, and Houston.

The aforementioned problems affect Kazakhstan very directly. The high economic growth rate that our republic has currently enjoyed is attracting the attention of the Asian countries with excess manpower to the south and east. To manage these risks effectively, we are making use of the experience of the countries that have already grappled with the problems that are linked to migrant labour and illegal immigration. However, to take a decision it is necessary to understand whether we are dealing with a crisis of multiculturalism as a socio-political model for society or the inhabitual behaviour of immigrant communities that has been triggered by specific social conditions in a series of Western European countries. It is obvious, to the extent that migration is not stopped by political measures, that henceforward the question in the countries of Europe and Eurasia as a whole is how to govern the conflicts of interest that arise between society's permanent values and a policy to foster tolerance and cultural diversity.

Extraordinarily great attention has been paid this year to the problem of energy security. The theme of international energy security has been put at the top of the G8's agenda on the threshold of the G8 summit in Saint Petersburg, Russia, this summer. European Union institutes have been conducting intensive negotiations about co-ordinating energy policies and uniting energy systems since the start of 2006. The US and the newly industrialised countries of Asia have placed the problem of energy security at the centres of their foreign policies.

The emphasis on energy security is justified, given the range of risks that it carries. Traditionally, the risks in this area in Europe were associated with instability in the Middle East, which was accompanied by rising energy commodity prices and threatened the reliability of oil and gas supplies for consumers. In connection with the continued violence in Iraq and heightened antagonism between the US and Iran over the Iranian nuclear problem, the existing risks will undoubtedly worsen. In addition, rising energy consumption in the successful Asian economies is a source of new worry for the states of Europe, given the prospect that they may divert some of the energy flows from Europe. As a result, competition on the energy commodity markets is rising significantly and the degree of conflictuality in the relations between the markets' key players is increasing. Under such conditions, OSCE Member States' dependence on countries with potentially unfriendly regimes may increase. Rising energy commodity prices are reflected in the socio-economic sphere.

The problem of energy security also affects Kazakhstan's interests. In the coming years Kazakhstan may become one of the leading suppliers of raw materials on the global energy markets. More than 61 million metric tonnes of oil and gas condensate were pumped in the republic in 2005 and plans are to raise this figure to 100 million metric tonnes by 2010. To ensure the stability of energy commodity prices we are interested in broad co-operation with all interested parties. With the joint efforts of Russia, the countries of the EU and Central Asia must work out the right answer to the energy risks, an answer that takes the interests of energy consumers and suppliers alike into account. Meeting these goals entails not only increasing oil and gas production, but also developing alternative energy sources and giving developing countries access to new scientific developments in this field. Potential probability must be factored into the equation and measures taken to prevent terrorist acts against oil and gas field facilities, power plants, railroad lines, and pipelines.

We cannot not pay attention to the rapid development of high tech and information communication technology. Around the beginning of the 21st century scientific and technological progress reached a "splitting point", after which not only a technological revolution, but also a social and cultural revolution must follow. At the same time, governments will gradually lose control over progress. As we see, the possession of modern technologies places the great powers and mid-sized countries on more equal footing. While high tech has until recently served the goals of modernisation, who can guarantee that it will not be used in the future by terrorists and problem countries? That is why our countries' bodies with powers in this area must co-operate, so as to be ready to deal with new forms of terrorism resulting from terrorists' abilities to use the latest scientific discoveries for their own purposes.

Mr Karl Widmer. – The four main geographical regions in Switzerland are the Jura region, Zurich, Lake Lucerne situated in the Pre-alps region and finally the peaks at the Bernese Oberland at over 4000 m high are part of the Alpine region.

In these regions the natural and man-made dangers are very different. Lake Neuchâtel is situated in the Jura region. Basel and the region of Basel with its important chemical industry also belong to the Jura region. Zurich is the largest city in the densely-populated Central Plateau.

The main routes linking northern and southern Europe run through the Swiss Alps, this means that Switzerland belongs to Europe even though it is not a member of the European Union yet. More than 1.5 million foreign residents live in Switzerland. Four national languages are spoken: German, French, Italian and Rhaeto-Rumantsch.

The foundation of modern Switzerland were laid down in the 19th century. The constitutions of 1848 and 1874 made it into a federal state, giving it central authority. Confoederatio Helvetica, the Latin name for Switzerland, and hence the CH stickers on our cars, shares borders with Germany, France, Italy, Austria and the Principality of Liechtenstein. Switzerland has agreements for bilateral support in cases of emergency with all of its neighbours. For example, Switzerland carries out exercises with Germany dealing with emergencies in nuclear power plants.

Switzerland is a federal state made up of 26 cantons, the cantons are its states. At federal level there is a two-chamber parliament elected by the people.

The seven members of the government called the Federal Council are chosen by the two chambers. The seven government departments (or ministries) are: 1. Foreign Affairs, 2. Home Affairs, 3. Justice and Police, 4. Defence, Civil Protection and Sports, 5. Finance, 6. Economic Affairs, 7. Environment, Transport, Energy and Communications. The Federal Chancellery is often called the eight ministry.

