FOI
SWEDISH DEFENCE
RESEARCH AGENCY

FOI-R--0533--SE
June 2002
ISSN 1650-1942
User report

Ola Dahlman (Ed.)

Science and Technology in Support of European Security

SWEDISH DEFENCE RESEARCH AGENCY

Defence Analysis
SE-172 90 Stockholm

FOI-R--0533--SE

June 2002

ISSN 1650-1942

User report

Ola Dahlman (Ed.)

Science and Technology in Support of European Security

Issuing organization FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	**Report number, ISRN** FOI-R--0533--SE	**Report type** User report
	Research area code 1. Defence and Security Policy	
	Month year June 2002	**Project no.** ES 111
	Customers code 1. Policy Support to the Government	
	Sub area code 11 Policy Support to the Government (Defence)	
Author/s (editor/s) Ola Dahlman (Ed.)	**Project manager**	
	Approved by	
	Sponsoring agency	
	Scientifically and technically responsible	
Report title Science and Technology in Support of European Security.		
Abstract (not more than 200 words) How can science and technology make a difference when it comes to confidence building, arms control and non-military threats to our societies? The minister of Foreign Affairs of Sweden, Anna Lindh, invited senior level indiviuals from security policy and research institutions in Europe, Canada, Russia and the United States to address this issue during a Workshop on Science and Technology in Support of European Security that was held from 24-26 April 2002 in Stockholm. This publication is the result of the Workshop, and includes the papers presented as well as a Rapporteur's Report of the proceedings. This Workshop is an important step in the process of applying science and technology to enhance security in our society.		
Keywords Science and Technology, European Security, Non-proliferation of Weapons Mass destruction, Vulnerability of Modern Societies.		
Further bibliographic information	**Language** English	
ISSN 1650-1942	**Pages** 144 p.	
	Price acc. to pricelist	

Utgivare
Totalförsvarets Forskningsinstitut - FOI
Försvarsanalys
172 90 Stockholm

Rapportnummer, ISRN
FOI-R--0533--SE

Klassificering
Användarrapport

Forskningsområde
1. Försvar- och säkerhetspolitik

Månad, år
Juni 2002

Projektnummer
ES 111

Verksamhetsgren
1. Forskning för regeringens behov

Delområde
11 Försvarsforskning för regeringens behov

Författare/redaktör
Ola Dahlman (Ed.)

Projektledare

Godkänd av

Uppdragsgivare/kundbeteckning

Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel (i översättning)

Vetenskap och teknologi till stöd för europeisk säkerhet.

Sammanfattning (högst 200 ord)

Hur kan vetenskap och teknik på ett avgörande sätt bidra till internationellt förtroende, öka förutsättningarna för nedrustning och rustningskontroll samt hjälpa oss hantera nya, icke-militära hot mot vårt samhälle. Sveriges utrikesminister Anna Lindh bjöd in ett fyrtiotal internationella experter att diskutera dessa frågor under en workshop om vetenskap och teknologi till stöd för europeisk säkerhet som hölls i Stockholm den 24-26 april 2002. Denna rapport redovisar resultaten från denna workshop och innehåller de föredrag som presenterades och en sammanfattning av diskussionerna.

Nyckelord
Teknik, vetenskap, europeisk säkerhet, icke-spridning av massförstörelsevapen, terrorism.

Övriga bibliografiska uppgifter

Språk Engelska

ISSN 1650-1942

Antal sidor: 144 s.

Distribution enligt missiv

Pris: Enligt prislista

Workshop 24-26 April 2002 in Saltsjöbaden, Stockholm, Sweden on

Science and Technology in Support of the European Security Policy

The Minister of Foreign Affairs of Sweden, Anna Lindh, invited senior level individuals from security policy and research institutions in Europe, Canada, Russia and the United States to address this issue during a Workshop on Science and Technology in Support of European Security that was held from 24-26 April 2002 in Stockholm. This publication is the result of the Workshop, and includes the papers presented as well as a Rapporteur's Report of the proceedings. This Workshop is an important step in the process of applying science and technology to enhance security in our society.

List of Contents

Workshop Summary Report

Jenifer Mackby, Fellow, Center for Strategic and International Studies, (CSIS), Washington DC, U.S.A.

Presentations:

Welcome

Bengt Anderberg, DG, Swedish Defence Research Agency, (FOI), Stockholm, Sweden: "*Introductory Address*".

Introductory Address

Richard Escritt, Director, Research Directorate-General, European Commission, Brussels, Belgium: *"Science and Technology in support of European Security: A European Research Area Perspective".*

The New Security Agenda

Mona Dreicer, Director, US State Department, Washington, U.S.A.: *"Science and Technology Support for U.S. Homeland Security".*

Lars–Erik Lundin, Head of Security Policy Unit, European Commission, Brussels, Belgium: *"Brief points from an EU perspective on the New Security Agenda".*

Jan Foghelin, Head of Division of Defence Analysis, FOI, Stockholm, Sweden: *"A Complex World Needs Complex Security Strategies".*

Arms Control and Disarmament

Bernard Sitt, Director, International Affairs, Atomic Energy Agency (CEA/DAM Ile de France), Bruyères-le-Châtel, France: *"What Role for Arms Control in the International Security Context of the New Century".*

Martin Dahinden, Director, Geneva International Center for Humanitarian Demining, (GICHD), Geneva, Switzerland: *"Use of Modern Technology in Humanitarian Crisis*".

Ian Anthony, Stockholm International Peace Research Institute, (SIPRI), Stockholm, Sweden: *"The European Union Dual-Use Export Control System after 11 September: Is There a Need for Reform?".*

Non-Proliferation

Gary Samore, Senior Fellow for Non-proliferation, International Institute of Security Studies, (IISS), London, UK: *"Impact of September 11 on U.S. Non-proliferation Policy"*.

The Vulnerability of the Society

Peter Bröms, Senior Analyst, Europol, The Hague, The Netherlands: *"Organized Crime in the European Union: The need for common action"*.

David F. Heyman, Senior Fellow and Director, Center for Strategic and International Studies, (CSIS), Washington, U.S.A.: *"Bioterrorism and the Vulnerability of Society*".

Erik J.G. van de Linde, RAND Europe, Leiden, The Netherlands: *"Critical Infrastructure Protection"*.

Gordon McBean, Professor, Institute for Catastrophic Loss Reduction, The University of Western Ontario London, ON, Canada*: "Vulnerability from Natural Hazards and Implications for Security"*.

Science for Security

Rolf Linkohr, Dr., European Parliament, Brussels, Belgium: *"Science for Security"*.

David Wilkinson, Dr., Director, Institute for the Protection and Security of the Citizen, (IPSC), Joint Research Centre, European Commission, Ispra, Italy: *"Technology for Stability and Security - Implications for the European Union"*.

Ken Peebles, Director, RTA, NATO, Paris, France: *"Defense Research: Part of the Answer to Terrorism"*.

Ralph W. Alewine III, Dep Ass to the Secretary of Defense, Nuclear Treaty Programs, Arlington, U.S.A.: *"The DARPA Example*".

Valerie A. Hood, Secretary General, EURISY Association, Paris, France: *"Humanitarian Aspects of Security"*.

Ruud M. Lutje Schipholt, Director, Netherlands Institute of Applied Geoscience, (TNO), JA Delft, The Netherlands*: "US - Europe Technology Gap"*.

Jaakko Iloniemi, Minister, Office of President Ahtisaari, Helsingfors, Finland: *"Information Technology and Crisis Management"*.

List of Participants

The Agenda

Workshop Summary Report

by **Jenifer Mackby**, Fellow
The Center for Strategic and International Studies, CSIS
Washington D.C., USA

Introduction

The security perspective of today and tomorrow is broader than that of yesterday. On the global scale we are moving from deterrence to confidence building, from armed conflicts to crisis prevention and management. Conflicts today occur within rather than between States, non-State actors are playing an increased role, and the security of each of us depends more and more on our ability to handle non-military crises. These can include terrorist attacks, organized, more "conventional" crime, trafficking or environmental disasters. In many parts of the world the greatest threats to human security are still famine and disease. The security problems we face today are due at least in part to famine, injustice, lack of development, democracy and hope in many parts of the world.

We are also facing a growing number of threats to our modern societies of an economic and technical origin. Deliberate attacks on our information systems to manipulate the very nerves of our societies can be launched from any point on earth by small groups of people. In short, we have moved from a situation where we were planning to cope with disastrous military confrontation that might occur with a low probability to a situation where we have to cope with a number of threats to our security and safety facing us every day. A challenge in the development of our future security structure is to find a proper balance between the military and the civilian components.

In considering European security we must take into account the joint European perspectives of the European Union and the European Commission as well as the perspectives of the individual States. This Workshop on Science and Security aimed to focus on some of the key issues for European Security:

- the vulnerability of modern societies, including terrorism, international crime, drugs and illegal trafficking, information warfare, disaster mitigation;
- non-proliferation of weapons of mass destruction: nuclear, chemical and biological;
- disarmament, arms control and confidence building measures.

European security involves not only diplomatic activities, but also the spectrum of society, including government agencies, industry and non-governmental organizations. Science and technology should be fully utilized as a force multiplier to enhance security, and this was the objective of the Workshop. The following questions were asked:

- How can science and technology play a role in promoting security in this new broad perspective?

- How could we focus our attention on these problems in a way similar to what has been done so far on the military side?
- How could science and technology make a difference when it comes to confidence building, arms control, international co-operation and non-military threats to our societies?

The new security agenda

Collective security and defence cooperation were not considered relevant for common European policy until the 1990s. The wars in the Balkans and Central Africa strongly influenced the European public opinion. Europeans realize that they cannot be impartial observers of collective carnage in a nation, but they can assist in making and keeping peace. Thus the credibility of European policy depends increasingly on its ability to provide collective security, which is its common interest.

The Treaty of the European Union states that the common foreign and security policy includes the framing of a common defence policy, which might lead to a common defence, should the European Council so decide. It is also able to support disarmament and arms control. The responsibility for the common foreign and security policy lies with the Council and thus within the governments of the member states, though the European Parliament can pressure the Council.

When considering the industrial technological base for conflict prevention, including military intervention, it is appropriate to look towards 2015-2020. Although Europeans seem to perceive that they are less of a security target than Americans, Europeans tend more towards conflict prevention and conflict resolution than confrontation in their international policies.

The United States spends some $26,000 per soldier, whereas the EU only spends $4,000 per soldier. If the disparity in defence efforts between Europe and the United States continues to grow, however, it will strain the transatlantic link and the European influence on security matters in the world will diminish. The discrepancy in technology in the material will render it impossible to hold joint military operations. The US will develop its own military doctrines, and NATO partners on both sides of the Atlantic may drift apart. As Europe cannot realistically compete with the US, perhaps instead it should complement the efforts and activities of the U.S.

Europe has responded to 11 September with its 69-point roadmap spanning a wide range of actions from increased airport security to enhanced relations with Pakistan. It also includes items such as common arrest warrants, a common definition of terrorist acts, freezing of assets, etc. However, Europe also maintains respect for the United Nations and international law and does not accept the death penalty.

Although the European Commission has no direct role in military affairs, it has defined security, in particular the security of the citizen, as one of its main priorities for 2003 in parallel with enlargement of the EU. The work plan of the Commission includes many actions to serve this goal, from civil emergency planning to justice and home affairs, environmental security, transport and energy security, cyber security, demining and general international assistance. In the search for methodologies and technologies to enhance individual accountability, it is also essential to enhance methodologies to protect individual liberties and rights.

The contacts and coordination between the EU and NATO should be improved *inter alia* in order to avoid duplication. The desire to share information in areas where both are engaged is welcomed, as is the cooperation in the Balkans.

Intelligence is a key issue that is not shared. It is used on a case-by-case basis. Exchange of information could start between the EU and NATO; the United States may not look favourably upon this, however, when the EU is enlarged. To what extent is there scope for distributing information without saying where it comes from? The intelligence-poor member suffers, as he has no information to share. How do we judge intelligence? We don't always want to use it. Intelligence and export controls should be further developed. Situations such as UNSCOM should use intelligence without revealing parameters; it became a trade-off between democracy and efficiency

September 11 presented a large political and technical challenge: about 70 countries were affected, as well as families and friends. Non-State actors played an important role, yet it is not a foregone conclusion that there is a link between non-state violence and WMD. In that regard, the "axis of evil" did not include India or Pakistan, though they pursue missiles and have terrorists; Bush is still interested in talking to North Korea and another regime in Iraq. Biological, chemical, or even radiological are ultimate terrorist weapons, and some had pointed to that link long before 11 September. What constitutes a strategic surprise? Sputnik, nuclear tests in South Asia, September 11, airline security, the mental thinking of suicide bombers? There are seven novelties in this era:

- in the field of security, the focus has shifted from Europe to central and south Asia (China, Taiwan, the Korean Peninsula, sea lanes in Asia, and southeast Asia);
- the United States has become a different ally; it is a more fragile power than perceived, and not powerful enough to prevent terrorism or proliferation of weapons of mass destruction, or to provide peace in the Middle East. Europeans find that it is no longer viable for the United States to fight and the Europeans to reconstruct afterwards;
- when asked if Europe is able to deal with the privatisation of violence, the answer would be negative; its bureaucratic order is unable to find quick solutions;
- the globalization of insecurity means that the attacks on the Pentagon can be planned in Asia; thus, Europe should think globally, beyond Europe;
- the confusion between security and insecurity, state and non-state, and even peace and war results in difficulty in understanding what is transpiring;
- the proliferation of nuclear power, ballistic missiles and weapons of mass destruction add to the sense of insecurity;

- strategic surprise will be witnessed more often and hence there is a need to increase a sense of predictability rather than seeing the major powers self-absorbed.

Has technology weakened European security rather than the other way around? Should Europe become a regional power first or something new and different? There is confusion regarding the role of Europe. It is committed to collective security (Article 5 of NATO), yet it should also organize peacekeeping missions and crisis management at the borders of Europe. Europe has not been able to make a threat assessment of its periphery.

Arms Control and Disarmament

The "golden decade" of arms control treaties is characterized by a wealth of both bilateral and multilateral instruments, some of which contained sophisticated and technical verification regimes. In 1986 Bush and Gorbachev held a historic summit in Reykjavik, and 1996 saw the Comprehensive Nuclear-Test-Ban Treaty (CTBT) opening for signature. In between, the Missile Technology Control Regime (MTCR) and Intermediate-range Nuclear Forces (INF) Treaty were realized in 1987, the Conventional Forces in Europe (CFE) treaty in 1991, the Strategic Arms Reduction Treaty (START) I in 1991, the US-Soviet joint unilateral initiatives on strategic nuclear forces in 1991, the START II and the CWC in 1993, and the indefinite extension of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) in 1995.

Subsequently, the end of the Cold War has ushered in an era of strategic doubt, with the bilateral stalemate of the START process that dated back to optimistic decisions taken at the 1997 Helsinki Summit as well as the multilateral stalemate in the Conference on Disarmament (CD) in Geneva. Some believe that the CD has become too intransigent to effectuate negotiations among its large number of countries. The fundamental strategic and political climate is essential for agreement to be reached in both bilateral and multilateral fora, which in any case provide an opportunity for an exchange of views on a broad range of issues.

The Russian Federation and the United States plan soon to reduce their nuclear weapons considerably, which will be a milestone in arms control and will redefine the strategic relationship between the two major powers.

In addition, non-state actors with invisible networks that possess no sovereign territory or political identity have injected terrorism as an unpredictable element into the equation of arms control. There is no negotiating table to which they would be invited. Can we improve the efficacy of existing agreements by preventing or detecting terrorist actions? In a number of treaties the standard article on national implementation measures obliges States Parties to adopt the necessary measures to prohibit persons under their jurisdiction from undertaking activities prohibited under the Treaty. The Chemical Weapons Convention (CWC) contains a provision to extend national penal legislation with respect to such activity. It further obliges each State Party to cooperate with other States Parties and afford legal assistance to facilitate the implementation of this article.

Over the years arms control has provided an overall global and regional security system based on the negotiation and implementation among sovereign states of treaties limiting or reducing or eliminating arms. These may be legally or politically and technically binding, with specific verification regimes. This architecture has been supplemented by other instruments such as export control regimes, confidence-building measures, unilateral initiatives, etc. which may be less legally binding but which are significant in the area of non-proliferation of weapons of mass destruction (WMD) and sensitive technologies. Since the strategic situation at the time a treaty is being negotiated is likely to change, it is important that the instruments be able to adapt to the changing political environment. In that context, the NPT and other impressive disarmament agreements have set standards and have very few violators. Therefore they should be kept, although one should not have false expectations. The CTBT is being respected in spite of the fact that ratification for some countries presents a problem; nevertheless, it is unlikely that countries will resume testing, as if one starts others may follow.

The Geneva Protocol prohibits the use of chemical and biological weapons, whereas there is no treaty prohibiting the use of nuclear weapons. This is clear in the NPT, which recognizes the nuclear-weapon States. The ABM Treaty, however, is no longer seen as the “cornerstone” of arms control, although States agreed that it was as recently as the 2000 NPT conference.

Further, implementing treaties is as important as negotiating them. For example, the CTBT is establishing its technologically sophisticated verification regime and is still working on the modalities for on-site inspections, and the CWC has an intrusive implementation regime. Undoubtedly science and technology could play a more important role in creating a safe environment for those who clear mines and the nearby populations. This in turn would affect crisis response, post conflict rehabilitation, the return of refugees and thus long-term social and economic development. It is important to use the lessons learned to know what technology can and cannot do, and how it can interact with the specific working environment (which is often not located in industrialized countries with access to expertise and infrastructure), and other technologies already being used.

Many technologies have dual use, and can be used for both humanitarian and military benefit. New yet simple, cost effective technologies, such as rats, can be promising in detecting mines. The users of the equipment should be involved with the technologists and industrialists in the development of equipment from the beginning, as they have a distinct experience. In the field of demining, in both emergency and long-term operations priority must be placed on information technology in order to have the correct information with the right people at the right place. For example, the Geneva International Centre for Humanitarian Demining has developed an Information Management System for Mine Action (IMSMA), which is a software based management tool for use at Mine Action Centre (MAC) level. It combines a relational database with a geographic information system (GIS). It provides the Mine Action managers with up-to-date information management capabilities to facilitate decision making in the framework of mine action.

How important is it to verify arms control agreements? Some believe that an arms control treaty that can’t be verified is an “animal without teeth.” The technology needed for verification of a treaty can be developed before the political will is present to negotiate it. Scientific expert work could be done in the CD, for example, on a fissile material cut-off treaty and on the protocol on physical protection of nuclear materials before negotiations begin. While disarmament develops slowly, technology develops quite quickly. Arms control agreements fold up not because of lack of technology but because of lack of political will. Is arms control linked to strategy and money rather than science and security? Industry is needed to control and inventory in order to prevent transfer. Science and security enter in three areas in particular: homeland security, treaty verification and compliance, and CTR. Science can also support European security in the areas of intelligence, new means of verification, non-proliferation, destruction of old weapons, detection of dangerous materials and new technical means for the police. Perhaps technology will open new avenues for conventional weapons to replace weapons of mass destruction.

From a European perspective, arms control is facing an uncertain future, as the United States seems distrustful of existing instruments that have maintained a strategic stability. As a political and technological power, what role can Europe play to contribute to the resolution of international security issues in its own region and elsewhere in the globe where it has influence and strategic interests? Do Europeans need their own instruments or are the global instruments sufficient?

A European Group of Scientific Experts, either in the CD or the European Security and Defence Policy (ESDP), could make an inventory of existing instruments with regard to terrorism, identifying the existing technologies and needs in the field of prevention, surveillance and detection of terrorist activities. It could also see how existing technologies could strengthen treaties. For example, recognizing the problem of potential global climate change, the World Meteorological Organization (WMO) and the United Nations Environment Programme (UNEP) established the Intergovernmental Panel on Climate Change (IPCC) in 1988. It is open to all members of the UNEP and WMO. The role of the IPCC is to assess the scientific, technical and socio-economic information relevant to the understanding of the risk of human-induced climate change. It does not carry out research, nor does it monitor climate related data or other relevant parameters. It bases its assessment mainly on peer reviewed and published scientific/technical literature. This could be used as a model for scientific, technical and socio-economic information relevant to security related issues.

The new U.S. administration views arms control treaties as delaying tactics that provide cover for hostile countries. It has taken a new approach towards multi-lateral arms control regimes, emphasizing compliance. It opposed the CTBT and rejected the BWC protocol because they were seen as potentially weakening U.S. defence and deterrence capabilities. Yet Washington clarified that it supported existing treaties such as the NPT and the CWC, and that it was in favour of negotiating new instruments such as a Fissile Material Cut-off Treaty (FMCT) and an MTCR Code of Conduct. It has identified countries that it suspects of violating the BWC and has proposed a series of international measures to strengthen the BWC in place of the protocol. Washington has advocated greater financial and technical support for the IAEA to strengthen its ability to inspect nuclear facilities and supports efforts to strengthen the International Convention on Physical

Protection of Nuclear Materials to make it more difficult for terrorists to acquire nuclear materials from civilian nuclear programs.

Non-proliferation

Non-proliferation is not just a European problem but also a global threat. Russia was the sole inheritor of 50-60,000 warheads deployed and in stockpiles. These have been reduced, but the major part remains. In the 1990s it was relatively easy to divert materials from Russian facilities; in 1996 a container of low-level radioactive material was recovered. Since then the cooperative threat reduction program (CTR) and material protection control and accounting (MPCA) efforts have led to greater protection. Russia needs assistance with the destruction of chemical weapons. The subject of biological weapons in Russia is still a "black hole," and remains a mystery. The EU, France, UK, Japan are assisting Russia with the "brain drain" through the International Science and Technology Centre (ISTC). This is helpful, though the ISTC is not mandated to solve the problem on a long-term basis. It provides grants for scientist in Russian "closed cities," but it will not solve the needs of those unemployed in the coming months and years. There is a strong need to prevent potential proliferators from immigrating, but even if their passports were to be retained the borders are transparent, in particular with Azerbaijan and Iran.

The importance of further strengthening cooperative threat reduction with former Soviet Union States has been demonstrated, and Europe should do more to assist these States dispose of materials and prevent their weapons scientists from leaving. The US is helping through the Cooperative Threat Reduction program, though certain Nunn-Lugar assistance will be frozen unless there is certification, or a waiver from such certification, that Russia is complying with arms control agreements.

The Bush administration has reversed its lukewarm attitude towards CTR since the events of 11 September, and is now seeking substantially higher funding for it in its 2003 budget request as well as much larger European contributions to this effort. The US is considering a proposal whereby it would continue to support CTR with US$ 1 billion a year for ten years if Europe and other countries contribute the same amount. Since this is a large amount for other countries to match--even if the amount is small compared to what is allocated to national military defence--perhaps different countries should think instead in terms of supporting projects of interest to them. For example, France could work on plutonium, the Nordic countries on attack submarines, Germany on chemical weapons, etc. Further, the idea of debt for security swap could be discussed in the EU Parliament. Europe could also cooperate not just through assistance, but also through industrial cooperation. Europe should take a leadership role in this fundamental endeavour, for if materials are diverted to e.g. Iran or Iraq, they pose a threat to all. They could end up in Europe rather than in the US.

The EC could agree to include research on nuclear, biological and chemical disarmament in the Framework Programme in order to assist Russia, Kazakhstan--where so many nuclear weapons were tested--Ukraine or others to destroy their large arsenals of WMD. Closer cooperation and common action are needed. Further, the EU Parliament should develop an energy strategy for the re-use of plutonium and uranium, though some partners prefer to immobilize it. The

Parliament has been trying to put together a joint action with Russia, called the Nuclear Disarmament Cooperative Initiative (NDCI).

Most States would not find biological weapons to be ideal for use in a battlefield situation because they have a delayed effect. This very character might on the other hand make it a most suitable tool for terrorists. A scenario, developed during a NATO workshop in February 2002, of some suicide terrorists who inoculated themselves with smallpox, travelled on a commercial plane, followed by a train or metro, contaminating 60 to 80 percent of the fellow passengers. All would be contagious for about 15 days without visible symptoms. Within weeks thousands of people would develop symptoms and start to die from this disease that has been eradicated from the planet since the 1970s and that has no treatment or cure. Should we re-introduce vaccine certificates on passports? Can we develop filters in the plane air conditioning system that would prevent the virus from spreading? Would people wish to apply the solutions used recently in Europe for foot and mouth disease to other human beings in order to address smallpox?

There is no verification arrangement for the Biological Weapons Convention (BWC), and although States spent six years trying to negotiate a protocol, it is believed that this effort did not succeed in part because the pharmaceutical industry suspected it might constrain its activities. By way of contrast, in the negotiations on the Chemical Weapons Convention industry took a leading role. Chemical weapons are exceedingly dangerous and are easier to pack, transport and produce; they are therefore considered more "usable" for military operations. Many believe that States should try again to negotiate a verification protocol for the BWC.

The U.S. has adopted a tougher strategy towards regimes pursuing WMD programs, focusing initially on Iraq. The events of September 11 reinforced the Administration's reliance on defence and deterrence as the primary instruments of non-proliferation policy and on creating political conditions to facilitate this policy.

The Vulnerability of Society

Organized Crime

There is a web of organized crime spanning the EU and reaching far around the world. It involves increasing amounts of drug trafficking, especially synthetic drugs; illegal immigration and trafficking in human beings; financial crime (fraud, money laundering, currency counterfeiting); commodity smuggling; property crime and illicit trafficking of vehicles. It involves groups in particular in Belgium, the Netherlands, and Italy, due to their international characteristics, and ethnic groups such as Albanian (Kosovo), Turkish, Colombian, Polish, Russian, with links to Afghanistan (drugs) and China (illegal immigration, trafficking of human beings). This crime poses political, economic, social and technological threats, and it is linked to terrorist groups.

Tens of thousands of members of thousands of groups control billions of euros each year through organized crime. Organized crime is increasing and it is increasingly international. Homogeneous and heterogeneous groups--often specialized, professional business entrepreneurs--cooperate across borders. Financial crime (fraud, money laundering, currency counterfeiting), commodity smuggling (cigarettes, etc.), violence and corruption are all growing. New types of crime involve cyberspace, credit cards, and child pornography on the Internet. Crime is gaining ground despite the technological and other progress made in countering it, in part because the perpetrators have become increasingly professional. Also, law enforcement agencies are hampered by judicial limitations, lack of familiarity with certain targets, and limitations in availability and sharing of information and intelligence.

Law enforcement is bound by national borders, whereas organized crime is not. There are fifteen judicial areas in the EU, and it has been difficult for the police patrol from one country to follow a criminal into another. This usually results in slow response to the threat from organized crime. It is difficult to identify the targets when the criminals commit crimes in countries other than where they reside, or when criminals engage in activities involving large profits and low risks. Information and intelligence is often not comparable among the members of the EU, and when intelligence is shared it is often based on old or incomplete data. These problems will increase when the EU expands.

An example of possible threat scenarios includes the global container system. The largest hubs of this container system are Antwerp and Rotterdam, where less than two percent of the containers are checked. They could contain weapons, biological agents, terrorists, among other things.

Europol is only 3 years old, and has shown remarkable potential. However, it still needs improved intelligence, surveillance, and border controls. It would be helpful for data banks to be integrated in all member states, because although law enforcement agencies can cooperate on a bilateral basis, it is difficult for them to cooperate multilaterally. In the future Europol looks towards prioritisation, to set long term aims and objectives, coordination, and implementation of guidelines for action.

Germs

In contrast to the large size of containers, five envelopes containing anthrax caused two thirds of the United States Government to shut down, five deaths, and 33,000 people requiring prophylaxis in the fall of 2001. The anthrax attacks revealed weaknesses in the U.S. public health infrastructure, in laboratory and diagnostic capabilities, in communications strategies and in ability to clean up contaminated sites. Yet more is known about bacillus anthracis than other biological agents. If the pathogen had been a contagious agent, it could have crossed borders and spread quickly, along with the accompanying panic. Should quarantines be imposed? If so, who would enforce them? Although sensors have been developed that can detect the release of an agent at the time of the release (used at the Salt Lake City Olympics), these are limited in terms of the number of diseases they can identify and the size of the area to be covered. With bioterrorism we must think locally but act globally. The U.S. 2003 budget calls for an increase by more than 300 percent in spending on biological terrorism, to $5.9 billion.

Research institutions need to look closer into the public health infrastructure, the threat, capabilities, and risks. Europe should consider investing in (possibly in collaboration with the U.S.) research in vaccines, diagnostics, prophylaxis, therapeutics, detection and communication systems, medical laboratories, funding for training, technology development and deployment. Medical education should include studies on how to detect and identify an outbreak, and thus trained epidemiologists are needed to provide scientific knowledge to policy-makers in case of catastrophic situations. Europe, the United States and Russia could establish a joint centre for biosecurity that would bring together the expertise to develop international standards, information sharing, training, strategies for communications, and expand surveillance.

Further, in order to expand civil defence, exercises and training can be conducted (such as the “Dark Winter” experiment last year in the United States) among local and national law enforcement officials, criminal investigators, epidemiologists, etc. Technologies that may have dual-use capabilities should be controlled in order to prevent the proliferation of biological weapons. We need the requisite security constraints for such non-proliferation, while maintaining at the same time scientific freedom and openness.

Noncommunicable diseases are expected to account for 73 percent of deaths worldwide by 2020. Investment in research and medicine can lead to new advances in the treatment for many diseases, such as tuberculosis, malaria and HIV/AIDS. Meanwhile, it must be borne in mind that by the year 2025 there will be 1.2 billion people over the age of 60, and thus the demands on medical services will increase, particularly in the case of a catastrophic event.

Modern technology has brought us the potential of knowing our own genome, and all the ethical consequences are just now being considered. Who owns it? What can and might be done with this knowledge? How do we track diseases and their carriers while also protecting their privacy? Among other ethical considerations, if one must screen for AIDS involuntarily, or register visits to doctors in a data base system, what happens to civil rights, ethical, legal and individual rights, not to mention insurance? Science can endanger certain civil rights and freedoms in democracies. There is a need to call on politicians to endorse new measures in this regard and to launch a regional and international effort to address the questions. The EU Parliament should also discuss these issues.

Critical Infrastructure

Technology has entered every part of society. The technological products are assembled from a growing number of components that come from all over the world. The products, processes and systems are linked to energy, trade, transportation and communication, and thus a small hiccup in one system creates ripples in another, affecting the whole global village.

People have become increasingly dependent on technology, as interdependent networks link food and water supplies, health and medical care, energy, transportation, communication, and finance. Many global systems for early warning, crisis management, rapid response, and information centres, seem to work well; yet cooperation in cyber-security could be improved. The most remarkable characteristic of 11 September was how the shock travelled so quickly through the globally linked system, costing billions of dollars in economic damage through losses in industries such as airlines and insurance, not to mention the political, sociological and psychological dimensions. This combination of interdependent technology and open society has produced a tremendous vulnerability to opponents. The enemy no longer needs bombardments, blockades or special force operation; it can now use small groups to selectively attack our technological networks.

Such threats and attacks must be met with coordinated responses involving police, military, and industry on both a national and international level. The EU, NATO, OECD and others are studying this problem. Strategic security in this regard needs to be approached not just at the diplomatic level. Industry is a crucial part of modern society. The vulnerabilities of this modern society dictate that the critical infrastructures and their interdependence be defined, recognized and protected. Vulnerabilities may range from a global container to the infiltration of a national education system. Some have not been thought of or identified. Nevertheless, we must meet the challenge to define and understand them, to monitor associated signals and be able to respond to an attack.

Natural Hazards

Human beings are affected by phenomena related to the atmosphere, such as hurricanes, tornadoes and drought, as well as geophysical events such as earthquakes or landslides. Natural disasters cause the largest impact on developing countries that do not possess a solid infrastructure, in particular with regard to housing. This creates environmental refugees and social unrest. The costs of disasters are escalating because of the increase in population and population density, growing inequality, an aging infrastructure, and climate change.

