Magazine National Safety & Security and Crisis Management

Special
March 2008

28 & 29 January 2008
The Netherlands

National Safety & Security

Responding to risks to citizens, communities and the nation

CabinetOffice

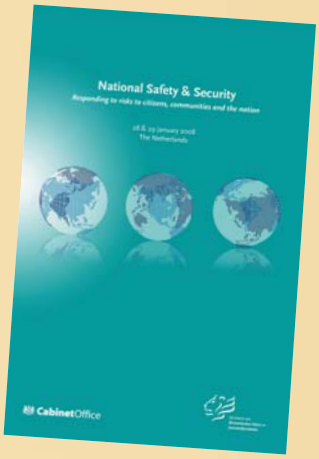
Ministry of the **Interior** *and* **Kingdom Relations**

Content

National Safety & Security – Responding to risks to citizens, communities and the nation
Conference at The Hague, 28 & 29 January 2008

The monthly Magazine for National Safety & Security and Crisis Management is published by the Directorate for Crisis Management of the Ministry of the Interior and Kingdom Relations in The Netherlands. The Magazine is a leading forum for the exchange of ideas on national safety & security and crisis management and is send in closed circulation to administrators and professionals.

National Safety and Security



On 28 and 29 January 2008, a conference was held in The Hague on the theme of 'National Safety and Security: Responding to Risks to Citizens, Communities and the Nation'. Over 100 high-level delegates from across the global community took part in this unique conference. Representatives from government, business, and research concluded that the key challenge for the future was to develop closer cooperation across borders and among all the actors playing a part in the international security community – government bodies, business enterprises and civil society organisations. This is not only because we all must deal with the same issues internally – analysis of threats and identification of the greatest risks – but also because threats are interconnected and do not stop at borders. Furthermore, in the event of a security situation, we will need to communicate better with each other in order that we can share knowledge, expertise and resources.

The conference explored the theme from three perspectives: the institutional (how we organise national security), the analytical (what methods and instruments we use) and the social (how we raise risk awareness). This Magazine reflects the discussions that took place at the conference in the context of these key themes.

Importantly, the conference should be seen as a critical first step towards bringing together different areas of security. We must now ensure that it was not just a one-off event, but that it represents the beginning of a journey towards greater cooperation and real progress against the issues facing us all. To that end, the participants have agreed to hold expert meetings on specific aspect of national safety and security and to commission international institutes to carry out research. They also agreed to explore further the value of developing an informal network, the beginnings of which were created at this conference.

In his summing up, the chair of the conference, Professor Michael Clarke of the Royal United service Institute for Defence and security Studies, felt that, 'the challenge of a crisis is a combination of time, threat and surprise' and with this in mind we have a duty to learn from each other in order to prepare ourselves for all eventualities and acknowledge that we cannot always prevent everything.

The UK and the Netherlands are fully committed to being a part of this network going forward but future initiatives should be driven forward and lead by the community more widely, so that we can truly make the most of its international nature.
We hope you will enjoy reading this special edition of the Magazine National Safety & Security and Crisis Management and be inspired by it.

Bruce Mann,
Director Civil Contingencies Secretariat, UK Cabinet Office

Dick Schoof,
Director-General Safety and Security, NL Ministry of the Interior and Kingdom Relations

From *need to know* to *need to share*

Openingsspeech by Minister Guusje ter Horst

Well, I won't beat around the bush: our very presence here today is not without risk. Although we are apparently safe and dry here, in the beautiful Kurhaus Hotel, I should warn you that this is one of the few sections of coast not protected by our famous sea defences. I'm not trying to alarm anyone. I simply want to show that there are genuine threats out there, which require our attention and vigilance. The Dutch government is only too aware of this fact. And we are working hard to get a full picture of all the threats to our national security.

Let me begin by explaining what we mean by national security. National security comes into play when our vital interests are at stake. These vital interests cover five categories: territorial, economic, environmental, physical, and socio-political interests. A failure to protect these interests could lead to social upheaval. I'd like to share two thoughts on the subject that are hopefully of interest to you.

1 National security is not simply the government's job. Companies and even individuals must also take responsibility. We need more clarity on this point. I will say more about this in a moment.

2 Today's global society means that we need each other more than ever. We stand to benefit far more from sharing knowledge and experience than is now the case.

I'm sure that since yesterday, you have already started sharing experiences. About last summer's floods in the UK, for example. Or the devastating forest fires in Greece. Some countries have had a lot to contend with, lately. I'll admit, it's tempting to concentrate on *past* incidents, rather than *future* challenges. Looking forward is complicated by the fact that today's problems always seem to demand immediate attention. Some threats appear out of the blue, like the SARS outbreak a few years ago. Others are more insidious. For years we thought antibiotics were protecting us. Yet now, they threaten to become our enemy. Increased resistance to antibiotics leaves us more vulnerable to new illnesses. Illnesses which climate change and migration are bringing closer to home. Dèngue fever, for instance, is a problem we are having to address in the Netherlands again. Pandemics are a contemporary national security issue, just like system crashes, flooding, livestock diseases and terrorism. In its own way, each of these things is a threat to our vital interests.

Last April, the Dutch government established a national security strategy, designed to address two central questions:

1 What threats do we face and how serious are they?
2 How can we prevent such threats from occurring, and if they do occur, how can we respond effectively?

It does not require a national disaster to demonstrate the importance of this kind of strategy. Let's consider a recent incident in the Netherlands that had *regional* repercussions.

Just before Christmas, a helicopter flew into an electricity pylon, which then came to rest in a river. Not only was shipping disrupted, but one hundred thousand people were without power for some fifty hours. Shops and schools had to close. Cows could not be milked. Sewage could not be drained, with potentially serious consequences for drinking water. The incident also exposed the fact that twenty per cent of Dutch households are particularly vulnerable to power cuts, thanks to the structure of our electricity grid. Solving this problem will cost around a billion euros. And this leads to a complex dilemma: do we alter our electricity grid, based on this risk assessment? Or do we tell twenty per cent of the population that they run a greater risk of power cuts and advise them to install emergency generators? Or is it up to the energy sector to provide these generators?

There is currently a similar discussion under way regarding evacuation in the event of a major flood. If a dike should burst, leaving much of the Netherlands under water, would the government be able to evacuate everyone in time? What if our motorways are jammed, or the emergency services are disabled because of a storm? Shouldn't we warn people that they may need to fend for themselves for the first twenty-four hours? I believe that this example touches on two important points:

1. The importance of establishing clear responsibilities among authorities, individuals and businesses.
2. The importance of solid threat analyses and risk assessments.

This brings me to the notion of 'capability-based planning'. Any good threat analysis should address the question: what capabilities do the government and the private sector require in order to deal with the threat? International assistance can play a crucial role here. You might be aware of the report on this subject by French agriculture minister Michel Barnier. In response to the forest fires in Greece, Barnier proposed the establishment of a European intervention force. It's a nice idea, but what kind of intervention force would this be, given the complexity and variety of the potential threats? I believe it is better to focus on making use of one another's capabilities as and when we need them. One example is the Dutch Urban Search and Rescue Team, which has been deployed abroad many times. I don't see much benefit in a central unit that sits around gathering dust when nothing is happening. I see more sense in sound 'mutual support' agreements between countries.

Cooperation is absolutely vital. It is also at the heart of this conference. We are all increasingly conscious of the fact that national security is not the sole domain of an individual country. Nor is it the exclusive domain of the public sector. National security is everyone's business. We are all linked together. You only need to look at the recent bird flu epidemic: when it came to sharing knowledge and taking measures, we all needed each other.
This type of cooperation requires a shift from 'need to know' to 'need to share'. At the moment, we often limit the information we share to what is absolutely necessary. And too often we share it right *after* the disaster, instead of at the planning stage. This is understandable. Security organisations are not exactly known for their openness. The same goes for the private sector. Fierce competition means that energy suppliers or telecoms companies are reluctant to discuss their vulnerabilities openly. After all, their image and their market position are at stake. Fortunately, we are coming to realise that we need each other. More and more, professionals from different countries are seeking each other out. Slowly but surely, a network of knowledge and experience is emerging. But perhaps we can give this network more structure, without formalising it too much. The main thing, of course, is that this network remains useful in practice. Today is a great opportunity for doing just that.

I would like to express my appreciation to our partners from the United Kingdom, who worked with us to organise this meeting. It is no coincidence that the Netherlands and the United Kingdom have joined forces on this.
In preparing the Netherlands' national security analysis, we used the 'all hazard' method of identifying risks. And the UK made use of the Dutch approach in establishing its own national security strategy. In short, we have each benefited from the other's core strengths. It would be good if this could be achieved on a wider scale. So I am also calling on all of you here today to take *concrete steps* towards this goal. Let us form a 'community of best practices': an outstanding idea which offers clear practical benefits.

I would like to close by expressing my hope that, by the end of the day, we have made the shift from 'need to know' to 'need to share'. We need to deepen our partnership.
If, during the course of the day, you find you need a little inspiration, look out of the window, at the sea. It may look beautiful, but remember: simply by sitting here, we are taking a calculated risk. I hope this place will inspire all of us to action. I wish you a successful meeting.

Thank you.

Mrs. Dr. Guusje ter Horst,
Minister of the Interior and Kingdom Relations,
The Netherlands

National Safety and Security: A Challenge to International Cooperation?

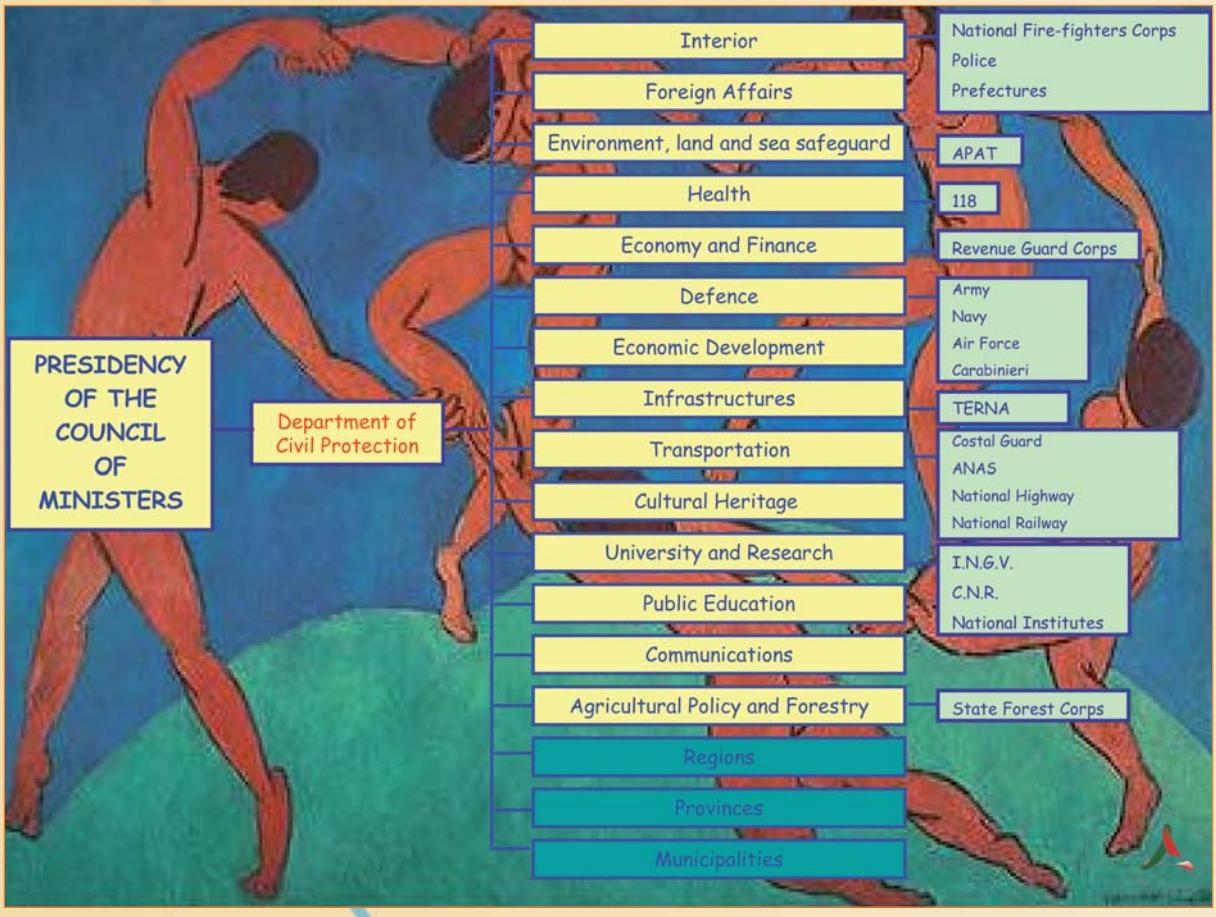
Guido Bertolaso, Head of the Italian Civil Protection, on current threats and the decision-making and operational structure in Italy

My intention in this report is to answer the question: do issues pertaining to safety and security in our Countries represent a challenge to International cooperation and collaboration between States?