The Federal Office for Civil Protection (FOCP) belongs to the Department of Defence, Civil Protection and Sports. The current minister is Mr. Samuel Schmid, who was president of the Confederation in 2005. The presidency rotates every year among the seven members of our government. Switzerland is a member of most international organisations, except the European Union (EU) and of NATO. Relations between Switzerland and the EU are governed by bilateral agreements.

Swiss civil protection has its origins in the Second World War, this means in the protective and rescue measures undertaken as a result of bombardments of cities in Europe. Based on this experience and the knowledge required; an article on civil defence, as it was formerly known, was written into the federal constitution at the end of the 1950s. In 1962, the first federal law on civil defence was created.

A groundbreaking move came in 1971 with the introduction of the ‘Protection’ Concept. This concept led to the intensive period of shelter construction: protective structures for everyone. Finally, work carried out in the 90s led to the legislation that is in force since 2004.

Switzerland has close to 100% coverage with regard to places in protective shelters for the population as well as all necessary larger protective infrastructures and warning facilities. Since 1970, all protective infrastructures in Switzerland have been standardised. Their construction is neither complex nor expensive as it is usual in Switzerland to build nearly every house with a cellar.

Since the 1990s, risk and vulnerability analyses, such as the Katarisk Report have been used to plan and organise resources and measures. The Katarisk Report investigated the relevance of a range of risks, excluding war, for Switzerland. The civil protection system has a pivotal role to play in ‘integrated risk management’ but only during certain phases above all during the preparation, intervention and recondition stages.

The new Swiss civil protection system was first outlined in the Report of the Federal Council to Parliament concerning Swiss security policy. This is also known as the 2000 Security Policy Report. Its guiding principle was and is ‘security through cooperation’. This report gave rise to reforms of three aspects of security policy: the reform of the army, the reform of the national security, in particular the police services, and finally the reform of the civil protection system, which involved ensuring cooperation between national security partners.

The milestones of this project, conducted between 1999 and 2002, were twelve political principles. These principles were submitted to the cantons and the relevant partners for consultation. The two most important achievements of this project were the guidelines and an entirely new law for the civil protection system. Following calls from opponents to this law a referendum was held in May 2003. Over 80% voted in favour of the law which was an excellent and rare result.

The scopes of dangers are highly relevant for the new civil protection system. Switzerland’s system does not take everyday incidents into consideration. There are disasters, emergencies and violence below the threshold of war which also covers terrorism. The civil protection system currently in place in Switzerland focuses on these risks and hazards, or in other words incidents which can occur with little or no advance warning. The consequences of armed conflicts are of lesser importance today as it is highly unlikely at the present time that they would occur in Europe.

The integrated civil protection system, which is jointly managed, consists of five partner organisations: the police, the fire service, the public health care services, the technical services as well as protection and support services. Three of these partner organisations are made up almost exclusively of professionals. However, the majority of fire service and protection and support service personnel are non-professionals, i.e. the two of them are militia-style organisations. For four of the services, responsibility lies with the cantons, the only exception being the protection and support service.

The civil crisis management staff mirrors the structure of the civil protection system. The staff unit which is subordinated to the political authorities is made up of representatives from each of the partner organisations. This staff structure exists at municipal, regional and cantonal levels.

The tasks of the civil protection system are divided between the Confederation, the cantons and the municipalities. In terms of operations, the cantons play the most important role. The resources of the partner organisation belong to the cantons.

The financing of the system has recently undergone a complete change. According to the new legislation the Confederation pays for those components for which it is responsible or for those which it uniformly regulates. This includes public warning systems which are the same for the whole country or for the whole population as well as protective infrastructures such as protected command posts and protected hospitals.

The reforms also included changes to compulsory national services. Men must serve in the army until the age of 30. For compulsory protection and support service, the age limit rises to 40. The cantons themselves regularise compulsory service in the fire brigade. Only men are subjected to compulsory national service. Women may volunteer to serve in all three organisations. Cadre functions are also open to them and they go through the exact same training as their male colleagues.

The figures for compulsory national services are still very high especially by international standards. The army counts about 120,000 and 80,000 in reserves. The protection and support service is approximately 105,000 people and the fire brigade also about 100,000 people.

The standard formation of the protection and support services has five areas of responsibility. These five platoons are generally incorporated in a company and therefore the commander usually has the rank of captain. The protection and support service also has specialist platoons which deal with cultural property protection.

The Federal Office for Civil Protection has six divisions, the policy division, the management and support division, the NBC laboratory, the National Emergency Operation Centre which was created after Chernobyl, the Training Division and the Infrastructure Division. In Switzerland when speaking of national security co-operation it means the civil protection system plus the army plus additional security policy partners. Work is currently underway to restructure this system.

The Minister for Foreign Affairs and the Minister for Justice and Police. The so-called steering group is made up of the directors of the relevant federal offices including the director of the Federal Office for Civil Protection. The crisis management staff is a new component, and as such, it is a work in progress.