According to many assessments there is a 90-95 percent chance that there will be more intense precipitation, a 66-90 percent likelihood that there will be increased summer dryness and risk of drought, increase in tropical cyclones, and spread of disease. The challenge is to anticipate through forecasts and warnings about such events, and adopt standards and codes to protect the infrastructure. Science and technology play a central role in monitoring, detection, prediction and information regarding the forecast of weather, and research is needed to divert disasters. Here too there is an interdependence, and cooperation and exchange of information are needed.

Science for Security

Science and technology issues are at the heart of security needs, and research activities play a crucial role in helping to counter threats to security. The Lisbon European Council of March 2000 set as a goal for the EU to become the most competitive and dynamic knowledge based economy in the world by 2010. In order to achieve this, the European Heads of State decided that it was a top priority to create an integrated European Research Area. This ERA aims, *inter alia*, to promote the coordination and opening of national or regional research programmes, enhance the networking of centres of excellence and support the integration of research capacities.

The new Framework Programme proposed by the European Commission for the period 2002-2006 is based on three principles: concentrating resources on a small number of priority research areas in which EU action can add the greatest possible value; defining activities in a way that will enable them to exert more structure on

European resources; and simplifying implementation conditions. The Framework Programme will have a budget of 17.5 billion Euros. The seven priority areas include: genomic and biotechnology for health; information society technologies; nanotechnology, knowledge based materials and new production processes; aeronautics and space; food safety and health risks; sustainable development and global change; citizens and governance in the European knowledge-based society.

Currently 85 percent of the public expenditure on research in Europe is managed nationally or regionally, which leads to unnecessary duplication of efforts. If the European nations, through the European Union, join efforts and increase civilian R & D investment, the growth in economy in the region will be secured. This presupposes a high level system of education. Furthermore, the military and civilian R & D investment should not continue to be separated, which is wasteful and inappropriate, as dual use technology for civilian and military applications are rapidly gaining in importance.

Europe should focus on new technologies to detect, monitor and control weapons and substances that lead to the construction of weapons. The EU/JRC has contributed technical assistance for the Trilateral Initiative (United States, Russian Federation and the IAEA) to develop safeguards for surplus weapons-grade material, and might continue to do so. The JRC has also been involved in scientific and technological work from sealing bolts to high-resolution satellite imagery and verifying crop acreage through satellite remote sensing, tracking livestock and fishing vessels, and detecting illegal discharges of oil at sea.

The use of satellites has increased dramatically over the years and will continue to do so. Emergency communications links can be established soon after disasters via satellites. The European Space Agency (ESA) Centre National pour Etudes Spatiales (CNES) initiative to programme the satellite and provide satellite remotely sensed data free of charge to areas struck by disasters has been adhered to by India, Canada and the U.S. National Oceanic and Atmospheric Administration. This enhances the chance of a remote sensing satellite being overhead at the time of a disaster. There is also a greater use of information derived from satellites: it can be used for reconstruction of roads, locating sites for refugee camps, and detecting land-use changes to identify possible mined areas, for example. High-resolution satellite data can also be used as an alternative to maps, albeit at a high price, and technology now provides general access to global positioning systems (GPS), where the new European Galileo system will be a significant contribution. Meteorological satellites provide continuous meteorological data that are widely available and useful for predicting bad weather in particular. In the future medical assistance data will probably be transmitted via satellite, and interactive educational programmes will be conducted by satellite. Future prospects for European security include the Global Monitoring for Environment and Security (GMES). Europe does not have as wide a gap with the United States in space activities; its launchers are competitive with those of the US.

As is frequently the case, the users and the providers do not meet or communicate with each other. A centralized clearing house should be established to relay the user requirements to the satellite providers in order to programme the satellite, contact a specialized commercial entity or the military to transform the data into information, and send it to the user. Such competence exists in Europe, however the actors must be brought together, and the operations would need to be financed. A clearing house could collect information on known trouble spots and create a data base of disaster information for Europe and the rest of the world.

While NATO has its own research programme focused on the military aspects of security, the EU research policy, according to the Treaty is the strengthening of the scientific and technological basis of Europe's industry and improving competitiveness. Article 163 states that research programmes can support all policies that fall under the Treaty's competences, if necessary. The EU's Joint Research Centre and ESA have no interaction with NATO and cannot be associated with military issues. Similarly, NATO has very limited contact with the EU. Coordinated efforts would be essential in a catastrophic event. The EU's Joint Research Centre could take on security research, if it agreed to do so; its experience with other European institutes could be used to develop a network with national and international centres of competence in order to work on a European Security Research Policy. The role of the European Parliament as a facilitator for strengthening RTD efforts in support to the Common Foreign and Security Policy (CFSP) of the European Union has been underlined. A first step could be to ask Scientific and Technological Options Assessment (STOA) of the European Parliament to execute a related study.

The EU also needs to develop stricter border controls and more non-proliferation efforts in the former Soviet countries. Further, Europe should use technology to prevent the development of weapons that might use genetic codes to fight racial wars. Because science and technology are no longer reserved by a single nation, the poorest countries are able to build WMD. Therefore, international safeguards and standards, and perhaps even military force, are needed to make countries comply with international law. Science should contribute to the elimination of mass poverty and helplessness in order to help improve security.

Science is crucial to the understanding of the global problems facing US foreign policy, and technology is central to their solution. Possession of superior technology has been the cornerstone of the military preparedness of the United States. Although the technology is plentiful, it is not always simple to deploy it effectively. Thus science and engineering play a central role in producing devices that can in turn become part of practical systems. One exception to this rule is the response to bioterrorism, where the United States believes that further research is needed.

The United States has invested so much in defence and its R & D that it has gained in world dominance. This has military and political consequences for the European partners in NATO. Expenditures on research in Europe are 1.9 percent of the GDP, compared with 2.6 percent in the United States and 3.1 percent in Japan. Part of this can be explained by the fact that the private sector finances 55 percent of R & D efforts in Europe, compared to 66 percent in the United States. The EU hopes to increase its spending on research to reach an average of three percent in 2010. The gap between what the EU spends on military R & D and what the United States spends will reach a ratio of one to five--$54 billion compared with about $10 billion—if Congress approves President Bush's 2003 budget proposal.

In response to the attacks of 11 September 2001, President Bush established the Office of Homeland Security and the Homeland Security Council. One of the 11 policy committees under the Council focuses on biological and chemical threats. In addition, chief science officials in 15 agencies have been meeting to discuss the role of S & T in combating terrorism as well as the contribution industry can make in homeland security. Another entity, the Critical Infrastructure Protection Board was established in October 2001 to recommend policies on emergency preparedness for communications systems and support systems, among other things. A committee for research under this Board promotes research to reduce vulnerabilities and develop technologies that will detect, contain and mitigate attacks against these infrastructures. Cyber systems are global, and some modest US-EU cooperation is taking place in this area. A task force was established in1998 under a US/EU S & T Agreement with the Directorate General for Information Society. Since then there have been a number of conferences resulting in cooperative exchanges between U.S. technical agencies and EU research organizations.

The proposed budget of President Bush calls for a total of about $112 billion in federal research and development funding, with $57 billion designated for Federal Science and Technology. The latter includes activities related to the creation of new knowledge and technologies. The proposed budget includes a total of about $40 billion on homeland defence next year. The portion to be devoted to bioterrorism, $5.9 billion, will focus on infrastructure, response and science; $2.4 billion will be allocated to medical R & D, for rapid chemical and biological identification and therapeutics.

The United States provides an opportunity for developing technology that addresses national problems and future systems for operational dominance of US forces. The Defense Advanced Research Projects Agency (DARPA) is complementary to the R & D provided by the military and is based on quick reaction to urgent national security problems. With a budget of US $ 2,000 million and a staff of 200, it can initiate new programs and technical ideas in short periods of time (weeks to a few months). Often these include high-risk technologies that can revolutionize military systems. Some recent areas of focus include combined manned, unmanned operations, robust mobile communications and networking, microsystems and nanotechnology, and beyond-silicon electronics. Europe would be pleased to have a European Advanced Research Projects Agency (ARPA) for security issues to complement the framework programmes with a quick response to research needs. While Europe has a widespread scepticism of military solutions and insists on political solutions, the US relies on its military precisely because it is so strong.

Conclusions[1]

Our new broader security agenda contains a number of non-military threats to the security of societies and citizens in Europe.

- Our ability to handle non-state actors on a global basis is key to our security. Terrorism has led to the globalization of the security dependency. To create security in Europe we must therefore be prepared to act globally.
- International arms control and disarmament treaties are in danger and no progress is being made in multilateral negotiations. There is a need for European leadership in preserving existing treaties and in finding new fora and new forms for multilateral arms control discussions.

To prevent the proliferation of weapons of mass destruction is important also for Europe. Increased and better coordinated cooperative efforts between the US, Europe and Russia (within CTR and other arrangements) are needed to secure and destruct Russian WMD. Handling the threat of proliferation of biological weapons must be high on the non-proliferation agenda.

- The threat from well organized crime is increasing and requires development of the national police forces and improved European police cooperation. The new role of the police in international peace and security-building efforts is an additional argument for integrating information systems and improving the police.

Science and technology can play an increased role in coping with the new security threats.

- The US has initiated coordinated and large-scale S&T efforts to meet the new threats
- The European Research Area provides the overall vision of closer and integrated cooperation in Europe through new instruments such as Networks of Excellency and Integrated Projects. The Sixth Framework program provides a mechanism for large-scale projects and a fair amount of resources in several related S & T areas. It is essential that research on security related issues also be promoted within those important frames.
- A number of concrete test cases could include humanitarian mine clearance, monitoring of containers, monitoring of maritime trafficking of people, and examining the use of space based tools for monitoring.

Science and technology is likely to provide important input on a number of specific issues. These issues might include the development of S & T to support the work of police forces, interpretation of intelligence information, humanitarian demining, and detection of drugs, explosives and materials of WMD.

Scientists and other experts and the scientific and technological results they have produced have played a key role in shaping our modern societies. Still, it is

[1] These conclusions are not intended to represent a consensus view among participants.

reasonable to assume that we are able to utilize and apply only a small fraction of the results and the knowledge created around the world. To create knowledge and to effectively apply knowledge are two different processes and they need different environments to develop in an optimal way. When we talk about transfer or use of knowledge we talk of a process to bridge the gap between those responsible for European security, the S&T community and industry. The challenge is to find a process by which knowledge that has been created can be shared by many and applied to a variety of problems. What could be the components of such a process? To successfully apply S&T to promote European Security requires a dialogue between those having the problem and those that might have answers.

Introductory Address

by **Bengt Anderberg**, Director general
The Swedish Defence Research Agency, FOI
Stockholm, Sweden

- The security perspective of today and tomorrow is broader than that of yesterday. On the global scale we are moving from deterrence to confidence building, from armed conflicts to crisis prevention and management. Conflicts today occur within rather than between States and non-state actors are playing an increased role**.**

- The role and tasks of our military forces have changed . The focus is more clearly on international joint operation for peace keeping and peace making. Sweden has a long record of participation in international peace keeping operation under the UN umbrella and some 100 000 Swedes have served in UN missions around the world. Recently the scope and size of these international operations have increased and we are now conducting joint operations with larger units and in close international cooperation. These activities and the joint force now being created in Europe is an important contribution to our security.

- The security of each of us depend more and more on our ability to handle non-military crises. The terrorist attacks in New York and Washington are tragic illustrations of the vulnerability of modern societies. Attempts have been made to interrupt an orderly democratic process during the EU summit in Gothenburg and during other similar events.

- The non- military crises can also include organized, more "conventional" crime, trafficking or environmental disasters. In many parts of the world the greatest threats to human security are still famine and disease. We are also facing a growing number of threats to our modern societies of an economic and technical origin. Deliberate attacks on our information systems to manipulate the very nerves of our societies can be launched from any point on earth and by small groups of people.

- Many of these threats confronting us are reflected every day on the front pages of our newspapers. We have, in short, moved from a situation where we were planning to cope with disastrous military confrontation that might occur with a low probability to a situation where we have to cope with a number of threats to our security and safety facing us every day. A challenge in the development of our future security structure is to find a proper balance between the military and the civilian components. How do we spend the resources wisely to cope with this broader spectrum of threats to our security?

- Security has to be considered and actions are to be taken at all levels nationally and internationally; UN has the key role on the Global Scene.

Difficult as it may be to make progress on many global issues today it is essential that we do not give up but try harder. The Security problems we face today are at least partly due to famine, injustice, lack of development, democracy and hope in many parts of the world. Support for democracy and development globally also promotes our own security at home

To enhance security of the European citizen is an important component of the increasing co-operation within Europe. When we develop European Security we have to take into account the joint European perspectives of the European Union and the European Commission as well as the perspectives of the individual States.

- In this workshop we have decided to focus our discussion on some of the key issues for European Security.
  - The vulnerability of the modern societies
    - Terrorism
    - International Crime, Drugs and Illegal Trafficking.
    - “Information warfare”
    - Disaster mitigation

  - Non-proliferation of weapons of mass destruction: nuclear, chemical and biological

  - Disarmament and arms control and confidence building measures

- When it comes to the vulnerability of our European societies it is essential to intensify the activities and the co-operation to identify and assess the different threats to our societies. It is also essential to increase the international co-operation among the national authorities that have to cope with those threats and to improve their tools. Well functioning cross- border information systems is a fundamental basis for such an increased co-operation. There may also be a need to develop additional tools to facilitate the need for our authorities that have to cope with these threats.

- Fear is the main weapon of the terrorists. We have to find ways to increase the trust and confidence in our institutions and authorities and to strengthen our democratic and legal systems also, and especially, in time of crises.

- To strengthen the non-proliferation of weapons of mass destruction is an essential activity to improve the security on a regional and global basis. We must increase our efforts to destroy the large amount of weapons or weapon grade material that exist in many States. In the meantime we have to ascertain that the material is properly accounted for and safely stored. The Cooperate Threat Reduction Program is one important international activity that should be further supported and developed. New tools to improve the safe storage and the destruction of weapons of mass destruction could be a significant contribution to the non-proliferation efforts.

- International negotiations and discussions on disarmament and arms control issues are today essentially stalled in forum such as CD. Given the present limited interest by the US it might be for the Europeans to take the initiative to seek some progress. It could be interesting to explore possible openings on specific Disarmament and Arms Control issues, such as "Cut-Off", from a S&T perspective, in a way similar to what (the Group of Scientific Expert did in the CD on CTB when there were no political development) I was involved in when we provided the scientific and technical groundwork on laser weapons and weapons having Indiscriminate Effects (CCW).

- Arms Control and Disarmament is not only a question of creating new treaties it is also a question to fully implement existing ones. The Ottawa treaty prohibiting the use of landmine is a good example where additional joint efforts are needed to ride the world of the tens of millions of mine that every day kill and injure people and prevent development and economical recovery in many third world countries. To day's activities are fragmented and there is an obvious need to improve coordination to make demining operations more efficient and also to create a market interesting enough for industry to develop and produce new equipment.

- To improve on the European security is not only a question of political will and diplomatic activities. It involves the whole spectrum of actors in our societies, including government agencies, industry and NGOs. To fully utilize the development in Science and Technology could be a most valuable force multiplier in enhancing our security and this is what we are going to address in this workshop. We may then ask the following questions;

  - How can science and technology play a role in promoting security in this new broad perspective? Not as a substitute for political will and action, but as a means to facilitate concrete results.
  - How could we focus our attention on these problems in a way similar to what we have done so far on the military side?
  - How could science and technology make a difference when it comes to confidence building, arms control, international co-operation and non-military threats to our societies

- EU has established a good basis for work in Europe with the new European Research Area and the 6th Framework program. The European Research Area provides the overall vision of closer cooperation in Europe with Networks of Excellency and Integrated Projects as the main tools. The 6th Framework program provides a mechanism for creating large-scale projects and a fair amount of money in crucial S&T areas. We must identify ways and means to use those valuable EU tools to intensify our efforts to use science and technology to improve our security.

- The broader security agenda contains both military and non-military issues. The existing cooperation between European defense communities on R&D within WEAG and the Six Nation Initiative could provide a good basis for work also on non-military issues.(You can develop this) To further develop the "dual-use" concept is an important challenge.

- To proceed with further concrete steps we do not need a “grand plan” for all possible activities. In fact any attempt to create such an overall plan would not only fail but would tie all creative thinking into further paper work rather than into practical activities. It would be more efficient to proceed with a limited number of activities of importance of the European Security. A number of good examples should be created that can be used as models and stimulation for further activities.

- There is a need for new answers to the new challenges. We have to create processes that can provide this input. Processes that are not limited by to day’s operational problems or narrow legal frames, but rather stimulate and promote creative thinking. We are facing a common challenge to create new ideas in interplay between those of us working in implementing security measures and those engaged in S&T.

- We see this workshop as one step, and we hope it will prove a useful step, in a process to further use Science and Technology to support Security in Europe. We hope that additional initiatives could come from actors responsible for, or dealing with, security issues and from institutions working with S&T.

Science and Technology in Support of European Security: A European Research Area Perspective

by **Richard Escritt**, Director
DG Research - European Commission
Brussels, Belgium

Introduction

Minister,

Ladies and Gentlemen,

I should first of all like to thank you for inviting me to this Workshop on "Science and Technology in support of European Security". Commissioner Busquin is unfortunately unable to attend due to other engagements, but he wishes to underline his considerable interest in this topic.

This workshop gives me the opportunity to present to you the perspectives for research for Europe as a whole, concentrating in particular on security issues.

In the first part of my speech, I should like to set out the broad lines of EU research policy, focusing on the concept of the European Research Area, on our efforts to bring it into being and on future opportunities which are opening up with the new Community Framework Programme for Research, which will be devoted to creating the ERA.

In the second part of my speech, I should like to deal with the question of European security, covering both internal and external aspects, by looking at a series of concrete research examples.

Why a European Research Area?

The Lisbon European Council of March 2000 set the EU an objective: to become the most competitive and dynamic knowledge-based economy in the world by 2010. To achieve this aim, and acting on a proposal from Commissioner Busquin, the European Heads of State and Government made creating an integrated European Research Area a top priority.

Why did Commissioner Busquin take this initiative? Because the European research effort is being held back because it is fragmented: 85% of public expenditure on research is managed nationally or regionally, and more often than not lacks coordination.

- The ERA project is based on the simple observation that the current Community programmes and initiatives, which are essentially aimed at promoting transnational cooperative research activities, are not enough to increase the efficiency and overall effects of the European research effort.
- Despite recognised excellence in a number of areas of science and technology, Europe is today at a turning point. We have to pull ourselves together quickly, otherwise we will fall further behind, including in the areas of excellence I have just mentioned.

There is a simple and overwhelming reason for this: every year, the United States pours billions of dollars more than Europe into investment in research. This gap is on the increase and is now in the region of €100 billion. In Europe, research expenditure accounts for barely 1.9% of GDP, compared with 2.6% in the United States and 3.1 % in Japan.

- This shortcoming is essentially due to a lack of private sector investment, which accounts for nearly 90% of the investment gap between Europe and the United States. In Europe, only 55% of R&D efforts are financed by industry, against 66% in the United States. The figures are even more alarming considering US budget forecasts for 2003.
- This is why Commissioner Busquin has proposed an objective that can mobilise Europe: to increase what Europe spends on research to reach an average of 3% of GDP in 2010. The Barcelona European Council has just endorsed this objective, which concerns all countries and all regions. The idea is not to require all countries to reach 3% in 2010 but to create a growth momentum in which all countries must participate.

  Industry will have to play a key role in achieving this objective as it should be capable of financing about two-thirds of R&D, as is the case in the United States and in the most advanced EU countries, instead of 55% at present.
- But a simple quantitative approach is not enough as most public sector research efforts in Europe are organised at national level. The European research system is compartmentalised and its efforts fragmented. All too often, this leads to unnecessary duplication of effort and prevents the achievement of a critical mass. The disparities between the national regulatory and administrative systems also hamper transnational transfers of knowledge and the mobility of researchers.

What are the broad objectives of the European Research Area?

- The aim of the: ERA, in short, is to create a "single market" for research, researchers and knowledge, an area in which research and innovation stakeholders, be they individual researchers, universities, research centres or firms, can define their strategies and operate without constraint at European level. Future Member States are directly concerned. They are fully involved in a process that will support their integration into the EU. Other European countries are also concerned and associated in this effort. From the simple point of view of cooperation, the ERA is a means of furthering integration on a global scale, thus contributing to security in Europe.

The Commission has defined a coherent set of objectives and action lines, addressing the various dimensions of the ERA and involving the use of a panoply of financial, legal and policy coordination instruments. They have been endorsed by the Council and the European Parliament and warmly welcomed by the scientific community and industry, which have been widely consulted. The nine thematic objectives of the ERA are:

- To promote the coordination and the mutual opening of national or regional research programmes and associated programmes in areas requiring the mobilisation of resources at a level not possible in a single country on its own, notably clinical trial platforms for malaria, AIDS and tuberculosis, and aeronautics.
- To enhance the networking of centres of excellence and support the integration of research capacities. We are all aware that research relating to security issues is very often linked to high technology or to the frontiers of science, be it the prevention of technological risks or the fight against certain forms of organised crime. To attain this objective, initiatives have been taken in relation to networks of excellence, which I shall come back to later, and in relation to the mapping of excellence in Europe. The first round of mapping focuses on specific fields in biotechnology, nanotechnology and economics. The information provided by this mapping exercise will in particular help policymakers to assess existing research capacities.
- To carry out comparative studies of national research and innovation policies in the EU.
- To increase human resources and their mobility.
- To enhance the protection and use of intellectual property.
- To intensify interactions between research and innovation.
- To define a European approach to research infrastructure in Europe.
- To stimulate investment in research (benchmarking of tax measures, promotion and coordination with the EIB).
- To address "Science and Society" issues differently.

The new Framework Programme:

- For its part, the next Framework Programme for Research and Development (FP), the principal financial instrument of Community research policy, has been designed to ensure that Community research activities have a more "structuring" effect on European research than is the case at present. And while it is a civilian programme, the new FP will not exclude defence sector `players. All research laboratories can play a crucial role in the context of the FP and the creation of the ERA.
- The FP has become a key point of reference for policymakers, but also for the scientific community and industry, which have been widely consulted and have expressed their views at length: It has given rise to a whole

series of novel initiatives; it has knock-on effects on the national research systems.

By definition, the Framework Programme cannot by itself make a reality of the European Research Area, but it can make a substantial contribution.

- The new Framework Programme proposed by the Commission for 2002-2006 was specifically designed with this aim in mind and is based onthree main principles and objectives:

1) concentrating resources on a small number of priority research areas in which EU action can add the greatest possible value;
2) defining the activities and instruments in such a way as to enable them to exert a more structuring effect on European resources;
3) simplifying and streamlining implementation conditions.

Among the instruments of the new Framework Programme, the networks of excellence and integrated projects will play a central role in the structuring effort. They are complementary instruments and both will normally involve cooperation between universities, research organisations and industry.

- The purpose of a networks of excellence is to strengthen excellence and to stimulate gradual and lasting integration of research capacities existing or emerging in Europe. Each network should aim at advancing knowledge in a particular area by assembling a critical Mass of skills.

  The activities concerned will generally be multidisciplinary and aimed at long-term objectives, not at achieving predefined results in terms of products, processes or services. The joint programme of activities will focus on research and include integration support activities as well as activities for spreading excellence outside the network. The EU's financial contribution will take the form of a grant for integration to complement the members' own financial resources. The grant will be calculated as a percentage, usually 25% of the value of the resources to be integrated.
- Integrated projects, on the other hand, are designed to have a stronger impact on industrial competitiveness or to contribute more effectively than many Community projects to resolving major social problems. Each Integrated Project must have clearly defined objectives in terms of scientific and technological progress and results applicable to products, processes or services.

In principle, they will comprise a set of specific components or subprojects addressing different aspects of the research needed to achieve their common objective. In addition to research and demonstration activities, they may include other activities related to their objective, such as training.

The EU's financial contribution will take the form of a grant, covering up to 50% of the project's budget. For some bodies, in particular public bodies, the EU's contribution could cover up to 100% of the additional cost they have to bear.

- In both instruments, the participants will havea large degree of autonomy in the management of the project and the flexibility to adapt their plan of activities and the composition of the consortium by replacing or adding new partners.

The overall budget earmarked for the Framework programme (the FP respectively for EC and Euratom combined) is €17.5 billion, of which €16 270 million have been allocated to the EC programme. The Sixth Framework Programme for Research is made up of three complementary blocks of activities:

1) The first block, with a budget of some€13.3 billion, aims to further the integration of European research in seven thematic priority areas; the major networks of excellence and integrated projects will be implemented under this block and will become the leading activities of European research. This block will also provide support for any new research needs required for the development of EU policies.[2]
2) The second block, with a budget of some€2.6 billion, aims to structure the European Research Area by strengthening the EU's research infrastructure network, encouraging the mobility of researchers, furthering Europe's innovation capacities and improving links between science and society.
3) The third block has a budget of some €330.million, to be used for less costly, but nevertheless extremely important, actions aiming at strengthening the foundations of the European Research Area through activities such as benchmarking policies, mapping European networks of excellence, technology foresight and other accompanying initiatives.

The Sixth Framework Programme (which has been sent to the European Parliament for a second reading under the co-decision procedure) should be adopted in June 2002, as the Heads of State and Government had intended at the Barcelona Council.

Science and technology in support of European Security

- Security in Europe is a major political problem, and measures taken to address security-related issues should be equal to what is at stake; they should also be consistent with the actions of organisations responsible for security matters such as the Organisation for Security and Cooperation in Europe (OSCE), NATO, and the Council of Europe which, together with the European Union, make up Europe's institutional architecture for security policy.

[2] For **your information, here** is the list of the seven thematic priority areas:
- Genomics and biotechnology for health - Information Society technologies.
- Nanotechnology, knowledge-based materials, and new production processes Aeronautics and space.
- Food safety and health risks.
- Sustainable development and global change.
- Citizens and governance in the European knowledge-based society.

- Following the events of l. l September 2001, we are facing increased fears of terrorism and war. The latest Eurobarometer public opinion survey (No 56) reveals that 86% of European citizens personally fear terrorism (+12 points compared with a survey conducted a year earlier), 79% fear the proliferation of nuclear, bacteriological or chemical weapons of mass destruction (+17), and 64% a world war (+19).
- Also, it has to be said that in some cases, scientific progress itself has led to the creation of high technology systems which are vulnerable to terrorist or non-terrorist threats. I am thinking in particular of the vulnerability of banking systems or communication networks, which is directly attributable to the vulnerability of computer systems.

It is therefore quite clear why both the current geopolitical situation and scientific progress lead us to reflect on the links between science and technology on the one hand, and security on the other.

Before talking about science and technology, let us first define what is meant by security. The term covers both external and internal security issues.

I am mainly going to talk about the issue of civil protection, which is an internal security aspect, but first let us say a few words on external security, which will be discussed at length at our first round table.

- External security, as terrorist attacks have shown, is closely interlinked with internal security. The EU's Common Foreign and Security Policy (CFSP) is one of the pillars of European construction, and one of its components, European Security and Defence Policy (ESDP), is a political challenge but also an economic, industrial and technical one, since Europe has set itself ambitious targets in terms of military capabilities. The Headline Goals of 2003, and the ensuing European Capability Action Plan (ECAP) of November 2001, focus in particular on military equipment, such as means of transport and intelligence. The long-term achievement of these objectives will make it necessary to strengthen the Industrial and Technology Defence Base (ITDB) in Europe, and in particular to carry out R&D in the defence sector. Several Member States are already considering changing their policy in this connection, but budgetary resources are limited.

These budgetary resources for defence research appear all the more limited since the gap between what the EU spends on military R&D and what the USA spends is set to widen and will reach a ratio of 1 to 5 - $54 billion compared with approximately $10 billion - if Congress approves the Bush administration's 2003 budget proposal.

In other words, the USA currently spends some $26 000 per soldier (budget of $331 billion) whereas the EU only spends $4 000 per soldier. The interoperability of means is threatened in the long-run. The danger of this budgetary gap is that it will create a gulf between Europe and the United States and will strain the transatlantic link which is so essential to European security.

In this context, it should be pointed out that the civilian and military sectors support similar research efforts in technical areas that are sometimes very close to one another, such as aeronautics, space and telecommunications. To ensure that resources are managed more efficiently, the civilian and military sectors should be decompartmentalised, and they should learn more from each other.

As regards internal security, the situation is very different, and in certain respects more alarming, as there is no common internal and security policy as such. We are confronted with a multitude of complex issues and problems which are difficult to solve, such as:

- the prevention and management of natural disasters and technological risks, in other words crisis management in the broad sense;
- the security of computer networks used in financial systems, banks and insurance companies, and communications security (we cannot do without the Internet);
- counter-terrorism, including security in transport, and the security of buildings;
- the prevention of organised crime;
- conflict prevention, in particular the fight against the proliferation of weapons of mass destruction (including export controls on arms and disarmament). In a wider context, border controls and controls of water points are other examples relating to security. At international level, the detection of minefields is still a sensitive issue.

In the short term, measures taken to solve these problems are either political or legislative in nature. Political measures cornprise, for instance, including network security as one of the five priorities of the 2005 eEurope plan, as decided at the Barcelona Council. Examples of legislative measures are the Council directive on dual-use goods, or Commission Directive No 96/82/EC called the Seveso 2 Directive.

Very often, the actual implementation of these measures falls within the ambit of science and technology because of the specialised scientific expertise it involves. Part of the work of the European Commission's Joint Research Centre is to provide such scientific and technological support to the Directorates-General of the Commission.

To illustrate this point, let us take the example of the control of radioactive and nuclear materials. The task of verifying and controlling the nonproliferation of these materials is undertaken by the Commission's European Safeguards Office (ESO) under the Euratom Treaty, and by the International Atomic Energy Agency (IAEA) under the Non-Proliferation Treaty. The Joint Research Centre (JRC) provides scientific and technical expertise to the ESO and the IAEA. Several JRC institutes conduct research (for instance in the field of tests and measurements) to improve the way in which control and verification activities are carried out in relation to the non-proliferation of weapons of mass destruction. This research is conducted within the framework of one of the oldest

European research networks, the European Safeguards Research and Development Association (ESARDA), created over 20 years ago.

I could have chosen humanitarian demining as a similar example. Several EU Member States have signed the International Test and Evaluation Programme for humanitarian demining (ITEP), and the EU has drawn up a common position on the fight against anti personnel landmines which was adopted by the Council and the European Parliament in July 2001. This means that there is a real need for specific JRC expertise, in particular in the area of multi-sensor detection. Research activities are therefore absolutely essential if such expertise is to be successful. Mr. Wilkinson, the Director of the JRC's Institute for Health and Consumer Protection (IHCR), will talk about this in more detail tomorrow afternoon.

- In the long term, and because of the technical nature of the issues involved, it is also essential to invest in research financially. R&D investment is not a substitute for the measures we have just mentioned, but it enables instruments to be developed which will in future directly contribute to resolving these issues.

  Let us consider a typical example: the EU's initiative on Global Monitoring for the Environment and Security (GMES). The technical objective of this initiative is to create an instrument which will improve the way satellite data is analysed and managed. The political objective is to increase the EU's decision-malting capacities in major areas such as the environment and civil security. Satellite observation can be a powerful tool in decisionmaking, but it requires considerable investment. The work undertakten by the Commission and the European Space Agency, in cooperation with the Member States, has shown that developing this instrument will require long-term work on a European scale so as to fulfil the needs of all European users in a globalised environment. Important research needs have already been identified and research projects will start to receive support under the next Framework Programme (particularly in relation to the collection, analysis and use of such data).

- There should also be a debate, in the field of research but also in a wider context, on ethical and legal questions, for it is sometimes difficult to reconcile the need for security with individual liberties.

A case in point is the use of DNA markers and the exchange of DNA test results, which have to take account of previous rules adopted by the Council on the protection and transmission of personal data.