The true question, in my opinion, apart from the opportunity of joining our efforts on an International level against phenomena such as pandemics of unknown pathogenic origin, terrorism, hardly controllable flooding of significant entity also in order to be able to face those so called "traditional" risks with greater efficiency and improved results, is "how" to join our forces in order to provide adequate responses to the increasing demands.

For this reason, I would like to shift the discussion on the ways to cooperate, since by looking at recent history we can already feel confident in a positive answer: if we consider what happened after the second world war, we can see that history has marked an ever increasing collaboration in a variety of sectors and occasions, taking the shape and name of the European Union, in our continent's case, or Nato in the military field and even the United nations if we wish to include the West and then the entire world.

Moreover, It is my main concern here to stress the fact that in our Countries, one of the most wide spread criticisms toward International cooperation bodies has to do with tiring, emphasizing the slowness of decision making processes, and the disproportion between the time imposed by different emergency scenarios, the time allotted and the time needed to collect the resources and the will power to intervene.



I believe that this kind of criticism is based on reality. My experience as Head of the Department of Civil Protection of Italy, makes me aware that the "time" variable represents the central focus of the new model of cooperation which we need to face the new emerging risks. Time represents the primary scarce resource in case of emergency. For this reason, we should learn to manage the new risks free from the binds of organizational schemes which we have resorted to in the past.

The second element which I would like to introduce along with the issue of time as a central element of our discussion on security, relates to the need to overcome the present State and International organizations model, that has existed for centuries .

First I'd like to consider this problem of organization. I have stated initially that the modern national State was born with the promise of being the best organizational model for a society to provide protection against the threats to people's lives and to the quality of their life.

By making a list of the traditional threats, in response to natural risks, every country disposes of an organization prepared to face the risk caused by fires – Vigili del Fuoco, Fire Brigade, Sapeur Pompier, Bomberos, etc. – and various public structures in charge of supervising the territory and its risks – from the Authorities regulating hydro geological matters, present in every Country, to the Vesuvian Observatory, the most ancient European institution involved in the monitoring of volcanic activity.

Today we wonder about the ability of institutions (such as for example at the UN level FAO, UNHCR, WHO, UNICEF) to face the new risks, because we are looking at a different scenario from the ones we were used to just a few years ago. I believe we should consider three factors in particular: the ever increasing distance between society and specialized bodies/institutions conceived to face emergencies and threats; the fact that we have become more vulnerable to the risks emphasized by the public opinion; the "massive" dimension of many catastrophes derived by the new risks and the complexity of the management of these emergencies, both in terms of damage, casualties/deaths and in terms of the impact on the public opinion.

Experts and researchers attribute this increased reaction to security threats as a consequence of various different causes. I would like to mention only a few:

- the gradual reduction of the extension of social protection networks and the widespread sense of threat created by this reduction, owing to budget reasons;
- the growing uncertainty regarding work and organization of the various phases of life;
- the emphasis that the media places on news regarding security, because of the enormous audience's response they have;
- lastly, the acceleration of economic and social changes caused by globalization, often experienced through the intensity of immigration flows and the return of "the foreigner" perceived as posing a threat.

It has recently become evident that the real, or media, consequences of the effects of certain catastrophes, associated with "new risks", lead us to doubt the adequacy of our means of traditional response. No country has a structure "organized by competence" with so large resources to be capable of facing alone Hurricane Katrina in all its effects, or the tsunami that in 2004 destroyed the coastal towns in so many Countries of the Indian Ocean. It also appears clear that no country can rely on a special dedicated structure capable of protecting the citizens from terroristic acts. These types of catastrophes, often predictable, often sudden, can be met with effective responses provided the model based "on competences" has to be set aside.

The "new risks", in fact, constitute a "new threat" perceived as being much more dangerous than others:

- if the predictability of catastrophes that are created is minor, since a risk is not known owing to its nature or unpredictability;
- if disasters have "disproportionate" effects compared to the levels that we are accustomed to managing and accepting, based on our appropriate level of preparation;
- if they generate media hurricanes causing uncontrollable emotional reactions that spark strong social

>>>

reactions;
- if the response to the threat involves costs that are judged as being unsustainable, or requires certain types of behaviour that the citizens refuse to carry out or judge as being unacceptable, since it implies giving up other rights that have been acquired.

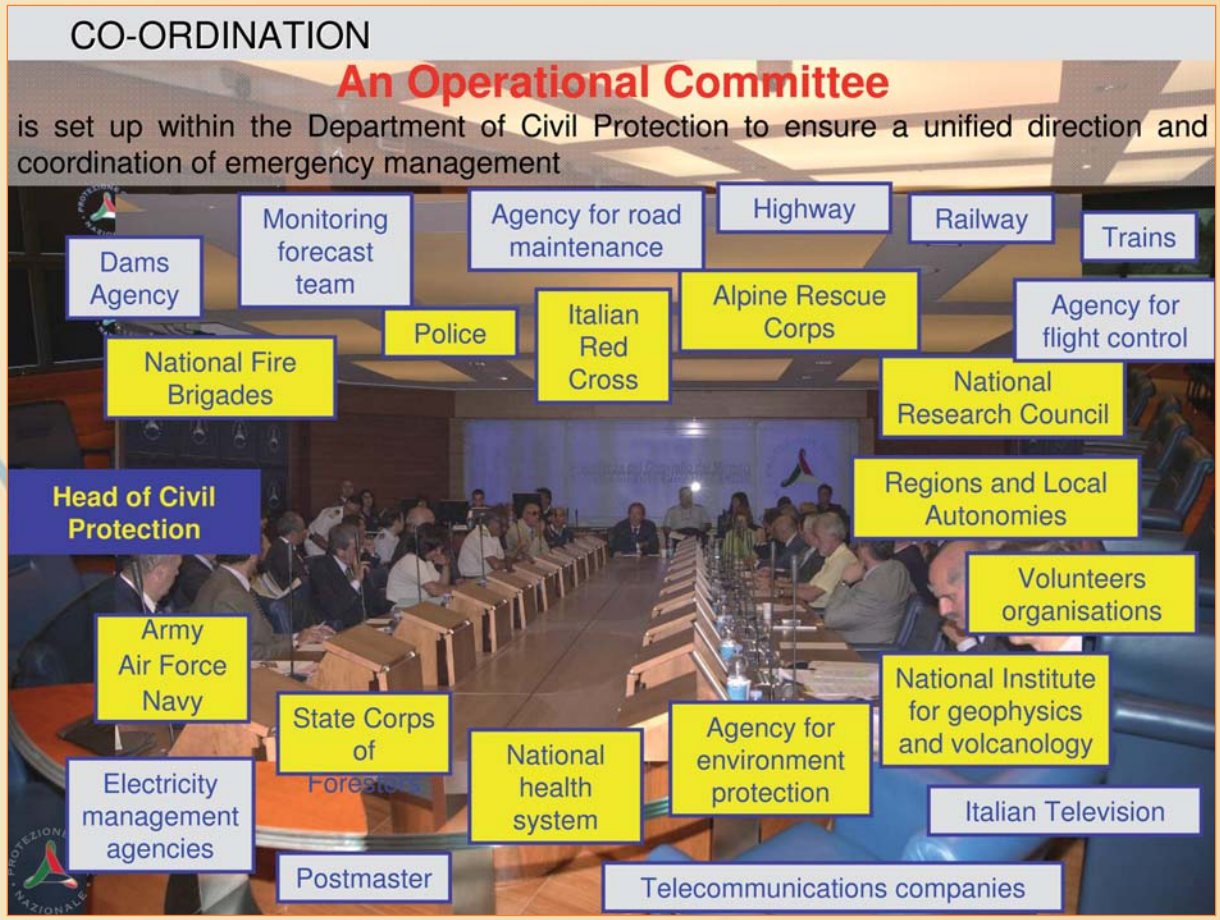
Reasoning on the characteristics belonging to these "new risks", we go back to the "time" variable I spoke of earlier, in the meaning of "real time", of the emergency's specific time. The "time" that seems to be lacking is actually "real time", with which in Italy we have begun to deal with, obtaining some significant results in improving our capability to face complex situations, even if they should occur immediately or without any notice. The capability to manage this "real time", specific to every emergency, was made possible by the fact we left the model of organization according to "competence" and we tried a type of public organization based on "functions".

In Italy, the civil protection's history represents an interesting case since our country has built a system that deals exclusively with the time of the emergency, of its dangers, effects of the catastrophe and the risks.

The civil protection system is assigned to permanently and continuously observe the risks that in real time could represent a danger for the population, the forecasting activities and their immediate prevention, in cases where such activity is possible and useful, to organize and direct relief and help, to manage emergency measures. These activities are carried out by a small staff of officials, directly responding to the Prime Minister. The same organizational structure applies to both regional and local levels.

The Civil Protection Department is a General Staff that has integrated within its structure a technical and scientific cognitive function, in order to obtain at all times information necessary for making decisions, but the department does not contain its own army. It does however have the powers necessary to mobilize the forces that are needed to face an emergency and is in the capacity of assembling specific task forces, case by case, recruiting all the elements that seem to be more appropriate to face a specific crisis, according to the "functions" necessary for taking action.
The head of this "emergency Government" can convene all the administrations that are "functionally" involved to participate in a decision-making process whose sole objective is the emergency at hand and the need to act immediately. From there, orders are imparted to the divisions, bodies and structures part of any of the government's ordinary administration, including the Armed Forces and the Police Force. The volunteer groups and health department units can also be mobilized, and specialized companies and experts in any type of risk can be called upon. This mobilization capacity is coded and regulated by shared procedures known to all: from the time of the possible occurrence of an event, or the sudden onset of the emergency and the action to be taken, no time is wasted for negotiations, clarifications and defining limits. Everyone, responsible for making decisions and participating in the decision-making process, knows what they have to do and how they have to act if mobilized in a civil protection emergency.

The existence and the real functioning of a "Government of the emergency time", while creating considerable difficulties, nonetheless has placed us in the condition of:
- reducing to the minimum the amount of time required for different types of action in relief of the population;
- reducing the time of intervention;
- building a system that permanently uses very few human and economic resources compared to those that it is actually capable of mobilizing;
- applying territorially the same model based on "mobilization according to function" of resources devoted normally to other tasks;
- obtaining in this way the highest degree of resilience;
- guaranteeing decision-making speed without excluding territorial Administrations from the decision and operational processes inherent to an emergency;
- not being obligated to create a hierarchy of risks on the



bases of their presumed seriousness, nor on priorities of intervention: the Civil Protection system considers all emergency situations, provoked by any cause, as being all equal;

- resolving the "competence" conflict between Administrations in the case of serious and complex situations, where a series of different competences comes into play at the same time; the possibility of treating them as "functions" that are necessary for solving the problem eliminates any possible uncertainty.

The Civil Protection's decision-making and operational structure has allowed Italy to give citizens the firm perception of a commitment based on visible, real and reassuring protection owing to its very existence and to the results achieved.

The way from an organization based on competence to one based on functions lies on a process, in which a horizontal coordination is tempted (such as the UN cluster strategy or the MIC procedures at European level). However, these attempts cannot be successful because they do not solve the problems bound to "governance". At the European and international levels, I am convinced that experimenting a system of "governance" according to functions could allow to reach quickly a better level of efficiency and effectiveness in protecting our citizens from the effects of "new risks" and in obtaining improved intervention methods on an international scale, when the consequences of a disaster exceed the management capabilities of the particular country experiencing the catastrophe. Organizing an international system based on functions is not a costly operation, since a fast coordinated level of command and quick decision-making lines are built based on procedures to be discussed prior to the occurrence of any calamity.
The prospect I have just explained does have a cost, and it's a cultural cost.

Italy has made the choices I have quickly explained after having faced countless tragedies of different nature and origin, experiencing dramatic moments that nature itself has spared other countries, where certain risks are completely unknown. I am thinking for example of seismic risks, or volcanic risks. The "new risks", unlike the traditional ones, now expose all of our countries to dangers and probability of catastrophic events much greater than those of the past. I hope that the experience of a country like mine, that has had to seriously examine the problems of emergencies originating from various sources before others, can be of help in identifying national solutions and forms of international collaboration, suitable for meeting the security and protection demand that our fellow citizens consider to be their acquired right.

Guido Bertolaso,
Head of the Italian Civil Protection

Security: The Role of Proportionality and Cooperation

Peter de Wit, President of Shell Nederland B.V.