The only intervention resources that the Confederation has at its direct disposal is the army or a part of the army. It may be deployed for subsidiary security operations as well as to provide military disaster relief – for this purpose we have a special battalion – and finally for air transport. There are clear rules which govern the subsidiary deployment of army resources.

The serious damage caused by storms and floods in August 2005 severely tested the Swiss civil protection system but it adequately passed this test. Havoc was wreaked by the natural disaster. In the tiny canton of Nidwalden in Central Switzerland 250 sites were damaged, there were 500 landslides and 500,000 m^3. In this instance, the primary intervention resource was the fire service and also the police. The protection and support service provided durable support over days and even weeks.

The figures concerning the inter-cantonal assistance for the small canton of Nidwalden were:

850 members of the protection and support service came from the canton of Basel-Landschaft.

150 members of the protection and support service came from the small canton of Appenzell Ausserrhoden.

The scale of non-military inter-cantonal support as well as military subsidiary support was proof that the guiding principle of ‘security through cooperation’ has been successfully applied nationwide. Based on recent experiences, the FOCP is convinced that the federal solution is perhaps not the best solution but it is currently the best possible solution for Switzerland.

Mr Said Tadlaoui. – Nous avons eu droit à deux exposés à caractère académique. Les deux intervenants ont pris de grandes distances avec les politiciens. En sociologie et en approche sociale, il n’y a pas de transitivité dans les préférences individuelles. Comment peut-on passer des choix individuels, à savoir un député, un sénateur, à des choix en fonction de sa région, d’un secteur déterminé pour avoir une courbe des choix collectifs. Donc il n’y a pas de transitivité.

Pour le second intervenant, c’est le problème de la statique. Quand on n’est pas en dynamique, comment actualise-t-on cette hiérarchisation ? De quel espace budgétaire dispose-t-on pour s’adapter à l’actualisation des choix ? Il s’agit d’un problème d’optimisation en fonction de la variable temps et non pas de la variable statistique.

Mr Ouadia Ben-Abdellah. – Ma question porte sur un sujet qui nous intéresse tous, à savoir l'immigration clandestine. M. Askar Nursha a évoqué le problème auquel son pays est confronté à cet égard. Le représentant suisse a également parlé du pourcentage d'étrangers vivant sur le territoire suisse. L'immigration clandestine nous interpelle car elle est susceptible de déstabiliser les pays d'origine, les pays de destination et les pays de transit. Le bassin méditerranéen est en mouvement constant et totalement déstabilisé. Les migrations provenant des pays subsahariens, passent par les pays du Maghreb qui pâtissent de ce phénomène. Il suffit de voir les catastrophes humanitaires dont on nous parle toutes les semaines.

Je voudrais savoir s'il y a réellement une coopération internationale dans ce domaine. En effet, la coopération ne doit pas se limiter à l'OSCE. D'où ma suggestion : ne pourrait-on créer une instance, à l'échelle planétaire, qui regrouperait tant des politiques que des chercheurs, lesquels étudieraient le phénomène des mouvements de population ainsi que ses conséquences ?

Mrs Muradova Bahar *(in Russian)*. – First of all I should like to thank the Parliament of Belgium for its wonderful organisation of this conference and creating the conditions for fruitful proceedings.

The subject being discussed today affects in one way or the other the issues of the security of Europe's energy resources and ensuring these resources safe and secure transport from the countries where they are produced to the countries where they are used. In this connection, I should like to underscore once more that Azerbaijan makes a mighty contribution to supplying Europe with energy sources.

Taking that as our starting point, we hope very much that the global community and international organisations will take the necessary measures to eliminate probable threats and risks from the Caspian Sea area. Our respected colleague from Lithuania observed that the three [former Soviet] states of the Baltic region signed a "communiqué" on guaranteeing their countries' energy supplies. We also should like to engage in this type of co-operation in the Southern Caucasus. However, this is not possible today, because of the occupation of a part of Azerbaijan's territory by Armenia's armed forces and the creation of a lawless area in the occupied territories where soldiers and terrorists are trained, narcotic substances are grown, trafficking in people and arms takes place, and radioactive waste is buried.

Despite its problems, Azerbaijan is in favour of multiple oil transport routes. At the current time, Azerbaijan, Turkey, Georgia, Ukraine, Kazakhstan, and, we hope, Turkmenistan are examining the possibility of building new pipelines to carry oil from Central Asia to Europe through Ukraine and Poland or through Turkey and Greece. We are ready to carry out such a project, but, in the final analysis, everything depends on the proposed routes' profitability and investors' willingness to invest their capital in such works. Investors, it is known, prefer to invest in projects in safe regions with the lowest risk levels.

In Azerbaijan, great attention is given to ensuring the safe exploitation of the oil and gas resources in Azerbaijan's sector of the Caspian Sea and on dry land. The construction and operation of Baku-Tbilisi-Supsa, Baku-Tbilisi-Ceyhan, and Baku-Tbilisi-Erzurum oil and gas export pipelines are currently planned.