This is an issue which is relevant in a number of areas, at the frontiers of science and society. Discussions should also tackle the issue of governance, and how to make use of resources and instruments which exist in other organisations such as the European Investment Bank.

As we have just seen, the European Research Area offers an appropriate framework for these discussions.

Conclusions

I should like to stress that all research activities have a crucial role to play in helping to counter security-related threats: the research activities themselves of course, both upstream and applied, but also activities such as providing continual training, transferring technology from one sector to another, connecting the various research areas (thus encouraging decompartmentalisation), and as we have just seen, engaging in cross-cutting discussions.

I have tried to show that science and technology issues are at the heart of security needs. The ERA has brought some solutions by creating a number of different legal and financial instruments capable of , addressing existing security needs and emerging needs in the most advanced high-tech areas.

I believe the ERA has set the right framework for action.

There is therefore no doubt that research, and particularly the next FP, will contribute to finding solutions to many security-related problems. Some of these still need to be defined, and that will be the task of this Workshop.

Before I close, I should like to underline the topicality of the Commission's current work by mentioning bioterrorism.

In the wake of the events of 11 September and the threat of bio-terrorist attacks, the Ghent European Council called on the Council and the Commission to draw up a programme to enhance cooperation between Member States in the fight against biological and chemical terrorism. This programme was presented in a Commission Communication and focuses on setting up a common strategy for civil protection. An essential component of this programme is the mobilisation of Europe's research potential. Both the Laeken Council in December 2001 and the Barcelona Council in March 2002 called on the Council and the Commission to finalise this programme.

On a proposal from Commissioner Busruin to the Research Council of Ministers, a working group made up of representatives from the Member States has been set up, as a preliminary to any operational initiative. The work, which will be monitored jointly by DG Research and the JRC, will concentrate on research issues relating to the detection and identification of biological and chemical agents, and the treatment of the effects of chemical and biological attacks. Against this background, the working group has drawn up an inventory of research activities, and is examining how these activities can best be mobilised and coordinated. It is also trying to identify:

- what gaps there are and what additional research is needed in the short and long term, taking account of the opportunities provided by the new framework programme for research;
- the activities and programmes of the JRC, which Mr Wilkinson will talk to you about tomorrow; and
- initiatives taken by the Member States in this area.

Some activities have already been identified as needing reinforced EU-wide coordination. They include in particular the development of instruments for the detection, early diagnosis and reliable surveillance of pathogens, and research on methods for producing and distributing existing or new-generation vaccines for emerging or re-emerging diseases.

The Commission has also examined, with the Member States, how these activities can be developed thanks to the new instruments available under the Sixth Framework Programme. As we have seen, this FP contains relatively flexible mechanisms capable of catering for both short and medium term research needs and longer term fundamental research requirements.

After the last meeting scheduled to take place on 16 May 2002, a final report will be adopted and subsequently presented officially by Commissioner Busquin at a forthcoming Research Council.

Today's Workshop is particularly topical. Because of this and thanks to the participation of high level speakers over these two days, I am sure the Workshop will contribute valuable input to the ongoing discussions. Thank you for your attention.

Science and Technology Support for U.S. Homeland Security

by **Dr. Mona Dreicer**, Director
Office of Nuclear Affairs, Verification and Compliance Bureau
U.S. Department of State

Introduction

I would like to start by telling you how honored I am to be here and then to relay that Secretary Powell's Science and Technology Adviser Dr. Norman Neureiter's regrets not being able to attend this important meeting. I know that he considers this a subject of utmost importance and is very sorry he could not participate.

Science and technology have clearly been among the principal determinants of change and agents of progress, particularly in the modern era since World War II. Possession of superior technology has been the cornerstone of our military preparedness. In virtually all facets of United States 21st century foreign policy, science is indispensable to understanding the global problems that we face, and technology is central to their remediation.

September 11, 2001 was a wake-up-call. Despite a decade of national security studies that pointed to increasing asymmetric threats to the continental United States, we had no real homeland security strategy in place before 9/11. Now we are in a protracted process of correcting this fundamental weakness, although the social, bureaucratic and financial hurdles are enormous. Science and technology pervade the many fronts that must be considered in homeland defense, and harnessing the collective national scientific expertise is considered to be critical for long-term success.

We need to improve tools to prevent, detect, protect, and treat victims of chemical biological, radiological, nuclear, and conventional terrorist attacks, as well as develop new and improved tools to recover facilities from those types of attacks, if they ever occur again. We are not starting from zero in this enterprise. We have much relevant technology already at our disposal, but the challenge is to deploy it effectively. Science and engineering have critical roles in turning known phenomena into devices and in building devices into practical systems. In many cases a system approach rather than simply perfecting a single instrument or device is what is needed.

The single greatest exception to this rule is in response to bioterrorism, where we believe that additional research is needed on the mechanisms of disease likely to be exploited. You will see how this is reflected in U.S. research and development (R&D) budget decisions.

I would like to start out by providing an overview of how the U.S. government has looked to science and technology in responding to existing needs for civilian protection, and then present some aspects of the 2003 budget proposed by President Bush, as it relates to research and development in this area.

Federal Government Response

On October 8 of last year, the President signed an Executive Order establishing the Office of Homeland Security (OHS) and the Homeland Security Council (HSC). Former Pennsylvania Governor Tom Ridge is the Assistant to the President for Homeland Security. He coordinates all efforts of the executive branch to prevent, detect, protect, prepare, respond, and recover from terrorist attacks inside U.S. borders.

Under this Council there are 11 Homeland Security Council Policy Coordination Committees (PCCs) that generally meet at Assistant Secretary level. There are six "Senior Directors" of OHS, including one for R&D. That position is filled by the OSTP Assistant Director for National Security. Over 100 different specific objectives have been identified to assess R&D programs. For example, in a review of R&D objectives for bioterrorism, a subgroup considered categories relevant to: personal protection, collective protection, detection & measurement of bioagents, recognition and characterization of covert biological weapon exposure, decontamination, vaccines and therapeutics, psychological effects, information systems, modeling simulation and analysis, and device disablement.

Overall, OSTP has executive and legislative mandates to coordinate federal science and technology activities, and therefore, is in a position to call on organizations, internal and external to the federal government, to provide support to the OHS and other offices responsible for aspects of the war on terrorism. For example, active information sharing and identification of areas of possible cooperation between agencies was facilitated by calling together the chief science officials in 15 agencies to discuss the role of S&T in combating terrorism. OSTP also has responsibility for coordination of technical support on issues such as mail security and baggage inspection at airports.

Under the OSTP's already established National Science and Technology Council, an Antiterrorism Task Force has been formed to address the following broad issues:

- Biological and Chemical Preparedness
- Social, Behavior and Educational Policies
- Radiological, Nuclear and Conventional Detection and Response
- Protection of Vulnerable Systems
- Rapid Response Action

These groups will deal with emergencies as they arise and serve as a clearinghouse for technical reviews of research and development proposals for technologies related to homeland security.

NGO Actors in U.S. Homeland Security

There is essentially a "virtual science corps" that can help make these Federal networks stronger and more effective. This can be achieved by the creative use of existing public and private sector mechanisms. OSTP has been meeting with umbrella organizations such as:

- The American Council on Education for effective and rapid communication to the higher education sector,
- The American Association of Universities for direct access to leaders of institutions that perform most of the nation's federally sponsored research,
- The National Association of State Universities and Land Grant Colleges – to link to the public universities that carry out important research and extension services throughout the nation.
- The National Academies for Science, Engineering and Medicine – who also provide access to the national research community. They have formed a committee to interact with federal agencies on terrorism
- Professional Societies (American Physical Society, American Chemical Societies, etc.) who have been willing to designate a point of contact on terrorism issues.

S&T Adviser Neureiter has also actively established links to the external S&T community in support of the State Department's offices of Counterterrorism, Political Military Affairs, and Consular Affairs. Each office has responsibilities related to homeland security, but no traditional relationships with the academic and non-Federal scientific community.

The President's Council of Advisors on Science and Technology (PCAST), co-chaired by OSTP Director Marburger and E. Floyd Kvamme, a Silicon Valley entrepreneur, can be used to facilitate private-public sector communication on these homeland security issues. The 22 Council members, appointed by the President, come from industry, academia, and other non-governmental organizations to advise on science and technology research priorities. In their first meetings this year, PCAST established a subcommittee to address science and technology to combat terrorism, and the supporting role that private industry can play in homeland security. This subcommittee is chaired by Ralph E. Gomory of the Alfred P. Sloan Foundation.

Cybersecurity – Keystone of Critical Infrastructure Protection

One area that I would like to address explicitly is information security, an area that the State Department has been actively involved. On October 9th President appointed Richard Clarke as Special Advisor for Cyber Security and a member of the OHS, and on October 16th a Presidential Executive Order established the Critical Infrastructure Protection Board responsible for recommending policies and coordinating programs that relate to protecting critical infrastructures. Secretary Powell named Undersecretary of State for Arms Control and International Security, John Bolton, as his representative to this Board.

The Board established several standing committees - the one for research and development, chaired by OSTP, is particularly relevant to this meeting. Some 20 federal departments and agencies participate in this committee. It's objective is to ensure that U.S. critical infrastructures are "trustworthy" and "resilient". This committee promotes and coordinates research to reduce vulnerabilities in the nation's critical infrastructure and to develop technologies that will detect, contain and mitigate attacks against these infrastructures. Many of the critical infrastructure protection problems that face the U.S. are not unique. Because cyber systems are global – we all face the same problems – so international S&T collaboration and coordination is essential.

A Task Force was established in 1998 under US/EU S&T Agreement with the Directorate General for Information Society. Since that time there have been a number of workshops and conferences resulting in cooperative exchanges between U.S. technical agencies and EU research organizations.

Proposed 2003 Budget

The President's 2003 proposed budget calls for a total of approximately $111.8 billion in federal research and development funding, with $57 billion designated for Federal Science and Technology. FS&T is defined as activities central to the creation of new knowledge and technologies more consistently and accurately than the traditional R&D reported. It accounts for nearly all of the federal basic research, over 80 percent of federal applied research, and about half of civilian development.

Over the past year OSTP and the Office of Management and Budget have worked with Federal Agencies and the science community to identify top priorities for federal R&D, allocated over the 20 agencies. R&D areas requiring multi-agency approaches specifically related to homeland security are: information technology, noted as a "critical" area (proposed $1.9 billion for a multi-agency Networking and Information Technology Research and Development Program), and nanotechnology, noted as an emerging area, that has a broach range of benefits in information technology, low-maintenance materials, biotechnical applications, and innovative solutions for detection and protection from Nuclear/Biological/Chemical agents (proposed $679 million across 9 agencies in 2003).

The budget document also cites a newly recognized need for multi-agency, anti-terrorism R&D. The proposed 2003 budget focuses upon improvements in information systems, operational costs for homeland security (combat air patrols, for example), first responders, and shortfalls in stockpiles of equipment, vaccines and other health measures. In many cases, this requires outright purchases of commercial, off-the-shelf technologies and services. As a result, multi-disciplinary R&D required to anticipate new threats – 3, 5 and 10 years in the future – must be more systematically addressed in the next budget cycle. Multi-agency and cross-budgetary information is being compiled by the National Science and Technology Council for this purpose.

All told, the White House has proposed to spend almost $38 billion next year on homeland defense to prevent another September 11th.

Defending against bioterroism will focus on infrastructure, response, and science for a proposed budget of $5.9 billion. $2.4 billion will be used to jump-start the research and development process needed to provide the medical tools from basic research in areas such as rapid chemical and biological identification and therapeutics. The remainder will be spread across many different government agencies over the broad range of homeland security issues.

Some Agency highlights on proposed R&D related spending to address our homeland security challenges are as follows:

- National Institutes of Health – increased funding to expand research on the effects of bioterroism attacks and develop treatments in the event we are attacked again. $1.75 billion for bioterrorism research includes genomic sequencing of dangerous pathogens, development of improved anthrax vaccine, and laboratory and research facilities construction and upgrades related to bioterroism. Z-chip technology research can provide us with the ability to identify a vast number of molecular signatures and be used on the front line of medical response for nearly instant diagnosis of a wide array of biothreats or naturally occurring diseases.
- National Science Foundation – $27 million for basic research programs in microbe genome sequencing and the transmission of infectious disease, two areas important for combating bioterrorism.
- Department of Energy - $3.1 billion for R&D that sustains the safety, reliability and performance of U.S. nuclear weapons and $283 million for nonproliferation and verification research in the areas of advanced technologies for detection of nuclear weapons proliferation, nuclear test monitoring, and chemical and biological response.
- Department of Defense – $5 billion in the FS&T budget. Including, research and development of technologies and systems that address terrorist threats: improved detectors of chem/bio threats (both remote and on-site), protective gear, vaccines, and surveillance systems.
- Environmental Protection Agency - $75 million for research into technologies and procedures to cope with future biological or chemical incidents by decontaminating buildings were bioterrorism agents have been released.
- Department of Transportation – safety of the U.S. transportation infrastructure, $95 million for aviation security technology research.

In general, the U.S. is in the first phase of establishing a comprehensive homeland security strategy. This will require a protracted approach to look for ways to improve on current capabilities, as well as make significant qualitative improvements with R&D to pursue more fundamental breakthroughs in the mid- to longer terms. We need a R&D program that is balanced between rapidly adapting off-the-shelf technologies into effective systems and doing basic research that can introduce new ideas, particularly as multi-disciplinary approaches will be required to develop solutions and countermeasures.

Since terrorism is a global threat, it compels us to work together to combat it. Fortunately, the tradition of scientific and technological cooperation between our nations is strong, so we are well prepared to move ahead on this new, common objective. We have some lessons to offer in this process, but also much to learn from you. I will be interested in hearing, over the course of the next two days, about how the E.U. is thinking about approaching these issues, and seeking other avenues of cooperation that might be considered.

Brief Points from an EU Perspective on the New Security Agenda

Speaking notes[3]

by **Lars-Erik Lundin**, Head of Unit Security Policy
Euopean Commission
External Relations Directorate-General
Brussels, Belgium

1) Vital to work for conflict prevention at all times, even if there is a necessity to plan for possible military intervention, as in the ESDP. At the same time, there is an obvious need to look ahead at security requirements if and when conflict prevention fails.

2) When discussing the industrial-technological base for such re

3) quirements, it is appropriate to look towards 2015-2020. Even if, for instance, defence-related industries such as BAE and EADS today hold a strong position in comparison with their U.S. competitors, this will not necessarily be the case in a longer time perspective.

4) The cognitive structure of security elites has changed over the last 30 years, with the energy crisis, the end of the Cold War, the wars on the Balkans, 11 September, etc. Some argue that we now see significant differences between U.S. and European perceptions. Europeans seem (with the exception of some countries and regions of Europe plagued by terrorism) to feel themselves less of a target in terms of security. The Europeans seem to be looking more towards possibilities of conflict prevention and conflict resolution in their international policies.

5) Americans often argue the need to move ahead in terms of meeting new security requirements. Military deterrence is not seen as enough, nor integration policies as a way to create areas of stability, interdependence and development. At this point a capability is required to identify those groups and individuals that refuse to accept normal standards of civil society and "to go after them", if necessary to eradicate them.

6) Europe has for its part responded vigorously to 11 September through its 69 point roadmap spanning a wide range of actions, from increased airport security to enhanced relations with Pakistan. The 69-point plan also includes items such as a common arrest warrant, a common definition of terrorist acts, freezing of assets, etc. But Europe does not accept the death penalty. Europe furthermore requires a respect for the United Nations and international law. Individual, cross-border accountability for terrorist acts is for Europeans intrinsically linked

[3] The views of the author do not necessarily reflect those of the European Commission.

with a simultaneous respect for human rights, the rule of law, including individual integrity in terms of data protection, etc.

7) To enable enhanced co-operation between the EU and the US in the fight against terrorism, a further rapprochement on these issues of principle needs to take place.

8) In terms of the role of science and technology for security it is, in this context, obvious that the new requirements pose a dual challenge. In the search for methodologies and technologies to enhance individual accountability, it will also be necessary to improve methodologies to protect individual integrity.

9) Threat perceptions in Europe are not identical with those in the U.S. To some extent this is natural. Most Europeans are fortunate not to feel that they are targets of terrorism or military threats. As noted above, it is prudent to assume that Europe in a longer-term perspective may fail in one or the other of its conflict prevention policies. It is therefore vital to retain a solid technological-industrial base, including a research base, which can serve the needs that later may be defined by Europe.

10) The European Commission has no direct role in military affairs. Still, it is concerned, given the ever-wider concept of security, and particularly the security of citizens as one of its main priorities for 2003, in parallel with enlargement. The annual work plan of the Commission contains a long list of actions which will serve this goal, ranging from civil emergency planning to justice and home affairs, environmental security, transport and energy security, cyber security, demining and (in general) international assistance. The sixth Framework Programme for research, the European Space strategy etc. are all powerful instruments to enhance long-term capabilities in fields relevant primarily to civil security. Of fundamental importance in this context is that extensive and highly relevant work is being carried out in contexts normally not associated with security. A case in point is the link between the work in the public health sector on protection against communicable diseases and bio-terrorism.

11) One word about EU-NATO- relations in this context. The increased political will for EU and NATO to compare notes in areas where both are engaged is to be welcomed. There is also a pragmatic co-operation with NATO in the Balkans. The parallel enlargement processes of the two organizations are also of fundamental importance for both. Obviously, it will be important for ESDP to reach agreement on the assured access to NATO planning assets soon. I know that the worry of duplication between NATO and EU efforts has been voiced both in this seminar and elsewhere. It will be important for those EU member States that are engaged in both organizations not to allow serious duplication to occur.

12) One word also about space co-operation. I believe that it is important to use the right language when discussing future European ambitions in security-related space areas. The European public opinion is likely to be wary about ambitions of the U.S., both in terms of content (missile defence) and funding levels. The

Commission is working hard with the industry to come up with a balanced perspective for July of this year in the context of the STAR 21 Advisory Group.

13) European ambitions in the area of non-proliferation and disarmament of weapons of mass destruction need careful review, not least in view of the upcoming G-8 Summit, and not least as regards Russia. Politically acceptable methods of dealing with the various dangerous substances and weapons need to be defined and realistic funding solutions found. It is already clear that a fundamental responsibility rests with Russia itself in this regard.

> *"The golden age of global negotiations in the Geneva-based Conference on Disarmament (CD) is probably over, because the CD has become too inflexible for managing complex trade-offs among large numbers of countries."*[4]

A Complex World Needs Complex Security Strategies

by **Jan Foghelin**, Head of Division
Division of Defence Analysis
Swedish Defence Research Agency (FOI)
Stockholm, Sweden

Lessons learned from arms control regimes

There seems to be a widening gap between Europe and the USA concerning lessons learned from arms control regimes. In Europe we tend to emphasize the positive effects of the control regimes e.g. non-proliferation and stability. The USA, especially the new administration and as a result of 9-11, criticize the regimes for its failures. Failures mainly in the area of inability to stop proliferation of WMD. Moreover, in a changed world US does not believe that ABM, START etc are important for stability.

A lack of engagement from the US side in arms control regimes is seen as a problem from the European side.

The new world (dis)order

During the cold war the main concern in global security policy was preventing a major war between USA/NATO and SU/WP. The main objectives for arms control regimes were to contribute to the stability between the superpowers.

The situation changed with the end of the cold war. Stability between major powers is still of great concern but many other security policy problems are also very important.

[4] Thomas Bernauer: Warfare: Nuclear, Biological, and Chemical Weapons (p. 611) in P.J. Simmons & Chantal de Jonge Oudraat (Eds.): Managing Global Issues - Lessons Learned. Carnegie Endowment for International Peace. Washington, D.C. 2001.

Two important changes in the world order deserve to be mentioned particularly:

- The different types and numbers of actors of interest for security policy have increased e.g.
  - states (increasing number, many types)
  - international organizations
  - multinational private enterprises (of importance for proliferation of technology)
  - NGO
  - non-state actors (e.g. terrorists, organized-crime organizations)

- The spread of technologies which could be used for violence.

It is easily realized that the old arms control regimes are not sufficient in the new world (dis)order. Problems of course arise when important actors are not participants (or under control of participant) of arms control negotiations.[5]

Organized violence can be used by states, ethnic groups within states, and other non-state actors. This is historically nothing new. What is new is that means potentially available to different types of non-state actors could be very dangerous to states. Dangerous means of violence have successively become privatized.

What can be done?

Arms control in the new world serves many purposes:

- contribute to stability between states
- contribute to more humanitarian forms of violence/warfare
- reduce terrorism
- hinder proliferation of weapons/weapon technologies.

In a complex world mixed strategies are necessary. The old arms control regimes still serve important purposes. Possibilities to adapt them to changing conditions should of course be taken into consideration.

It is however not sufficient with the old arms control regimes. Measures have to be taken directed especially towards non-state actors. The whole chain from preventive measures to use of force in preemptive actions could be used.

There seems to be a difference in emphasis on different means between Europeans (preventive actions, civilian means) and Americans (preemptive actions, military means). This can be seen as a problem. It can however also be seen as an opportunity. Europe and the USA can be seen as complementary e.g. in the war against terrorism.

[5] There will be problems in each of the steps of agenda setting - negotiation - implementation and compliance - reactions to noncompliance.

Science and technology can give important contributions to a safer world.

Examples of important areas:

- intelligence
- verification with new means
- non-proliferation in a new world
- new technical means for the police
- destruction of weapons
- detection of dangerous materials.

What Role for Arms Control in the International Security Context of the New Century

by **Bernard Sitt**, Director for International Security
Affairs Commissariat á l'Energie Atomique, CEA/DAM
Bruyères-le-Chatel, France

Ladies and Gentlemen,

It is a great pleasure for me to be in this country and in this beautiful city, as a person, as a French and as a European, and it is an honour to address such a distinguished audience. I want to thank the Swedish Ministry of Foreign Affairs, and also particularly Ola Dahlman, for inviting me to participate in this meeting on issues of major importance and to give an introductory talk on the r61e of Arms Control in the international security context of this new century.

I guess you will allow me to make the usual disclaimer that my views do not necessarily represent those of my institution, and are strictly mine at this stage.

Arms Control is such an old concept, and so much has been said and written about it, since its invention in the fifties, that there would seem to be nothing really new to say. I was recently at the 12th International Arms Control Conference in Albuquerque, where we heard many elaborate and up to date analyses concerning the present state of affairs and the new strategic framework that is being implemented by the United States, especially in its relation with Russia. And really, I do not know what else I could add, except maybe this: I belong to the category of long term optimists in Arms Control ; but as far as the short and medium term mechanisms and trends are concerned, in my view, new ideas and arguments are obviously still needed. And in this regard, a specific european contribution would certainly be able to bring some new substance to the overall debate and to have some significant influence in terms of shaping policies.

Before I get to my main points, let me try to recall, in very global terms, the historical successes and failures of Arms Control in the recent past.

To accompany the end of the Cold War, we have witnessed what I like to call a golden decade » for Arms Control, characterized by a wealth of instruments, both bilateral and multilateral, with sometimes very sophisticated and very technical verification regimes, from 1986 to 1996 (1986 being the historical Reykjavik Bush-Gorbatchev Summit and 1996 being the year of the opening for signature of the CTBT and, in between, the MTCR and the INF treaty in 1987, the CFE treaty in 1991, the START I treaty also in 1991, the US-Soviet joint unilateral initiatives, essentially on SNF, also in 1991, the START II treaty and the CWC in 1993, not to mention the NPT prorogation for infinite duration in 1995 with the adoption of the Decision n 2 on the Principles and Objectives of nuclear non-proliferation and disarmament).

Afterwards, what has marked and accompanied the end of the post-Cold War period is unfortunately an era of strategic doubt marked, in the bilateral realm, by the stalemate of the START process that actually followed the promising decisions of the 1997 Helsinki Summit and, in the multilateral realm, by the persistent deadlock of negotiations and discussions at the Disarmament Conference in Geneva.

And above all, this uncertain period has been ended in a tragic way by the massive terrorist attacks of September 11, which demonstrated the irruption of a new category of strategic threat, with non-state actors having the form of invisible networks without territory, without political identity, and without rules of the game, and therefore offering no possibility of dialogue and negotiation.

And now, to-day, in the context that I just mentioned, we have in addition the new american strategic framework, that has led some observers to announce the twilight (not to say the death) of Arms Control, and the advent of a new era with a general pattern of mistrust regarding a number of existing instruments of strategic stability and, as a consequence, an era with inherent unpredictability.

In order to contribute to the debate and to the thinking of a renewed and constructive vision, which should be pragmatic and well-founded, I would like to make a few remarks along four lines of thought, that is to say regarding four generic questions:

1. From our experience of the cold war and post-cold war context, what do we think are the essence and the fundamentals of Arms Control, and what are its basic objectives ?
2. What may be its fate in the foreseeable future, and under what form would it continue to play its role (and by the way, do we need a new definition for it)?
3. What are the challenges that Arms Control shall have to meet in the post-post-cold war era (i.e. the post September 11 era)?
4. How could Europe, as a political and scientific and technological power, play a role of its own and be a strong actor by effectively contributing to the resolution of international security issues, in its own region and in other regions of the world where it has prestige, potential influence and strategic interests ?

I would like to address these questions rather briefly, and in so doing I take the risk of oversimplifying things, but my objective here is only to underscore some fundamental ideas.

As far as the first question is concerned, to start with, we should never overlook the fact that, since the Westphalia Treaties which ended the Thirty Years War in Europe in the middle of the 17th century, and quite probably for some centuries to come, the actors of Arms Control are nations-states with a well defined identity, a territory, a population, a political leadership, and military, scientific and technological capabilities. Of course, particularly during the 20th century, new non-state actors, such as various circles of expertise and NGOs have come into play, but that does not change the basic institutional role of the key actors.

Now, regarding these nations-states, it should be obvious that national security interests have always been the ultima ratio of Arms Control, which naturally emerged over history as a basic component and as a way of implementation of foreign policies.

What Arms Control has been up to now is an overall security system, both global and regional, based on the negotiation and implementation, between sovereign states, of treaties of arms limitations or reductions or elimination, which may be legally or politically and technically binding, with specialized verification regimes, and with the objective of providing transparency and predictability. The permanent function of such a sophisticated system is, in theory and in practice, to establish and maintain a stable strategic relation, whose balance may of course evolve in any positive or negative direction.

This subtle architecture has been over the years complemented by some other instruments such as export control regimes, confidence-building measures, unilateral initiatives, etc., which may be less legally-binding but nevertheless may have a significant political importance in the field of non-proliferation of massive destruction weapons and of sensitive technologies.

What can be derived then, and almost by definition, is that Arms Control will take the ways and means that will be best adapted to the regional or global geopolitical and security context of each state. By way of consequence, Arms Control will always simply reflect the current state of relations between a given country and its political and strategic environment and has never been and will never be ahead of the political context of foreign relations.[6] Arms Control works when conditions are fulfilled, when there are appropriate political and military needs and readiness. When more disarmament and more control means more security for all parties, agreements turn out to be easy to reach. In this respect, one very demonstrative example among others was the transition from START I in July 1991 to START II in January 1993. As a final comment on this point, I would like to say that the question as to what arrives first, treaties or improvement of political relations, is not a real one: we actually have a self consistent process where both go intimately together.

Let me now turn to the second question. From what we have just seen, which by the way tends to prove that there exists somewhere an intangible definition of Arms Control, we may infer that the basic mechanisms of Arms Control will only continue to work, as an inevitable instrument of strategic dialogue,[7] whether on a confront-

[6] Note that this remark is also valid in the world of multilateral relations. To take a particularly revealing example, the present dead-end situation of the Disarmament Conference is basically not a consequence of any supposed inability to amend itself. It is rather due, among other factors, to a bilateral US-China confrontation on the prevention of arms race in outer space, which may simply reveal more fundamental strategic issues. After all, in a not too distant past, the CD managed to negotiate two fundamental and very complex instruments, namely the CWC and the CTBT, which represent essential international norms, and is still potentially able to do the same in other fields if and when the outer political context becomes more favorable.

[7] In any context, bilateral and multilateral fora will always play an essential role for the expression and exchange of declaratory policies.

ational or on a cooperative mode. The purely abstract scenario of no Arms Control is actually a scenario of conflict between states.

Now, my sense is that the new Arms Control framework will be, just like the old one, a strategic bilateral or multilateral relation seen as a slow dynamic process where each actor will adapt its level of force in view of

- a gain for its own security,
- a gain in political status.

What about verification and control regimes? Let me recall that the most elaborate ones, technically and in terms of intrusiveness, are products of the "golden decade", that is to say of a post-cold war mood. In the present context, where tensions have been reduced, and where distrust has been replaced by an interest in cooperative security, the approach to Arms Control instruments should logically become both more flexible[8] and more adapted to the urgency and technical nature of the threat under consideration.

But whatever the issue, one should just not confuse the underlying principles and rules of Arms Control on the one end with the mode and context of their application on the other end.

As far as existing instruments are concerned, their fate is certainly not linked to the conditions which prevailed at the time of their negotiation, but rather to the possibility to adapt them to a changing strategic context. States will be flexible if the instruments themselves are flexible.

And moreover, confidence building will always be an objective that only Arms Control can reach.

I think I can now deal with the third question. The September 11 attacks did not eliminate the preexisting threats of proliferation of weapons of mass destruction, because they certainly did not change the determination of proliferating countries to pursue their programs. They just added a new category, due to their origin and nature, to the way they were designed using ordinary technologies, to the fact that they have deliberately given a massive dimension to private violence.

Therefore we are faced with one big political and technical challenge: How to deal with a threat that is not amenable to any cooperative work and that comes from non-actors, either by amending and possibly reinforcing existing agreements and control regimes if they can be amended, or by negotiating new ones? Can we evaluate or improve the efficiency of already existing agreements and regimes for preventing or detecting terrorist actions? And, as far as technologies are concerned, can we identify those that need to be developed?

[8] Which is what seems to be the case in the current US-Russia strategic nuclear reduction talks.

Of course the task ahead is immense, and requires a great deal of political will and technical effort, and initiatives of stronger international cooperation between police operations and appropriate intelligence gathering and analysis. It seems that some actions have already started, for instance, for the IAEA as far as nuclear materials and technologies are concerned. But this is just a modest beginning in view of the risks that everyone can perceive after September 11.

As far as the fourth question is concerned, I just said that we have a real need. We all know that having one good idea is an exceptional chance, but knowing the extreme importance of the challenges we have to face as seen from Europe, I would like to try two propositions beyond the current Arms Control business.

But I have a preliminary question first: Do Europeans need their own instruments, or does it suffice that they are part of global instruments on a national basis? It may be so in some cases, but here I would tend to make the strong statement that, if a multipolar world is to ever exist, a prerequisite is that Western Europe is one of the poles. And why not apply to

Arms Control and the associated fight against terrorism the fashionable saying: "Think globally, act locally".

Therefore, very quickly, one or global "and one of local" suggestion.

1. We could have a concerted initiative at the CD to have a new item on its agenda, something like a new ad hoc group of discussion or negotiation on "Reduction of terrorist threats by Arms Control". This may seem to look like an unthinkable revolution, but it could greatly contribute to save its life and its future, and it may have a chance to gather some consensus, at least among Europeans, among the P 5 and in the Western Group.
2. Thinking about what was accomplished up to a recent past, and Ola Dahlman knows a lot about it, by the Group of Scientific Experts (GSE) who worked, under some CD guidance, on the development of appropriate technologies to verify a Complete Test Ban Treaty, I would suggest the creation of an EGSE, a European GSE, which would have to make an inventory, including an assessment of the efficiency of the existing instruments with respect to terrorism and to identify the existing technologies and the needs in the field of prevention and surveillance and detection of terrorist activities and action. After all, one might consider that the ESDP could need and greatly benefit from such a group, which of course could associate at some stage interested experts and partners from outside.

We need vision and pragmatism, let us think about it.

Thank You.