Before looking at Shell's vision of safety and security in greater detail, I'd like to dwell for a moment on how ideal the location for today's conference actually is.Indeed, the local transport system was operating well enabling you to arrive on time. Traffic might have been a little heavy, and if it did come to a standstill, this would not have been due to a lack of fuel.Here the lights are on, the heating works, computers and BlackBerrys display various pieces of data and nobody is asking themselves whether food and drink will be available at lunchtime.The sea is pounding outside, but millions of people are safe, several metres below sea level, behind a narrow row of dunes, and are going about their daily routines.

Nobody generally dwells on this for even a second. It's as though everything takes place automatically. But that is not the case. It is like the movement of a clock that has been put together with the greatest precision – and which tells the time surprisingly accurately. But on no account may a grain of sand ever be allowed to find its way into the clock's movement. We find these proverbial grains of sand everywhere, sometimes occurring naturally, and sometimes strewn around deliberately by certain individuals. At the same time, ever more safety and security professionals are deployed to keep these grains of sand out of the clock's movement. They are more successful at this than many think – after all, something you fail to see might appear not to exist, or appear to take place automatically. Such as food on the table, electricity from a socket and fuel from a filling station.

However, in our highly specialised world, the semblance of something taking place automatically has little to do with simplicity but actually with the highest level of professionalism. I have already mentioned security in this connection, and would like to expand on several aspects of this here. I will touch on:

- vital infrastructure and the protection thereof;
- the security of supplying oil and gas to Europe;
- how Shell organises its security policy;
- and finally I will address the issue of;
- how governments and trade and industry can

optimise their security infrastructure through improved collaboration.

Critical Infrastructure and Protection therof

Things almost always proceed without a hitch, but then something goes wrong unexpectedly. A malfunction occurs in what proves to be vital infrastructure. As was the case here in the Netherlands recently, when a helicopter damaged three power lines while flying over a river. A hundred thousand people were without electricity for 48 hours. While this was not a full-blown disaster, it was certainly very problematic and expensive. It emerged that the electricity supply of the affected area depended entirely upon those three lines suspended high above a river which naturally widens during winter. The lesson learned here, again, is that every piece of vital infrastructure must always be installed in a loop. If it is impossible to open the front door, it must be possible for supplies to enter unimpeded via the back door, or through an upstairs

window if necessary. In the first place this increases security of delivery. It also makes management systems more reliable and increases the capacity and efficiency of the infrastructure.

If potential terrorists know that vital infrastructure is always present in duplicate or even triplicate, this will shift at least some of the focus from such targets. After all, terrorism's goal is to disrupt society and hence influence political decision-making.

In the Netherlands Gas producer NAM, which is managed by Shell, has been designated as a 'vital enterprise'. Hundreds of NAM work locations have been placed into one of four categories, each representing different levels of disruption to society if objects at the location in question were eliminated.

NCTb has since become the process owner of all these systems and operates the pilot National Advice Centre for Vital Infrastructure (*Nationaal Adviescentrum Vitale Infrastructuur*, NAVI) across the country. This centre contributes advice, expertise and best practices from government bodies and other relevant fields. As the owner and manager of significant vital infrastructure, Shell now maintains intensive contacts with this Advice Centre. It is a second direct line between Shell and the government bodies responsible for security; the other is the inclusion of Shell's refining and chemical activities in the National Alert System. This body is responsible for setting the levels of alert to which related companies can react with internal security efforts. This concludes my comments on how the protection of vital infrastructure is organised in the Netherlands and Shell's position within that organisation.

Security of Supplying Oil and Gas to Europe

The world's largest energy resource in terms of volume is oil, which incidentally also significantly influences the price of gas. Oil is an exception to the ubiquitous 'stockless just-in-time logistics' seen so widely in today's economy. Several OECD countries set up the IEA (International Energy Agency) after the 1973 oil crisis. The main task of this Paris-based coordinating body is to secure and allocate oil supplies in times of crisis. The participating countries (26 in all) have reached the following agreements:

- countries maintain stocks of at least 90 days net oil imports. These stocks need not necessarily be held in the countries themselves. Much Western European oil, for example, is held in the ARA region (Amsterdam, Rotterdam, Antwerp);
- in the case of problems, countries will take appropriate measures, such as a reduction in consumption, a switch from oil to other fuels and – if possible – a boost in domestic energy production;
- if supplies are seriously disrupted – and according to the norm this is a reduction of at least 7 per cent – an IEA-controlled oil-allocation schedule enters into effect.

In that case, oil from the strategic reserves and from current supplies is allocated and distributed over the member states.

The allocation schedule was activated in 1990-91, for example, after Iraq's invasion of Kuwait. This, and the ensuing American actions meant that 4.3 million barrels of oil production were lost on a daily basis, from a total global figure at that time of 65 million barrels of oil per day. Putting things into perspective: current global consumption amounts to 87 million barrels per day, and may rise to between 102 and 116 million barrels in 2030, the IEA claims. On a smaller scale, the schedule was activated two years ago to mitigate the effects of Hurricane Katrina in the Gulf of Mexico. At the time, a considerable volume of Dutch and British petrol reserves were transferred to the United States, where numerous production platforms and refineries were out of operation.

Strategic oil reserves are only deployed to supplement imminent shortfalls, not to intervene in the marketplace in the case of price rises. The world's largest strategic oil reserve is that of the United States, currently 700 million barrels of crude oil – roughly equivalent to 55 days of imported oil.
Late last year, President Bush signed into law an act by which the Strategic Oil Reserve will increase to 1.5 billion barrels as of 2027. China has also started to build up its own 'safety buffer'. The strategic oil reserves have >>>

operated well to date, and while they have only been used very occasionally, they discourage countries to use oil as a political lever.

In theory, oil-exporting countries, collectively or otherwise, do have the opportunity to use oil as a means of coercion and indeed have done so in the past. After all, global production capacity is currently only slightly higher than global consumption. If one of the larger exporting countries decided to halt supplies for whatever reason, there is limited free production capacity elsewhere to counterbalance this. This risk should not be exaggerated, however. Oil-exporting countries cannot maintain their economies without oil revenues; they would very soon face domestic social unrest.

The low level of excess oil production capacity makes it clear that terrorist attacks on large oil production centres – or port facilities and shipping routes – may form a serious threat. As a graphic example I would like to mention the excistence of physical bottlenecks. Every day, 13.4 million barrels of crude oil are transported through the Strait of Hormuz, while 12 million barrels are transported through the Strait of Malacca. The IEA anticipates that by 2030, 30 per cent of the total global oil consumption will be transported via the Strait of Hormuz, almost twice today's percentage.

The 1984-1987 tanker war in the Gulf saw a 25 per cent decrease in oil transport – but the world still had ample excess production capacity elsewhere at that time. Today, however, almost the entire excess production capacity of oil is concentrated beyond the Strait of Hormuz.

Turning to Natural gas, this is largely transported by pipeline. This is a safe but much less flexible means of transport, and as we have seen, is almost impossible to fully physically protect in many places. Pipelines form a direct link between supplier and customer. LNG (liquefied natural gas) is an interesting diversification, as it offers the flexibility of using ships which while vulnerable, offer more potential focus on safey. Although the number of suppliers is limited at present, this business is growing rapidly. European imports of natural gas in particular will continue to grow substantially: according to the IEA, annual imports will rise from 235 billion m^3 today to 520 billion m^3 in 2030.
Ultimately, greatest supply security for gas will come from an increased supply portfolio. Pipelines, such as the Nordstream pipeline, soon to be constructed from Russia across the Baltic Sea and many LNG import terminals across Europe will facilitate this. It is clear that all this vital energy infrastructure must be protected.

Which is why I am now turning my attention to another dimension of security: the protection of the facilities themselves.
Because Shell operates across the globe, we have first-hand knowledge of the difference in approach to this by numerous official bodies. We actually observe two different approaches to security in respect of physical installations:

- threat-driven;
- consequence-driven.

The European approach takes potential threats into consideration and is therefore threat-driven. It is a system that provides adequate answers to an analysis of the threats. Threat levels are subdivided into phases and the owners of vital infrastructure tune their security systems and measures to take account of this.
The European model offers the best likelihood of proportionality in response. In the United States the tendency is to analyse the maximum effects that might take place, for example in the case of a large-scale attack on installations. On the basis of this 'consequence-driven' approach, installations, buildings and systems receive added protection. In practice this means large sums of money are invested in fortifying complexes to withstand any eventuality. A high level of security is maintained there continuously, even when the level of threat is low.
Putting it in somewhat black and white terms, this is indicative of the difference in mentality and world view. Europeans are quick to conclude that American security measures are 'over the top'; Americans think that Europeans are naive and fail to take things very seriously. Strangely enough, the opposite tends to be the case when it comes to coastal protection. Proportionality is key here. The effects of security on society must not be as far reaching as those of the evils against which it is designed to protect.

How Does Shell Organise its Security Activities?

We employ an 'All Hazards Approach', which means we are prepared for any conceivable incident, irrespective of its nature or origin. This includes both safety (HSE) as well as security, thus including 'acts of God', i.e. extreme weather conditions, earthquakes and flooding.

In response to the events of 9/11 and its aftermath, Shell configured, expanded and professionalised its Security organisation at Group Level, responsible for security of physical assets and people. The Corporate Affairs Security (CAS) department is responsible for this at Group level. CAS is a global network of security professionals embedded in the individual businesses and led by a core group of specialists at Shell's Headquarters in The Hague. Concurrently but separately, we have a Business Integrity department within the Finance Function.
This department is responsible for conducting internal financial forensic analysis. Again separately, Shell also has its own IT Security department, the goal of which is to prevent the threat of and raise awareness about cybercrime. CAS thus bears primary responsibility for identifying threats to personnel and installations. CAS's operating procedures are set out in manuals that reflect the content of the Group Security Standards and describe the five levels of threat that we use within the company, ranging from 'Occasional/Unlikely' to 'Extreme'.
Our Group Security Standards dictate that security risks must be identified and assessed at regular intervals. This also applies for the measures designed to manage these risks and minimise the consequences.

The Security processes and procedures so developed proved their worth just before Christmas 2006. Following several kidnaps and bomb attacks, it was decided to repatriate employees' family members from Nigeria. Three days' later, three airplanes carrying these family members landed in Amsterdam and London – a perfectly executed emergency operation.

Sometimes the security problems are huge in size and complexity. Take for instance Shell's Pearl project in Qatar where natural gas will be converted into high quality middle distillates. During our peak construction period some 40,000 workers production workers will be at the site.

Including other gas projects, in mid 2008 some 120,000 construction workers can be counted in and around Ras Laffan Industrial City – in a country with only some 900,000 inhabitants. This puts a stress on the national security forces of Qatar and a responsibility on all the companies to police the camps humanely, with all due sensitivities for human rights and political rivalries.

Collaboration Between Government, Trade and Industry

The national Security Manager of Shell Nederland is the direct point of contact for government organisations such as AIVD, NAVI, government departments, and NCTb.

In April 2005, the Oil and Chemical sector joined the national alarm (*alertings*) system, which is managed and controlled by NCTb. If NCTb decides to raise the level of alarm for this sector, Shell's Security Manager will be notified of this, upon which he will activate a series of measures. The formation of NCTb in the Netherlands has proved a significant step forward. This body is our direct point of contact in the case of threat and hence also for upgrading the protection of our vital infrastructure in the Netherlands. NAVI will hopefully also develop in a similar vein.

As a commercial enterprise, there are three things we hope the authorities will be able to maintain:

- high-quality threat analysis (intelligence);
- open and rapid communication, and;
- a rapid and clear response to any incident.

We all know that we will always be vulnerable as a result of the openness that is an undeniable characteristic of a democratic society. 'Democracy is not for the faint-hearted', as we say. Notwithstanding this vulnerability, however, we must have the wherewithal to resist those who are a threat to our values and together we can achieve a great deal to minimise the risk by further professionalizing our collective security efforts. We in Shell acknowledge our responsibilities and will act accordingly.

Peter de Wit,
President of Shell Netherlands B.V.

Workshop: How Could We Assess These Threats?

One of the four workshops organized at the National Safety and Security Conference in The Hague (29/01/2008) focused on methodologies to assess threats. The main goal of this semi-interactive workshop was to present, discuss, exchange and compare (innovative) threat assessment methodologies and to initiate international co-operation/collaboration on methodological issues related to the assessment of threats.

First, two risk assessment methodologies were presented: the Dutch *National Risk Assessment* (NRA), and the European Commission's *European Programme for Critical Infrastructure Protection* (EPCIP). Here, both articles are introduced by discussing reasons for their presentation in the same workshop as well as interesting points of similarity and difference between them.