If one talks about security, one must bear in mind that this means not just ensuring the physical safety of the facilities and people by creating the corresponding safety and security departments in the oil and gas pipeline companies, but also creating the corresponding state safety and security departments and ensuring co-operation, information exchange, and planning approval. Such departments have already been created and are working successfully, and interrelations among them are governed by the appropriate agreements and additional protocols. It is extremely important that in carrying out safety and security measures on the ground, governments, companies, and their respective safety and security departments should be guided as well by the standards and requirements in the relevant international agreements, conventions, and other documents.

In addition, extreme attention is paid to applying the best international standards for designing and operating the works and equipment, using technical safety devices and safety/security measures, and protecting the environment and human health and safety. Constant, constructive co-operation with the population, municipal authorities, civil non-governmental associations, and scientific and educational establishments is also a factor of safety and security that must not be discounted.

As we can see from the foregoing, Azerbaijan is doing everything possible to guarantee the safety and security of the oil and gas pipelines on its territory. However, the probability of a risk nevertheless exists. Here we have in mind the part of the Baku-Tbilisi-Ceyhan oil pipeline that runs along the border with Armenia, where acts of diversion, terrorist acts, and on the whole, the risk of the resurgence of military activity in the region are possible.

That is why Azerbaijan thinks that ensuring the security of energy projects in the Southern Caucasus region completely is possible only once all of the armed conflicts in the region are settled fairly.

We are in favour of the peaceful resolution of all the conflicts occurring in the various regions of the globe, as only peace and stability can guarantee the security of the many energy projects that are required to meet the interests of the peoples of all the countries that span the globe.

Mr Gratchev Oleg *(in Russian)*. – Today a series of representatives taking part in this conference rightly touched upon the question in connection with the twentieth anniversary of the Chernobyl disaster. I shall thus add nothing new in this regard. However, I would like to focus on two things. First, let me remind you yet again that a parliamentary hearing will take place in Kiev on the 26th of this month in which MPs from not only the countries that suffered directly from the disaster (Belarus, Ukraine, and Russia), but from other European countries as well will participate. Second, I see with regret that a series of agreements and written documents linked to the closing of Chernobyl Nuclear Power Plant have still not yet been consummated. A series of European countries have not met their obligations. On the eve of the Chernobyl disaster's twentieth anniversary, that of course triggers a certain feeling of bitterness.

In addition, today we touched upon the matter of security in the energy field. As a representative of Ukraine, let me start by saying that we observe no political pressure of any kind from Russia. Russia is acting fully appropriately in this regard. Her position is quite pragmatic, which is very natural for a country that has such resources. So, the recent crisis in our country did not result from any pressure, but was a natural process. For that reason we wanted to point out that the Baltic sea floor pipeline will of course exist, which will not reduce the importance of the ground-surface gas pipelines crossing the territories of Ukraine or Belarus into Western Europe. Moreover, it gives Western Europe the possibility of an even more secure energy supply, given that the ground-surface oil and gas pipelines have been operating for years and are in need of re-equipment.

In conclusion, let me say that the discussion that has taken place forces us to think about the fact that, as I see it, two major threats are hanging over humanity. First is ecological disaster, which it may be possible to avert by dealing properly with nature and its resources. Second is impatience in the interactions of certain groups that differ in size. These may be interactions between countries or groups of countries. It is precisely in the combination of these two threats that I see the death of today's civilisation. It follows that we must direct our efforts towards overcoming these two, in my view chief, threats. In so doing, co-operating within and between countries and seeking out compromise around the negotiating table are the main means for solving the problem at hand.

Mr Tigran Balayan. – It is deeply regretful that other delegations keep repeating the baseless allegations against Armenia and the de facto sirtuation of Nargona Kharabakh. No single allegation of Azeri sites has been proved by the international delegations and commissions visiting the region of Nargona Kharabakh. It is Azerbaidjan that is blocking participation of Armenia in regional projects and it is Azerbaidjan who is giving shelter to Czech terrorists and to other terrorists coming from the Middle East.

Mr Jean-Pierre Contzen. – Je voulais signaler à M. Daoudi que la communauté académique se préoccupe déjà des flux migratoires. Des études sont réalisées, en particulier par l'université des Nations unies, mais également par l'UNIDO et d'autres. Un des deux vices-recteurs de l'Université, M. Ramesh Thakurs'occupe spécifiquement des problèmes liés à la paix, à la sécurité et donc, aux migrations.

Mr Christopher Bunting. – The most important thing to emphasise is that for now the IRGC risk governance framework remains theoretical. One or two people are now looking to test it in real life. Warner North overviewed some of the factors he found in testing it in the specific instance of gas supply. It is also being tested in listeria in raw milk and cheese and in extreme tourism, for example, climbing and different risk types to see if it actually works. This may help with trade-off issues.

The thing to bear in mind about the framework is that it is at the moment essentially theoretical and it is not known if it works yet. The hope is that it will help people think about risk in a broader way and think about how it might help to make a decision by involving more people in the management process.

Frantisek Bozec demonstrated what happens within risk-assessment, particularly in the construct of critical infrastructure, a very topical theme worldwide, and in some areas the subject of considerable investment, both financial and in terms of human resource and attention. What he proposed was a possible methodology that could be used to help nations or regions identify which infrastructures and which elements or areas of them merited the most attention.