Use of Modern Technology in Humanitarian Crisis

by Ambassador **Martin Dahinden**, Director
Geneva International Centre for Humanitarian Demining
Centre International de Deminage Humanitaire - Geneve, Switzerland

The problem created by the use of landmines is one of the major humanitarian challenges of our time. Removing landmines in a safe way is today very costly and dangerous for those involved. There is no doubt that science and technology could play a more important role in creating a safer environment for mine clearers and for affected populations which would have a significant impact on crisis response, postconflict rehabilitation, on the return of refugees and on long term social and economic development.

I am aware that landmine technologies are for most of you a highly esoteric topic. I therefore will not focus on specific technologies or solutions but on the lessons learned that are in my view also useful for other areas. To respect the time credit given I will limit myself to a series of key points.

Before investing in a new technology, it is important to know what can and what should be solved by the introduction of this technoloy. This statement may seem simple, but very often investments are made in the wrong areas. In the field of demining there is enthusiasm about robots. However it is the detectors and other working tools that are missing - not the platforms on which to put them.

It is important to know what technology can do and what it cannot. Too often researchers strive for technically interesting silver bullet solutions without having an in-depth knowledge on how the new technology needs to interact with other technologies already in use, the working environment and with existing practices.

The research community has often very specific interest not necessarily aligned with donor wishes. Particularly where public money is involved, and market forces discounted, it is important to know what you get from the money in real terms. You may find you are funding specific researcher's interests, or subsidising commercial activities that will create benefits in other areas.

It is extremely important to involve users from the beginning. The word users and not experts should be emphasised. Even though this seems trivial, it does not happen enough and can prove to be quite difficult, because researchers and users very often have distinct experience and perceptions, different interests and even speak a different "language" as well. Communication and dialogue between users and technologists is not easy but vital if the development of technology is to be driven by field demand rather than industrial pressure.

Providing the right technology is in most cases a step-by-step process rather one self-contained project. Trial and error is important, as are powerful feedback mechanisms. For those funding projects it is important that the research and development process is steered by user needs in an efficient and inclusive way. Normally, policy makers are not the best qualified to manage such a process, but it is their responsibility to make sure that it happens.

Information technology is paramount. To have the right information with the right people at the right place is not only decisive for emergency operations, but also for long-term effectiveness. Information technology and the templates it creates are powerful instruments for co-operation, for the development of common perception and language. This is why the Geneva Centre has developed the IMSMA system for the area of mine action.

Exploit and improve existing technologies before inventing new ones. There are many advantages in further developing existing technologies. It is normally less expensive and less unpredictable in outcome. In many areas investments in cutting edge technology can be too costly to be considered, or development time would be too long. It is therefore important to have an overview of promising existing technologies.

Do not hesitate to look for new technologies in other, and even remote, disciplines. Most scientific innovations come from people new to an area, from people working in the margins of a discipline, or across several different disciplines. When staff members of the Geneva Centre told me about contacts with Belgian scientists specialising in rats I was puzzled at first. Now I am convinced that rats have an enormous potential in becoming a powerful and cost-effective mine detection tool.

Beware of people who pretend to know everything and who claim to be the most experienced. The protagonist in Graham Greene's novel "Our man in Havana" made his career with the motto "never learn from experience". I would not commend you this motto, but experience is not only a source of knowledge, it can also be a deterrent to innovation.

Assess the collateral risks of technology. Much modern technology is or has the potential to become dual-use technology. Geographical Information Systems are decisive for humanitarian relief operations, but some of them can easily be transformed in systems with military purpose, such as missile guidance. This could be the case with many other technologies. Pay attention to this, or you might be forced to withdraw technology or to restrict its use for security reasons. But also remember that a military use can be found for even the most humanitarian of technologies, and vice versa.

Pay particular attention to the sustainability and vulnerability of technology. Technology is very often developed in an advantageous environment, mostly in industrialised countries with a permanent access to expertise, qualified labour or infrastructure. This is often lacking in the areas where the technology will be used. The simpler the solution, the less vulnerable the technology will be.

The European Union Dual-Use Export Control System after 11 September: Is there a Need for Reform?

by **Ian Anthony,** Dr.
Stockholm International Peace Research Institute, SIPRI
Stockholm, Sweden

Introduction

During the 1990s the European Union gradually became more engaged collectively in the effort to reduce the risks of proliferation of nuclear, biological and chemical weapons. The individual EU member states are all signatories to the NPT, BTWC and CWC and have an obligation to ensure that they are in compliance with all aspects of these treaties. Export controls are one instrument that can increase confidence that legitimate trade is not contributing to nuclear, biological or chemical (NBC) weapon programmes. In 1994 the European Union established a common regime for controlling exports of dual-use items (items developed for civilian use that can be used for military purposes).

Events that occurred on and after 11 September 2001 increased attention to threats that are different in kind from those that the nonproliferation regime was developed to address. The fact that international transfers of dual-use items could contribute to illegal weapon programmes was brought home by the discovery that European suppliers had contributed to the clandestine nuclear and biological weapon programmes discovered in Iraq. It is now of vital importance that the EU member states reduce the risks that they could contribute, unintentionally and unwittingly, to the emergence of new threats.

One new dimension of the threat was the direction of attack (launched from within the target state). Subsequent operations have provided evidence that has strengthened the concern that non-state actors have actively sought to acquire a range of unconventional weapons. The non-state actors involved include, but probably are not confined to, members of the Al-Quaeda terrorist network. Such developments do not mean that the original threats have diminished in importance. However, it is necessary to review whether the basic premises on which existing instruments, including the export control system, rest are still valid. The current EU dual-use export control system aims to facilitate trade in dual-use goods where the risk that such trade will contribute to the illegal weapon programmes *of states* is considered acceptable. The system was not designed to take into account conditions where non-state actors seeking, for example, a biological weapon capability are already located and operating within the European Union.

Apart from the changing threat environment, the European Union continues to develop both its legal form and its geographical scope. In 2000 the European Union reformed the dual-use export control system. The legal basis for the system was changed so that the system is now fully part of the supranational common commercial policy. As part of the ”first pillar” there is an exclusive right of initiative for Commission in further reform of the system. At the same time, critical operational decisions are still taken at the national level, with limited Commission participation

In Nice in December 2000 the European Council decided to try and complete accession negotiations before the end of 2002 with those countries that are ready. While all of the existing EU member states participate in all of the multilateral export control regimes, this is not the case as regards the candidate countries. After enlargement items on the lists agreed within multilateral regimes will move freely (without the need for a licence) within the internal market, including to end-users in states not currently participating in multilateral export control regimes. The questions of how the enlargement of the European Union will affect the implementation of both the EU dual-use export control system and the wider non-proliferation regime has become a somewhat more urgent consideration.

Overview of the existing system

In 1994 the European Union established an export control system for dual-use goods that divided responsibility for different aspects of export control between the intergovernmental EU and the European Community, which was created through several treaties.[9]

The initial stimulus for the creation of the system was a complaint by the Commission that existing national export controls prevented the completion of the European single market by introducing restrictions on the movement of goods and technology between EU countries. The creation of an internal market was a legal requirement stemming from the Single European Act that entered into force in July 1987.

In 1991 the states that formed the European Community signed the Treaty on European Union at Maastricht.[10] The European Union not only extended the scope of activities of the European Community within existing policy areas but also extended the activities of the EU into new policy areas. The implementation of a common foreign and security policy (CFSP) forms one new policy area; development in the area of justice and home affairs forms another. In these new areas EU cooperation has a more intergovernmental character. The Commission does not have the same enforcement rights with regard to either the CFSP or justice and home affairs that it exercises in the area of commercial and trade policy.

[9] The treaty establishing the European Coal and Steel Community was signed in Paris in 1951. The treaties establishing the European Community and the European Atomic Energy Community were signed in Rome in March 1957. The European Community is a supranational arrangement. Community law is directly applicable in each of the member states and the Commission of the European Communities (hereafter the Commission) has the right to enforce this body of law, including through prosecutions of member states before the European Court of Justice. All EU documentation can be found at the EU Internet site, URL <http://europa.eu.int/>.

[10] Excerpts of the treaty are reproduced in *SIPRI Yearbook 1994* (Oxford University Press: Oxford, 1994), pp. 251–57.

In setting up the dual-use export control system in 1995 this complex internal arrangement was reflected in the decisions taken. Responsibility for aspects considered strategic in nature was deemed to fall under the CFSP and was reserved to the legal competence of the intergovernmental EU. At the same time the elements of the system related to the internal market were elaborated separately. These aspects were identified in the Council of the European Union (hereafter the Council) adopting two texts on 19 December 1994.[11]

When the export control system entered into force on 1 July 1995 it was recognized to be a first step that would lead to future adaptation. The Commission monitored the implementation of the dual-use export control system during its initial period of operation and drafted a proposal for a new European Community regulation that would, if adopted, replace the existing system.[12]

After discussion, the EU member states accepted almost all the modifications proposed by the Commission and drew up a new regulation that was agreed on 22 June 2000 as Council Regulation (EC) no. 1334/2000, setting up a Community regime for the control of exports of dual-use items and technology.[13] This regulation changed the legal framework, operational aspects and scope of application of the dual-use export control system.[14] Regulation 1334/2000 repealed Council Regulation (EC) no. 3381/94. On the same day the Council also took a new decision that repealed Council Decision 94/942/CFSP.[15] This brought the system entirely within supranational Community law rather than dividing legal competence between the

[11] Council Decision 94/942/CFSP and Council Regulation (EC) no. 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods. The Council of the European Union is composed of 1 representative at ministerial level from each member state, who is empowered to commit his government. Council members are politically accountable to their national parliaments. The EU dual-use export control system is described in Anthony, I., Eckstein, S. and Zanders, J. P., 'Multilateral military-related export control measures', *SIPRI Yearbook 1997: Armaments, Disarmament and International Security* (Oxford University Press: Oxford, 1997), pp. 345–63.

[12] European Commission, Proposal for a Council Regulation (EC) Setting up a Community Regime for the Control of Exports of Dual-Use Goods and Technologies, COM(1998)257 final, Brussels, Aug. 1998. The basic elements of the review are described in Anthony, I., 'Multilateral weapon and technology export controls', *SIPRI Yearbook 2000: Armaments, Disarmament and International Security* (Oxford University Press: Oxford 2000, pp. 667–87.

[13] Council Regulation (EC) no. 1334/2000 22 June 2000. The regulation (which, as Community law, is directly applicable in all member states) entered into force on 28 Sep. 2000.

[14] Directorate General I External Relations: Commercial policy and Relations with North America, the Far East, Australia and New Zealand, 'Proposal for a new regulation regarding the export of dual-use goods: main issues', Press Release, Mar. 1999.

[15] Council Decision repealing Decision 94/942/CFSP on the joint action concerning the control of exports of dual-use goods, 00/402/CFSP, 22 June 2000.

European Community and the EU. The dual-use export control system is now accepted to be an element of the European Community common commercial policy established under Article 133 of the Treaty of Rome and not an element of the CFSP.

At the same time, EU member states are still sensitive about policy areas that directly affect their security and still remain bound by treaty-based non-proliferation and disarmament commitments. These factors led to the inclusion of an article in the new regulation clarifying responsibility for authorization of dual-use exports.[16] Under Article 6 of the regulation, the competent authorities of the member state where the exporter is established grant authorization for all exports for which authorization is required except those that are authorized by a Community General Export Authorisation.[17]

The Community General Export Authorisation is available for exports of specified items and exports to specified destinations. The specified items are all of the items on the dual-use control list that forms Annex I to Regulation 1334/2000 except for subsets of items listed in Annex II, part 2 to the regulation (made up of Annex IV together with some additional items). The specified destinations (a so-called 'white list') are listed in Annex II, part 3, and consist of 10 countries that are legally bound by all relevant non-proliferation treaties, cooperate in informal multilateral export control via participation in the various regimes and are considered to have national export control systems of a high standard.[18]

The implication of this arrangement is that most trade in dual-use items with the 'white-list' countries can be controlled using a general authorization with no risk of contributing to prohibited nuclear, biological or chemical weapon (NBC) programmes or missile programmes of concern.

Items listed in Annex II, part 2, may not be exported to white-list countries or to any country outside the European Community under a general authorization. As for intra-community trade, items listed in Annex IV remain subject to controls.[19] However, Annex IV is divided into two parts. For items listed in part 1 of Annex IV, member states may use a national general authorization to control the movement of items to other member states. For items listed in part 2 of Annex IV (items that could be considered the most sensitive for non-proliferation purposes) member states may not grant national general authorizations for intra-Community trade.

Two effects flow from these measures. First, the regulation underlines the fact that export of dual-use items is seen as a privilege (that could be withdrawn if necessary

[16] Article 6 of Council Regulation (EC) no. 1334/2000 (note 5)

[17] Article 6.2 of Council Regulation (EC) no. 1334/2000 (note 5)

[18] The 10 countries are Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland and the USA.

[19] Article 21 of Council Regulation (EC) no. 1334/2000 22 June 2000 established conditions under which authorization could be required for intra-Community trade to ensure that these controls were consistent with the obligations of member states under the legislation establishing the European single market.

through a new decision by EU member states) rather than a right exporters enjoy under Community law (which the member states could not withdraw). Second, trade with the white-list countries—which include many of the most important EU trading partners—should be simplified for exporters. Exporters have to keep records of all such transactions according to specifications laid out in the regulation. However, exporters do not have to apply for individual authorizations prior to export. Therefore, while licensing procedures are not simple (the regulation itself is a complex document), they have been simplified.

The 1994 European Community regulation introduced an end-use or 'catch-all' principle into the national export control laws of many EU member states for the first time. The catch-all principle provides a legal basis for controlling items that are not on control lists. The 2000 regulation extended its scope.

Export control systems have generally been based on lists of items subject to control. However, on occasion, governments have considered it desirable to be able to control the export of items that do not appear on existing control lists. Export control authorities occasionally become aware of an item that is not currently controlled but that is or could be used in a way that would be inconsistent with the objectives of export control policy. The inconsistency may reflect the fact that an existing but uncontrolled item is being used in a particular way or it may reflect the development of a new item that was not previously available. Rather than waiting for a review of the control list, it may be useful to have a legal instrument subjecting this item to control with immediate effect. The principle creates an obligation on an exporter to seek the permission of the responsible authorities before exporting any item to a particular end-user or for a specified end-use whether or not the item appears on a control list.

The 1994 EU catch-all obligation related to exports to destinations or end-users known to be associated with NBC weapon programmes or associated missile delivery system programmes of concern. The 2000 regulation extended the obligation to two additional types of export: cases related to the implementation of arms embargoes, and cases related to exports that support or are associated with illegal or illicit exports.

Under Article 4.2 of the 2000 regulation, authorization is required for any item (whether or not included on the dual-use control list) exported to a destination subject to an arms embargo decided by the EU, the Organization for Security and Co-operation in Europe (OSCE) or the UN Security Council if the exporter has been informed by the competent authorities in the member state where he is established that the items are intended for military end-use.

Military end-use is defined in the regulation as: (*a*) incorporation into military items listed in the national military equipment or munitions list of member states (military list); (*b*) use of production, test or analytical equipment and components therefor, for the development, production or maintenance of military items in the military list of member states; and (*c*) use of any unfinished products in a plant for the production of military items in the military list of member states.

Under Article 4.3, authorization is required for the export of any item (whether or not included on the dual-use control list) if the exporter has been informed by the competent authorities in the member state where he is established that the items 'are or may be intended, in their entirety or in part, for use as parts or components of military items listed in the national military list that have been exported from the territory of that Member State without authorisation or in violation of an authorisation prescribed by national legislation of that Member State'.[20]

Article 5 gives member states legal discretion to introduce a national requirement to introduce export controls on items that are not designed or adapted for military use for reasons of public security or on the basis of human rights considerations. This allows the use of restrictive trade measures on non-military items to be applied according to a new set of criteria, namely in support of human rights policy.

The new regulation also modifies the customs powers of member states. The previous export control system allowed an individual member state that considered a particular export to be contrary to its essential foreign policy or security interests to prevent those items from leaving the European Community through its customs space, even if the export had been authorized by another member state. In the new regulation this right is taken away and a member state concerned about a particular export is instead required to halt the export temporarily while consultations take place with the state that authorized it. If this original authorization is confirmed, the export takes place. In essence, the member states now agree to recognize one another's export licensing decisions without exceptions.

In another modification to administrative cooperation, the new regulation makes clear that, when authorization for an export has been denied, member states are obliged to share that information with the Commission as well as with one another. Previously, whether to share this information with the Commission was at the discretion of member states. The Commission complained that this made it impossible for it to make a comprehensive evaluation of the dual-use control system—a task that it is obliged to undertake.

Under the 1994 regulation a member state was obliged to consult bilaterally with a member state that had previously denied authorization for an essentially identical export before authorizing that export (the so-called 'no-undercut' principle). Under the new regulation this obligation is retained and supplemented with a requirement that, if an export is authorized in spite of a previous denial, the member state that makes the authorization must inform all other member states and the Commission, providing 'all relevant information to explain the decision'.[21]

The new regulation introduced changes in the approach towards updating the control lists that form a key element of the dual-use export control system. Before June 2000 these lists were of three kinds: a list of items subject to control, a list of destinations and a list of guidelines. With the decision to move the export control

[20] Article 4.3 of Council Regulation (EC) no. 1334/2000 (note 5).

[21] Article 9.3 of Council Regulation (EC) no. 1334/2000 (note 5).

system fully into the European Community domain it was not possible to maintain these lists as Council decisions to be taken in the framework of the CFSP.

The new regulation establishes that the control lists will be updated 'in conformity with the relevant obligations and commitments, and any modification thereof, that each Member State has accepted as a member of the international non-proliferation regimes and export control arrangements, or by ratification of relevant international treaties'.[22] Amendments agreed in the various treaties, regimes and arrangements will now be translated into European Community law through usual EC procedures.

The list of guidelines that were published as Annex III to the Council Decision concerning the control of exports of dual-use goods (94/942/CFSP) of 19 December 1994 contained factors to be taken into account by member states in deciding whether or not to grant an export authorization. These guidelines are incorporated into Article 8 of Council Regulation 1334/2000.

A final modification to the dual-use control system is the inclusion of an obligation to control exports of so-called transfers of technology. For the first time, Council Regulation 1334/2000 includes as part of the definition of an export 'transmission of software or technology by electronic media, fax or telephone to a destination outside the Community'. Authorization is now a legal requirement for exports of dual-use items using intangible means.

Implementing the reformed system

The Commission participates and enhances information exchanges and administrative cooperation with member states licensing authorities. It also chairs the Coordination Group established to enhance best practices. However, the reforms introduced in the export control system included the adoption of certain instruments that are new and untested in the European context. It would be very surprising if implementation difficulties have not been encountered. Four aspects in particular stand out as being in need of evaluation.

First, the use of the new licence (the Community General Export Authorisation). How is it being used in practice and how it is viewed by export control authorities and industry? How well does the cooperation between national and community institutions needed to evaluate the system function in practice?

Second, the application of the catch-all provisions, including the extension of end-use controls to items that relate to conventional weapons when exported to countries subject to a EU, OSCE or UN Security Council arms embargo.

Third, and perhaps most challenging, how have the controls of intangible transfers of technology been implemented for exports outside the European Community? It should be noted here that Joint Action 2000/401/CFSP (same date of adoption and OJ) concerning the control of technical assistance related to certain military end-uses, including oral transfers, when there is movement of persons and provision of this technical assistance outside the Community.

[22] Article 11 of Council Regulation (EC) no. 1334/2000 (note 5).

Fourth, while the system is established in community law, it is enforced at the national level. Member states are obliged to lay down penalties in cases of infringement and these penalties are to be effective, proportionate and dissuasive. The way in which member states have interpreted these obligations should be compared along with the means used to investigate suspected violations.

Issues for further consideration

As noted above, the establishment of an effective EU dual-use export control system has always been envisaged as a process rather than a single event. Meeting the challenges of implementing the existing system is a significant challenge in the short term. However, if the European Union is to play its full role in nonproliferation further changes to the system should be expected.

Future changes can be anticipated as a result of changes in the threat, in technology and in the constitutional arrangements of the European Union. It should be stressed that none of the ideas presented below are considered fully worked out. However, they indicate directions in which the EU might move in order to contribute to nonproliferation efforts.

The overall objective of the EU should be to create an export control community that feels its work to be an important element of national and international security building rather than a mundane and routine administrative activity. The development of an export control culture can, over time, raise the effectiveness and efficiency of this important instrument.

Relationship to the regimes

One of the main roles of the European Union system has been to translate agreements reached in the multilateral export control regimes into community law. Establishing the dual-use control list that forms Annex I to Regulation 1334/2000 contributes to uniform application of regime decisions through a law applied in all of the EU member states.

The current system can be characterized as ”passive” in that agreements reached in regimes are incorporated into EU decisions the EU plays no role in shaping regime decisions. The question arises whether the EU system should continue to be tied to the regimes or whether it should attempt to play a more active role by presenting initiatives.

Since the EU per se lacks a legal personality as well as the institutions that could lead and implement any initiative within the regimes, a more active role would have to be organized through greater participation by the Commission. At present the Commission is a participant in the Australia Group and an observer in the Nuclear Suppliers Group.

The main emphasis of an enhanced role by the Commission would probably be in the area of list development where smaller member states in particular already find participation in discussions challenging. The Commission would be well placed to use its own resources as well as drawing on technical specialists from member states to develop initiatives that could then be introduced into the regimes for discussion. Over time the Commission would become a centre of technical expertise related to dual-use technology.

The challenge of keeping track of the spectrum of dual-use technologies relevant to regime activities is already significant for many states. However, there are certain items (such as radiological materials) that are not currently subject to export controls at all whose importance for national and international security is currently being debated. Moreover, there are new developments not currently subject to export control for purposes related to national and international security whose security implications are unclear. One example is the rapid development of biotechnology and another is the development of nanotechnology (manufacturing by manipulating atoms individually and placing them exactly where needed to produce micro-machines).

In other areas (items directly related to more traditional military products and the licensing of exports) member states are not yet ready to move away from a system based on national decisions. However, in the area of licensing there are probably also initiatives that could enhance the overall effectiveness of the system. The present system allows for mutual recognition throughout the EU of licences granted by national authorities and allows an exporter to apply for a licence in any member state regardless of the physical location of the goods to be exported.

This common system depends on the information exchange among member states and the Commission related to licence denials as well as a ”no-undercut” provision that requires consultation before one member state issues a licence authorizing an export that is essentially identical to an export that has previously been denied authorization by another member state.

The main requirement for the further development of export controls is a real time community-wide information system that would be available to licensing officers. The system would need to contain information about developers, producers and exporters of controlled items within the EU as well as current information about both legitimate end-users of controlled items and entities known to participate in programmes of concern.

Building such a comprehensive system could facilitate the preparation of a single, common report to regimes about export developments from the EU.

Role in fighting terrorism

As noted above, recent developments have increased attention to changes in the nature of the security threats that may be posed to European states.

There is now free movement of dual-use items that are of potential proliferation concern within the European Union under the Community General Export Authorisation. In conditions where terrorist groups are already active in the EU area, one implication of free movement of dual-use items within the EU could be to facilitate procurement of items for use in illegal programmes. Export control authorities have also begun to think in a systematic manner about how controls can be applied to intangible technology transfers—perhaps the most likely method by which procurement agents will seek to move controlled items out of the EU in a clandestine manner. As a first step, the conditions in the General Export Authorisation should be reviewed with this point in mind to see whether any change is required in the wording or application of the licence.

In thinking about the relationship between export controls and terrorism it is also useful to consider which items (materials, goods and technologies) are relevant, what quantities of these items are relevant and the identity and location of the end-user of controlled items.

Export controls have been developed to control items intended for use in programmes that are state sponsored. The items controlled are associated with known and recognized weapon types. The objective of controls is to prevent the acquisition of militarily significant quantities of these items.

Several characteristics of recent attacks make them different from traditional threats. There was no claim of responsibility for the attacks and no demands were made. The attacks were launched from within the target state (but planned abroad and supported by a transnational network). No items were used that are subject to export controls. However, the distribution of anthrax in the United States during the period immediately after the attacks on New York and Washington on 11 September indicated that non-state actors can gain unauthorized access to dangerous materials. Information gathered in Afghanistan during military operations undertaken subsequent to the attacks on the United States indicated that the Al-Quaeda terrorist network had begun to accumulate materials that could be used in so-called radiological weapons.

The dual-use export control system was never intended to combat such threats. However, there are certain features of export controls that may make them of relevance in constructing an overall response to the terrorist threat.

First, export control authorities (including enforcement agencies) are accustomed to dealing with non-state actors both on the exporting and importing side. Information collection and exchange as well as assessment of the end-use and end-user helps build a picture of programmes of concern as well as providing information about legitimate exporters and end-users.

The experience in implementing the catch-all or end-use controls can be evaluated with a view to considering the application of a catch-all to exports to identified terrorist organizations. This provision might supplement the ”smart sanctions” introduced by the EU in December 2001 intended to freeze the financial assets of identified terrorists and terrorist groups. Incorporation of such a measure would add one more instrument to the range of police and judicial cooperation measures established after 11 September.

The impact of EU enlargement

The organization of a discussion about export control implementation among the EU member states might become more difficult after the accession of current candidate countries. While some of these countries have developed modern export control systems and have a cadre of experts able to participate in discussions, others have not.

Post-enlargement controlled items will move freely to member states that are not members of the multilateral export control regimes. Consideration should be given to whether an attempt should be made from the EU side to ensure that all new candidate countries are members of the regimes at the time of accession.

The new members will be expected to implement all existing community laws, including on export control. Therefore the earlier these countries are engaged in discussions of how the dual-use export control system works in practice the better. In particular the issue of how catch-all controls and controls on intangible technology transfers are applied would be an important issue to discuss.

Final remarks

Prior to the terrorist attacks on the United States there were a significant number of outstanding issues related to the implementation of the EU dual-use export control system in need of closer attention. These issues are no less urgent in the present conditions but new issues have now been raised that also need to be considered.

The discussion of these issues within a Europe-wide network could contribute to the further development of a distinctive European approach to nonproliferation.

Impact of September 11 on U.S. Non-proliferation Policy

by **Gary Samore**, Senior Fellow for Non-proliferation
International Institute of Security Studies, IISS
London, UK

I'd like to discuss the development of U.S. nonproliferation policy from President Clinton to President Bush, focusing on the impact of the September 11 terrorist attacks and subsequent anthrax scare on the Bush Administration's policies to prevent and respond to the proliferation of nuclear, biological, and chemical weapons and ballistic missiles.

It seems to me that September 11 had four main effects on U.S. nonproliferation policy:

First, it reinforced the Bush Administration's pre-existing emphasis on defense and deterrence as the primary instruments of nonproliferation policy and created political conditions that made it easier for Washington to pursue those policies.

Second, it prompted the Administration to seek a new approach towards multilateral arms control regimes, emphasizing compliance with existing treaties.

Third, it caused the Administration to reverse its previous lukewarm attitude towards cooperative threat reduction programs with Russia.

Fourth, it drove the Administration to adopt a tougher strategy towards the so-called rogue regimes pursuing weapons of mass destruction (WMD) programs, focusing in the first instance on Iraq.

Defense and Deterrence

It's important to remember that defense and deterrence first began to assume a greater importance in U.S. nonproliferation policy during the Clinton Administration. In response to the lessons of the Gulf War, missile proliferation, and threat of WMD terrorism, Washington pursued polices to develop theater and national missile defenses, CBW protection for armed forces, and homeland security against WMD terrorism. Some of these measures created great unease in Europe that the U.S. was pursuing a more unilateralist nonproliferation policy that threatened to undermine the multilateral treaty regimes, but the Clinton Administration was also active in pursing traditional multilateral instruments, such as Comprehensive Test Ban Treaty (CTBT) and protocol to the Biological Weapons Convention (BWC).

The incoming Bush Administration clearly identified the proliferation of WMD and ballistic missiles as the primary security threat facing the United States, and advocated missile defense as the most important response to deal with this threat. In particular, many experts on the incoming Bush team had a genuine intellectual conviction that proliferation of WMD and ballistic missiles is widespread and inevitable. In their view, hostile states such as Iraq, Iran, and North Korea are bound to acquire WMD and ballistic missiles (unless the regimes were replaced) and, moreover, these “rogue regimes” cannot be reliably deterred by threats of massive retaliation. In this view, multilateral treaties are at best delaying tactics. At worst, they are dangerous - creating a false sense of security, distracting energy and attention away from the need to strengthen defenses, and providing cover for hostile states to gain access to technology.

Moreover, the Bush team saw some international instruments, such as the CTBT and BWC protocol, as potentially weakening U.S. defense and deterrence capabilities. Whatever value the CTBT had in terms of limiting proliferation was outweighed by the concern that it would undermine the credibility of U.S. nuclear forces. Similarly, the BWC protocol was seen as providing very little value in detecting covert BW programs, while potentially exposing U.S. bio-defense secrets and commercial information.

It wasn’t long, however, before the Bush team realized that its case for missile defense would be stronger – and more likely to be supported internationally - if it was presented as part of broader comprehensive strategy that included traditional nonproliferation elements. Thus, even while the Bush Administration reiterated opposition to CTBT and decided to reject the BWC protocol, it also made clear that it supported existing treaties like the Non-Proliferation Treaty (NPT) and Chemical Weapons Convention (CWC) and even supported negotiation of new instruments, such as Fissile Material Cut-Off Treaty (FMCT) and Missile Technology Control Regime (MTCR) Code of Conduct.

In addition, although many Bush experts preferred outright withdrawal from the Anti-Ballistic Missile Treaty (ABMT), the Administration realized that it could limit domestic and political opposition to missile defense if it first made an effort to negotiate an agreement with Russia to amend the ABMT. For their part, the Russians signaled that they were prepared to make a deal that would at least relax constraints on missile defense testing and some limited deployments.

The September 11 attacks fundamentally changed these political calculations. Domestically, the attacks dramatically increased the American public’s sense of vulnerability and therefore increased support for strengthening defenses of all types. As result, U.S. domestic opposition to the Administration’s approach on missile defense as an important political issue was completely overwhelmed.

Internationally, President Putin’s strategic decision to side with Washington in the war against global terrorism gave the Administration more confidence that it could walk away from the ABM Treaty without damaging other elements of the U.S.-Russian relationship, including a deal on offensive arms. In fact, this calculation has proved correct. Even though an agreement with Moscow to amend the ABMT was clearly achievable, the U.S. decided to exercise its preference for outright withdrawal, and Putin’s reaction was decidedly mild. Rather than provoking a new arms race, it now seems clear that Bush and Putin will announce a new agreement to dramatically cut deployed offensive systems in May.

September 11 and the anthrax scare also caused the Administration to dramatically increase efforts to strengthen Homeland Defense, beyond the programs already established under Clinton. Much of this effort is focused on defense against possible terrorist use of WMD. Of course, experts in the U.S. have long been aware that groups such as al-Qaida were interested in acquiring WMD, but the September 11 attack made the threat more vivid to the American public and political leadership because it demonstrated that some terrorist groups were willing to use any means available to attack the U.S.

Multilateral Treaties

As I pointed out, the Bush team came into office with great skepticism about the usefulness of international treaty regimes in dealing with the real proliferation threats – countries like North Korea, Iran, and Iraq that are prepared to violate their treaty commitments – but quickly realized the importance of supporting some of the international treaties.

September 11 did not fundamentally alter this approach, but the Administration is trying to develop a more positive approach that uses existing treaties to support its broader nonproliferation efforts against rogue regimes and the threat of WMD terrorism. In part, this has translated into a greater emphasis on compliance. For example, the U.S. has publicly identifying countries that it suspects are violating the BWC and has proposed a series of international measures to strengthen the BWC in place of the protocol.