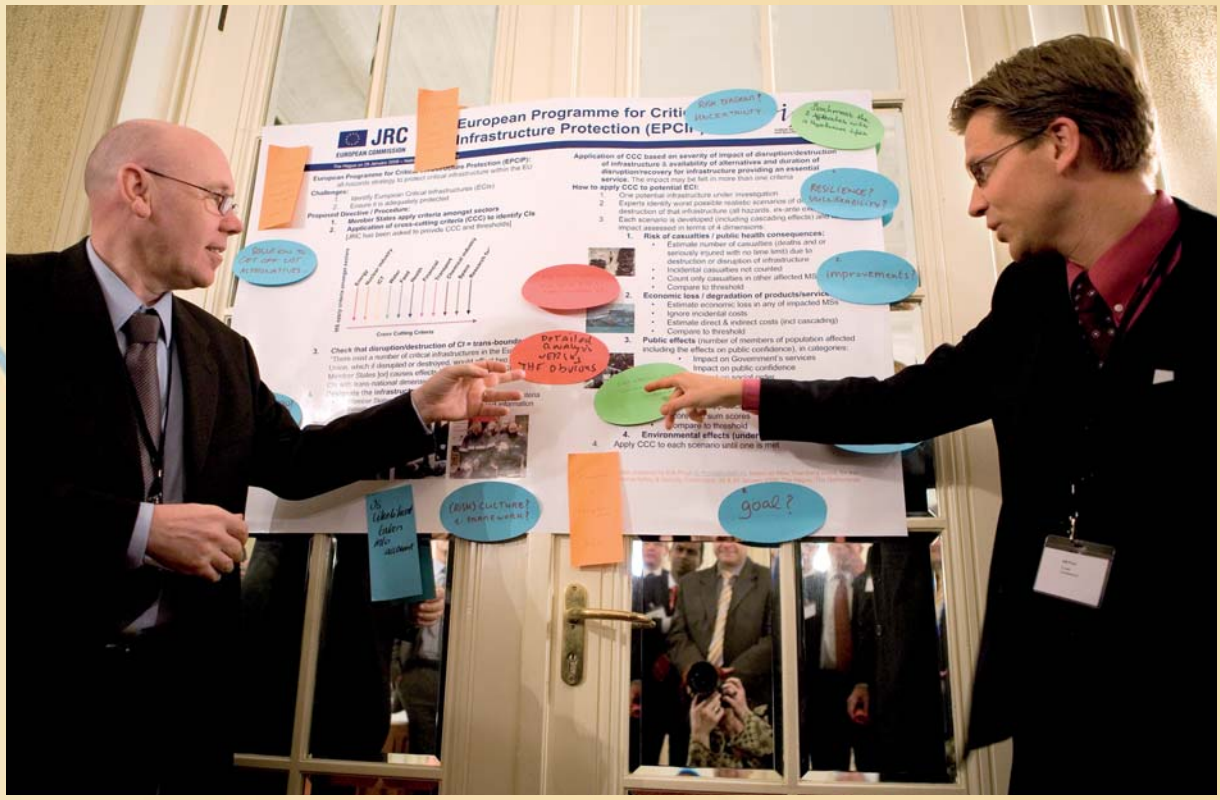
Important reasons for the presentation of these methods are that:

- Both approaches are in their final stages of development and could still learn from other approaches and timely criticisms and remarks.
- Both approaches will soon be used in practice. The EPCIP will soon be a directive and hence affect (at least) all EU Member States. The Dutch NRA will soon be used to inform the cabinet about potential risks and capabilities that need to be improved.
- The development of risk assessment approaches requires a serious amount of time and effort. Both approaches may therefore inspire friendly nations and organizations currently starting to develop similar approaches. The Dutch and UK experience might for example help other countries develop their own approaches at a much higher speed and avoid many of the hurdles, pitfalls and difficulties.
- Both approaches contain some innovative, interesting features.
- Comparing different approaches by analyzing points of similarity and difference actually leads to a better understanding of the approaches and of the purpose, circumstances and culture they need to serve.

The first similarity between the EPCIP and Dutch NRA approaches is that they are "all hazard" approaches for dealing with malicious threats *and* non-malicious hazards. Another similarity is that they both use multiple criteria to assess the impact of incident scenarios on many different (qualitative and quantitative) aspects and dimensions. Although Multi-Criteria Analysis (MCA) approaches have been developed for over 50 years, their application to (National) Safety and Security issues might still be seen as innovative. Both approaches require many high-quality scenarios. The scenario generation processes are therefore important for both approaches.

But the EPCIP and Dutch NRA approaches also differ considerably. The differences in level (the EU level versus the *national* level) and scope (only *EU trans-boundary* versus mostly *national*) are obvious. The differences in motives and foci of analysis are probably less obvious. The motive for the EPCIP is the protection of European Critical Intrastructures, and the focus of the analysis is therefore the identification of these European Critical Infrastructures. Motives for the Dutch NRA are the improvement of the capabilities to deal with, and the preparedness to face, potential risks, as well as the improvement of the co-operation between ministerial departments. The focus of the analysis is therefore the joint identification and robust classification of the widest set of potentially devastating risk scenarios – as well generating insights related to the underlying reasons for the impacts and classification – and the identification of the capabilities that could be improved to deal with them.

The MCA methods and techniques used consequently differ to a large extent. The EPCIP is on the one hand a minimum threshold approach that does not aggregate multi-dimensional effects, which means that degrees of magnitude between alternatives are not taken into account and that there is no compensation between effects on different criteria. An infrastructure might therefore not be classified as "European critical" if all impacts fall slightly short of all thresholds. The Dutch approach on the other hand, takes the degrees of magnitude of the impacts on the multiple criteria into account and partially aggregates these multi-dimensional effects, which means that there are compensatory effects between the criteria, which are conscientiously analyzed.
The impact criteria also differ: the EPCIP criteria are



defined specifically to assess *EU* trans-boundary effects, whereas the Dutch criteria are specifically designed to assess instrumental and intrinsic national effects important for the Dutch.
The EPCIP scenarios need to be very specific and contain cascading effects, whereas the Dutch scenarios need to be as generalized as possible in order to represent similar scenarios and still sufficiently specific to score direct effects within ordered classes. Extensive sensitivity analyses (uncertain scores, uncertain weights) and robustness analyses (different methods) are – given the generalized character of the scenarios and the specific MCA methods used – therefore very important in the Dutch approach.
Both approaches actually reflect the culture and process in which they were developed. The EPCIP approach could be seen as a compromise approach, whereas the Dutch NRA is a consensual approach. Consensus is typical for Dutch decision-making culture: the Dutch approach was developed jointly by representatives from several ministerial departments, knowledge institutions (planning bureaus, universities, think tanks) and the business community.

After the presentation of the two approaches, an interactive post-it activity and a discussion of the posted comments followed. Discussions during this interactive part of the workshop centered on questions such as:

- Should these approaches deal with *safety* and/or *security*?
- Are these approaches fundamentally *consequence-based* and/or *threat-based*? What could be learned from different approaches?
- Does the detailed analysis add any value?
- How could fundamentally surprising risks be dealt with?
- Could – and how could – fruitful collaboration between and within the regional, national, and local levels be established?
- Could information about methodologies be shared?
- Could information about events/scenarios be shared?
- Could the approaches developed in one context be used (almost directly) in another context?

Finally, some ideas to improve international collaboration on threat assessment were proposed and discussed. Among else, it was suggested to establish networks – e.g. networks of excellence – and organise follow-up conferences/workshops focussed on risk assessment methodologies, to extend the collaboration to other organisations and levels, and to rethink current incentives for international collaboration.
This conference and workshop might in that respect be considered to be the start of a fruitful collaboration related to threat assessment and threat assessment methodologies.

Erik Pruyt,
Delft University of Technology

National Risk Assessment: the Dutch Approach

This paper gives a summery of the presentation of Marc van Nuland, director of Aon Risk Management the Netherlands, during the workshop 'How could we assess these threats?'. The paper reflects the development of a National Risk Assessment Methodology for the Netherlands by an expert group during the year 2007. The so-called National Risk Assessment Methodology provides the Dutch government with high-level and comprehensive guidance on the prioritisation of potential malicious and non-malicious events and a consistent basis to develop a strategic planning process for tasks and capabilities related to the identified potential (national) catastrophic events.
The methodology has been successfully applied on a limited number of catastrophic events (malicious and non-malicious). In 2008, the methodology will be refined and from then on, it will be the basis for the annual National Risk Assessment.

Introduction

The Dutch government has decided to develop a National Safety and Security Strategy in order to protect the following five national interests against potential catastrophic events:

- territorial safety;
- physical (human) safety;
- economic safety;
- ecological safety;
- social and political stability.

The main goal of the National Risk Assessment (NRA) – which is part of the National Safety and Security Strategy – is to provide the Dutch government with a prioritisation of potential catastrophic events in terms of their likelihood and impact on the five national interests.
The following pre-conditions have been set for the NRA method:

- it should be suitable for an all hazards approach (malicious and non-malicious events);
- and generate risk prioritisation based on integrated weighting of multiple impacts.

Risk assessment is a process of understanding the significance of potential events on the basis of their likelihood and their impact. In general, risk assessment methods are well described in the literature and have been developed for a range of working areas: industrial safety, enterprise risk management, decision analysis, et cetera. Nevertheless the development of the NRA method has been a great challenge because of:

- the need for integration of very different criteria (loss of territory versus deaths);
- likelihood assessments for new risks (malicious threats), extreme hazards (no statistical data), or time developing events (climate change);
- the complexity of prioritising risks.

The characteristics of the developed NRA method are shown on the poster. The following paragraphs will discuss the major steps of the NRA methodology.

Impact Assessment

The first step of the NRA process is the identification and selection of the potential catastrophic events. For example a pandemic flu, flooding, terrorist attack or energy supply disruption. For any of these individual events, incident scenario's are constructed by a group of domain experts. They are supposed to give a comprehensive description of the event including sufficient information to evaluate their impact and likelihood. The impact assessment covers the five national interests; each national interest has been translated into one or more criteria. In total, ten criteria have been defined. Together these criteria are considered representative for the impact on the five national interests. The vital interest *physical (human) safety* is for example covered by the criteria *number of fatalities* (1), *number of casualties* (2) and *physical suffering* (3). Each criterion has been defined such that it could be assessed/scored rather easily. The criterion *fatalities* is for example defined as the

number of people killed by an event, immediately or within one year. The evaluation on each criterion is translated into 5 classes A (minimum) – E (maximum). For example *fatalities*: class A represents 10 fatalities or less, class E represents 10.000 fatalities or more. If a specific event does not relate at all to a specific criterion, it scores a '0'. A *pandemic flu* does for example not affect the ecological safety. The criterion *long term ecological disruption* is therefore irrelevant and scores a 0. These 0-scores are not varied during sensitivity analyses.

Multi-Criteria Analysis

The Dutch NRA uses several Multi Criteria Analysis (MCA) methods to aggregate the scores on the different criteria into an overall impact score.
In order to avoid methodological choices that might greatly influence the final results, it has been decided to use:

- three different MCA methods:
  - the weighted sum method – a purely quantitative utility function approach
  - the medal method – a purely qualitative approach
  - the Evamix method – a mixed qualitative/quantitative approach.
- five different preference profiles. In the basic analysis, the five national interests are considered equally important. In addition, calculations are made based on four social/cultural preference profiles, each characterised by different weights sets.
- different bases to rescore the A-E scores, ranging from linear to exponential.

To have a better understanding of the uncertainty and the robustness of the results (i.e. ranking of the impact scores for the different incident scenario's) calculations have been performed, using different MCA methods, preference profiles, bases, uncertainty intervals for scores and weights, et cetera. The results for the 2007 incident scenario's show a very reasonable robustness. The ranking of the different scenarios only changes slightly when the methods, preference profiles, bases, weights and scores are varied.

Likelihood Assessment

All analysed incident scenarios are characterised as 'uncertain' and the risk can for this reason also be characterised by the likelihood of each scenario. In order to assess the relative priority of the selected scenarios (risks) the likelihood of each scenario can then be set out against the impact score. Likelihoods are assessed for a period of five years, and are also presented on a 5 point scale: A-B-C-D-E. Class A stands for 'most unlikely to happen' and class E stands for 'most likely to happen'. Because of the fact that most incident scenarios will be unlikely to happen, the character of the chosen scales is exponential. It prevents that almost all scenarios are rated in the same scale (A). The exponential character of the scales (quantitative scale: multiplier 10) makes it more robust, and gives some compensation for the most important problem for assessing the likelihood, namely the lack of knowledge and statistical data. The consequence is that expert opinions become very important, and the process of elicitation should be done very carefully. >>>

Different scales have been defined for the malicious risks and non-malicious risks.
Likelihood assessment for the non-malicious risks are directly scored and can be rated quantitatively or qualitatively, which depends on the availability of historical data, statistics, and so on. Statistics and historical data are not meaningful for the malicious risks. The likelihood (in terms of plausibility) is assessed on the basis of intelligence available and analysis of relevant trends.
The result of the threat analysis (plausibility score) can be influenced by the vulnerability for the identified risk.
The vulnerability is a measure for the expected success of an attack, and is related to the control measures. In case of low vulnerability the score is decreased by one class (C changes to B), in case of high vulnerability the score is increased by one class (C changes to D).