Bart D'Hooge described a large number of activities, mostly within the confines of the EU-25 member states, but I suspect candidate countries are also now involved, covering mainly the crime arena and policing of inter-territorial crime which if you have no border control then seems to be a fact of life. There used to be a manned border in Switzerland, there was no crime because the gates were shut at night and it was manned. But now it is not manned and most of the crime is committed by young boys from Leon. It just seems to be a part of modern life in Europe. I found that Bart D'Hooge concluded with a very interesting statement which was essentially a concern about the coherence between and the responsibilities of the many bodies being set up. There was a governance process in creation but you seemed to suggest that it was yet to be proven whether it would work.

Askar Nursha presented a very wide-ranging piece, covering such things as migration, integration, national identity, energy supply and consumption in one piece. He also joined everybody else in calling for the creation of competent bodies that extended beyond national borders, for coordination and cooperation. He even went so far as to mention the creation of super national powers. OSCE is one of many.

Karl Widmer described a system that is refreshing to an immigrant which is both this participative approach and the fact that all of your neighbours are the people responsible for saving your life if you are in trouble because they are all in the communal service.

One reason Mr. Widmer was asked to speak was because if the OSCE is to look at risk-governance and collaboration between not just the 55 members but between observers and neighbours, which is essential for risks that are not just European in origin or type, then it is useful to listen to what goes on in a country in Switzerland. where literally if you want a fire put out, the ticket seller at the local railway station, half of the *vignerons* in my village, the chef in the *auberge* all have to down their tools, put on their uniforms and go and put it out. This is done at a communal level, this is a village of less than 400 people but it is done under a federal framework. To cap it all it is paid for with my taxes which do not go anywhere near Bern but straight into the local municipal kitty. This is a real delegated and empowered approach within a large framework. It may not be perfect but this is how it works.

The IRGC has decided that as a new organisation looking at risk it is a little too young to tackle some of the migration issues.

Mr José Mariano Gago. – Risk governance, for politics, is an opportunity. Rather than regarding risk governance as a burden policy makers increasingly embrace it as an opportunity to develop and build public trust. The general public requires governments and regulatory authorities to deliver the best possible risk governance to society.

Global companies now face a renewed demand for social and public responsibility. The problem of trust is a critical issue, it is critical in the relation between the public and companies but also concerning governments. The debate about risk sharing, sharing between government, companies and individuals is constantly being reassessed mainly in view of the changing nature and of the dimension of the risk.

The problem of the future of insurance companies in their current form is an open problem. It will probably require that some new, large and mostly unpredictable risks are shared across society. This largely depends on the agreement that can be reached between governments, companies and individuals.

If risk sharing is not decently distributed then the business of insurance is impossible. This is probably one of the main triggers for the debates on risk sharing nowadays. This problem was seen immediately after 9/11 concerning civilian aviation.

Another point concerning the building up of trust is the credibility of independent bodies. In many countries, independent regulatory bodies were established in certain areas. However, the idea of independent bodies stemmed out of economic competition and not in view of building up public trust. It was to build up trust among competing partners. There are regulatory bodies in areas where the state have to intervene in matters of price of quality for instance. The idea that regulatory bodies also have to play a role in building up the trust of security and building up the standards of security in relation to different areas relative to the public is a new one.

The problem which is being addressed by many governments is the following: can regulatory action be dealt with without a strong network of independent research or scientific organisations that are perceived as credible and unbiased sources of competence? This is a new problem which makes science policy extremely important in the area of risk governance. Science is increasingly seen as a tool for risk governance. Science has been used during the last decades, in the area of risk governance, as a source of 'culture of evaluation'.

The areas in which the internalisation of risk governance have been most successful are the ones which copied the ways of evaluating, assessing, cross-checking the data, cross-checking the results from the scientific institutions. For instance in the nuclear fields, the regulatory framework in the nuclear fields is essentially based on the institutional techniques that have been developed by modern science. This does not exist in many other areas.

If you wish to address the questions of risk in the area of critical infrastructure or other epidemics you will find that national organisations are normally not cross-checked by other national organisations, that international evaluation of national bodies is normally not present in the usual political machinery of national governments.

In June 2003, under the auspices of the Swiss Government, the International Risk Governance Council (IRGC) was formally established in Geneva with the mission of, as an independent organisation, trying to bring together companies, governments and scientists.

The IRGC's mission is to:

- develop concepts of risk governance
- mobilise the best scientific and technological expertise available
- network the relevant social actors, namely the private and the public sector
- undertake anticipation of major risk issues
- provide policy recommendations

There is a variety of perspectives and origins sitting on the board. The main asset of the IRGC is its scientific council. The scientific council of the organisation is built up of mainly scientists, either pharmacodemia or from industry from many parts of the world. The scientific council is the living body of the organisation in terms of providing technical and scientific expertise, providing ideas and suggesting the areas that should be investigated.