In the chemical weapons area, the replacement of Director General Bustani will hopefully strengthen the OPCW and make it possible to conduct challenge inspections against countries suspected of violating the CWC such as Iran. In the nuclear area, Washington advocated greater financial and technical support for the IAEA, to strengthen its ability to inspect nuclear facilities, and supports efforts to strengthen the International Convention on Physical Protection of Nuclear Materials, to make it more difficult for terrorists to acquire nuclear materials from civilian nuclear programs.

Cooperative Threat Reduction

Coming into office, many Bush officials had a lukewarm attitude towards co-operative threat reduction (CTR) programs with Russia to assist Russia to destroy strategic weapons, secure and dispose of fissile material and chemical weapons, and help find alternative employment for Russian weapons scientists. At best, these programs were viewed as inefficient and wasteful. At worst, they were seen as helping to subsidize Russia's military.

After taking office, the Bush Administration began a comprehensive review of these CTR programs, which was clearly intended to look for ways to cut rather than expand these efforts. Before September 11, it appeared that many programs would be sustained at current or slightly lower levels of funding, while a few big-ticket items, such as plutonium disposition, was slated for restructuring or total elimination.

After September 11, the Administration did a dramatic about face, prompted in part by strong Congressional support for CTR programs. The new alliance with Moscow against terrorism removed many of the political objections to providing assistance to Russia. Even more important, Washington's increased concern about terrorist groups seeking WMD prompted the Administration to make greater efforts to prevent leakage of materials or expertise from Russia. As a result, the Bush Administration is seeking substantially higher funding for CTR programs in its '03 budget request and is seeking much larger European contributions to this effort.

The Rogues

Finally, I want to conclude with some thoughts on the most controversial element of U.S. nonproliferation policy - dealing with the so-called rogue states or what President Bush called the "axis of evil".

It's important to remember that the Clinton Administration also identified Iraq, Iran, and North Korea as the most dangerous proliferation threats to U.S. interests. While lumping all three together as "rogue states", however, the Clinton Administration actually pursued a differentiated approach.

With Iraq, the U.S. used intrusive UN inspections backed by the threat of military force, actual bombing of suspect facilities when inspections failed, and covert attempts to overthrow Saddam Hussein.

With Iran, the U.S. sought a diplomatic opening to negotiate WMD issues, while making strenuous efforts to delay Iran's programs by cutting off the supply of technology and materials from countries such as Russia and China.

With North Korea, the U.S. pursued a diplomatic strategy, using carrot and sticks to achieve agreements to freeze on plutonium production and long-range missile tests and seeking to negotiate a deal to end North Korean missile exports.

Coming into office, the Bush Administration was divided about how to deal with these rogue states.

On Iraq, there was general agreement (as in the Clinton Administration) that removing Saddam was desirable, but disagreement on whether this goal was attainable without the massive commitment of U.S. forces. Some Bush officials emphasized better containment through smart sanctions and the return of UN inspectors, while others advocated greater U.S. support for the opposition to topple Saddam.

On Iran, some officials hoped to create new openings to Teheran to strengthen moderate forces, while others believed that Iran was unalterably committed to support terrorism and pursue WMD. On North Korea, some officials favored a continuation of the Clinton negotiations to limit North Korea's nuclear and missile program, while others felt strongly that such deals amounted to buying off Pyongyang and propping up a nasty regime.

September 11 and the subsequent war against Afghanistan altered the terms of the debate on how to deal with these rogue regimes – especially Iraq - in three ways. First, it created a new sense of peril in Washington that these hostile countries might provide WMD to terrorists who would have no reservation about using it against the U.S.

Second, it created much strong public support to use military force to eliminate America's enemies, even if it means American casualties.

Third, the Afghan War and relatively easy overthrow of the Taliban regime strengthen the case for those advocating a similar approach to overthrow other unpopular regimes, such as Saddam's. (Of course, others pointed out the many differences between Afghanistan and Iraq.)

The effort to extend the war against global terrorism to rogue regimes got off to a difficult start with President Bush's "axis of evil" speech in January, in which the President tried to draw a connection between three countries pursuing weapons of mass destruction (Iraq, Iran, and North Korea) and the threat that these countries would provide WMD to terrorist groups willing to use such weapons against the United States.

As many critics pointed out, Iraq, Iran, and North Korea do not constitute an "axis" or alliance in any meaningful sense, and many countries were uncomfortable with the label "evil" (especially for Iran). Moreover, the extent to which these three governments actually support terrorism varies widely and there is no hard evidence that they have provided WMD to terrorists. In particular, despite reports of contacts between the Iraqi government and al-Qaida operatives, most observers doubt that Baghdad was behind the September 11 attacks or the subsequent anthrax scare.

Finally – and I think most important – many argued that the "axis of evil" formulation created the impression that the U.S. had adopted a general policy of "regime change" to prevent hostile countries from acquiring WMD. This perception threatened to distract attention away from the real focus of U.S. policy on Iraq, which is the only case where the U.S. has a plausible option to use military force to change the regime. Furthermore, Iraq is seen as the greatest threat to possibly use WMD (perhaps by arming terrorists), and there is a broad consensus in the United States that the most effective way to remove this threat is to remove Saddam Hussein and replace him with a government in Baghdad prepared to honor Iraq's international treaty commitments and UNSC resolutions requiring Iraq to disclose and abandon its WMD programs.

After the President's speech, Administration officials were quick to explain that the administration hoped that political change in Iran would open the door for a more responsible government and was still prepared to resume discussions with North Korea. For example, Washington now seems poised to resume negotiations with Pyongyang, and there appear to be some hints that Tehran will finally take up Washington's long-standing offer to hold direct talks. So, in fact, the Bush Administration's policy – like Clinton's – appears to be differentiated – pursuing different approaches to deal with Iraq, Iran, and North Korea.

Conclusion

To conclude, the September 11 terrorist attacks have affected U.S. nonproliferation policy in several key ways. First, it reinforced the Bush Administration's predilection to emphasize defense and deterrence as the most important element of its nonproliferation policy. Second, while not changing the Administration's basic skepticism about the value of multilateral regimes, it has created a search for a more positive agenda, including the need for stronger compliance measures. Third, it made the Administration a believer in the value of CTR programs. And, finally (and most important) it has created conditions for a more assertive policy to deal with the rogues, but this policy will take different forms with Iraq, Iran, and North Korea.

Organised Crime in the European Union

by **Peter Bröms**, 1St Officer
Analysis Unit, Serious Crime Department
Europol
The Hague, The Netherlands

The Organised Crime

Situation

The Situation, in Quantitative Terms:

- Tens of Thousands of Members, in,
  - Thousands of Groups, Controlling
  - Billions of Euros, Annually

Organised Crime Is Increasingly Flexible and international

The Threat from Organised Crime Is Increasing

The Organisation of Crime

Concerning Both Groups Composition and Criminal Activities

Inherently Flexible

- Monolithic Groups -> Entrepreneurial Networks
- Crime Type Specialisation -> 'Crime Facet Specialisation' and Resulting Multi-Crime Activities

Increasingly International

- Homogeneous Groups -> Heterogeneous Groups operating Across Borders
- Intra-Border Crime -> Cross-Border Crime

Organised Crime Groups

- Business
- Meet Supply and Demand Requirements for Profit
- Flexible entrepreneurs
- Heterogeneous
- Transnational
- Professional and Specialised
- Often Employ Specialists

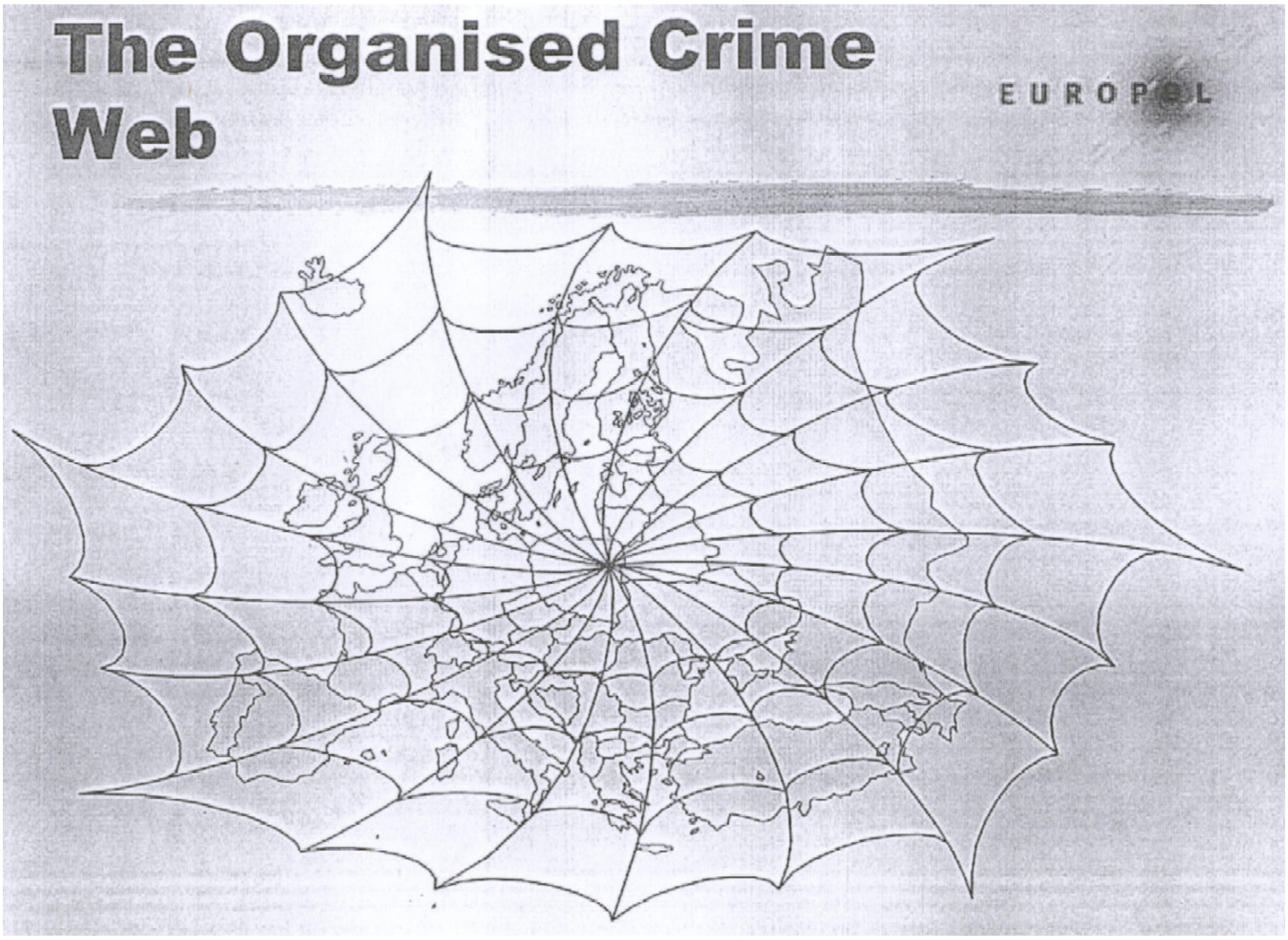
Particular Organised Crime Groups

Indigenous Groups, in Particular Certain

- Belgian,
- Dutch, and
- Italian Groups

Due to their International Manifestations Closed Ethnic Groups, such as

- (Kosovo) Albanian,
- Colombian,
- Polish,
- Russian, and
- Turkish Groups



Terrorist Groups

- Linked to Traditional Organised Crime Groups
- Organised Crime In Itself

Types of Crime

- Integration of Criminal Markets
- Multi-Crime
- Poly-Drug Trafficking/'Cocktail Load Trafficking'
- Extension of Criminal
- Markets New Customers
- New Suppliers
- New Distribution Networks

Particular Types of Crime

- Increasing Involvement In Drug, trafficking Especially Synthetic Drugs;
- Larger Involvement In **Illegal Immigration** and **Trafficking in Human Beings;**
- Growing Involvement In Financial Crime (Fraud, Money Laundering, Currency Counterfeiting;
- Extensive Commodity Smuggling;
- Significant Involvement In Property Crime;
- Still Substantial Involvement In Illicit Vehicle Trafficking.

Other Key Organised Crime

- Violence a Permanent Facet of Organised Crime,
- Corruption Is an Invaluable Tool for Organised Criminals
  - Acquiring,
  - Hindering Access to, or
  - Preventing the Use of Information,
- Substantial Resources Are Amassed Invested in legal Companies.

Technical Issues

High Technology Has Opened Up Two Parallel Avenues for Organised Crime:

- Crime Execution as Such
- Crime Facilitation

Crime Execution

- New Types of Crime:
  - "Cyber Crime'
  - Child Pornography on the Internet
  - Streaming of Payment Card Details
- New Areas for Traditional Types of Crime
  - Fraud
  - Money Laundering
  - Drug Sales
  - Prostitution

Crime Facilitation

- Encryption
- Paid Cards in Mobile Phones
- SMS Messaging
- Internet Communication Financial
- Transactions

The use of Technology

- Intelligence Collection, Analysis and Dissemination
- Surveillance and Monitoring
- Border Controls

The Threat from Organised Crime

- Political
- Economic
- Social
- Technological

Problems in Countering Organised Crime

- Judicial Limitations
- Target Unfamiliarity
- Limitations in Information and Intelligence Availability and Sharing

Judicial Limitations

Law Enforcement Bound by National Borders Whereas Organised Crime Is Not Resulting In

- Slow Response to the Threat- from Organised Crime (Almost Always)
- No Response to the Threat from Organised Crime (Sometimes)

Target Unfamiliarity

Problems of Identifying Law Enforcernent Targets

- When Criminals Reside in One Country and
- Commit Crimes in Others
- When a Criminal Group Is Too Flexible and Thus Not Representing a Tangible Target
- When Criminals Engage In Low Risk/High Profit Activities
- When Criminals Become (Superficially) 'Criminal Business'

Information and Intelligence Limitations

- No Information or Intelligence Available
- Information or Intelligence Not Comparable Between the Member States
- Too Little Information or Intelligence Shared Between the Member States
  - Available Data Is Often Old, or
  - Incomplete

Steps Forward

Prioritisation

Setting Long Term Aims and Objectives
Acting Pro-actively Against Organised Crime

Co-ordination

Defining Roles and Responsibilities

Implementation

Developing Guidelines for Common Action
Formulating Guidelines for Translating
Common Decisions into National, Activities

Bioterrorism and the Vulnerability of Society

Remarks Delivered

by **David F. Heyman**, Senior Fellow and Director of Science and Security Initiatives
Center for Strategic and International Studies (CSIS)
Washington D.C., USA

Greetings

Thank you. And thanks to the Swedish government, to Ola and to Marie for their hospitality and for taking on this very important issue.

Introduction - Historical Events

Let me begin with two historical events.

First, the Renaissance, which began on May 29, 1453. This is the day that Constantinople fell to the Turks. It is an event that historians mark to coincide with the end of the conflicts between Christians and Muslims in the Middle Ages and the transition from a traditional to a more modern society.

The second historical event takes place nearly five hundred years to the day after the fall of Constantinople. In April 1953, an article was published in the British scientific journal *Nature* by two scientists—James Watson and Francis Crick—reporting the discovery of the structure of DNA.

So why do I start a talk about "the vulnerability of society" with these two significant events? Because, strangely, I believe we may be standing today at the cross roads of these two historical trajectories.

We hear from the Bin Ladens of the world and from those that believe in the Clash of Civilizations that we are at the re-emergence of conflict between western and eastern cultures. And, at the same time, with the mapping of the human genome and the understanding of the instructions that describe life, I would argue we are also witnessing the denouement of the age of physics and the ascendance of the age of biology.

What this leads to, I fear, could be the convergence of global terrorism with widespread availability of molecular biology .... and at the heart of this collision is the use of disease as a weapon with global implications.

So I want to talk about this and about exploring the consequences and opportunities of bioterrorism of global reach.

Anthrax - The U.S. Experience

The first significant acts of bioterrorism against the United States took place last fall and consisted of as few as four or five letters containing bacteria that causes anthrax, mailed in the U.S. postal system. As simple as these attacks were, their impact was far-reaching:

- Two of the three branches of the U.S. Government—parts of the United States Congress and the Supreme Court—were shut down temporarily, as were postal operations around the country.
- Eighteen individuals contracted anthrax in five states and five of these individuals died.
- Over 33,000 people required post-exposure prophylaxis.
- Direct costs to the U.S. Postal Service may approach as much as $3 billion.
- The buildings in Florida and U.S. postal facilities in the nation's capital that were involved in the attack were shut down and are still closed, and cleanup efforts at the U.S. Congress are expected to exceed $24 million.

And the response from the medical, public health and law enforcement communities was massive:

- Over 1,000 physicians, epidemiologists, public health officials and medical practitioners from the private and public sectors and from all levels of government were involved in the investigation, the clinical evaluations, environmental sampling and treatment of patients.
- The District of Columbia initiated the largest ever mass-medication program in the U.S., dispensing medication to over 17,000 individuals.
- The level of response from law enforcement was also massive. Thousands of police officers, FBI agents and government officials have contributed to the ongoing criminal investigation. It's worth noting that in calendar year 2000, the FBI responded to only 257 cases potentially involving weapons of mass destruction (WMD), of which 200 were anthrax matters (all of these turned out to be hoaxes). By comparison, between October and December 2001, the FBI launched over 8,000 WMD investigations. These hoaxes took valuable resources away from the ongoing September 11th terrorist investigations.
- And, on the recovery side of our response, it took over a six-month period, around 800 people to cleanup the U.S. Capitol. Other buildings in Florida, New Jersey, and Washington, D.C. are still closed.

All of this again, was because four or five letters were mailed in the U.S. postal system containing anthrax bacteria.

As massive as this response was, the anthrax attacks in America may turn out to be among the easiest of bioterrorist strikes to confront. *Bacillus anthracis* is the most studied pathogen of possible biological agents; the use of mailed letters as a delivery mechanism provided a readily identifiable, overt means of attack; and the areas attacked were for the most part easy to isolate.

Despite this, the anthrax attacks revealed weaknesses in almost every aspect of U.S. biopreparedness and response. We saw weaknesses in our public health infrastructure, and in our laboratory, forensic and diagnostic capabilities. We learned that our scientific base was lacking, and our abilities to detect an attack early on are extremely limited. We witnessed the vital importance of establishing a clear chain of command for incident response, and comprehensive communications strategies to implement during a crisis. We saw a need for better plans for local distribution of medication and providing treatment in the event of mass casualties. And we realized how challenging it could be to cleanup large-scale contaminated sites.

What is alarming about the anthrax attacks is that they could have been far worse had the pathogen involved in the attacks been a contagious agent, an unknown agent, or an agent delivered in a covert widespread attack across multiple jurisdictions. Bioterrorism utilizing a contagious pathogen could spread disease rapidly throughout the country, across borders, and overseas. The delays, technical limitations, resource constraints, and lack of preparedness we witnessed during the response to the anthrax attacks would have resulted in far deadlier consequences had the pathogen been a contagious agent.

Threat to Others

The risks to society from a biological attack are not unique to the United States. With contagious agents, a biological attack is likely to spread disease across borders, and countries may well close their borders to protect their populations. The 1991 and 1994 cholera and plague epidemics in South America and India showed us that even with the World Health Organization reporting that disease was unlikely to spread beyond the local areas affected, the threat was significant enough for European and North American countries to curtail commerce, travel and tourism to these regions. The impact of these actions amounted to severe losses of close to $2 billion for the affected countries.

We saw with anthrax that even with a non-contagious agent, an attack is rapidly internationalized with hoaxes, spread of fear, and copycats. Europe had over 7000 hoaxes in the first couple of months following the U.S. attacks and this very much stressed the system.

I would argue that we are not prepared to handle a massive attack anywhere. Had this attack been a contagious pathogen, could quarantining the affected population have been an effective solution to containing the outbreak or at least limiting it? Who should have the authority to direct, mandate, and enforce quarantines? What are the political and legal ramifications? What agreements and standards must be established to ensure that resources can be shared across borders? What are the rights of foreign nationals if quarantines must be imposed? What steps must be taken to maintain international trade activities and essential services?

U.S. Domestic Preparedness against Bioterrorism

So what are we doing? In the United States, the President announced that his FY2003 budget includes $5.9 billion to defend against biological terrorism, an increase of $4.5 billion - or 319 percent from this year. These investments will go to improving detection and surveillance systems; strengthening medical capabilities; improving planning and coordination among law enforcement, medical and public health officials at all levels of government; bolstering research; expanding training and exercises; and developing communications systems.

An Agenda for Science and Technology in European Security

Even with these investments, with all the challenges we face confronting bioterrorism, biodefense is one issue where the converse of the old adage is true…*we must think locally, but act globally*. Particularly as the inclination to respond by shutting borders becomes our only option.

This conference seeks to assess the role for science and technology in European Security. Let me therefore offer suggestions for an agenda in biosecurity in five specific areas: research, people, institutions, activities, and new thinking.

1. **Research Agenda.** A review of U.S. biopreparedness and the gaps identified in biodefense following the anthrax attacks reveals a wide-range of potential investments. They include: research in vaccines, diagnostics, prophylaxis, therapeutics, detection and communication systems; investments in medical capacity, laboratories, and public health infrastructure; and funding for training, basic research, and technology development and deployment. Similar investments should be considered in Europe and, in many areas, in collaboration with U.S. investigators.

2. **Human capital.** Bioterrorism has not been emphasized in medical schools or in medical training programs. Practitioners must develop better awareness of signs, symptoms and pathologies of biological agents that pose a threat to national security and their potential use in acts of bioterrorism. We must also increase those trained in epidemiology and communicable disease control. Each outbreak is different and requires a unique plan for investigation and control. Trained epidemiologists are needed at all levels to perform these functions and to provide policy-makers with the best scientific input possible in the face of potentially difficult decisions**.**

3. **Joint Center for Biosecurity**. Europe should join with the United States and Russia to establish in one place an organization that can develop international standards; begin information sharing; provide training; expand surveillance; develop communications strategies; examine policy issues and most important bring together in one place the liaisons whose leadership in a crisis is vital.

4. **Exercises/training.** The military performs exercises to prepare for war. Bioterrorism is a war on our civil society; and our governments, public health officials and law enforcement professionals provide our first line of defense. We must strengthen our civil defense, if we are to fight the war on bioterrorism. The *Dark Winter* simulated smallpox attack on America that was held in America last summer significantly influenced public policy and preparedness in America, not just because it help to convince the Vice President, the Secretary of Health, the National Security Advisor and members of Congress of the vulnerability we face against a smallpox attack, but also because it raised questions about U.S.

preparedness unlike any paper or speech could have. Perhaps more important, it also brought together communities who previously operated in isolation but whose cooperation is essential in the event of an actual crisis. These include: the military and law enforcement (e.g., for attribution and acting on state sponsorship), local and national law enforcement (e.g., for information sharing), local and federal governments (e.g., for resource sharing and coordination), and criminal investigators and epidemiologists.

5. **New Thinking (policies)**. Increased security may lead to concentration of power, increased surveillance and emergency provisions not previously imagined. We must be vigilant in our policies to ensure we do not degrade the society we seek to preserve while imposing new practices that attempt to protect us from bioterrorism.

Global Opportunities – Positive Externalities

If we assume a global response to these new threats, then new investments and new attention on biosecurity may provide global opportunities. At the same time, if we are wrong on the threat, there is still a silver lining in terms of the positive externalities derived from these new investments. Let me just mention three opportunities here:

1. **Surveillance** - The increasing burden of noncommunicable diseases particularly in developing countries, threatens to overwhelm already-stretched health services. Worldwide, noncommunicable diseases currently represent 43% of the burden of disease and are expected to be responsible for 60% of the disease burden and 73% of all deaths by 2020. Most of this increase will be accounted for in developing countries. In addition to providing early-warning sentries for bioterrorist attacks, expanded surveillance networks may help expand prevention and control of these diseases as well.

2. **Emerging Infectious Diseases** – Investments in public health infrastructure, in vaccines, therapeutics and other medicines is the largest portion of investments in the United States. If all the predictions are true then the research we do to fight bioterrorism is likely to deliver great new advances in the treatment of many other diseases, such as tuberculosis, pneumonia, malaria and HIV/AIDS. This is the so-called spillover effect: improvements in vaccines for smallpox, for example, may help development of other vaccines. At a minimum, increased global investments in our health care infrastructure may expand the reach of these and other programs to others.

3. **Global Aging and Developing country health care needs** – In 2025, there will be about 1.2 billion people over the age of 60. A quarter century later, eighty percent of older persons will live in developing countries. At the same time, the number of over-60-year-olds will almost double in developed countries. Governments will need to fund the provision of health care for this maturing population. New breakthroughs may not only help bring forward life enhancing technologies but also they may help bring down costs of health care as well. In developing countries, where the cost of medicines may easily exceed the

purchasing power of people, reduced costs may also increase the availability and use of medicines.

Global Challenges

These opportunities provide added incentives for additional investments, but there are also great challenges.

1. **Resource Sharing** – First, we must continue to address concerns about the access to health care — the so-called gap between the "haves" and the "have-nots". This is not new, but if one country can procure vaccines for its entire populations against a global contagious pathogen, the inequities may be felt even more.

2. **Governance** – Second, preventing the proliferation of biological weapons entails controlling technologies that may have dual-use capabilities. How do we develop a non-proliferation regime that provides appropriate and necessary security constraints while also continuing to support and promote scientific freedom and openness?

3. **Privacy** – Third, the potential for knowing our own genome in the future raises questions about who owns our genome and what is the fair and appropriate use of its information? Also, to bolster our early warning capabilities, increased bio-surveillance should be able to track disease down to the individual level to be able to respond to bioterrorism. How do we track unusual disease patterns, be able to get back to potentially exposed individuals, and yet also protect their privacy?

4. **Biohackers and Suicide Attackers** – We have to ask ourselves if in 1980, we could envision computers in every home, in our briefcases, or in our pockets? Increased advances and the prevalence of technology in the years ahead, particularly genetic engineering techniques to modify organisms could lead to desktop laboratories and backyard scientists and increase the risk of an accidental release of genetically modified organisms with catastrophic implications. Or it could lead to the development of the disease equivalent of 'love bug' that wreaked havoc on computers across the world. And if we do not succeed in the war on terrorism, we may see suicide attacks simply go on www.priceline.com and for the price of an airplane ticket spread virulent disease across the globe. We will need to protect against this.

Assumptions about National Security may Need to be Re-examined

Finally, if we are to overcome these challenges and embrace the opportunities, our assumptions about national security will need to be re-examined. In 1998, 200,000 people in Africa died from war; 2.2 million died from AIDS. In some countries now we have 30 percent of the military, 40 percent of teachers who are suffering from HIV. So what you have is an epidemic that is eating at the very civil society of nations and their potential for economic prosperity. And with the risks to national security that weak states and collapsed states already pose on global stability, the potential for AIDS and perhaps other health crises to further weaken states in Africa and elsewhere is great.

Even from just an economic perspective, Harvard's Jeffrey Sachs argues that malaria has powerfully shaped the global distribution of income and poverty. He calculates that, if the disease had been eliminated 35 years ago, up to $100 billion could be added to sub-Saharan Africa's current GDP of $300 billion.

Lastly, I think it is instructive that the much-needed investments in U.S. public health infrastructure were inspired not so much because they were desperately needed — which they were — but as a reaction to recent terrorist attacks.

Conclusion

The convergence of global terrorism with the ascendance of molecular biology presents us with great opportunity and great challenges. At the best, we may at long last develop the capacity to relieve tremendous human suffering, confront global aging, and perhaps even permanently eliminate certain diseases. But there are underlying assumptions that we must confront and investments—in research, people, activities, institutions and ideas—we must make if we are to transform the way we conceive of and shape health and national security.

'Critical Infrastructure Protection'

by **Erik J.G. van de Linde**
RAND Europe
Leiden, Netherlands

Introduction

Often, people have extreme perspectives on the issue of security. One is that modern societies have become more secure than ever and will continue to improve. The other is that our modern societies are supported by a very fragile interdependent fabric of critical infrastructures (energy, transport, ICT, etc.) that may break down by a domino-effect initiated by discontinuities in just one system or even subsystem. To illustrate this, I will first take two oversimplified looks at the issue. In reality however, the issue is not that simple. Systems are far from perfect, but they also do not break down that easily, as a result of continuous efforts for improvement. Therefore, I will briefly describe the development of approaches to improve the reliability of systems. Subsequently I will discuss what the challenge of the new terrorism – aimed at using and attacking infrastructures – means for this development. I will conclude that we need a more holistic approach to dependability research and analysis.

Oversimplified positive look at European security through science and technology

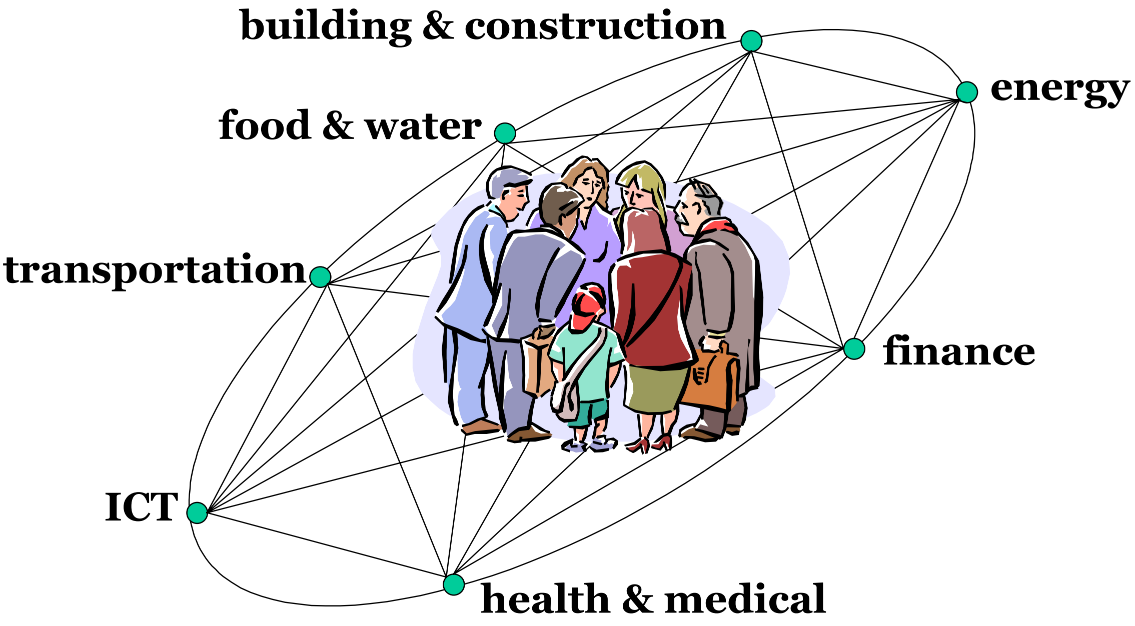
Science and technology were jumpstarted by the Utopian Novel 'Nova Atlantis' (1626) by Sir Francis Bacon. Bacon foresaw systematically organised empirical and applied scientific research. The Baconian scientists, working together in Solomon's house, studied nature and man in order to improve food production, food quality and human characteristics. People in Nova Atlantis were healthier and lived longer than in real life at the time. In 1660, the Royal London Society laid the foundation for modern science and technology, based on the Baconian vision. Until today, science and technology have remained truthful to their mission. As a result, in the developed world today, people live twice as long as in Bacon's age, and in relatively good health. People no longer have to be afraid of pandemic diseases and starvation. Also, societies are prepared to battle crime and disasters. All in all, science and technology, over the years, have done a good job providing security to people. Some say utopia has been realised.

In addition, the European Union, starting with the Coal and Steel Community shortly after the end of WW II, was built on a strong desire to prevent future wars (by sharing coal and steel) and to foster political and socio-economical stability and interdependence. This desire was subsequently institutionalised in the EU in democratic, economic, R&D and many other processes and procedures. This process is still ongoing and will provide increasing security.

S&T and the realisation of the EU can be looked at as two separate entities both strengthening security. So, strengthening science and technology within the European Union, one could say, means double security.