Risk Diagram

To provide an overall risk score for each incident scenario (risk) the impact score and likelihood score are plotted in a so-called risk diagram. When 'reading' such a risk diagram, it should be taken into account that:

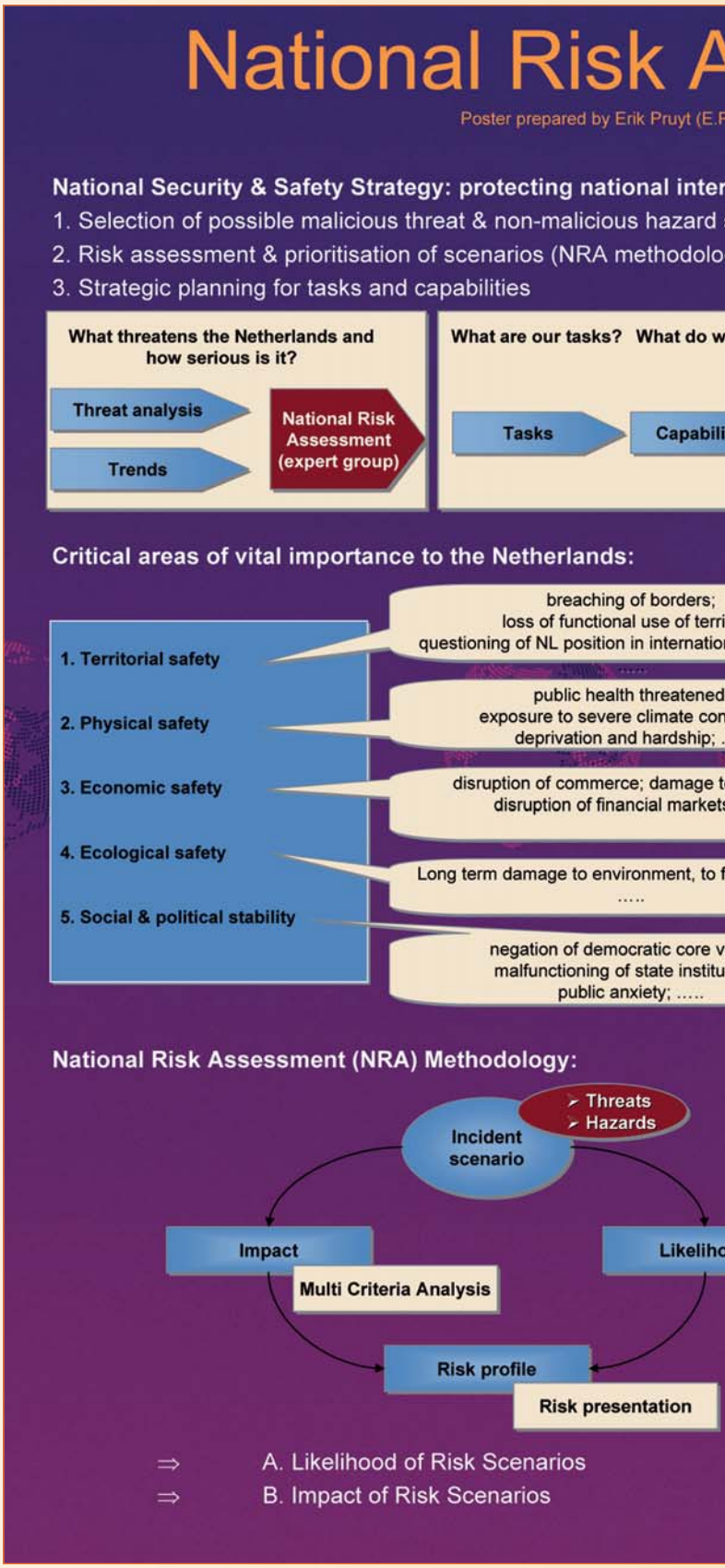
- Risk consists of Likelihood *and* Impact
- Extreme impact scores *cannot* be ignored, irrespective of the likelihood
- Maximising risk reduction (gap between 'before' and 'after' capabilities implementation) is what matters.

Following subjective considerations – related to political preference or societal concerns – might also play a role when decision makers read such diagrams:

- Political preference profile related to national interests and/or impact dimensions
- Time scale and available budget for implementation
- Dominant trends or events in society, etc.

Reading and interpreting such a risk diagram and prioritising risks given such a risk diagram is thus a rather difficult task. That is why the results are not only plotted, but policy recommendations are also formulated alongside.

Jasper van der Horst,
Aon Global Risk Consultants
Erik Pruyt,
Delft University of Technology



ssessment: the Dutch Approach

ruyt@tudelft.nl) for the National Safety & Security Conference, 28 & 29 January 2008, The Hague, The Netherlands

ests by means of:
scenarios
gy, see below)

e need?
ties
Implementation
tory;
nal community;
ditions;
....
o property;
; .....
lora and fauna;
alues;
tions;
od

A. Likelihood of Risk Scenarios

- Rating scores for hazard scenarios
- Rating scores for threat scenarios

Likelihood Score	(quantitative) (% / 5 years)	(qualitative)
A	< 0,05	Rare
	...	
E	... - 100	Highly probable

Rating score	Threat plausibility
A	No concrete indications and event is rare
...	...
E	Concrete indications that event will be effectuated

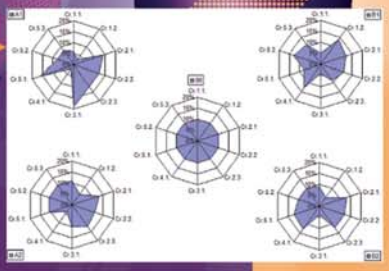
area → duration ↓	local (< 0.1 %)	regional (< 1 %)	provincial (< 10 %)	national (> 10 %)
Days	A	(X)	(X)	(X)
1-4 weeks	(X)	(X)	(X)	(X)
1-6 months	(X)	(X)	(X)	(X)
> 6 months	(X)	(X)	(X)	E

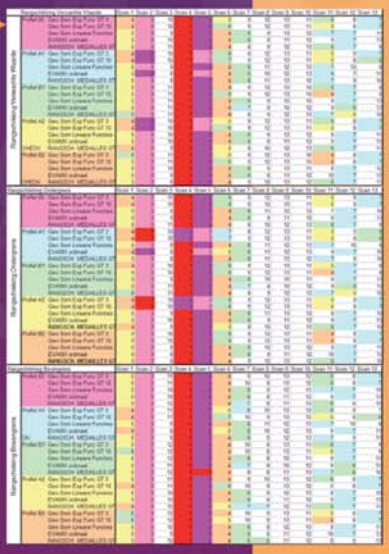
(X) ∈ {A, B, C, D, E}
large population density: +1; small population density: -1

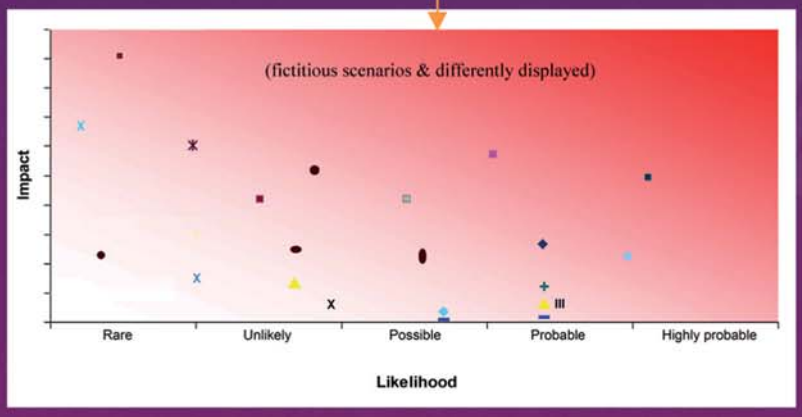
B. Impact of Risk Scenarios

1. Development of worst credible scenarios
2. Impact assessment on 10 impact criteria
   - Expected value (+ highest & lowest values)
   - Subcriteria & indices -> 10 criteria scores
   - Scores in outlined classes 0, A-E
3. Multi-Criteria aggregation (MCA) of the scores on the 10 criteria into 1 overall impact score
   - 5 preference profiles: 1 equal weight profile + 4 social/cultural preference profiles
   - 3 MCA methods:
     - a (well-known) purely quantitative MCA method,
     - a (new) purely qualitative MCA method,
     - a quantitative-qualitative MCA method.
   - linear and exponential bases (1, 3 & 10)
4. Uncertainty, sensitivity and robustness analysis of rankings:
   - Different scores, weights, methods, …
   - Small changes – Limits – Monte Carlo simulation
5. Understanding & insight + risk diagram

National interests	Impact dimensions		Rating score (0-A-B-C-D-E)	Scenario S01
Territorial safety	Territory	m², t		0
	International position	#		0
Human safety	Fatalities	#		D
	Casualties	#		C
	Suffering	#,t		A
Economic safety	Costs	€		E
Ecological safety	Long term disruption	m², t		0
Political & social stability	Disruption to daily life	#, t		A
	Integrity of democracy	#, t		A
	Outrage & anxiety	#, t		E







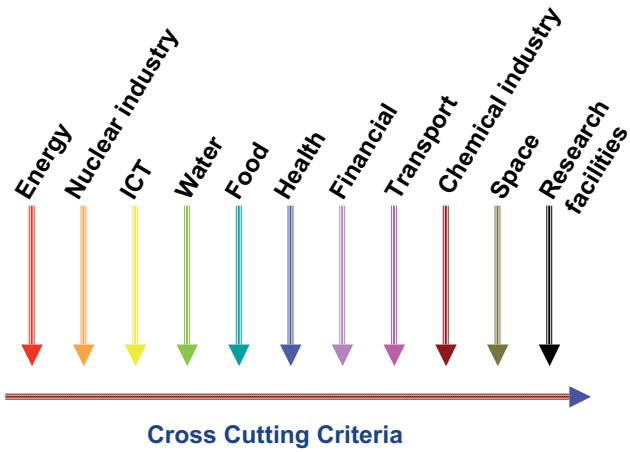
Protection of Critical Infrastructure: The European Approach

The atrocities of 11 September 2001 in New York and the Madrid train bombing in 2004 have indicated terrorists' willingness to target infrastructure as well as people. Following these events, the European Council asked the European Commission to prepare an overall strategy to protect critical infrastructure[1] within the European Union. As part of this strategy, the European Commission proposed a directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.[2] While recognising the threat from terrorism as a priority, see figure 1, we must also recognise that naturally occurring events or accidents can have the same effect, see figure 2; the disruption or destruction of infrastructure. Therefore the protection of critical infrastructure will be based on an all-hazards approach.

European Programme for Critical Infrastructure Protection (EPCIP)

Within the European Union there may exist infra-structures that, if disrupted or destroyed, would affect two or more Member States. It may also happen that failure of an infrastructure in one Member State causes an effect in another Member State. Such an infrastructure with a trans-national dimension and whose loss would cause a significant impact should be identified and designated as European Critical Infrastructures (ECI). Because of the trans-national dimension, when investigating the weaknesses and vulnerabilities and identifying gaps in protective measures, an integrated EU-wide approach would usefully complement and add value to the national programmes for critical infrastructure protection, already in place in the Member States.

The proposed Directive requires each Member State to apply criteria amongst sectors followed by the application of cross-cutting criteria, in order to identify those infra-structures which may be designated as European Critical. As the infrastructure is identified by assessments carried out by the individual Member States utilising sectorial criteria, this does not guarantee a coherent and uniform identification of ECI, either across sectors, or across Member States. To avoid inconsistent identification, Member States must subsequently apply a set of cross cutting criteria to the infrastructure previously identified. The role of the cross cutting criteria is therefore to provide harmonization.



The 11 sectors of European infrastructure and the horizontal placement of the cross-cutting criteria

[1] *Critical infrastructures can be broadly described as those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens.*

[2] *Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, COM (2006) 787 final, 12 Dec. 2006.*

Failed terrorist attack at Glasgow airport

Cross-cutting Criteria

The directive defines four categories of potential adverse effects to society. These can be used to define a minimum societal consequence that the failure of an infrastructure must have, before being classified as European Critical. The four categories of criteria identified by the directive are:

- Potential to cause casualties and public health consequences (an estimate of the number of deaths or seriously injured), due to the destruction or disruption of an infrastructure.
- Economic effects (significance of economic loss and/or degradation of products or services). In effect, an estimate the economic loss caused by destruction or disruption of infrastructure in any of the impacted Member States.
- Public effects (number of members of the population affected including the effects on public confidence)
- Environmental effects

The directive also adds explicitly that the cross-cutting criteria shall also take into account the availability of alternatives and the duration of disruption/time for recovery of service. Although estimates on the number of casualties or potential for economic loss can be made, no direct method of quantifying public effects is known. Therefore a qualitative approach has been taken, whereby five different categories of impact are considered:

- Impact on Government's services;
- Impact on public confidence;
- Impact on social order;
- Population impacted;
- Geopolitical impact.