The strengths of such an organisation are the fact that it is international, the fact that it has access to policy-makers, access to risk-management and access to the best scientific knowledge. The IRGC is quite a recent organisation, the Inaugural Conference was held in Geneva in June 2004, the second General

Conference was held in Bejing at the invitation of the Chinese government in 2005, a Conference on Nanotechnology will be held in July in Zurich this year and in the Autumn of 2007 the third IRGC General Conference will be held in Lisbon.

The first white book on ‘Basic Concepts of Risk Characterisation and Risk Governance’ was finished, published and discussed in 2006. The new publication including issues about biotechnology, stem cells research, integrated disaster risk management will be available later this year. The first recommendations on our Critical Infrastructures will also be published this year.

We are now working on our nanotechnology project and the risks of nanotechnology and the risk governance in the area of nanotechnology as well as other areas. It may be asked why choose the following areas: critical infrastructure, nanotechnology, epidemic diseases and so on? Or for instance a new area that is being considered now is carbon sequestration, why choose this area and not other areas?

The scientific council of the IRGC have suggested a certain number of potential new projects which can be dealt with in the future: the comparison between storage of carbon and the storage of nuclear waste, the emerging infectious diseases, the critical infrastructures or the large scale manufacture of packaged goods. In all of these areas the combination of scientific expertise and the policy making is a critical element.

What the IRGC tries to bring together is scientific and technical expertise on the one hand and policy-making on the other hand, policy-making from parliaments, from governments, but also strategic policy-making by heads of companies and industrial groups. These are also part of the policy-making of the modern world.

The discussion about the politics of risk governance can be summarised in the following way: it is ‘they versus we’. ‘They’ is how the public view policy-makers, governments or parliaments.

The first question which arises when there is a tragedy or an emerging risk is announced is ‘are they doing all they could do’? ‘They’ are the government or the parliament, those who have the power to decide. This is a very tricky question because we can never say ‘yes’. A gauge is needed in order to answer this question. What should be done? The best way to deal with these types of problems or the new types of problems should be agreed upon.

One traditional way of dealing with this question is to set the gauge up internationally, we will say to our constituencies that ‘yes, we are doing all we can do in terms of what the world at large has agreed upon.

A second questions arises from this, ‘are they, governments, parliaments in our own country following international risk governance norms?’ Again we can’t answer ‘yes’ to this question because there are no international risk governance norms. Or to be more precise, there are some risk governance norms in some specific areas. In the field of nuclear safety these have been set up by the Agency in Vienna. In the field of civil aviation there are some international norms at least in the network of the countries subscribing the civil aviation international norms.

In some areas of pharmaceuticals there are international norms. But looking at many other areas, the quality of food, the risk of collapsing bridges or tunnels, there are no international norms. There are professional norms that are used as a basis for professions such as civil engineering, electrical engineering and so on but these are not enough to set up and to define risk governance norms.

In any country the control of dams is given to a specific entity, a specific civil engineering laboratory or a regulatory authority in the area of critical infrastructure. This body has the task to review and monitor the existing dams and to inform the authorities in charge if anything goes wrong or if some intervention is needed.

These national technical bodies do not respond to any type of international norms and they are not internationally reviewed, assessed and analysed by other bodies. This is contrary to what happens in the area of nuclear safety or in the area of civil aviation where national bodies cross-check each other. This does not happen in the area of critical infrastructure.

Why is it so difficult to set up international risk governance norms? If you go to organisations like OECD you may find it extremely difficult to address the question of norms. Even the word norms is considered as a taboo. International norms, they do not speak about norms, they speak of ‘best practices’, exchanging best practices but never about norms. Setting up norms is difficult because of competition, many of these norms could be the result of a consensus among different partners, governments but also companies in many areas.

Setting up the standards would freeze competition in many areas and economic competition in many of these areas is intense and has not stabilised at a level that allows acceptable norms to emerge. This is seen in the area of environment. Chemicals are dangerous for the environment.

The discussion about the level of danger is in fact not a discussion about public health but also about competition. When a new chemical or a new product is developed the norms tend to change, the regional norms tend to change, for instance within the European Union. These norms are not accepted worldwide. They are provisional norms that are tangled up in the world of economic and political competition.

There is another problem concerning these international norms. Part of this is the usual problem of public bodies in national states being too jealous and not accepting being subjected to scrutiny by other bodies from foreign countries. Governments and parliaments should not accept this. It is extremely difficult for a government or for a parliament to be confronted with the responsibility they thought were in the hands of a specific public body at the very last minute. If a dam collapses the responsibility is the responsibility of the government of that country and not the responsibility of that public body.

In areas where trans-boundary risk is at stake then it is important to have an international system. For instance if you discuss critical infrastructures like railways or electricity then it is immediately international by nature. The areas of bridges and dams is also international because of the increasing flow of people and goods.

The globalisation of commerce will bring a different level of responsibility with it. The Member State is also responsible on a wider scale than before. There are many countries, namely in Asia, discussing this problem and imagining that setting up international risk governance norms should be part of the United Nations machinery and should be part of the revision of the United Nations Administration.

The third point is the usual question asked by the public when something happens and this is ‘why did the parliamentarians and the governments keep it secret? This is such a common question because the public find out about many emerging risks through the press. These emerging risks become political objects. Without the press, without the media many of these risks would never have been made known.