Oversimplified negative look at European security through science and technology

The technological revolution has empowered itself, leading to an upward spiral of economic development, involving the entire global village. Technology has become ubiquitous: it has entered every corner of society. Technological products are being assembled from ever-larger numbers of components, strongly differing in nature (hardware, software) and origin, with suppliers coming from all over the world. As well, products, processes and systems are linked through networks for energy, trade, communication and transportation, forming complex systems. Consequently, a small change in one system may have a large effect in another. Some call it the domino-effect of modern infrastructure.

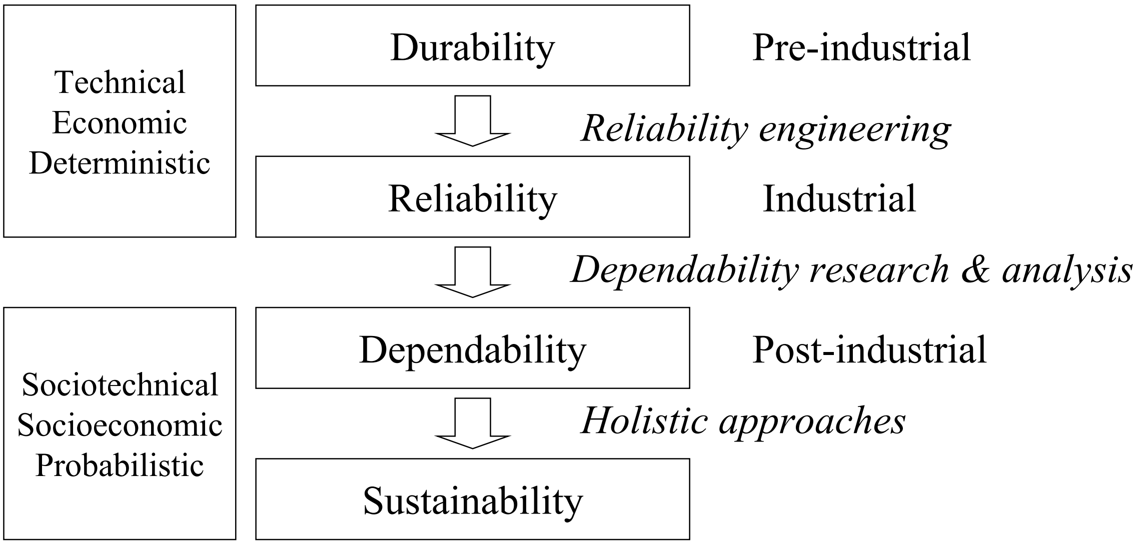


Increasingly, people and societies are becoming dependent on technology. Food and water supply, health and medical care, energy supply, transportation, building and construction, communication and finance are just a few examples of interdependent technological networks that together form the supporting canvas of our societies. Some say we cannot function without it.

From durability to dependability: a more realistic chronological look at security and science and technology

In the pre-industrial age, products were made by individual craftsmen. They focused mainly on durability of materials: wood, stone, metal. Improvement of products was by trial and error, and if a better material was needed, but not available, redundancy was the answer. In the following industrial age, products were increasingly manufactured by assembling components. Soon it became apparent that the reliability of products was a function of the reliability of the individual components. Reliability has many definitions, but it is widely accepted that reliability is expressed in terms of a system being able to perform a certain fraction of its functionality during a certain period of time provided all needed external resources – in particular maintenance, but also for instance energy and data – are being taken care of.

In the sixties, the US military started to put together databases of failure rates of thousands of individual electronic components of weapon systems, in particular radio vacuum tubes, allowing for the deterministic calculation of reliability of for instance radio navigation equipment. This deterministic approach was quickly copied in many other sectors, such as the car industry and nuclear power generation, allowing for the structural, computational safety of systems. It was the start of what is now called reliability engineering. Along came precise standards for individual components such as in aerospace. But in practice, calculated reliability did not always hold. This quantitative approach therefore was later supplemented with a qualitative approach, recognising the fact that systems are becoming so complex through interdependencies, including the human factor (both in design and operation) that the deterministic approach does not suffice. This led to predictions of dependability through probabilistic approach. Dependability covers reliability, availability and maintainability (RAM). The first probabilistic safety studies were done on nuclear energy reactors in the early seventies, and quickly thereafter on many other complex systems, such as aviation. The probabilistic approach also led to more general standards, for instance focusing on the quality of business processes, such as ISO 9000. This brought the element of trustworthiness of people and organisations into play and widened the scope from purely technical to socio-technical. It also meant that reliability engineering transitioned into dependability research and analysis, combining the skills and knowledge of sociologists, psychologists, economists, historians, political scientists and others with those of engineers into multidisciplinary teams. Such teams now stress, in addition to technical aspects, items such as stimulating and responding to whistle-blowers, fostering innovative cultures, continuous education and adaptive, learning organisations. This is a new approach which has yet to mature and become common practice.



In summary, in a period of about a century, we have seen a transition from durability to reliability to dependability. The next step, as we all know, is sustainability. Related approaches to improve systems have transitioned from deterministic to probabilistic, from technical to socio-technical and from reliability engineering to dependability research and analysis. With sustainability as a widely supported future goal, we may expect new transitions towards even more holistic approaches.

Murphy's law

'If something can go wrong, it will'. This well known law of Murphy has inspired many to reduce the chance that something will go wrong and to reduce the consequences of failure, including responding to and managing disasters. Low probability, low impact is the best combination to strive for. Distance between maintenance for cars has been increased from 2.500 to 50.000 kilometres and more, and if cars do fail, the consequences may remain small, even if cars crash. Aeroplanes can now fly around the globe on two engines with dependability better that one in a million. Self-diagnosing and self-repairing systems are coming to the market shortly. Food, water and energy supply, financial and telecommunication networks function better than ever before, both quantitatively and qualitatively. One reason is that networks, in particular information networks, are designed for resiliency. For instance, packet switching on telecom networks allows for rerouting of information packages (text, sound, video) if parts of the network are unavailable. Similar technologies are being implemented in the electricity network. Since IT is an enabling technology for many other critical infrastructures, resilience of IT networks carries through in these as well.

But, danger is looming. Market mechanisms and liberalisation may put heavy pressure on some socio-technical infrastructures. In the food sector, we have seen a number of failures and disasters, such as mad cow disease, food and mouth disease, swine fever, colon bacteria contamination, antibiotics, hormones and other scandals, some of which have been attributed to market pressures and human factors. In the electricity sector, power irregularities and blackouts may result from the extra burden put on the grid by electricity trade, for which the grid has not been designed. In telecommunication, companies are under heavy pressure because of mergers, acquisitions, auctions and fierce competition. In the health and medical sector, productivity does not increase a quickly as in others, putting a burden on the financial integrity and keeping salaries low, thus shutting this sector off for people wanting to make a career in health care. Similar observations hold for other sectors, for instance education.

Countries world-wide have recognised this new danger. To counteract it, initiatives have been set up to protect at least the most critical infrastructures. The millennium bug, Y2K, was a starting point that sparked many countries to put public-private initiatives into place to develop action plans for protecting critical infrastructures. Often, measures include early warning systems, self-regulation, crisis management scenarios, quick response teams, information centres, etc. This seems to work well, although in particular for some global systems, world-wide co-operation could be further improved, such as in the case of cyber-security. Also, in some cases, political and trade issues may stand in the way of successfully protecting critical infrastructures.

Bin Laden's law

But now we have a sequel to Murphy's Law. We could call it Bin Laden's Law, leaving no doubt about the major shift this law entails: 'If somebody can do wrong, he will. It brings into the equation acts of disruption that are committed on purpose. On the lower, non-terrorist end of the scale, this law means that car drivers drive faster because their cars are equipped with ABS, kids sometimes purposely crash cars because they feel protected by seatbelts and supplemental restraint systems, people smoke more cigarettes because they contain less nicotine, Internet is used to publish pornography, viruses are distributed digitally, containers are used for smuggling drugs, etc. In general: the socio-technical system bites back. Often, the damage of this burden remains small. But at the highest end of the scale, terrorists will use our infrastructures to attack them, as they have done on the 11th September.

The lessons of 11 September

What were the real lessons of 11 September?[23] Not that we faced 'new terrorists' willing to inflict mass casualties; not that the aviation system was vulnerable; not that the al-Qaeda network was active in many nations. These were all known to the security community; indeed, it was also well known that Islamic radicals had previously sought to crash airliners into cities, to topple the World Trade Centre and to disrupt the US aviation system. In other words, on this occasion, al-Qaeda 'got lucky' and the threshold that was crossed was one of perceptions, not of terrorist intentions or capabilities.

[23] The next paragraphs are in large part based on an earlier briefing note by Andrew Rathmell of Rand Europe to the House of Commons Defence Select Committee, UK, 9 January 2002.

What was so striking about 11 September, though, was that a few terrorists with box knives and partial flight training could create such havoc. It was a clear demonstration of the vulnerability of modern society. The way in which the shock was transmitted rapidly throughout a globalised, interconnected system, costing billions of dollars in economic damage through direct losses, lost growth and instability to certain industries, such as the airline and insurance industries, surprised everyone, but also the damage was not nearly as big as it could have been.

We know we live in a globalised, interconnected world. We now begin to recognise the ways in which this interconnection – our membership of the global village – can be used to harm us. Global economic chaos was a by-product of the al-Qaeda attacks but more imaginative opponents of the West have already begun to understand the ways in which they can use our own vulnerabilities against us.

The fact that we live in an interdependent, highly connected and technology dependent but socially and politically open society means that we live in a more vulnerable society. This is a society in which economic, technological and political changes have left us more vulnerable to massive disruption. Throughout much of the last century, massive disruption to the economy and the infrastructures upon which we relied could only be caused by a large-scale campaign of aerial bombardment, blockade and/or special forces operations. In the 21st Century, the threat may be from small groups using our technological networks to carry out asymmetric attacks. Countering such threats and attacks is a task that requires action not only by the military, the police and security services, but also by the regulators of critical industries, including self regulation. Our industries themselves as well as our citizens are in the frontline of this struggle.

Our vulnerable society

The vulnerabilities of modern society are beginning to be addressed by leading international organisations since there is an emerging consensus that these risks cannot be dealt with on a purely national basis. The EU, NATO and the OECD all have working groups examining this issue, as well as individual nations.

The problem is threefold:

- contemporary society is inherently more vulnerable to malicious attacks
- terrorists use modern infrastructures to attack them
- shocks to one infrastructure may cause ripple effects in others

Note that the means of possible attacks on our infrastructures are varied. They include physical attacks, cyber-attacks, NBC attacks and psychological attacks (e.g. through market and media manipulation). Note also that the ‘old terrorism’, focusing on individuals as targets (often VIPS and dignitaries) while using conventional weapons, has not been replaced by the new terrorism.

Why are we more Vulnerable?

The causes of increased vulnerability are clear:

- Privatisation and market liberalisation that have put key infrastructures in private hands, with concomitant pressures to cut overheads (including security)
- Pressures in a globalised market which encourage leanness (building out redundancy) and speed to market[24]
- Rapid development of globalised new infrastructures and services which outstrip capabilities of sectoral, national regulatory regimes to impose controls
- Globally integrated value chains and markets that transmit shocks rapidly (hence tight coupling amongst infrastructures)
- Adoption of new technologies and practices in response to market pressures without adequate focus upon security (e.g. use of public information networks and remote control systems in power networks)
- Difficulties faced by local and national police/military/emergency planning authorities in mapping, modelling and developing risk management plans for the new environment
- Public perceptions of risk

What can be done about it?

The vulnerabilities that we have built into our societies would be unimportant if we did not have to face the reality of Bin Laden's law. But there is no reason why terrorists should not develop and use the operational plans and technical skills to exploit and target our vulnerabilities again in the future.

In the face of these vulnerabilities, the strategic question then must be: "can our normal approaches to dependability provide a basis for strategic planning in the face of such threats and vulnerabilities?" The answer is: "No". Some countries have therefore begun to respond to these challenges by proposing a holistic approach to dependability. Of course it goes way beyond reliability engineering. But it also goes way beyond the foreign policy-led diplomatic efforts or the traditional counter-terrorist approaches which are threat led. The new dependability approach should start with identifying the very aspects of the vulnerabilities of society: critical infrastructures, their complexity, and their interdependencies.

An important step in dealing with this challenge is a workshop such as this which ensures wider recognition that these problems exist and that they require the help of science and technology. Government may be initiating this effort, as government is responsible for various stages in preventing, responding to and recovering from terrorist threats and attacks. However, in modern societies, industry has a central role to play, as do citizens. At the end of the day, our citizens need to understand the

[24] One of the reasons why software is notoriously insecure.

risks they face. If they want to reduce these vulnerabilities then they will have to bear the burden, either through higher investments in security by industry or through taxation if the public sector is to bear the burden.

Our proposal to the workshop

We propose to approach the challenge of protecting our vulnerable societies by increasing the dependability of our critical infrastructures. We need to define systematically what these critical infrastructures are in terms of their complexity, their interdependency and the strain that has already been put on them by rapid technological development, privatisation, globalisation and market effects. We need to prioritise them based on risk analysis (including likelihood, consequence and vulnerability), cost/benefit analysis (including feasibility of protection) and importance of the functionality of the infrastructure. In doing so, we need to combine reliability engineering with dependability research and analysis, using multidisciplinary teams, with qualitative and quantitative approaches, consulting public and private actors. Anti- and counter terrorism actions should take into account the entire spectrum of relevant factors: scientific, technical, economical, social, psychological, historical, political, global, public and private. It may well be that certain combinations of weapons and targets on one hand and infrastructural dependability on the other hand will lead us to discover challenges and vulnerabilities that we had not identified before. Candidates for discovery may vary from using the global container system as a weapon, to infiltration of national education systems. We should mobilise our scientific and technological capabilities to define and understand these challenges and vulnerabilities in all their dimensions, to prevent and deter them from developing into a serious threat, to monitor associated signals, to manage risks, to respond to an attack should it occur, including crisis and disaster management, law enforcement, military and diplomatic action. In the recovery phase, after an attack, we should act as learning, innovative societies, thus strengthening ourselves to prevent and withstand subsequent threats and attacks.

Vulnerability from Natural Hazards and Implications for Security

by **Gordon A. McBean,** Professor
Institute for Catastrophic Loss Reduction
The University of Western Ontario London,
ON, Canada

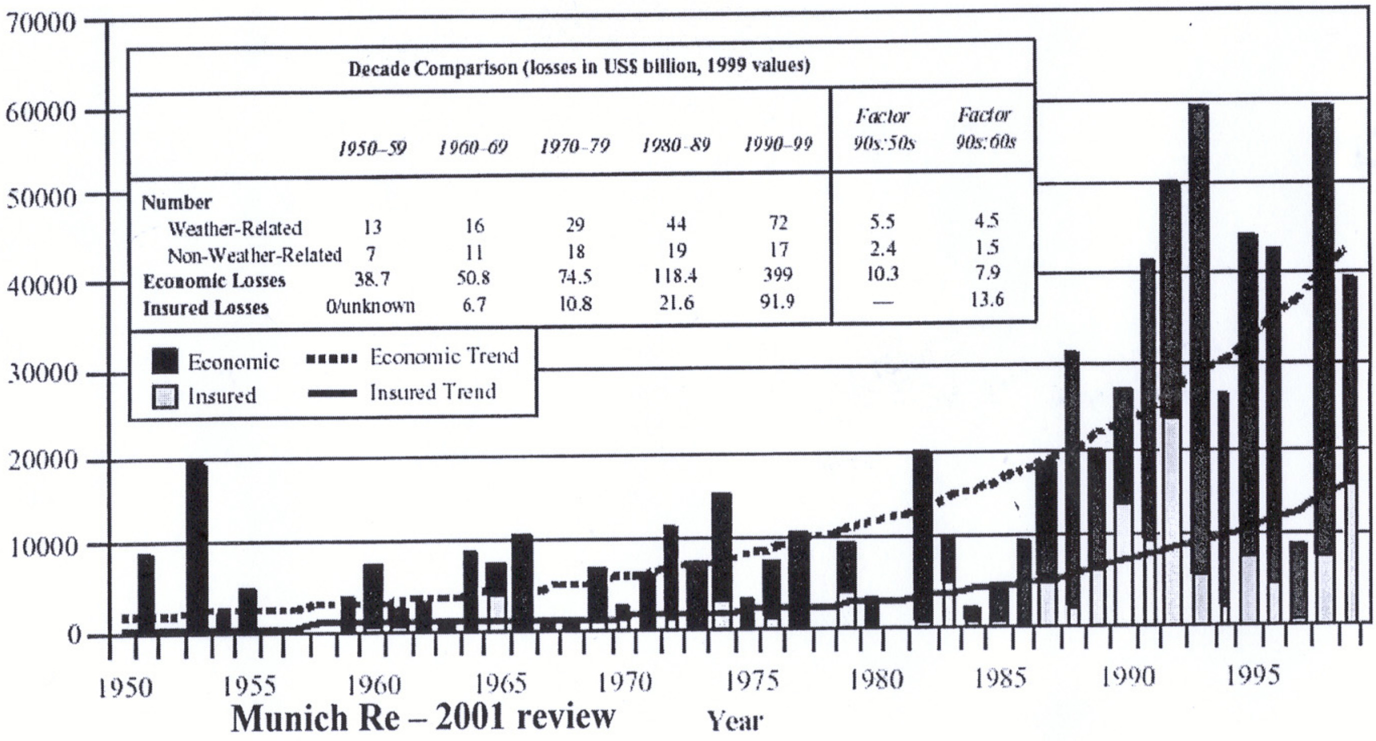
Humans are impacted by a range of natural hazards

- Atmosphere related - windstorms, precipitation, - Hurricanes, typhoons, storm surges
  - Tornadoes, lightning, hail storms - Floods (flash, riverine, . . .)
  - Drought - famine
- Geophysical
  - Earthquakes
  - Volcanoes, ash plumes
  - Land slides

Natural and Human Caused Disasters

- Huge impacts on society - could be additive
- Hazards (natural or human-caused) plus human vulnerability leads to Disasters
- Causes of vulnerability overlap • Fear - acceptability
- Focus on reducing vulnerability and prevention of disasters (and hazards where possible)

Losses due to Extreme Events



Decade Comparison (losses in US$ billion, 1999 values)

	1950–59	1960–69	1970–79	1980–89	1990–99	Factor 90s:50s	Factor 90s:60s
Number							
Weather-Related	13	16	29	44	72	5.5	4.5
Non-Weather-Related	7	11	18	19	17	2.4	1.5
Economic Losses	38.7	50.8	74.5	118.4	399	10.3	7.9
Insured Losses	0/unknown	6.7	10.8	21.6	91.9	—	13.6

Munich Re – 2001 review

- Lives lost -25,000 -(10,000 in 2000)
- Events -700 -(850(record) in 2000) (long term average 650) -Economic losses -$36B (US) -($30B in 2000)($100B in 1999) -Insured losses - $11.5B -($7.5B in 2000)
- Windstorms and floods - 2/3 of events and 91% of insured losses

Natural Disasters have their biggest impact on developing countries. Major issue of security. Creates environmental refugees and unrest.

Insurance Industry concerns

- "The WTC disaster has resulted in a greater awareness than ever before of the major losses caused by human hand. The inconceivable must now be considered by clients, insurers and reinsurers alike. The same applies to natural hazards as well. According to our calculations, extreme loss burdens from natural catastrophes may be even higher than the insured loss of 11th September 2001."
- Dr. W.-O. Bauer, member of Munich Re's Board of Management.

Escalating disaster costs; why?

- Social and demographic characteristics
  - Increased population
  - More exposure
  - Growing inequality
- Built and commercial environments
  - Growing density
  - Dependence - vulnerability
  - Aging infrastructure
  - Transportation - people and goods
- Physical environment
  - climate change

Climate change – The IPCC

Assessment

Very likely - 90-99

- more intense precipitation events

Likely - 66-90

- increased summer continental drying and associated risk of drought
- increase in tropical cyclone peak wind intensities
- increase in tropical cyclone mean and peak precipitation intensities
- spread of disease (malaria, ...)

Risk assessment

- Think locally - act globally

Approaches to Disaster Management

- **RECOVERY**
- **ANTICIPATE** through Forecasts and warnings
  - advise about impending events and advise on response strategy
    examples: tornado, flood; seasonal drought; climate change
    - tornado - 10 minutes - run for cover
    - River cresting in next 5 days - Prepare for evacuation
    - Terrorist attack in next 48h - protect yourself
- **MITIGATION - ADAPTATION**
  - adopt standards and codes to protect infrastructure, people, etc., from changing risks due to extremes or extremists
    examples:
    - increased likelihood of tornados or terrorist attack in next month, year, ...
    - modify practices; prepare response strategies

Scientific research - ceded to head off disasters.

Lessons Learned from the Weather Community

- Global issues
- Mutual reliance, interdependence
- Cooperation, exchange of information
- Redundancy of communications and other structures
  - international support
- Joint research projects

Forecasting weather - Warning of Terrorist Attack

- Monitoring dection prediction information
  - S&T needs in each step
- Detection Prediction
  - Probability of detection False alarm ratio
    E.g., tornadoes, bioterror
- Information dissemination - media -timeliness, accuracy
- Commercialization, role of private sector
- When citizen's chose to act - value of information and education

Science for Security

by **Dr. Rolf Linkohr**, MEP
European Parliament
Brussels, Belgium

In my short presentation I would like to address three topics. The first one refers to the European Union's Common Foreign and Security Policy and the question, whether we have a political competence in security policy, then I would like to touch on some scientific and technical aspects of arms control and disarmament and the EU's possible contribution in this field. Finally, I will make some rather general remarks on science and security in the 21St century.

Until the 1990s collective security and defence co-operation were not considered relevant issues as, far as Common European policy is concerned, a fact that was corrected to a large degree in the 1997 Treaty of Amsterdam and the 1999 Treaty of Nice. The change came about after the strong impressions left by the bloody wars in the Balcans and in Central Africa, which radically changed the European public opinion. Europeans have understood that they can no longer behave as impartial observers of the collective killing of a whole nation but they must and can play an active role in bringing and keeping peace. And the more they act together the more efficient they are. If you ask Europeans today whether they want foreign and security policy to be a common responsibility they answer yes. One could even say that the credibility of European policy depends more and more on our ability to provide peace and stability not only at home but world-wide.

The Treaty of the European Union is very clear. Article 1 of the Treaty of Nice says:

1. The common foreign and security policy should include all questions relating to the security of the Union, including the progressive framing of a common defence policy, which might lead to a common defence, should the European Council so decide.

And in Acticle 2 it says:

2. Questions referred to in this Article shall include humanitarian and rescue tasks, peacekeeping tasks and tasks of combat forces in crisis management, including peacekeeping.

The Treaty of Nice imparts a new quality to the process of shaping the European identity in matters of security and defence. Although its primary intention is to build a European crisis management capability its wording and the underlying spirit allows us a much more courageous initiative to support world-wide disarmament and arms control.

The European Union has taken a whole series of initiatives across the spectrum of nuclear, biological, chemical and conventional weapons. The Stockholm International Peace Research Institute SIPRI dedicates an entire chapter in the appendix of its Yearbook 2001 to the European Union approaches to arms control, non-proliferation and disarmament and gives an impressive list of all the actions and Common positions of the EU, from arms embargo on Nigeria or Sudan to combating the destabilisation, accumulation and spread of small arms and light weapons.

The responsibility for the Common Foreign and Security Policy lies within the Council and therefore within the governments of the member states. The European Parliament cannot decide on joint actions or force the Council to act against its will. But we have the right to be informed and thanks to our budgetary rights we can put pressure on the Council in those cases which are financed by the European Budget.

Parliament has also a say when it comes to sustainable development and the precautionary principle, both mentioned in the treaty and in the meantime part of our common law as ruled out by the European Court of Justice. Although the precautionary principle applies rather to environmental and food quality standards, it is a general principle and should be respected in all actions we undertake, be they civil or military. To give you an extreme example: there is no sustainable development in a climate of civil war. Countries like Angola, Afghanistan or Cambodia can only dream of sustainable development, if they do not succeed in freeing their fields from the millions of landmines that were laid in the bloody times of their civil wars.

In order to reduce risk, wherever this risk may come from, we must apply the Treaty. And if science and technology can contribute to reducing risks we must make use thereof, be it in civil or military cases. The treaty allows us some flexibility and its application depends very much on its interpretation.

Now, what about our own science policy? Whereas NATO has its own research programme focused on the military aspects of security, the European Union's research policy is exclusively civil although the treaty does not verbally exclude military research. The main purpose for European research policy as laid down in the Treaty is the strengthening of the scientific and technological basis of Europe's Industry and to improve our competitiveness. But the Treaty says also very clearly in its Article 163 that our research programmes can support all policies that fall under the Treaty's competences, if deemed necessary. Therefore the European research programmes can be accessible to all and used to do research in all fields of security, if we agreed so.

As a way of conclusion we can clearly state that the European Union is competent in this matter and has the duty to reduce risk wherever the risk comes from. Security policy is a common policy, according to the Treaty as well as in the eyes of our people.

In the last years I tried to convince my colleagues, the Commission and the Council that this must be reflected in the wording and in the content of the Framework Programme for Research. In the meantime it is agreed that research in new technologies to detect and destroy landmines is a task that falls within the competence of the Union and must therefore be financed under the provisions of the Framework Programme. I hope that the Council will agree to include research on nuclear, biological and chemical disarmament in the Framework Programme in order to assist countries like Russia or Ukraine to destroy their still large arsenal of weapons of mass destruction.

Some member states have their own national programme and they assist the above mentioned countries in shaking off the burden of the cold war. I do not want to replace national Programmes by Europeans, but we need a much closer cooperation and some common actions. Think about Kasachstan, which in the past was the country where the Soviet Union tested its nuclear and biological weapons. How can they - with their scarce resources - cope with the deadly heritage of the former USSR? A common action would be the best confidence building measure we can take, it would mobilise our young scientists who await ambitious humanitarian programmes and it would improve the image of the European Union in the eyes of its own people.

First of all we should focus on the disarmament of weapons of mass destruction. Such a programme would enable us to learn how to work together, to develop new technologies of control, verification and destruction - and it would reduce the risks of terrorism. One of the nightmares of our time is the illicit trafficking in nuclear, biological and chemical weapons. We therefore need to focus on new technologies to detect, monitor and control not only the weapons as such, but also the substances that lead to the construction of weapons. Border control must be tight and we need more non-proliferation programmes in these countries.

Several times already I have asked the Council and the Commission to provide the European Parliament with a report and develop their own proposals on security and disarmament which we would then discuss. I know about the institutional problems, particularly the Commission's which is as much an observer in matters of security as the Parliament is. Most of the competences lie within the Council. But not all.

Let me give you an example. Some months ago Senator Sam Nunn, a Democrat from the state of Georgia, USA, proposed that the US and Europe could write off Soviet-era debt owed by Russia in exchange for cold war weapons, a debt for security swap, as he called it. Senator Nunn's move would require substantial coordination from the EU states, starting with Germany, which alone is owed 40% of the Soviet-era debt. I think it deserves a European answer. I particularly like the idea of a debt for security swap, something that could be further developed and requires a deeper discussion in public and in our Parliaments.

Disarmament is only one face of the security coin. Armament is the other. And it is true: new weapons and threats are developed, by our states and also by the socalled rogue states. Weapons are traded or stolen, sold or bought. The threats stem from states but also from individual terrorists or their networks. Modern or old science offer a whole range of possibilities. The next generation of weapons will use nanotechnology as well as information technology, the weapons become smaller, invisible and more targeted, they will use brain science to influence our thinking, they might even look at possibilities to use our genetic footprint to develop weapons in future racial wars. The fantasy of killing has no limits. Sometimes the technologies work, sometimes they don't. There is only one certainty: security will not increase.

What could we do? Let me give one of many answers.

The European Union has a Joint Research Centre with different research priorities. It was created in the 1950s under the EURATOM Treaty in order to develop a new type of nuclear reactor. In the meantime its main activities are non-nuclear and they respond to our needs in environmental and food security. The vocation of the Joint Research Centre always reflected the needs of the European Union because it has been created to support the Union's policy. I therefore ask myself wouldn't it be reasonable to add an element of security research to this very European research centre? By the way, we could rely on the already existing experience in earth observation, material science, nuclear, chemical and biological research, electronics, etc. And we could use their experience of networking with European institutes to develop a European security research policy. They need not necessarily do everything, but as they have a European vocation they could create a synergetic effect in security research.

Security covers everything. It has a military and a civil aspect. For example, if we could develop a sniffing device as accurate as the nose of a dog we could detect drugs and put a blow to the international drug traffickers. Or we could detect landmines by sniffing. Whatever we measure, it must become more accurate. We must learn to identify precisely the origin of a product or material. Our electronic devices must become more robust against electromagnetic attacks. We must learn about the effects of microwaves on our health. But in order to do it we need more coordinated european research.

Let me come to my third point which refers to science and security in the 21.century. It brings me back to the question about our science culture. Genus humanum arte et ratione vivit - mankind lives through ars and ratio, wrote Thomas of Aquin. Ratio is reason. Ars is art, a translation into latin of the aristotelian techne, which refers to the word technology. We, the people of today live by technology and reason as far as they are compatible. But is technology reasonable?

The question whether technology is good or bad is clumsy and useless. Better would be to ask: "What should we want if we technically could?" Or: "What should we leave although we technically can?" These questions transforms technology into a political process.

These questions are not new. They stem from the post-war period when scientists began to ask whether it is morally admissible to build a nuclear bomb. But although many symposiums were held and many excellent books were written about this subject the question is not out of date. Globalisation brings a new element in the debate. Science and technology are no longer reserved to a single nation. Even the poorest countries are now able - if they oppress their people enough - to build nuclear bombs or develop other types of weapons of mass destruction. They can host terrorists or finance terrorist attacks. We therefore need international safeguards, international standards, in the extreme case we even need military force to make these countries comply with international law.

Science is not only a tool to develop new devices to make our life more safe and our world more secure. Science is also a culture and a method to understand the consequences of our acts. For example the consequences of a nuclear war. In the early eighties of the last century a group of scientists in the then USSR and the US studied the consequences of a nuclear war on the earth's atmosphere and biosphere. They found that even a "limited" or "protracted" war would eliminate human life because our natural environment would be irreparably damaged. Temperature would fall and create what was then called the nuclear winter. In other words, they found out that in a nuclear war even the winner would be a loser.