Assessed, scored and compared to a preset threshold.

For potential infrastructure under investigation, Member State experts will identify the worst possible realistic scenarios of disruption or destruction of that infrastructure (all hazards, ex-ante exercise). Each scenario is developed, (including cascading effects where possible) and its impact assessed in terms of the 4 dimensions (risk of casualties, economic, public and environmental effects). These cross-cutting criteria are applied to each scenario until one is met. The thresholds for meeting the criteria will be set in such a manner that only infrastructures that would cause a major event upon failure would be considered as critical.

An Infrastructure that exceeds both the thresholds set for sectorial and cross-cutting criteria, which if disrupted or destroyed would cause a trans-national effect, shall be subsequently designated as European Critical Infrastructures (ECI).

Michael Thornton,
Researcher, Joint Research Centre of the European Commission, Ispra (Italy)

Emerging Security Challenges to the United Kingdom[1]

Over the last two decades, the global security landscape has changed dramatically, shaped by defining events such as the end of the Cold War and the attacks of 9/11. As a result of these developments, new issues, actors and challenges have emerged, with far-reaching implications for UK security policy.

Central to this new security environment is the reality that conventional notions of a single security front-line no longer apply: today we face multiple front-lines across a broad spectrum of issues. Indeed, the range and character of today's security challenges includes, but also goes well beyond traditional concerns for terrorism and the military defence of our home territory.

It is becoming abundantly clear that in order to deal effectively with the range of challenges facing the UK today, we must re-think our notions of what constitutes the front-line in the battle for security and re-formulate our responses to them accordingly.

In this article we present an account of the key drivers of the contemporary security landscape through a treatment of five key themes, which we believe when taken together provide a valuable framework for thinking about the new security environment as a whole. These are:

- Globalisation and Power Diffusion;
- Poverty and Failing States;
- Climate Change;
- The growth of Political Islam;
- Socio-Economic Vulnerability.

We also briefly discuss the implications of this changing security terrain for UK policy-making, advocating an approach which is both collaborative and holistic. Finally, we highlight a number of key questions that we feel ought to be addressed in the formation of a new national security strategy for the UK.

The Changed Strategic Landscape

Globalisation and Power Diffusion

A key feature of today's security landscape is an ongoing process of power diffusion. Occurring largely as a result of globalisation, this diffusion is taking place on a number of levels.

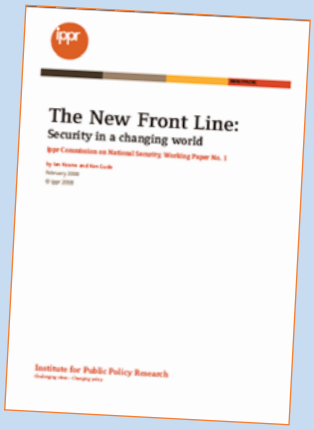
Firstly, we have seen a relative diffusion of power within and across the community of states. This is manifest through a redistribution of power from the Atlantic seaboard to Asia and the Pacific; signalled primarily by the rise of China and India. Such developments represent an important change in the geopolitical landscape and may point to a shift in great power rivalry, from the European stage in the last century, to the global stage in this. Other factors currently driving the diffusion of power across the community of states include the rise of a new group of potentially powerful energy states and regions, and the spread of nuclear weapons technology to new states, which may lead to the emergence of new regional power struggles.

Secondly, we have seen a diffusion of power from state to non-state actors, including terrorist groups, transnational organised crime networks and transnational political movements. Such groups present a long-term structural challenge to the UK since they are not only managing to acquire some of the power attributes of states, but are also altering the character of some states and even undermining the legitimacy of states in a way that calls into question traditional notions of power politics.

The third dimension of power diffusion relates to increased security interdependence between states, where the security of one state is more reliant than ever before on what happens in others. As a result of their own interface with the globalised economy, states are becoming increasingly vulnerable to changes happening beyond their borders. For the UK, a number of international

[1] *This article is based on a longer paper, The New Front Line: Security in a changing world by Ian Kearns and Ken Gude (ippr). This is the first working paper presented to ippr's Commission on National Security in the 21st Century. The full paper, and further details on the work of ippr's Commission on National Security is available at www.ippr.org/security*

Commission on National Security in the 21st Century



Over the last twenty years the national and international security environment has changed dramatically. The end of the Cold War and the horrific attacks of 9/11 are but two developments among many that have signalled the arrival of a new 21st century security landscape. New processes and drivers, from globalisation to climate change, and from the growth of political Islam to a more infrastructure reliant society have come to the fore and now challenge both old analytical frameworks and old policy prescriptions.

Policy-makers are working hard to adapt and to keep up with the pace of change but the challenges are profound and the progress uneven. As a result, while we both commend many of the efforts already underway and welcome the government's recent publication of a UK national security strategy, we also believe now, more than ever before, that the need for constructive external challenge is great.

As such, the Institute for Public Policy Research (ippr) is hosting an independent Commission on National Security in the 21st Century. The Commission was launched in May 2007 and will run until mid-2009. It is co-chaired by:

- **Lord George Robertson**, former Secretary of State for Defence and former Secretary General of NATO
- **Lord Paddy Ashdown**, former leader of the Liberal Democrat Party and former High Representative for Bosnia and Herzegovina.

The ippr Commission on National Security will:

- conduct a detailed assessment of the changing global security environment and the specific challenges and opportunities this poses for Britain
- identify the values and interests that should shape British security policy over the next decade and beyond
- make specific policy recommendations for how Britain can make a more effective contribution to the promotion of global security and enhance the security of its own citizens at home.

The Commission will address a range of domestic and international security challenges. Current research streams include:

- strengthening multilateralism
- defeating islamist terrorism
- conflict prevention and peacebuilding
- critical national infrastructure and resilience
- managing the vulnerabilities of interdependence

developments such as the increased movement of people and goods across borders and the proliferation of trans-national organised crime groups are resulting in increased insecurity within our own shores.

Poverty and Failing States

Our second driver of change is the so-called 'security-development nexus' – the point at which global poverty, inequality, violent conflict, failed states and international terrorism interact, with potentially devastating results.

Although the links between poverty and armed conflict are complex and by no means direct, poverty is an important explanatory factor for armed conflict, particularly when combined with widening inequalities within and between groups. Moreover, since conflict is a key driver of poverty and under-development, poorer states are at increased risk of falling into mutually reinforcing cycles of under-development, conflict, fragility and even collapse.

Failed states are a human tragedy in their own right, but can also be a major source of regional destabilisation. Moreover, these ungoverned spaces can provide a direct threat to our own security, acting as honey-pots and safe havens for terrorist groups and transnational criminal gangs who may wish to do us harm.

Climate Change and Resource Scarcity

A third driver of the new strategic security environment, which has recently leapt up the global political agenda, relates to climate change. >>>

For some states, such as Bangladesh and the island nations of the Pacific, climate change will soon pose the most critical threat to the security of the state and its people. But even elsewhere, according to recent International Panel on Climate Change (IPCC) estimates, the long-term effects of global warming could include major loss of land due to sea-level rises, severe water and food shortages and large-scale population displacement. This in-turn has the potential to exacerbate existing problems in the global security agenda and generate new sources of tension.

Ideological Conflict: The Challenge of Political Islam

The fourth driver of the contemporary security landscape is the growth of violent Islamism, which represents both a direct threat to public safety and a long-term political challenge to western liberal democracies. Modern Islamism is best viewed as a political movement that utilises a particular interpretation of religion rather than as a fundamentalist religious movement that at times practices politics.

Through a combination of globalised communications and increased movement of peoples, political Islam today has extended its reach beyond Muslim-majority countries into western liberal democracies. Indeed, the radicalisation of Muslims both within and outside the UK by violent Islamist groups poses a major threat to UK security, as evinced by the London bombings in 2005.

Despite the seriousness of the Islamist challenge, there remains a lack of understanding amongst UK policy-makers over the complex causes of violent Islamism and radicalisation. Consequently, progress is likely to be slow and the Islamist challenge is likely to remain a key driver of both the domestic and international security agenda for some time.

Socio-Economic Resilience

The fifth driver of change that we have identified is that of socio-economic resilience. Over the past decade, British companies have adopted an increasingly lean approach to business operations, moving to 'just in time' manufacturing, shedding excess staff and squeezing out stock. Such an approach necessarily depends to a great extent on the security and reliability of supporting infrastructure, such as energy, communications and transportation. However, UK infrastructure is increasingly vulnerable to disruption, largely due to the interdependence of its constituent parts. The result of this interdependence is a so-called 'cascade effect' where the loss of one key infrastructure sector – as a result of a deliberate attack or natural disaster – could lead to consecutive losses in other areas, with severe consequences.

The New Front Line: Delimiting the Terrain of Security Policy

The changing global environment outlined above clearly necessitates a shift in the way we think about security. Traditional notions of national security policy, centred on the primacy of states, inter-state competition and military issues remain relevant in many ways but fail to adequately capture the complexity of the current security landscape. The front-line in the battle for security has now shifted; it exists both at the global level, overseas in fragile states such as Afghanistan where British forces are currently stationed, and in the international battle to tackle climate change. But it also exists at a more local level, within our communities, as we work to tackle radicalisation and extremism. In short, there is no longer a single security front-line, but many, ranging from military to environmental to economic.

We must therefore situate the formation of any new national security strategy within a wider strategic context that takes into account a broader range of issues, actors and levels of analysis.

Collaborative Security: A New Approach

If we are to succeed in enhancing and extending our mechanisms of government over this new security terrain, then we must also adopt a collaborative approach to security that is able to deliver a coordinated response using a wider range of policy instruments and actors.

The core principals of a collaborative approach to security are as follows:

- *Adopt the notion of integrated power*. This involves utilising a wider range of policy instruments in order to arrive at tailored solutions to security challenges, drawing on both 'hard' military or coercive instruments and 'soft' social and economic instruments, rather than making a choice between the two.
- *Work in partnership with others*. This notion goes to the heart of a collaborative approach, and is relevant to partnerships at the multilateral level, the regional level and to partnerships between different actors within the same state.
- *Commit to legitimacy of action*. Effective partnership requires a common objective across the spectrum of actors and this can only be achieved if there is a widely perceived basis of political legitimacy in decision-making processes. If we undervalue political legitimacy, then we risk alienating potential partners in the international and domestic sphere and eroding our capacity to deliver security.
- *Move to more open policymaking*. Legitimacy can only be achieved if all actors feel that the security policy-making process is open and transparent. Government must therefore seek ways to open up decision-making processes where it is possible and safe to do so.
- *Be open to institutional reform*. Given the new security environment and the need to integrate policy instruments, it is likely that significant institutional reform will be necessary at a number of levels within government. Existing institutional boundaries should not be allowed to hinder such innovation.

Key Questions and Conclusions

The analysis presented above is rich in its implications for UK policy-making. The security environment has undergone a radical transformation in recent years, and UK policy-makers must work hard in order to adapt to this rapid pace of change. In light of announcements by the UK Government that it will shortly publish an official National Security Strategy for the United Kingdom, we conclude this article by presenting a number of questions that we feel are in need of urgent attention:

- How can we best reform key *international institutions* in order to ensure that they reflect current realities in the international order and promote a collaborative approach to security?
- What can we do to strengthen a *rules-based international order* and build legitimacy of action into the international security arena?
- What more can we do to support national and international efforts to mitigate *climate change*?
- How should we best support the *nuclear non-proliferation* regime and re-invigorate the Non-Proliferation Treaty?
- How can we successfully manage the relationship between international supply and demand for *energy* in the face of tightening international energy markets and the expansion of civil nuclear power?
- How should we effectively tackle the growing threat of *violent political Islamism* at home and abroad?
- What more can we do to tackle *global poverty and inequality* and prevent state failure and violent conflict in the developing world?
- How can we best prepare for the potential outbreak of a *pandemic* in the UK?
- How can we successfully reduce the UK's socio-economic vulnerability and strengthen the resilience of its critical national infrastructure?
- How can we best integrate policy instruments in order to tackle to roots and effects of *transnational organised crime*?
- What more should we be doing in order to ensure the security of vulnerable stocks of *fissile material*?

These are some of the pressing issues that will be addressed by the IPPR's *Commission on National Security in the 21st Century*, and that we believe should inform the government's own thinking on national security policy.