This question from the public is a very important one. Should the parliamentarians and the government keep it secret? Why do technical bodies in charge of risk governance inside each country try to avoid open scrutiny from the public? This is a problem of trust. If this problem is not overcome it will be extremely difficult to build up trust. This question is a question being addressed by many countries in terms of individual and collective responsibility by public bodies.

Imagine the following situation and how it would be addressed in different countries: A national laboratory is asked to review the risk in a particular infrastructure or a particular situation and is commissioned to do so by government. This laboratory finds that the risk is enormous, the risk of collapse, the risk to human life is enormous. However, the report is confidential because it was requested by the government.

How can the problem of civil and criminal responsibility be solved? Should the law stipulate that the director of the laboratory must go public if the government does not go public? Should research prevail? Should the responsibility lie entirely with the government if the government fails to act?

These are difficult questions which are dealt with in legislation on different scales in different countries. This is something which should be discussed politically. No cross-check of the legislation has been performed comparing legislation in different countries. It is not just a question of the integrity of the scientific organisations but also a question of the responsibility and the relation of the technical responsibility in contrast with the secrecy, confidence or publicity.

Whose advice should be trusted? If in some situations governments or technical bodies are entitled to keep it secret then it should be of no surprise that technical advice, scientific advice, and political advice can not always be trusted.

Results from the last polls carried out in Europe and the United States analysing this problem showed that doctors and scientists are among those best trusted by the public at large. The public did not show any trust for politicians and companies at all. If this is so, then there is a problem for governments and for parliaments in using scientific organisations in the medical profession as public mediators to build up public trust.

This is not a question of individuals but a question of institutionally building trust through organisations related to the medical profession and organisations related to the scientific profession. In many countries this problem is normally addressed in terms of the problem of the integrity of these organisations.

It is essential for the politics of risk governance to preserve and to make clear that strong organisations – scientific, technical, medical organisations – strong organisations, who are the recipients of public trust need to exist in order to be able to deliver the best possible politics for risk governance.

In many areas risk should be taken and not avoided. This is certainly the situation in emerging economies of developing countries. It is impossible to imagine that many emerging economies can go forward without taking risks, without accepting risks. When should risks be taken and when should they be avoided? This is a very complex situation concerning individuals, local authorities, governments or companies. It requires the sharing of risks, the decision cannot be taken individually, it must be somehow shared. The sharing of risks is embedded in the structure of society itself, of policy-making itself.

In stable advanced economies the question of risk-sharing is essentially a legal question and the evolution of legislation concerning the role of the insurance companies in government, and in individuals, was a measure in providing relief to major risks.

The situation is totally different when speaking about developing countries and fast-growing economies. Here it is not a question of insurance companies or the insurance business. It is a question of trying to accept the risk and define the level of acceptability of the risk without which the economy cannot grow fast enough to reach the level of advanced companies.

Mr Nevzat Yalcintas. – This last point ‘have to share the risk’, to share among those who face the risks or among the countries in Europe. ‘Sharing the risk’. Could you explain this further?

Mr José Mariano Gago. – The debate is dominated by the aftermath of 9/11. I think we should look at the whole picture. After 9/11 reinsurance companies decided that the risk was too high and they ordered insurance companies to stop. They could not accept insuring civil aviation. Before a new settlement was reached it had to be decided in cabinet a week after 9/11 that the government should take the risk instead of the insurance companies concerning our own civil aviation companies.

This is normally the case in times of war. If there is a major catastrophe or if there is war then reconstruction has to be dealt with by government and by society at large. The State has to provide for the reconstruction of the infrastructure that was destroyed. No insurance company will account for this or will take care of this. These are extreme cases.

The problem is how extreme should the case be in order to go there. Is global war just counted as extreme or is any type of terrorist act extreme. Is disease a case for war? The fight against viruses can be seen, in some cases, if there is a very large epidemic, as a war. Should the reinsurance companies tell the public and the government, that beyond a certain level they are unable to cope.

What is the relation between governments, insurance and reinsurance companies and individuals? How much responsibility should each have and how should these responsibilities be shared.

There is no formal answer to this question. It is a question of debate and it depends on the circumstances. The change in circumstances will change the relative weight of one of these actors against the others. If society is rich enough then individuals can take more risk and bear more responsibility than those in poorer societies. Unfortunately it is normally the opposite, individuals are more protected in richer societies than in poorer societies.

The other point mentioned is risk-sharing among nations. Risk sharing among nations is extremely important. This can be seen with epidemics. It can also be seen in infrastructures supplying energy, supplying gas or electrical power. If these electrical networks are largely interconnected then any disruption in one country or in one region will affect all the other regions if the interconnection is global.

The interconnectivity of energy supply chains and in fact of any type of critical networks will require some type of risk sharing in advance just before the catastrophe occurs. If you privatise all the electrical companies and if you do not establish a provision for extra capacity in all the countries which are inter-linked then it is certain that there will be blackouts. If there is extra capacity someone has to pay for it so who should this be? Should this be the consumer or should this be the government?