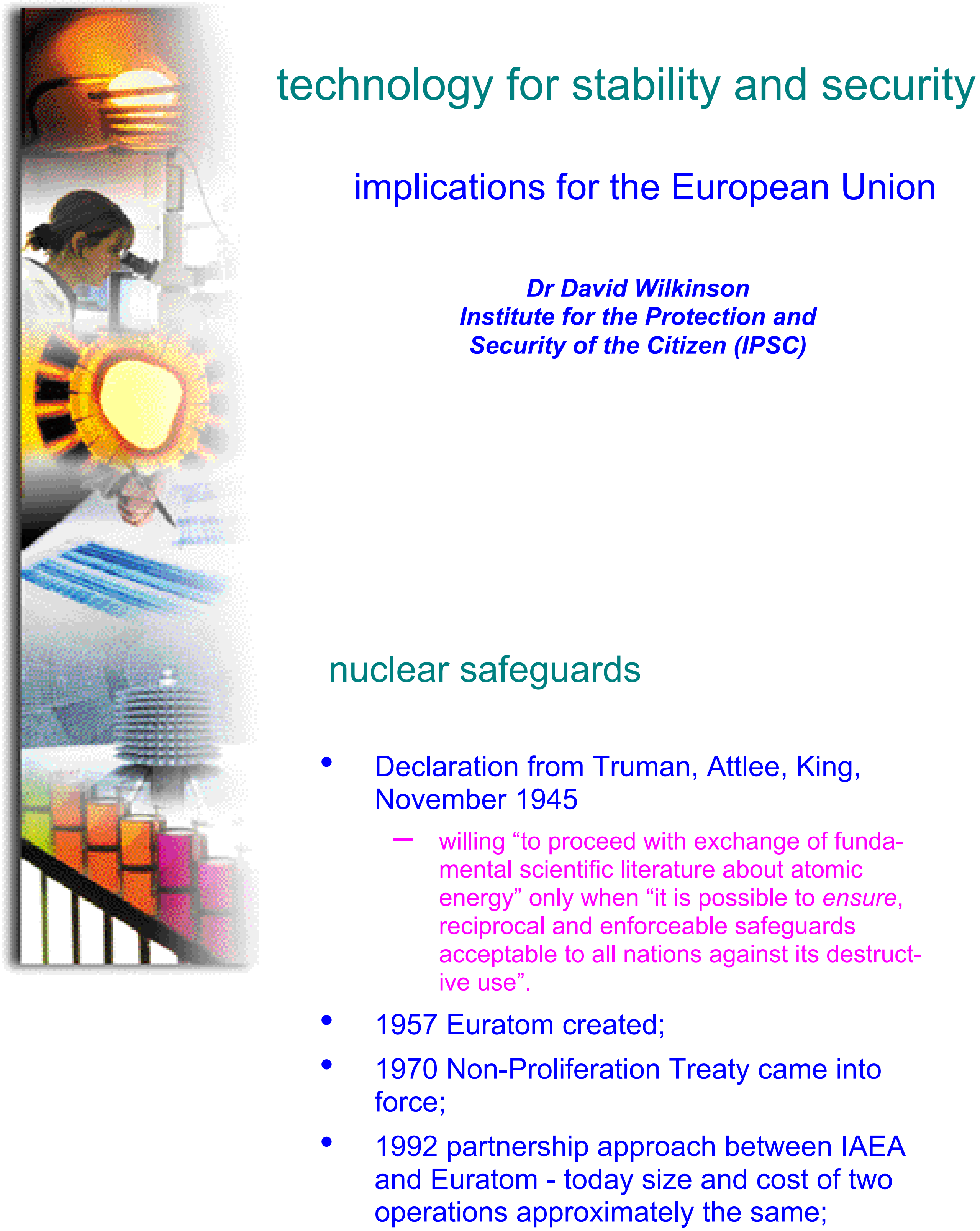
The awareness of the climatic and biological consequences of a nuclear war lead to this new way of thinking which then triggered various phases of further nuclear disarmament. The leading politicians learned from the scientists that the bomb can perhaps be built but should not be allowed to be used. This was a major contribution of scientists to disarmament and an excellent example of how science can influence politics.

Today we not only have to deal with states, but with individuals who might endanger the whole world. We have to deal with people who do not even respect their own life, who want to become martyrs. There is no deterrence against martyrdom. You can only detect and kill them or you have to educate them in order to prevent them to become martyrs.

Therefore, in the end there is no substitute to education. And education is based on science and pedagogy. Whereas in science a theory is either true or wrong, pedagogy needs credibility to be efficient. But in order to be credible our society - our world society - needs justice and development. As long as the world is what it is - unjust and hopeless for many people - the temptation to change the world by force remains alive. Terrorists find willing people. The always more unjust world, but also the fact that more and more people are poor although the overall wealth increases must become a subject of concern for scientists in the 21st century as the nuclear winter challenged physicists and biologists, chemists and physicians in the 20th century. Certainly, to reduce poverty is not a guaranty against terrorism, but it helps to convince people that there are other and better possibilities to reach their objectives.

Will the world then be safe? Safer perhaps but not safe. At the end there is no absolute security. The motivation for terrorism - in its individual or state form - is multiple and cannot be reduced to poverty. Otherwise all inhabitants of Haiti would be born terrorists which is fortunately not the case. Even scientists can become terrorists. Or serve the cause of terrorists. We have a saying in german: "when a head and a book knock together and it sounds hollow, it must not necessarily be the book". So be careful. Also scientists need education, values, principles. Again and again we must learn what is allowed and what is forbidden.

My conclusion is very simple. If we want to make security and science a European subject, if Europe wants to use science to make the world safer, it has to introduce security in its own research policy. Research in technologies to detect and destroy landmines is a good example. Research in the elimination of weapons of mass destruction is another one. But if we really want to reduce the risk of terrorist attacks or of rogue states' hostile actions we need to understand the reasons behind this behaviour and we have to eliminate them. One - not the only one - is poverty. If science could contribute to eliminate mass poverty it would also help to improve security.



technology for stability and security

implications for the European Union

Dr David Wilkinson
Institute for the Protection and Security of the Citizen (IPSC)

nuclear safeguards

- Declaration from Truman, Attlee, King, November 1945
  - willing “to proceed with exchange of fundamental scientific literature about atomic energy” only when “it is possible to *ensure*, reciprocal and enforceable safeguards acceptable to all nations against its destructive use”.
- 1957 Euratom created;
- 1970 Non-Proliferation Treaty came into force;
- 1992 partnership approach between IAEA and Euratom - today size and cost of two operations approximately the same;

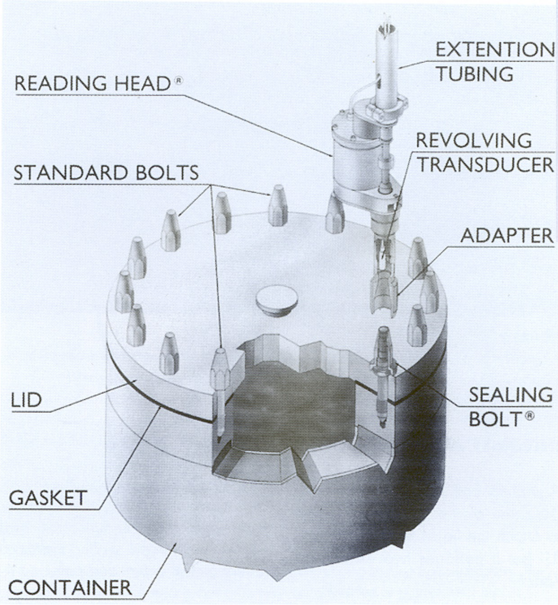
objectives of verification

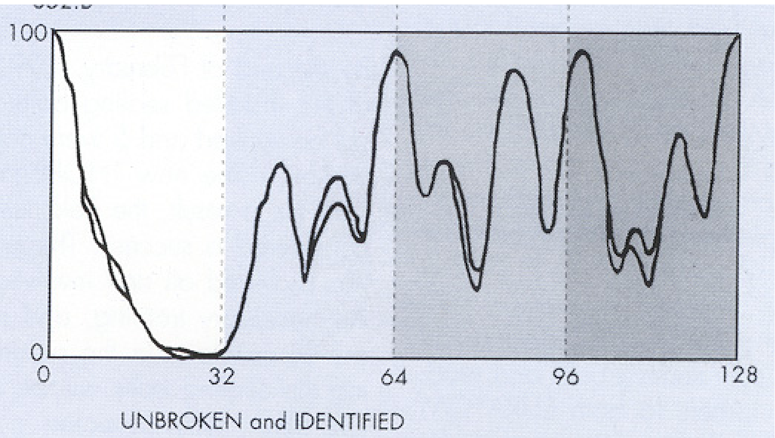
- detecting non-compliance;
- deterring parties that might be tempted not to comply; and
- providing compliant parties with the opportunity to demonstrate convincingly their compliance;

scientific challenges

- measurement of mass and volume;
- non-destructive measurement of composition (particularly of fissile materials);
- tamper-proof seals;
- surveillance of unattended areas;
- secure communications to allow remote monitoring;

sealing bolts



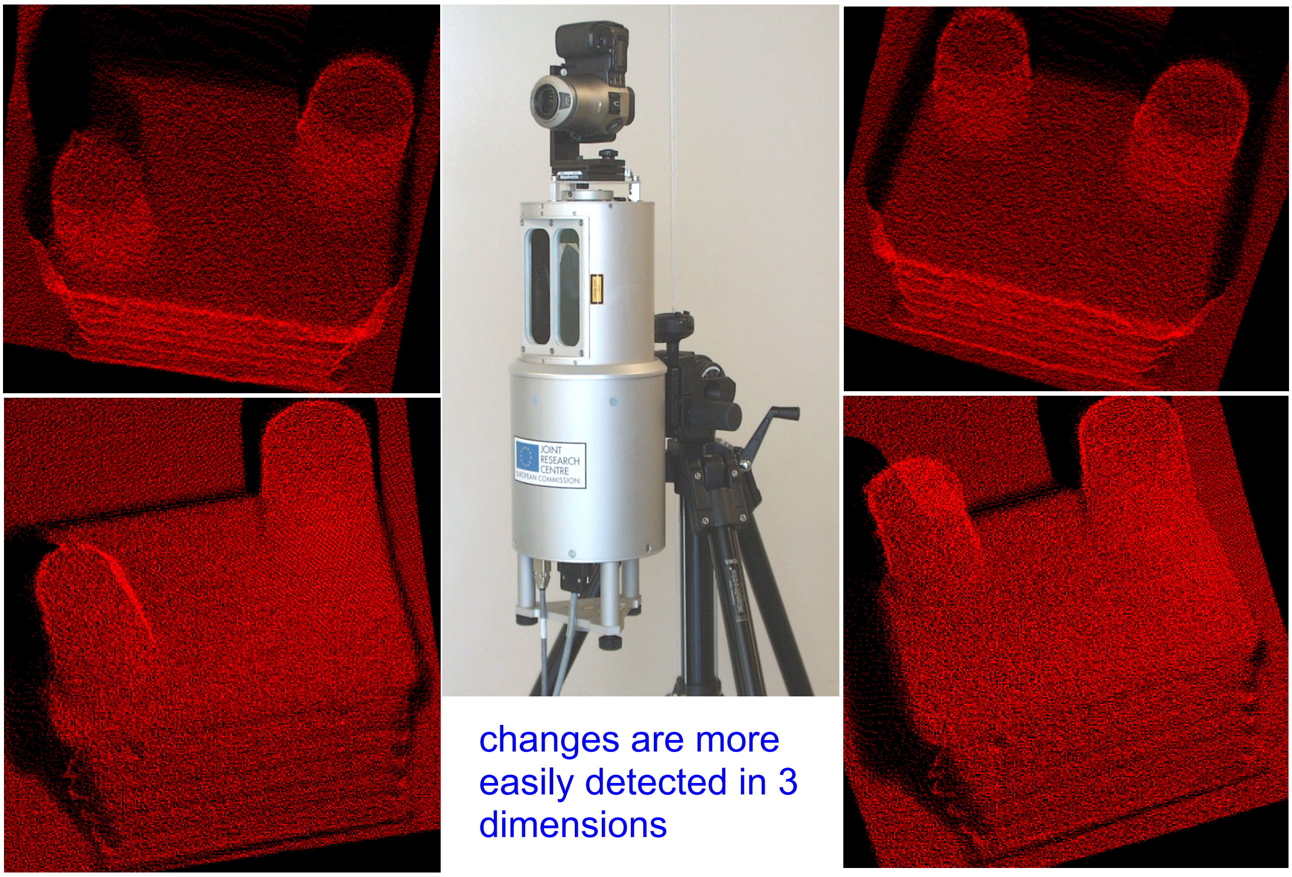


- uniquely identified:
  - head of bolt scanned ultrasonically;
- tamper-proof:
  - unscrewing breaks seal;
- remote operation;
  - underwater;
  - radioactive;

surveillance

- monitoring unattended areas
  - detecting and documenting changes in complex environments or invisible to human eye;

3d laser surveillance



changes are more easily detected in 3 dimensions

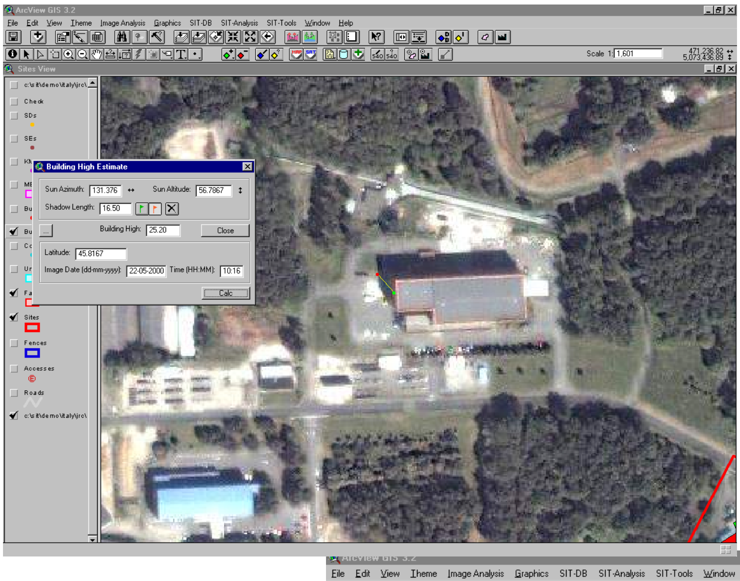
Initial Position

Final Position

new challenges to the system

- 1991, Iraq was discovered to be conducting an extensive nuclear weapons programme, undetected by IAEA safeguards, even though it had ratified the Non-Proliferation Treaty in October, 1969;
  - need to check completeness as well as accuracy of declarations;
- 1996, Trilateral Initiative to develop safeguards for surplus weapons-grade material;
  - verification whilst maintaining confidentiality;
- 2001, September 11
  - integrating efforts of inspectorates, civil and military authorities;

high resolution satellite imagery



Building High Estimate

Sun Azimuth: 131.376 ↔ Sun Altitude: 56.7867 ↕

Shadow Length: 16.50

Building High: 25.20 Close

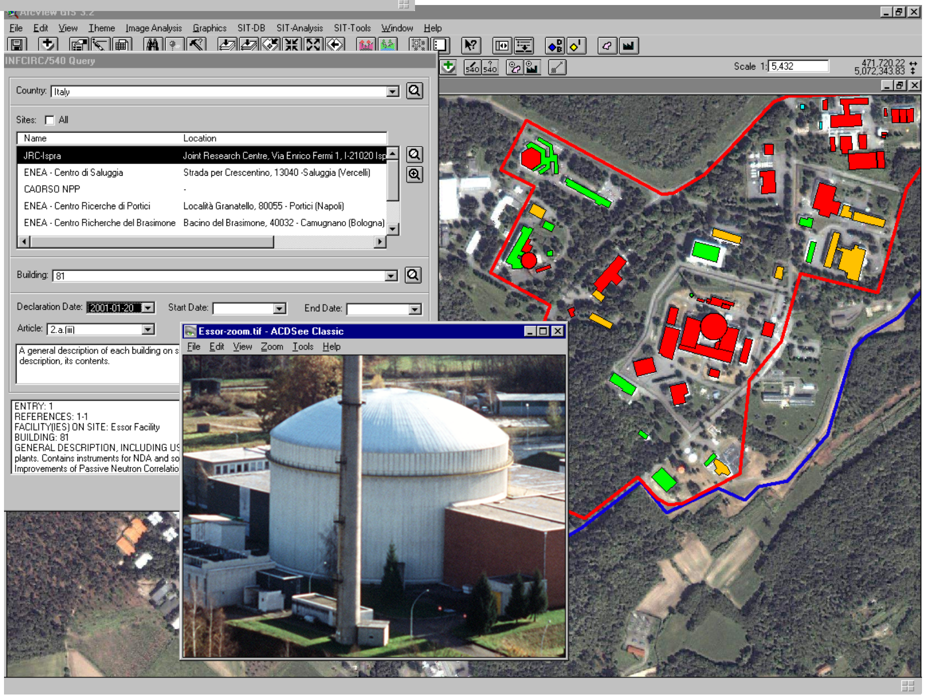
Latitude: 45.8167

Image Date (dd-mm-yyyy): 22-05-2000 Time (HH:MM): 10:16

Calc

- Launch of Ikonos in October, 1999 offered new verification possibilities

- Quickbird will be offering even higher resolution;


ArcView GIS 3.2
File Edit View Theme Image Analysis Graphics SIT-DB SIT-Analysis SIT-Tools Window Help
Scale 1: 5,432
471,720.22
5,072,343.83
Essor-zoom.tif - ACDSee Classic
File Edit View Zoom Tools Help

INFCIRC/540 Query

Country: Italy

Sites: □ All

Name	Location
JRC-Ispra	Joint Research Centre, Via Enrico Fermi 1, I-21020 Isp
ENEA - Centro di Saluggia	Strada per Crescentino, 13040 -Saluggia (Vercelli)
CAORSO NPP	-
ENEA - Centro Ricerche di Portici	Località Granatello, 80055 - Portici (Napoli)
ENEA - Centro Richerche del Brasimone	Bacino del Brasimone, 40032 - Camugnano (Bologna)

Building: 81

Declaration Date: 2001-01-20 Start Date: End Date:

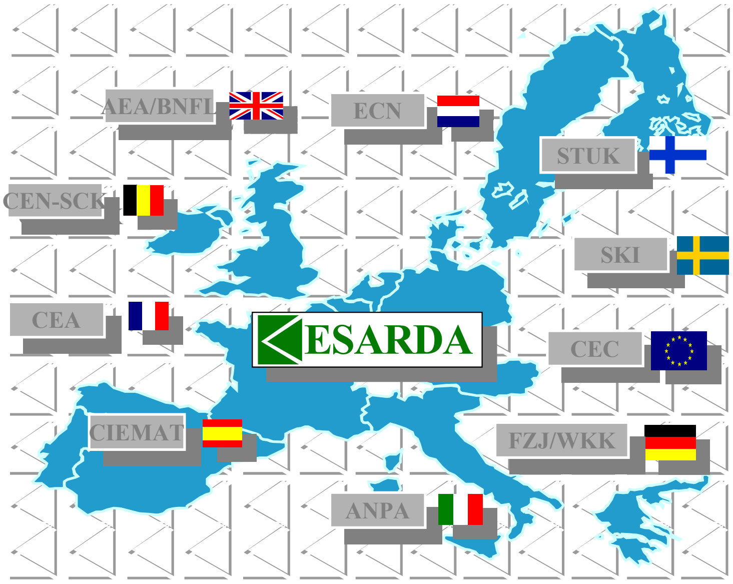
Article: 2.a.(iii)

A general description of each building on s
description, its contents.

ENTRY: 1
REFERENCES: 1-1
FACILITY(IES) ON SITE: Essor Facility
BUILDING: 81
GENERAL DESCRIPTION, INCLUDING US
plants. Contains instruments for NDA and so
Improvements of Passive Neutron Correlatio

networking

- European Safeguards Research and Development Association (ESARDA)
  - 12 partners, 10 states
  - liaison with Institute for
  - Nuclear Material Management (INMM)
- P-8 International Technical Working Group for Combatting Illicit Trafficking
  - JRC is founding member and co-chairs the working group
- Inter-Laboratory Evaluation Programmes
  - REIMEP: Regular Inter-laboratory Measurement Evaluation Programme
  - NUSIMEP: Nuclear Signatures Inter-laboratory Measurement Evaluation Programme



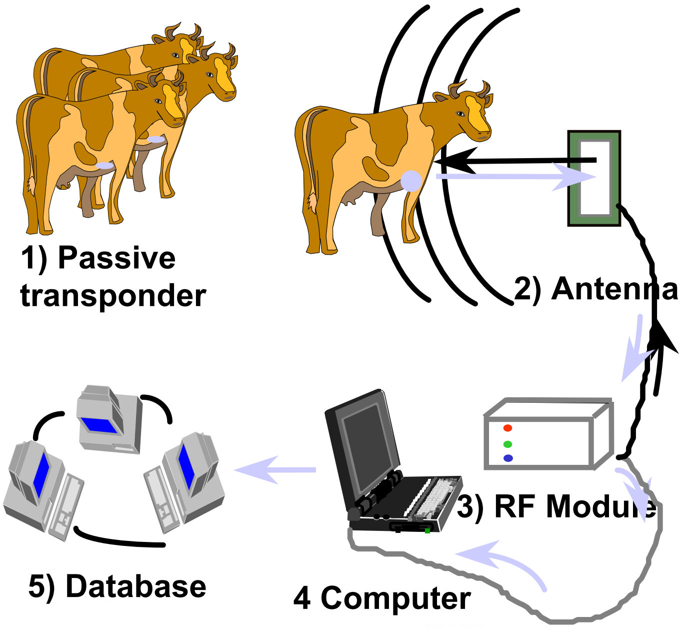
objectives of verification

- detecting non-compliance;
- deterring parties that might be tempted not to comply; and
- providing compliant parties with the opportunity to demonstrate convincingly their compliance;
  ⇨ applies to EU Policy monitoring;

compliance monitoring for other EU policies

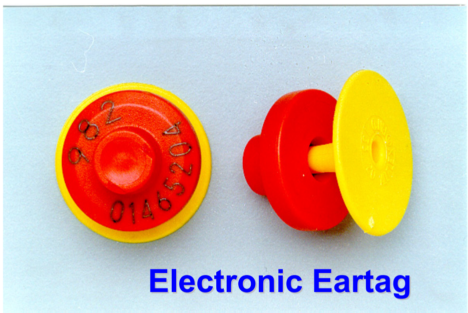
- Agriculture;
  - verifying crop acreages with satellite remote sensing;
  - tracking livestock from birth to slaughterhouse;
- Fisheries;
  - verifying vessel positions with spaceborne SAR;
- Customs and Taxation;
  - tracking containers across borders from open-source data;
- Environment;
  - detecting illegal discharging of oil at sea;

animal tagging



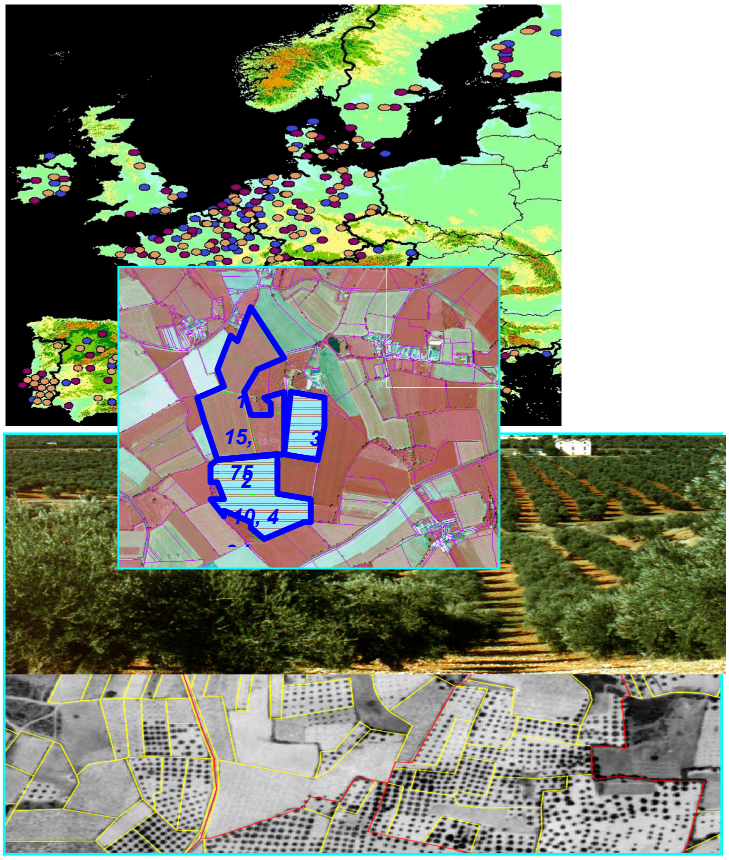
Injectable Transponder

Ruminal Bolus


Electronic Eartag

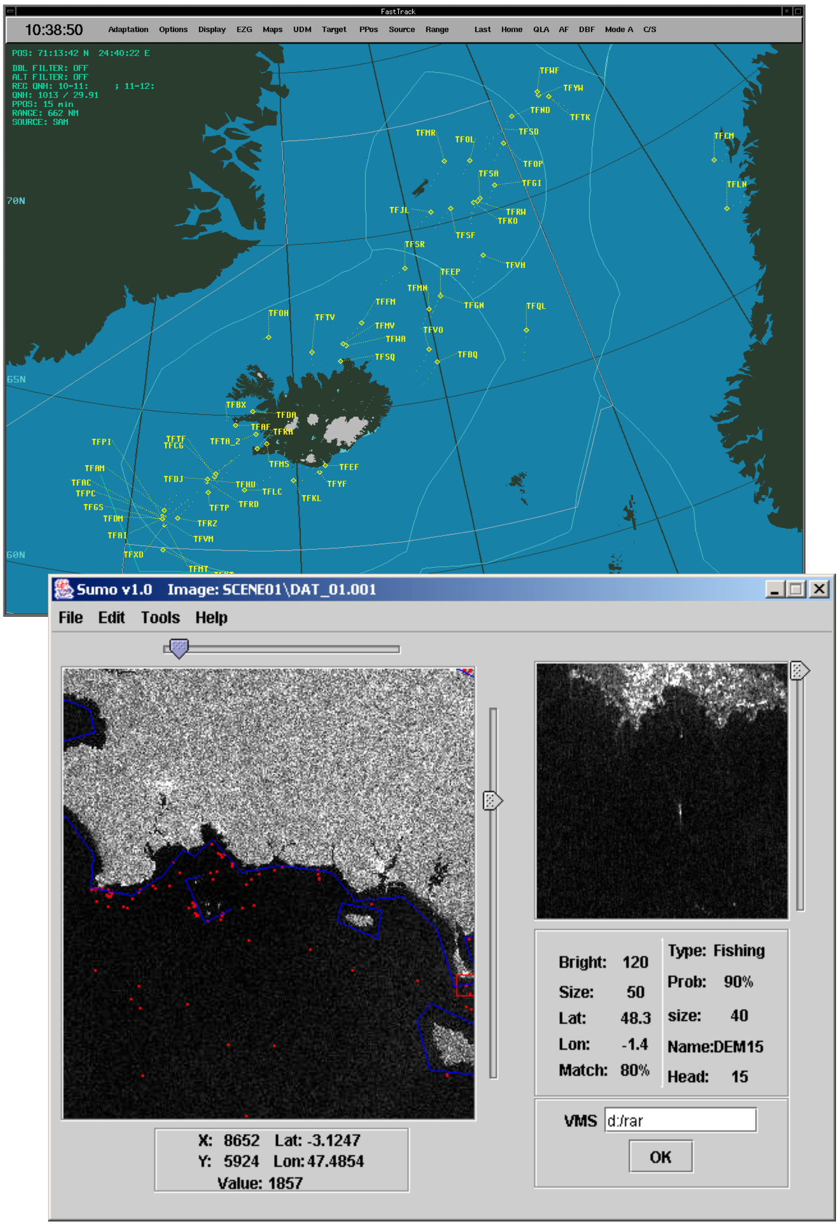
monitoring agriculture

- 1992 reform of CAP changed emphasis from price support to area subsidies (30 bn euro/y) and made better monitoring essential.
- MARS project:
  - develops and assesses EU land-parcel information system;
  - supports olive-tree and vineyard registers;
  - provides crop yield forecasts.



monitoring fisheries

- all EU vessels over 24 metres and vessels fishing in EU waters are monitored with GPS-based system;
- JRC using space-borne SAR to identify non-compliant vessels;
- partnership with EU authorities (and Norway and Ice-land), industry and academia



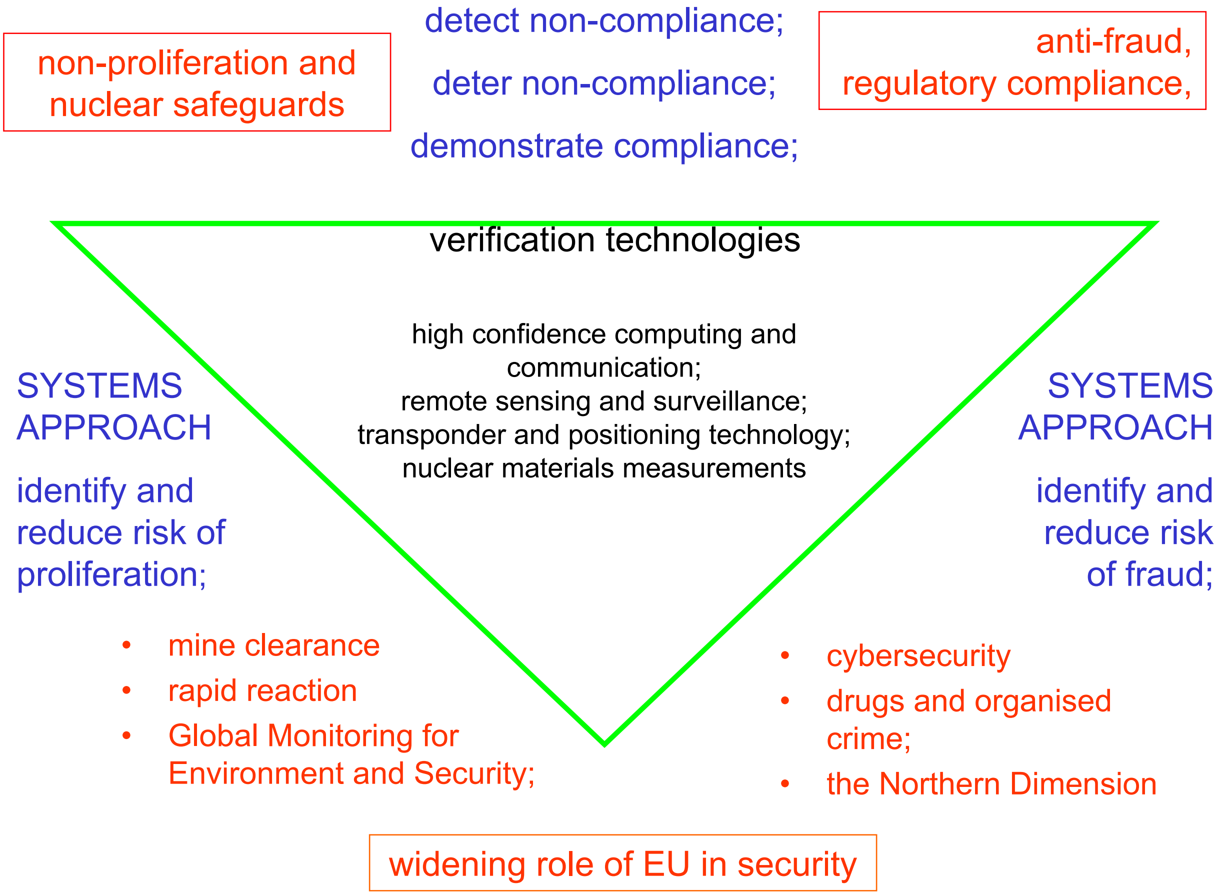
POS: 71:13:42 N 24:40:22 E
DBL FILTER: OFF
ALT FILTER: OFF
REC QNH: 10-11: ; 11-12:
QNH: 1013 / 29.91
PPOS: 15 min
RANGE: 662 NM
SOURCE: SAM

Bright: 120
Size: 50
Lat: 48.3
Lon: -1.4
Match: 80%

Type: Fishing
Prob: 90%
size: 40
Name:DEM15
Head: 15

VMS d:/rar

X: 8652 Lat: -3.1247
Y: 5924 Lon: 47.4854
Value: 1857



non-proliferation and nuclear safeguards

detect non-compliance;

deter non-compliance;

demonstrate compliance;

anti-fraud, regulatory compliance,

verification technologies

high confidence computing and communication;
remote sensing and surveillance;
transponder and positioning technology;
nuclear materials measurements

SYSTEMS APPROACH

identify and reduce risk of proliferation;

- mine clearance
- rapid reaction
- Global Monitoring for Environment and Security;

SYSTEMS APPROACH

identify and reduce risk of fraud;