Ian Kearns and Katie Paintin,
Institute for Public Policy Research

21st Century Crises: A New Cosmology Urgently Needed

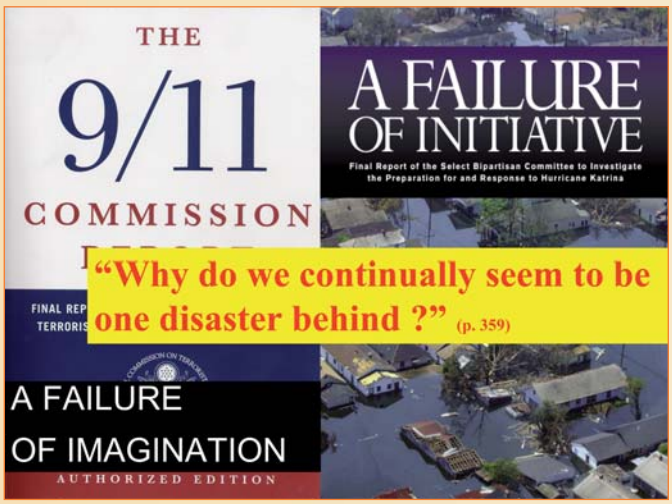
"*Why do we continually seem to be a disaster behind?*"[1]. This is the key question behind "Failures of Imagination" or "Failures of Initiative". The worrying news is that, crisis after crisis, we react as if programmed to do no more than call for "more of the same": more ready-made answers, more plans, more Command and Control. The good news is that some are beginning to understand that emerging issues and contexts of the 21st Century demand a decisive breakthrough in crisis culture and strategy. Just as Magellan did in his own 16th Century context[2], we also need a new cosmology. The time has come to take on the risk of sketching new maps, and give birth to new strategies, new tactics, new models of education and training.[3]

Here lies Crisis Management

Everyone agrees that Hurricane Katrina was a traumatic fiasco. But, beyond the specific event, we have to acknowledge a global warning. First, Katrina was just the kind of cataclysmic event that are becoming increasingly common: "*We must expect more catastrophes like Hurricane Katrina and possibly even worse.*" (The White House report)[4] Second, we are strategically overwhelmed by these emerging issues: "*Our current system for homeland security does not provide the necessary framework to manage the challenges posed by 21st Century catastrophic threats.*[5] Third, we are culturally reluctant to make the drastic changes necessary to meet the challenge: "*Many government officials continue to stubbornly resist recognizing that fundamental changes in disaster management are needed.*" (House of Representatives)[6]

Of course, at the level of tactics and assets, much can be done – and must be done – to strengthen our operational capabilities, to re-write texts and plans, to clarify some sensitive questions such as "push" or "pull" mechanisms (we can barely fathom the difficulties that the implementation of a European-wide "push" system would bring about), to train people at all levels. But the real challenge is that the theatre of operations must be entirely reappraised.

Our emergency culture is embedded in an outdated model. In the last century, crisis was defined as an acute problem that could be resolved and overcome through rapid response; we simply had to be ready to bring the necessary means to bear in order to return to normalcy; the problem was specific, isolated, and the context stable. Today, however, events can be much more disruptive; more importantly: they occur in contexts that have become fundamentally unstable, in continuous mutation.



[1] *U.S. House of Representatives, A Failure of Initiative, Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, US Government Printing Office, 15 February 2006 (p. 359).*

[2] *Laurence Bergreen, Over the Edge of the World – Magellan's Terrifying Circumnavigation of the Globe, Harper Perennial, New York 2004, pp. 73; 10; 73, 201-202.*

[3] *Patrick Lagadec, 'Over the edge of the world', in: Crisis Response Journal, Volume 3, Issue 4, p. 48-49, September 2007.*

[4] *The White House, The Federal Response to Hurricane Katrina – Lessons Learned, 23 February 2006, p. 65.*

[5] *The White House, idem, p. 52.*

[6] *U.S. House of Representatives, p. xi.*

Connectivity is the leitmotiv of our strengths and weaknesses; speed, ignorance, hypercomplexity, "inconceivability", are the names of the game. *Any* event, not only "Category 5" disruptions, can trigger unthinkable domino effects.

A Whole New Ball Game

Crisis management now goes much beyond emergency response. We have to adapt accordingly.

Intelligence

We used to have a static approach, with pre-designed categories of disasters, pre-planned answers, pre-defined organizations, and strict chains of command. Today, we must develop a new intelligence model for chaotic environments, when nothing is stable, where a minor loss of balance can lead to the collapse of our posture, and any action triggers multiple reactions[7]. We used to have fixed doctrines in order to guarantee the proper implementation of fixed answers. Now we must develop *Rapid Reflection Forces*[8],[9] to develop new tools of understanding and to invent uncharted pathways through all *terrae incognitae*.

Organization

Our plans were neatly laid out in a "Russian Dolls" concept – adding up separate stratas at the Local, State, National, and International levels. We must create more complex dynamics, moving away from sequential logic – biology supplants mechanics.

Leadership

We used to rely on officers who relied on a set corpus of best practices. Now, "*at all levels of government, we must build a leadership corps that (...) must be populated by leaders who are prepared to exhibit innovation and take the initiative during extremely trying circumstances*".[10]

Networks

We used to require a clear definition of who was in command, and comprehensive mapping of the stakeholders who should be coordinated. Today we must adapt to increasingly complex networking processes, and realize that preparation, action and reaction involve a kaleidoscope of players. It is not enough to speak of

"partnerships". What is needed is a "global new deal", which will fundamentally redefine the roles of each player and most especially the repartition of tasks among public authorities and critical networks operators.

Empowerment

Our leaders used to obsess about the risk of "populations panicking", even though historical evidence shows that populations will most often be resourceful and composed. Now, "Empowerment" must be an omnipresent building block in the systems we build. Which means that we must accept to rely on trust, beyond the usual Command and Control principle.

Communications

Communication is the cornerstone of the whole process: to link people, to adjust to a very rapid mutating environment. Technical sophistication should not obscure the fact that even basic communication can be at risk: "*Katrina interoperability problems were masked to some degree by the larger more serious breakdown of operability resulting from the destruction of facilities or power outages*"[11]. However, the most pressing challenge in terms of information sharing is, again, cultural. Satellite phones and blackberries are little help if turf wars make their users reluctant >>>

[7] *Mike Granatt's re-interpretation of Newton's principle. Personal communication.*

[8] *Pierre Béroux, Xavier Guilhou, Patrick Lagadec, 'Implementing Rapid Reflection Forces', in: Crisis Response, vol. 3, issue 2, pp. 36-37.*

[9] *Pierre Beroux, Xavier Guilhou, Patrick Lagadec, 'Rapid Reflection Forces put to the reality test', in: Crisis Response Journal, forthcoming, vol 4, issue 2, March 2008.*

[10] *The White House, idem, p. 72.*

[11] *U.S. House of Representatives, idem, p. 165.*

New York, NY, September 21, 2001 – Smoke still billows from the remains of the World Trade Center. The clean up operation is expected to take months.

to communicate. There is more to the problem than the mantra "You should not be exchanging business cards when a crisis hits": even if stakeholders are indeed familiar with one another, the question remains whether they are culturally willing and able to communicate instantly with others, know or unknown, in fast-changing contexts, and without perfect information or clear chains of command.

Recover

In the more stable world of the last century, emergency response was the focus; restoration of normalcy was presumed to be somewhat automatic, and aimed at specific damaged assets. But in today's unstable and complex world, the issue is no longer to "restore" walls, bridges and roads – after the heroics of search and rescue. It becomes essential to build into the system, years in advance – and not *the day after* –, the conditions that will help a complex societal texture to find new sustainable dynamics in a fast-moving environment.

Education and training

We used to train people to apply a known set of rules. We now have to educate them to face the unknown, and be creative, even if the process is untidy. As specified in the White House report: "*When training, Federal officials should not shy away from exercising worst-case scenarios that "break" our homeland security system.*"[12]

Static stance is lethal in a rapidly evolving world, where speed and connectivity are vital to safety and sustainability. It is crucial to think and act differently. The issue of systemic crises has to be put high on Head of states agendas. Let's not wait for the next event to be the wake-up call for strategic initiatives.

Patrick Lagadec,
Director Research, Ecole Polytechnique (Paris)
www.patricklagadec.net

[12] *The White House, idem, p. 73.*

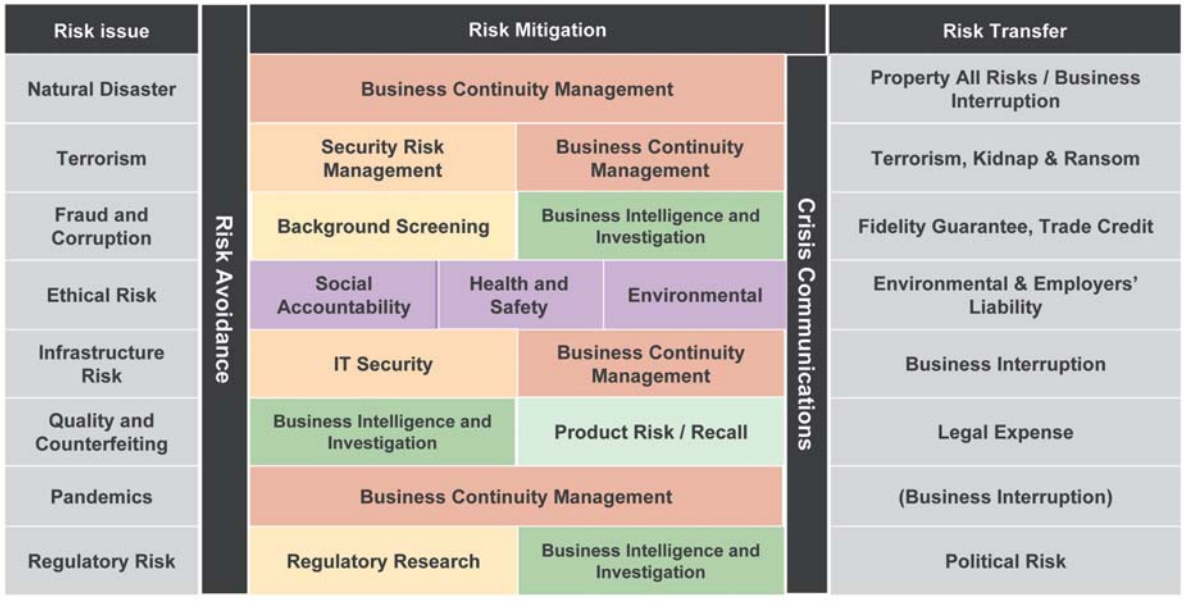
Private sector companies face a highly diverse range of risk exposures that they must effectively manage if they are to be successful. Many of today's companies have global operations and supply chain dependencies, operate in stringent regulatory and dynamic environments, and face intense competition. The size and complexity of risk that businesses face can be extreme, presenting a formidable management challenge. However, failure to understand and address risks appropriately can negatively affect profit and reputation and may even cause insolvency.

Approaches to Risk Management in the Private Sector

There are many approaches and techniques companies adopt to manage risk and there are some common themes that are generally used by firms with advanced risk management sophistication, which are described below.

No company has unlimited resources for risk management so the focus must be applied to those parts of the business that have the greatest corporate value. Definition and measurement of value is highly subjective and will vary by company but will broadly include consideration of metrics such as profit, reputation and brand, and growth strategy. Qualitative and quantitative analysis of the company's key functions will identify those activities that provide the greatest corporate value to the firm, facilitating their prioritisation for risk management focus and optimisation.

Once the key areas of focus have been agreed, an evaluation of the function's value chain is needed to map resource dependencies in terms of people, technology, facilities and suppliers and so on to identify potential points of weakness and resource vulnerabilities to threats. Knowledge of the latter may already be available in-house though generally it is best practice to augment this with structured risk assessment, so that a holistic view of the threats that critical resources face is understood. >>>



Risk management optimisation – Avoidance, mitigation and transfer

Value mapping

Thorough assessment and analysis will enable informed decisions to be made on formulating an appropriate risk management strategy. This should be supported with an appreciation of corporate risk appetite and tolerance thresholds to loss, so that it is objectively understood what levels of value-at-risk are acceptable to the firm and that subsequent process alterations and investment in risk management reflects this i.e. resource deployment is optimised. For example, it could be decided that an existing level of resiliency or corporate preparedness is excessive compared to corporate tolerance and can be lowered for certain functions, liberating cost savings. Alternatively a decision to increase resiliency via strengthened business continuity management (BCM) and more extensive insurance may be preferred if an exposure and value at risk is found to be unacceptable.

Such an approach to risk management can further be applied to threats on an individual level, where estimated cost/benefit analysis of proposed risk management is supplemented with corporate risk tolerance knowledge. If we take natural catastrophe risk as a case in point, firms have a variety of options in their risk management arsenal to deal with the impacts of such an event, including avoidance i.e. choosing not to site a facility in a susceptible zone, mitigation such as BCM techniques, and risk transfer such as property damage and business interruption insurance. The optimal mix chosen by the firm will ultimately be subject to cost/benefit factors and the levels of assurance and certainty required e.g. insurance may help with short term cash flow but will not protect against reputation damage, whereas avoidance may provide greater degrees of certainty but may have financial trade offs.