It is not enough that a specific country provides this extra capacity. There must be an agreement at international level. If one country provides extra capacity and not the other ones then this extra capacity will either be sufficient for the whole network and in this case that particular country is paying for all the others or it is not enough and the particular country in question is paying for all the others with no results.

The problem of risk sharing is difficult but it is a problem which has to be solved because of the interconnectivity of diseases, viruses and the circulation of energy.

Mr Nevzat Yalcintas. – In relation to the Amendment the paragraph stating ‘the setting up of a permanent crisis management team composed of experts in risk governance and attached directly to the president of OSCE’ needs to be clarified. This should be clarified as there will not be a permanent staff all of the time in OSCE buildings but only in emergency situations.

The joining of Turkey, as a full member, to the European Union will be very good for the security and risk management of Europe as a whole. Politicians in any countries of the EU who are opposing Turkey’s full membership, for internal and political reasons are not doing a good job for Europe.

Mr Oleh Bilorus. – I have several corrections, recommendations, and amendments to the draft resolution. Some important words should be added to the first part of the draft and these are ‘growing importance to the security in the future’, the key words here being ‘growing’ and ‘in the future’. Not only the general meaning of security should be added here but also the specific international and global security meaning.

In the introductory part, in the last paragraph when we discuss ‘related to risk governance’, I would put ‘systemic’ risk governance, not all possible risks but systemic.

In the results section, in the first paragraph, ‘The conference recommends…’, an important amendment should be made. Instead of ‘due to meet on July 3-7 2006 consider the launch of activities’.. From my point of view here it should be the ‘adoption of the programme of actions relating to security and systematic risk governance’.

In the next paragraph, in the first sub-paragraph after the words ‘between countries about risk’, I would put ‘about future risks in the multification assessment and management’ with a special accent on the future because we have no possibility to manage former risks and accidents.

The last sub-paragraph of this large part I would put here one amendment concerning the principle nature, instead of ‘permanent crisis management team’ I would put ‘the setting up of our standing OSCE crisis management special committee’. We have general committees but we could also have special committees for very special reasons.

And the last amendment contained in the last paragraph of the draft resolution should speak in the language of the country proposal. Instead of the last three words ‘of these actions’, which is a little too general, I would put here ‘and implementation of integrated and strategic programmes of actions’.

I believe these amendments and proposals are acceptable and important.

Mr Ben-Abdella Ouadia. – En lisant ce document, je me remémorais le débat sur l'Europe, des Pyrénées à l'Oural, et la thèse de François Perroux « l'Europe sans rivages ». Selon moi, le risque n'a pas de rivages, il n'est pas lié à une frontière déterminée. Tchernobyl ne faisait pas partie de l'espace dit européen à l'époque de la catastrophe. Il convient dès lors d'intégrer l'environnement immédiat de l'Europe. Je parlerai de « contiguïté du risque ».

Je propose d'ajouter à la troisième conclusion, après les mots « coopération entre l'OSCE », les mots « d'une part, et les pays voisins, d'autre part ».

A la deuxième recommandation, quatrième point, je propose d'ajouter, après les mots « à travers l'OSCE » les mots « et les pays voisins ».

Mr Nurali Rioev *(in Russian)*. – I would like to express the Tadzhik delegation's enormous gratitude to Mrs Anne-Marie Lizin and the Belgian Senate for the conditions that we enjoyed during the time of the conference.

We, too, have underscored many things from this conference and concur with the opinion expressed by a series of participants, who spoke with regret about the fact that a number of problems in the world continue to be solved militarily and through conflicts, which has negative effects on the countries neighbouring these regions of crisis, countries that are often OSCE members.

That is why we propose adding the adjective "military" to the sentence in the fifth indent under the second bullet point, which reads, "… when any crisis, be it nuclear, industrial or natural, …". We would be delighted if this proposal were accepted.

Mr Giovanni Kessler. – It seems to me reading the second part of the resolution that we are only addressing the OSCE parliamentary assembly. It might be too little for us just to address the OSCE parliamentary assembly.

My proposal is to clearly define whom we are addressing as a conference. I believe that we have at least three categories of subjects that need to be addressed: The OSCE countries and neighbouring countries, the OSCE organisation and the OSCE parliamentary assembly. We are recommending consideration for 'launch of activities or adoption of a programme of action' as was suggested by Mr. Bilorus.

When we are recommending the creation of an OSCE working group I think we need to address the OSCE as an organisation. A specific paragraph could be added for the OSCE assembly which encompasses all political representatives of all of these countries in order to recommend the OSCE parliamentary assembly to pay special attention to these issues. I think that at the end the resolution will not only be clarified but will be stronger if we clearly identify our counterparts.

Finally, I have a minor suggestion. In the very first paragraph when referring to this conference a short reference should be made to those who participated. Otherwise, people who did not take part in the conference and are reading the recommendations do not know who attended the conference.

Mr Oleh Bilorus. **–** I believe that this version is good and can be adopted as the final version.

Mr Chairman. **–** The resolution is adopted.