Finally, companies are now starting to exploit technology for provision of real time risk intelligence data that can provide rapid alerts on threats that could be problematic to the firm and lead to value destruction. Such early warning systems can form a key line of defence for avoidance and containment of negative impacts arising from certain classes of threat.

Matthew Elkington,
Vice President Risk Consulting Ltd., London
matthew.elkington@marsh.com

Workshop: What Can We Do About These Threats?

Facilitator: Neil Ellis, Consultant, PA Consulting Group

Speakers:

- **Bengt Sundelius, Chief Scientist, Swedish Emergency Management Agency (SEMA)**
- **Garry Hindle, Head of Security and Counter-terrorism. Royal United Services Institute (RUSI)**

The workshop aimed to consider the question of what we can do about these threats from two different perspectives; the preparation of an effective response to a situation and taking actions to reduce these threats. Both of the speakers highlighted different techniques and quoted examples to demonstrate ways in which we can deal with threats more effectively.

Sundelius began by questioning the relative importance of prevention and preparedness. Although there was clear value in prevention, you often can often fail to prevent something happening; it is therefore vital to be prepared. It is clear that there is a very delicate balance between investment in prevention or in preparation.
Given the focus on preparation, the speaker continued by emphasising how, in a crisis, leadership is vital. The public expects a leader to perform when the stakes are high and have no regard for how effective they are in their day job. Continuing, he pointed out how crises are not just risk or threats; they are opportunities too. Intelligent public leaders grasp these opportunities to legitimise their role through effective handling of situations. Sundelius then continued to outline his six points of leadership:

- Sense Making – situational diagnosis,
- Decision Making – strategic choices,
- Meaning Making – framing public views,
- Accounting – taking responsibility,
- Ending – achieving closure
- Learning – intelligent reflection and reform.

In summary, he proposed that, in order to deal with risks, it was necessary to help those with responsibility to do well and invest in preparations. There ought to be Europe wide crisis management with "interlocking" systems rather than "interblocking" systems. It was suggested that there would be a vulnerability surplus and a capacity deficit in the next 10 years and so this is vital.

Hindle chose to present an example of a current initiative that is aimed at reducing the threat at grass routes level. He explained that, in general, it has become increasingly important to look more locally at the citizen as well as to cooperate more effectively at a global level. In a world of threats, people must be the players through devolving and enabling more at a local level.

Continuing, he noted that since the 7th July bombings in 2005, police communication with mosques has improved, there has been recruitment of more informers and the need to develop and expand on these and other links has become increasingly clear. He also outlined the UK government's Pathfinder initiative which was begun early in 2007 and is aimed at empowering Muslims to counter extremism, formalising the relationships developed post 7th July and encouraging innovative ideas to be filtered upwards from the community. In 2007/2008, £5m was invested in building links with Muslim youth, who are most at risk of radicalisation, and Muslim women who are key influencers in the community.

The group then had a discussion about the issues raised in the presentations. Initial conversation was around the framing of public views and how you do this in practice by being aware of the consequences of actions or lack of action. It is important in crisis management to not just be focusing in the situation at hand but also at the meaning for the community.

The discussion then went on to the perceived vulnerability surplus and capacity deficit and how this can be managed. The group felt that politicians would not thank you for raising issues without solutions but there is a danger of being overwhelmed by the range of risks. The tools that support crisis management should be in place and risks should be linked to allow for better management of the consequences. Importantly, the group felt that it is important to know how to receive help from other countries. What are the specialist needs and where >>>

might they come from? National risk assessments should be put to governments so that they can make educated decisions about priorities.

Following on from this, the concept of a "creeping crisis" was raised. The group felt that climate change was a good example of this as it is difficult to get money for preparing for something that has not yet happened. Countries tend to, when it comes to threats to security such as terrorism, concentrate solely on national security plan but for something like climate change there should be an international mechanism in place to prepare for that. When looking for investment it is vital that the consequences of the threat, not just the threat itself, should be made clear.

Finally, the group felt that a discussion should be had around terminology. "Safety" has become "security" which pushes the conversation behind closed doors. Perhaps National Security should be kept separate from Societal Security.

From left to right: Sundelius, Ellis and Hindle

Workshop: What Will Threaten Us (*Foresight*)?

Facilitator: Stephen de Spiegeleire, Director Defence Transformation, The Hague Centre for Strategic Studies.

Speakers:

- **Peter Schwartz, Founder and Chair of the Global Risk Network**
- **Michael Oborne, Director, Advisory Unit on Multidisciplinary Issues, OECD**

Peter Schwartz: The Art of the Long View: Strategic Thinking and Future Scenarios

Anticipating threats presents a challenge for most organisations. However, it was argued that the biggest barrier to seeing threats is denial rather than an inability to see it; we chose not to see the threat as identification requires action. A failure of imagination and a failure to challenge their own thinking has often crippled those in power; an external perspective provides an essential challenge function.

Scenario building does not predict the future but gives the ability to identify and recognise trends when they appear. The benefit in scenario planning was not to predict the future, but to encourage people to act. It can also provide a focus for strategic conversations which can help address the challenge of aligning different parts of security organisations.

A number of novel threats and changing trends were presented and discussed including the fragmentation of political centres; impact of second order effects; impact of a knowledge-driven economy; privatisation of foreign policy; advances in biology; and concerns over access to water.

Michael Oborne

It was proposed that the main problem facing the foresight community is not the message but rather the issue of getting the attention of the audience. Four different

From left to right: De Spiegeleire, Schwartz and Oborne

categories of futurist were outlined and discussed; Merlin, Cassandra, Dr Strangelove and the Court Jester.

A number of medium-term policy problems were presented, including the risks posed by financial markets; maritime pollution and its associated impact on fishing stocks; migration (both immigration and emigration); changes to values of identity and social cohesion; and lack of clarity about what India and China will look like when their economies have matured.

Discussion

In discussion the following points were made:

a Much of the planning for predictable trends had been catered for; large investment decisions now required to be made regarding the less predictable issues.

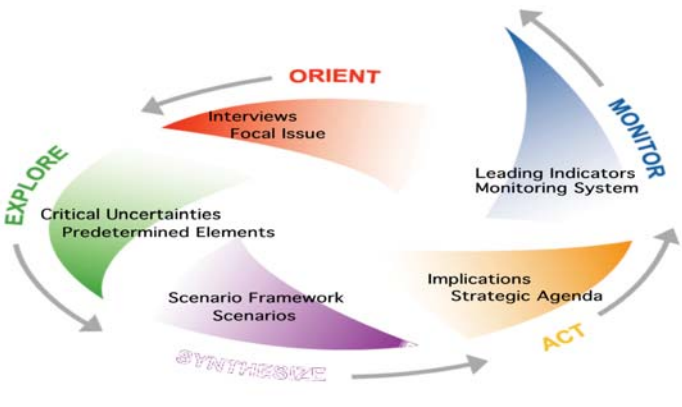
b Convincing people to make decisions required credibility which can only be built over time. The best approach was to give people the tools to identify indicators themselves rather than be prescriptive.

c Creating a list of trends benefits from a systematic approach involving reading, interviews and the use of a 'network of remarkable people' that can identify signals from the edge of change. The Organisation for Economic Co-operation and Development (OECD) approach draws on dialogue with 117 different institutes to develop a rich list of topics; uses global science forum to distil trends; engages with policy making groups; and scans literature in the field.

d 'Security' is a defensive concept and is often perceived as trying to maintain status quo. Discussion surrounded whether the concept of security is still the best frame to shape our thoughts or if a new concept and term should be developed to help our thinking. It was suggested that 'resilience' might provide a better frame than security.

e In the virtual world, there is a strong move towards bringing down the walls, known as de-perimetrisation. This is in stark contrast to moves on the physical side.

f Many countries committed resources to foresight. Instead of duplication, it could be more effective for countries to work together on the subject of national security. However, organisations require involvement in and hence ownership of risk assessments to ensure they are used as a tool for action and that there was unlikely to be a 'one size fits all' solution. It was suggested a mixed approach would be the optimum solution, engaging external experts and internal policy makers. This would capitalise upon all the information available and allow internal engagement in the process and hence ownership.



The scenario thinking process

Colophon

Address
Ministry of the Interior and Kingdom Relations
P.O. Box 20011, 2500 EA The Hague, The Netherlands
E-mail: crisisbeheersing@minbzk.nl
Internet: **www.minbzk.nl/veiligheid**

Editorial Committee
Editorial Committee: Henk Geveke, Nico de Gouw and Geert Wismans (editor-in-chief)
Editorial assistant: Maddy Ockhorst
Secretariat: Nalini Bihari (+ 31 (0) 70 – 426 73 54)

Editorial Board
Prof. dr Ben Ale (Delft University of Technology)
Prof. dr Joost Bierens (Free University Medical Centre, Amsterdam)
Dr. Arjen Boin (Louisiana State University, USA)
Mr. dr. Ernst Brainich von Brainich Felth
Dr. Menno van Duin (Netherlands Institute for Physical Safety)
Prof. dr. Georg Frerks (University of Wageningen)
Prof. dr Bob de Graaff (Universiteit of Leiden)
Prof. dr. Ira Helsloot (Free University of Amsterdam)
Prof. dr. Erwin Muller (University of Leiden)
Prof. dr. Uri Rosenthal (University of Leiden)
Dr. Astrid Scholtens (National Police Academy / Netherlands Institute for Physical Safety)
Prof. dr. Erwin Seydel (University of Twente)
Prof. dr. Rob de Wijk (The Hague Centre for Strategic Studies)

Contributors
Eva Barneveld, Guido Bertolaso, Ruth Clabbers, Matthew Elkington, Natasja Hartzema, Mrs. Guusje ter Horst, Jasper van der Horst, Ian Kearns, Patrick Lagadec, Bruce Mann, Katie Paintin, Eric Pruyt, Dick Schoof, Michael Thornton, Peter de Wit

Photography
ANP, FEMA/Michael Rieger, Arenda Oomen, Reuters, Shell

Design
Grafisch Buro van Erkelens, The Hague

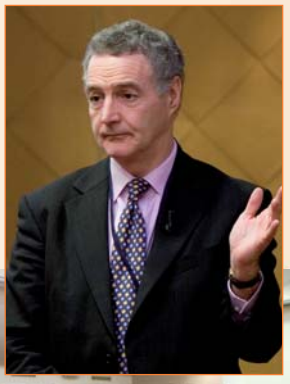
Production support
Ministry of the Interior and Kingdom Relations/Directorate Communication and Information/Graphic and Multimedia Facilities

Print
OBT bv, The Hague

ISSN 1875-7561

For free subscription mail to: crisisbeheersing@minbzk.nl
The Magazine is available online at www.minbzk.nl/veiligheid.

End Conference Summary



In summary, the Chair identified 3 key themes. The first is the need to follow a process of identification, assessment and mobilisation in any crisis situation. Secondly, a key theme was that the "Novelty" factor should be reduced as far as possible. Things that occur that we say are surprises, should not be surprises. Finally, creating the right political structure is key. Making sure that someone is in power who can actually drive this agenda forward. If the leadership is not legitimised, it will be hard to get buy in to a common goal.

Following on from the Chair, Bruce Mann reiterated these three themes but wanted to highlight two aspects in particular to take away from the day; the journey and the people.

In terms of the journey it is important, despite any nervousness and fear of the unknown, to differentiate between

- what we already understand on the journey;
- where this is more than we have done before or where it has been done before but outside the security field and we can bring techniques in;
- what is genuinely and wholly new. This is probably more on the social/people side.

Continuing, the idea of building partnerships with people is clearly not radical but there is a lot that we can learn about how to go about doing this. The softer words and skills need to be focussed on more: relationships, trust, legitimacy, empowerment. Bruce's belief is that these concepts are not new, but they are new to the security field. Security is now very broad indeed and so there is now a much wider family to bring in.

There must be expansion of both institutions and analytical tools. The latter have been mostly within institutions' comfort zones and should start to consider more behavioural analysis. In terms of institutions, there is a need to move them on to the next level, especially security related ones, but frustrations come with not being able to have cross-boarder dialogues around risks. With the new and wider nature of the subject, it is now no longer possible to box things and it should be more about institutional cooperation; institutes working together and bring their own disciplines to bear.

The Way Forward

Participants were asked to consider a number of possible outcomes from the conference.

1. Set up a network of people interested in either issues in the round or particular aspects – this could develop into a website.
2. Organise another of these events. The UK is happy to consider hosting this but more than happy to receive offers from other countries.
3. Hold specific events on specific themes; these might include
   a. risk assessment methodology;
   b. risk communications and management of public;
   c. foresight (longer term);
   d. protection of critical infrastructure;
   e. public/private partnerships;
   f. national security strategies.
4. Specific research propositions.