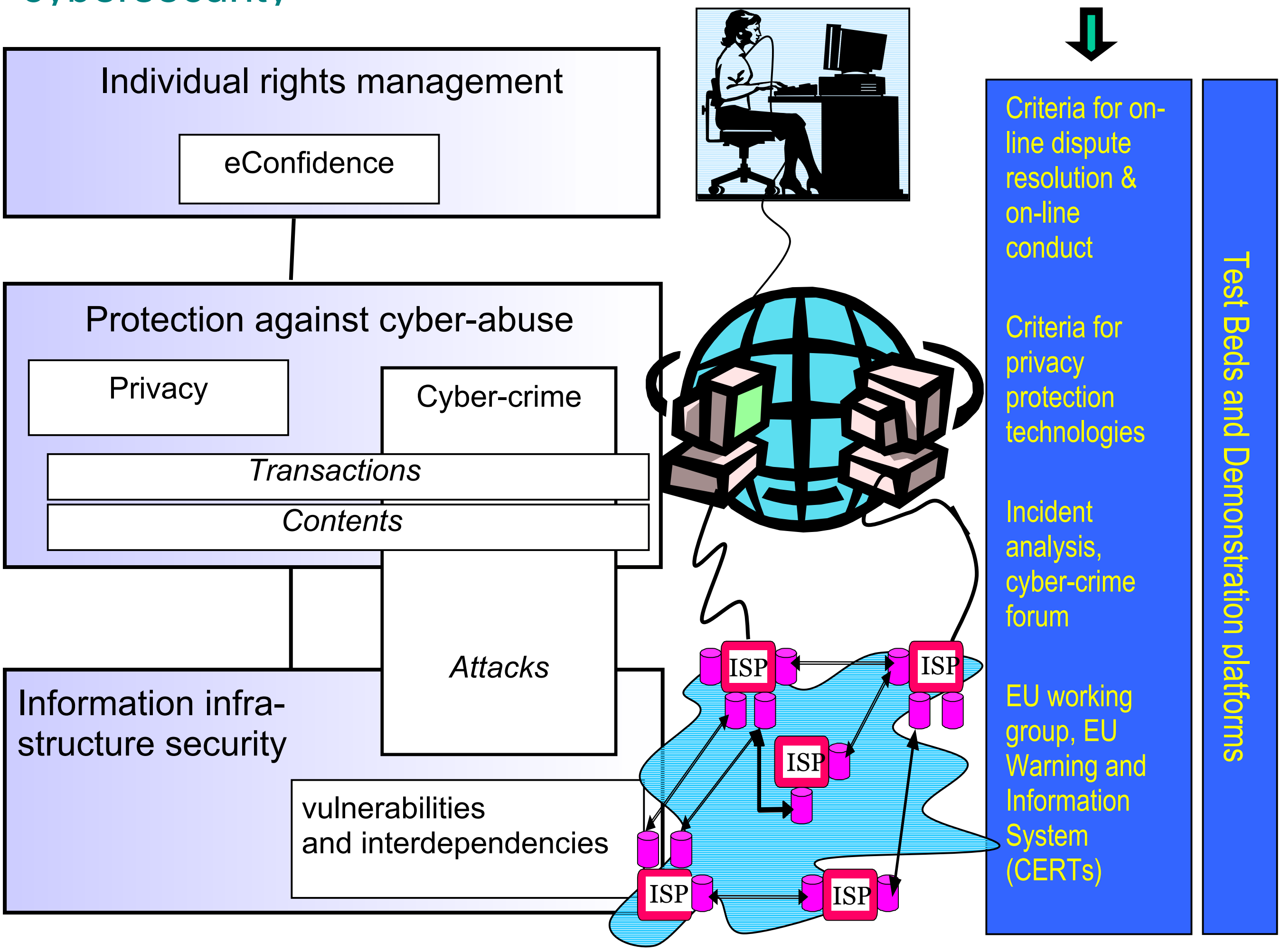
- cybersecurity
- drugs and organised crime;
- the Northern Dimension

widening role of EU in security

wider concept of security

- in the EU:
  - vulnerability of information infrastructure;
    - developing requirements for research needs;
    - benchmarking internet filtering tools;
  - natural and technological risks;
    - harmonised EU-wide information systems
- in the developing world:
  - the land mine challenge - technology used for clearance unchanged since Second World War;
    - evaluation and benchmarking of present and proposed technologies;
  - improving EU aid in humanitarian crises;
    - faster information - global monitoring for environment and security;

cybersecurity



Individual rights management

eConfidence

Protection against cyber-abuse

Privacy

Cyber-crime

Transactions

Contents

Attacks

Information infra-structure security

vulnerabilities and interdependencies

Criteria for on-line dispute resolution & on-line conduct

Criteria for privacy protection technologies

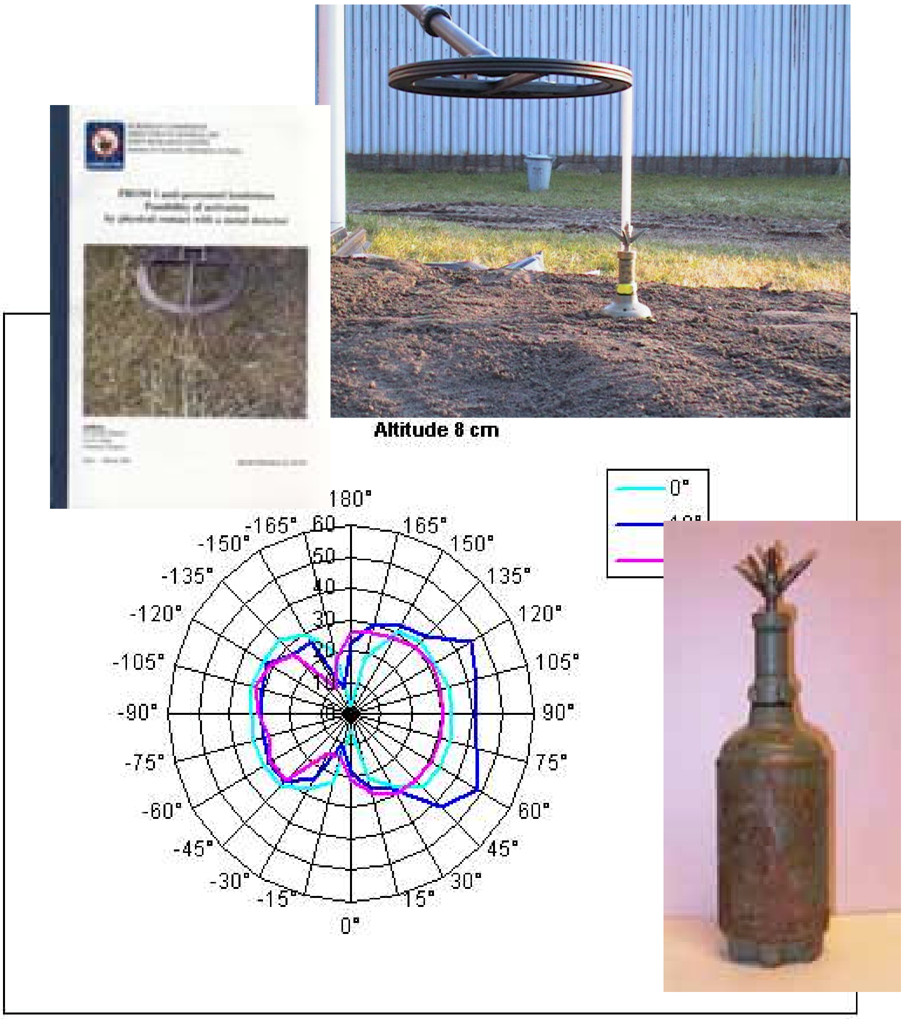
Incident analysis, cyber-crime forum

EU working group, EU Warning and Information System (CERTs)

Test Beds and Demonstration platforms

humanitarian demining

- one particular type of mine - PROM1 - causing most of casualties during demining operations in Balkans;
- measurements indicated reduced sensitivity in front of metal detector could cause mine to trigger before detection;
- recommendations for improvements in operating and training procedures;
- to reduce false positives need to develop methods for detecting explosive material - NQR, electronic noses;



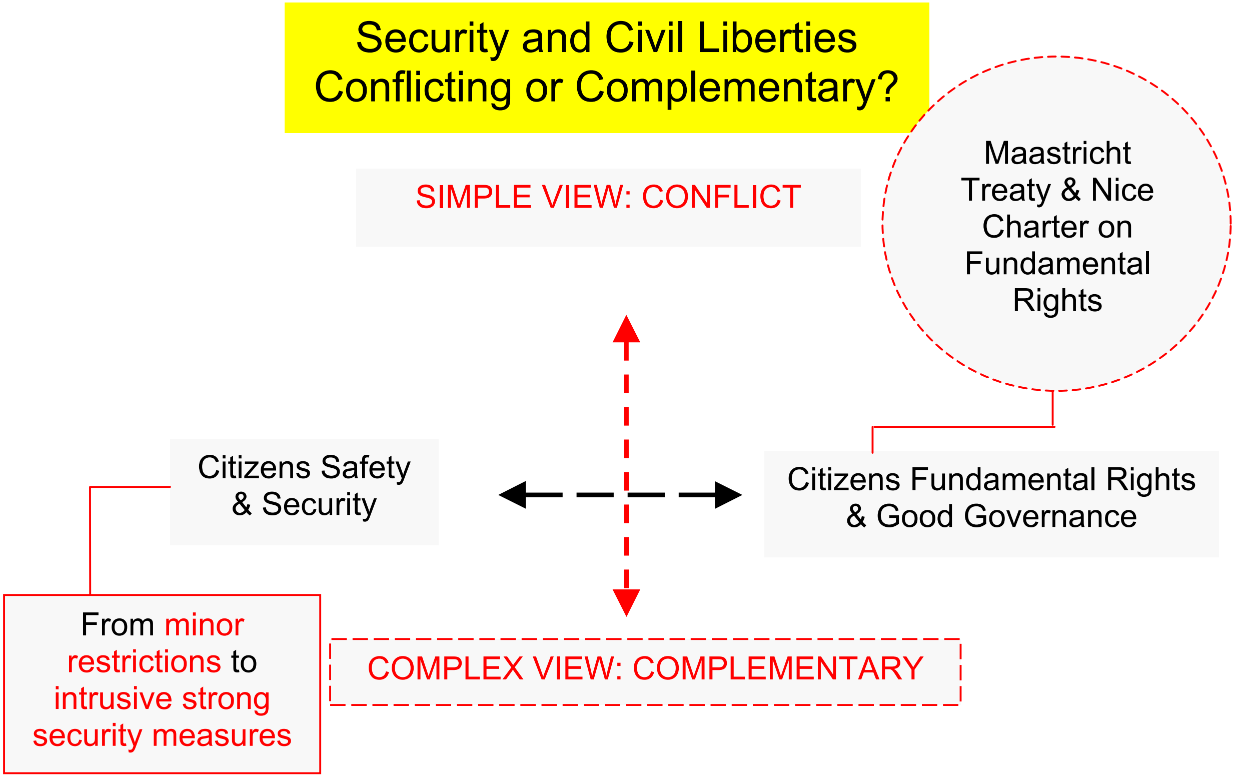
SAPITS proposal

- Safety of Arctic Pipeline and Transport Systems
- Geographic focus: NW Siberia & NW Russia
- Participation: Sweden, Finland, Germany, Russia, JRC
- Goals:
  - Integrated methodology (satellite, airborne, ground-based) for monitoring pipeline, marine & road transport systems
  - Identification/quantitative assessment of main risks of hydrocarbon-related marine operations in Russian Arctic
- Policy support:
  - EU-Russia Energy Dialogue; EU-Russia Space Dialogue (GMES); Northern Dimension Action Plan
- Current status - project under consideration

prospects and challenges

- increasing responsibility for security at a European level;
  - Common Foreign and Security Policy, European Security and Defence Policy. Schengen, European Union Monitoring Mission (in Former Yugoslavia)
- increasing integration of European scientific research;
  - European Research Area
- construction of European security infrastructure:
  - Galileo
  - Global Monitoring for Environment and Security;

vulnerability of society



Security and Civil Liberties
Conflicting or Complementary?

SIMPLE VIEW: CONFLICT

Maastricht Treaty & Nice Charter on Fundamental Rights

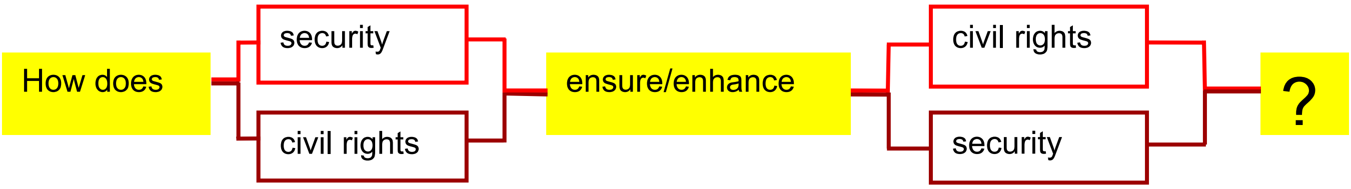
Citizens Safety & Security

Citizens Fundamental Rights & Good Governance

From minor restrictions to intrusive strong security measures

COMPLEX VIEW: COMPLEMENTARY

security and civil rights



How does

security

civil rights

ensure/enhance

civil rights

security

?

- potential contamination of blood supply:
  - need to identify HIV carriers to protect society;
- individual’s potential difficulty in obtaining health cover, work, insurance, mortgages:
  - confidentiality guaranteed by law to protect individuals;

Defence Research: Part of the Answer to Terrorism[25]

by **Mr Ken Peebles**, Director
NATO Research & Technology Agency
Neuilly sur Seine, France

Security in Europe is a broad subject, ranging from social to physical security, and covering economic, labor, medical and environmental amongst other types. I can speak with what little expertise I possess only about physical security of a nation or an alliance.

Threats to physical security can come from within a nation or from without. In the past the internal/external lines were clearly drawn, the threats were well defined (though not necessarily easy to counter). This has now changed; lines are blurred. Defence forces no longer have clearly defined threats or theatres. They have a mandate which is also quite blurred, a subject to which I will return.

In this talk I want to narrow the area of discussion to dealing with threats to our national and international security. We are focussed on terrorism now – with good reason. We should realize though that other threats – international crime and malicious informatics activity raise the same questions and can call for similar responses.

This threat to our society is working to disrupt and destroy the structures and means by which our western society operates. It aims, at a minimum, to demoralize us, to make us unable to function, and ultimately, to destroy us.

If we have defined the generic threat, how do we characterize the person who wields this threat?[26]

- He is willing to kill on a massive scale.
- He considers that the war is unrestricted
- He considers that the enemy might have vastly superior military power but is infinitely inferior in all moral aspects.
- He feels that the enemy is beneath contempt and it is therefore inconceivable to negotiate with him.
- He does not waste time to claim responsibility for or justify his attacks, to an audience he has no affinity with.

[25] Presentation to S&T Workshop in Support of European Security – Stockholm, 26 April 2002.

[26] F.E. van Kappen, MGen(Ret'd.), Policy Advisor Netherlands TNO,

These elements define what van Leewen (a Dutch specialist) defines as Catastrophic Terrorism. Based on the characteristics we have cited, you will realize that governments have no choice but to force such terrorists to accept unconditional surrender. They are not trying to make a point for subsequent negotiation. They are fighting to the death. This is a change. In the past we had small acts (in general, though not for those who were directly affected), against limited targets. They raised the profile of the terrorists and frequently there was negotiation. This has ended. The attacks are massive and they are devastating.

Who is it that undertakes such attacks? Here again we realize that we confront a new situation. In the past, spokespersons stood up to claim credit for an attack, and negotiated a desired end. No longer; as we have stated, negotiations are not the point.

The attackers are now anonymous and unrecognizable. There is no uniform, no facial or racial profile, no accent or stylistic characteristics that can be used. (We need to ensure that we do not think of Muslims as the source of terrorism, as the Oklahoma City bombing, the Sarin attack in Tokyo, as Northern Irish people and those living in the Basque regions of Spain will testify). The attackers may look perfectly "normal" and may have been apparently totally integrated into our society until such a time as they are ready to "emerge" and attack. Their behaviour until this time can seem to be perfectly ordinary.

They are not necessarily linked with states, though they may be.

They are sophisticated. The crude bombs of the past will continue to haunt us, but our adversaries are capable of much worse. They have access to and the necessary expertise for weapons of mass destruction – especially chemical, though the possibility of biological attack is real. And we are disturbed at the thought of a nuclear weapon – clean or dirty.

They have access to, and the skills to use, the informatics technology which is part of our daily life – a cornerstone of western society. We depend on the Web and its local counterparts, for banking, health, economics, shopping and communication. Terrorists are skilled in this technology, enough that they could use their knowledge to disrupt and destroy our ability to use it. Information warfare poses a significant threat, for it can be waged from a distance, anonymously and selectively.

There is an element which mitigates this threat, at least in its broadest form, and this is the fact that the utility of the Web and its global reach is such that the terrorists themselves depend upon it. Not perhaps to the extent we do, but enough that its total destruction is not probable. This does not preclude malicious bugs or viruses directed at specific targets.

This is the situation we face – an implacable foe, dedicated to destroying our society, horrifically, a foe who is almost impossible to identify and fanatical in his belief. This foe targets our citizens and our infrastructure. His attacks are surreptitious, unpredictable and devastating.

Another dimension to the security problem is the assignment of responsibility for response and overall security. Who does what? In the past, security responsibility was fairly straightforward, defence against physical attack – our armed forces. Police fought crime. Counter-espionage looked after spies. Pretty simple.

11 September has confronted us with a new set of rules, for the agencies involved include:

- Police
- Firefighters
- Military
- Health care
- Transport
- Security
- Private industry
- Postal services
- Public utilities
- Communications

Of the government agencies, some are local, some state or regional and some are federal. Put bluntly, many of these bodies do not know each other, and do not know how to talk with each other. Without talking, the possibilities of coordinated defence are minimal. And it is not just the people, those responsible in the agencies, who are not talking, for as we will see, databases are of fundamental importance. They exist in almost all the offices, they are needed to counter terrorism, and they are not designed to be accessed by, or communicate with, other agencies.

On a larger scale, we see the same problems of communication and interaction between nations. If, within a country, departments and agencies must act together, then so, when it comes to global security issues, must countries. Yet countries have different reactions to the same set of circumstances, the same event, and it is very hard to arrive at a coherent posture and a common approach. The speed of response on an international stage is not usually rapid. (The declaration by NATO of Article 5 was an outstanding contradiction of this last statement.)

What have I described so far?

- an implacable foe who will wage catastrophic terrorism
- a foe with whom we cannot talk
- a foe who is almost impossible to identify beforehand
- a foe who will strike at targets which can be almost anything – anywhere in our western society
- a host of dissimilar government agencies who must coordinate their efforts to respond
- national governments which assume different stances vis-a-vis the threats and required responses

This is not the most encouraging picture.

Let me move to the positive. We are not helpless, we have a strong capability and we can address what still needs to be done. The romantic in me also adds that we have the will and the love of our own values to prevail.

I want to address the theme of my talk - what can defence science, defence R&T contribute to the security issues I have been discussing? I have been a defence scientist all my working life, and at this moment have the privilege of directing NATO's Research and Technology Agency. We coordinate and support the activities of some 3500 experts each year, experts from across the alliance.

This past February we held a 3-day workshop (a brainstorming session, really) in Washington. Our goal was:

- To develop a list of high impact R&T areas that the RTO can sponsor as part of NATO's overall effort to combat terrorism; and,
- To foster a multi-national exchange of ideas that will enhance both national and multinational R&T activities for combating terrorism.

We arranged for 4 or 5 experts from each of our seven technology and systems panels to participate.

The first day of the Workshop was primarily devoted to Context setting presentations covering the following areas of interest:

- Threat Analysis and Status;
- Political, Military, Technological and Cultural Aspects;
- National Views and Initiatives.

Among the many highly qualified speakers, we had the honor to listen to Ambassador Francis Taylor (US), Ambassador at Large and Coordinator for Counter-terrorism, US State Department.

The two following days, participants were placed in one of four facilitated workgroups to discuss approaches to the Combating Terrorism issue based on generic attack scenarios. I will describe one imagined scenario in a moment showing how these categories of combat enter the total picture.

INDICATIONS & WARNING:

The workgroup studied improved terrorist and agent identification, surveillance and tracking capabilities to help prevent terrorist acts by facilitating the timely interdiction of terrorists and threat agents and devices, and the identification of emerging terrorist threats at an early stage.

Early warning of impending attack to enable the implementation of protective countermeasures was also part of its work.

SURVIVABILITY & DENIAL:

The second group looked at effective means for limiting access to facilities, combined with advanced threat detection and screening capabilities in order to inhibit many actions by terrorists by preventing them from reaching intended targets.

CONSEQUENCE MANAGEMENT & RECOVERY:

Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism were the main topics of the third workgroup.

ATTRIBUTION AND COUNTER-ACTION:

Finally, rapidly and reliably identifying the perpetrators of terrorist incidents will enable the planning and execution of appropriate counter-action operations as well as the implementation of effective countermeasures to possible additional attacks.

Improved forensic capabilities will also support criminal prosecution efforts by the appropriate governmental entities in each country.

New capabilities for conducting such operations with greater speed, precision and a higher level of assured effectiveness were studied with the aim in mind of reducing casualties suffered by national/coalition forces and minimizing fratricide problems, particularly in hostage situations.

For all sub-groups, a systematic approach has been followed:

- Threat
- Scenarios
- Capability
- Technology
- Research Topic
- Potential Collaboration

This approach prevents jumping directly from a problem to a particular solution.

It required each group to describe a set of realistic scenarios, to demonstrate a comprehensive list of necessary capabilities, to review the range of technologies that would fulfil these capabilities, and to systematically prioritize necessary research, evaluating opportunities for co-operation.

The sub-groups described a variety of scenarios. These scenarios were derived by the attendees, and as such are in no way official. They were used for exploring the parameters of the threat and the combat. They included:

- Attack on a highly populated point target with explosives
- Cyber attack on critical infrastructure
- Radioactive attack against a key node (either military or civilian)
- Medical pandemic – smallpox

Of course, a combination of different scenarios would have a devastating multiplier effect, weakening multiple parts of society.

To be more explicit, let’s take an example, in order to illustrate how the categories of combat worked, and the kind of issues that are raised (issues, not necessarily solutions).

The selected threat is ‘smallpox’.

We can even imagine that the virus has been genetically modified in such a way that it can generate a medical pandemic (transmissible to both humans and animals).

Imagine that a group of terrorists has a stock of smallpox viruses. It’s not fiction: our intelligence knows that there are such stocks in countries outside NATO. We know the location of some of them and some we don’t.

Imagine that some “kamikaze” terrorists decide to inoculate themselves with the virus. This means that they (in fact about 60% of them) would die: prevention and cure present immense problems. And, they would be contagious for about 15 days, with no visible symptoms.

The terrorist team boards a commercial plane. After one hour, probably 60 to 80 % of the passengers will have been inoculated with the virus.

The same day, or the day after, all the passengers of the plane will take another mode of transportation, such as train, cab, or metro, and will contaminate other people. Finally, they will arrive at their home and/or their office, and contaminate their families and colleagues. It will continue like that for about two weeks.

Then, the first inoculated persons will develop symptoms: just headaches and fever. Some will not consult a doctor.

Others will likely consult a medical generalist, and possibly contaminate his office. Very probably, the diagnostics will be inadequate: almost nobody can at present recognize smallpox, which has been officially eradicated from the planet since the 70s.

After another ten days, the infected population will start dying, some pustules appearing on the skin and in the lung, resulting in asphyxia. That will be the first trigger for the epidemic.

After some days, hospitals will have to face the arrival of tens or hundreds of thousands of dying people.

Let’s now come back to the workshop sub-groups.

One dealt with indications and warnings.

In our example:

How to detect stocks of smallpox viruses? It’s mainly a matter of intelligence, but there is a capacity shortfall and technology can probably help.

How to detect a virus in somebody’s body? No solution now, certainly not in the near or middle term.

How to detect biological agents in a plane? Again no solution now, but we can imagine that the air conditioning system could be adapted to include detection features.

How to discover that there are some ‘abnormal’ symptoms appearing in several dispersed medical facilities? Here, there are clearly potential solutions, based on the networking of medical generalists, hospitals, and clinics, linked to a central agency where statistics can be analyzed, and from where guidance and warnings can be transmitted to individual medical teams.

The second sub-group discussed survivability and denial.

Again, in our pandemic example:

How can we prevent a group of infected persons from entering a plane? Maybe by procedures, such as re-introducing the use of vaccine certificates on passports?

How can we prevent the virus from propagating in the plane? Clearly again, no solution for the moment. Perhaps by using adapted filters in the plane air conditioning system.

How can we keep the medical units that are on the first line in our example from being among the first victims of the virus? Perhaps by special masks, or different techniques for interacting with dangerously infected patients.

The third sub-group dealt with consequence management and recovery.

In our example:

How would a city like Berlin or Rome manage the treatment of tens of thousands of infected men and women? It’s not medical treatment per se since there is no cure for smallpox.

It’s population management: Where to put these persons (quarantine), how to manage their last days, and, what to do with them after their last day?

We have seen some solutions in addressing the foot and mouth epizootic disease in Europe.

Is the population ready to apply the same solutions to human beings? Is it possible to apply better solutions?

Again, there is a clear lack of capability. Perhaps equipment solutions can be identified, and probably technology will help.

The fourth sub-group discussed attribution and counter-action.

In the chosen scenario, it would be extremely difficult to identify the guilty (attribution). Intelligence would have to be used intensively. It's not intelligence based on satellites, but on viruses' signatures, pathogens' characteristics, etc.

Here, and in counter-action, key capabilities have to be determined, and, in the long-term, we would hope that technology development would provide solutions.

The constraints we had to face during this workshop were that:

- we had no clear political guidance, nor formal NATO requirement statement;
- and, several non-technical, non-military factors, such as;
- sociological considerations;
- infrastructure vulnerabilities and strengths;
- psychological effects;
- intergovernmental coordination issues, etc. - appeared to be critical factors that the NATO Defence R&T Community alone could not deal with.

I might point out here that, while Defence R&T does not hold all the solutions for the scenarios we looked at since most solutions lie outside defence science, it is often defence scientists who are able to define the problem and who possess expertise which is unique in its contribution to solutions.

The workshop produced ideas for technologies and technological issues that need to be addressed in combating terrorism.

Given that the work of the experts was conducted over only a bit longer than one day, a large volume of topics was not expected.

Given that the participants represented a wide technical spectrum and many nations, it was expected that the ideas would be worthwhile, and could well be unique.

The areas of proposed cooperative research are listed here in summary form. They are detailed in the body of the report.

- Sensors & Biometrics
- Database Technologies (e.g. NATO Information Architecture for Rapid Warning and Attribution Analysis)
- Cyber Security / Protection
- Decision Support / C2 (e.g. Risk Communication & Management)
- Modelling & Simulation

- Biological
- Access Control
- Training
- Material Tagging
- Weapons (e.g. Novel Energetic Materials)
- Physical Protection

The report will be distributed throughout the nations of the Alliance. They are expected to further distribute it within their R&T communities for consideration by national experts as to whether the ideas and suggestions are suitable for the definition of a national program based on one or more of the ideas. A related benefit of the workshop is that national representatives who participated are expected to carry home with them the ideas that were discussed (even those that were not documented fully) and to expand these ideas in a national context.

The report will be distributed to each of the panels of the RTO and to the NMSG. These bodies are charged with considering the issues and studies recommended in it and to define how they might contribute to them, either individually or jointly. They will be asked to report back to the RTB on their conclusions and recommended way ahead.

The Strategic Commands could take advantage of this report to define new capability & equipment requirements.

Finally, this study could trigger better cooperation between the military and the civil world at least in the area of Command, Control & Consultation.

Another study is on the way: a Specialist Team from our Systems Analysis and Simulation Panel will develop terrorist scenarios before the end of this year.

The DARPA Example

by **Ralph W. Alewine III**, Deputy Ass to the
Secretary of Defense
Nuclear Treaty Programs
Arlington VA, USA

Introduction

- Mission - Radical technical innovation for national security
  - Lead change and prevent/create technological surprise
- Secretary of Defense's research & development agency
  - DoW s corporate center for revolutionary ideas

Major Investment Areas

- National Level Problems
  - Deter, defeat threats to national survival
- Operational Dominance
  - Evaluate, demonstrate future systems concepts that provide decisive advantage to U.S. warfighters
- Core Technologies
  - Develop, demo high-risk, high-return technologies that can revolutionize military systems

Comparison of Roles - The DoD requires both radical innovation and requirements-based R&D

DARPA

Bottom-up, opportunity, event-driven
Great process flexibility
Integrated research
Radical change
Central DoD agency for R&D
Planned product obsolescence

Service R&D

Top-down, requirement, schedule-driven
Highly formalized processes
6.1 - 6.5 research separated
Reliable, sustainable gains
Support Service mission
Planned product improvement

Making Innovation Work

Strategy

- Anticipate and create the military future
- Quick reaction to urgent national security problems and needs
- Emphasize high impact payoff or revolutionary technology potential despite high technical risk
- Focused programs, not collections of contractors
- Compete openly and widely for the best ideas, capabilities, and technical managers
- Employ the best performers for program execution

Operations

- Keep organization small and limber; maintain no facilities
- Support fast turn-around through rapid, flexible, but carefully monitored, contracting procedures
- Work with Services and operational forces to understand their needs and concerns, but do not fund R&D which: does not involve high risk; does have a near-term focus, and the Services are capable of doing for themselves

Management Approach

Each program creates a virtual organization:

- Drawing performers from industry, academia, national labs, not-for-profits, domestic and international entities (Ni
- Drawing technical evaluation, management expertise, and contracting services from other DoD and US Government sources
- Partnering with military Services for experimentation and transition

Program Selection

- DARPA's primary mission is to effect Revolutionary Change
- Applications or extensions of existing technology are rarely if ever approved for DARPA funding
- There is no set funding level or percentage for any focus area
- DARPA programming is bottomup
- DARPA Management evaluates:
- Program goals and objectives
- Program structure and content
- Whether a program concept represents a Revolutionary versus Evolutionary change

Some Current Focus Areas

National-Level Problems

- Emerging Asymmetric Threats: Protection from Bio, Info & Terrorist Attack

Operational Dominance

- Mobile Target Detection & Kill
- Classification of Hard, Deeply Buried Targets
- Combined Manned, Unmanned Operations
- Littoral Dominance
- Robust, Mobile Communications & Networking
- Dynamic Planning/Replanning

High-Risk, High-Payoff Technology Exploitation

- Information Exploitation
- Microsystems & Nanotechnology
- Beyond-Silicon Electronics
- Materials
- Intersection of Biology, Information and Microsystems

Humanitarian Aspects of Security

by **Valerie A. Hood**, Secretary General
EURISY Association
Paris, France

Security in this connection is one of the very few "politically correct" possibilities of the use of this word in the current climate in Europe. Despite comments to the contrary and concrete examples of ongoing dual use where the civil and military overlap, e.g. Kosovo, launch of military satellites on civilian launchers such as Ariane, use of civilian remote sensing and meteorological satellites by the military, civilian use of declassified data from military satellites for archaeological research, dual use of communications satellites, mutual interest in scientific developments, European organisations are reluctant to be seen to have any connection whatsoever with anything remotely military to the extent that although security covers a multitude of topics from politics to food it is the silent "s" in the EC/ESA initiative of GMES.

Relief workers dealing with the aftermath of a disaster whether as a result of human error, such as Bhopal, military action such as Kosovo, or natural disasters such as the earthquakes in Turkey or Hurricane Mitch, need three basic tools – communications facilities, accurate meteorological data and maps.

Thanks to communications satellites for most of the world emergency communications links can be established soon after the disaster via satellite. This is also true for computer links provided there are laptops. Now technology has also provided general access to GPS, although this may at the moment not be available if the US military have decided to cut off access. However the ESA/EU Galileo system will remedy that problem. In the longer term of reconstruction and for medical aid data transmission via satellite and educational interactive programmes are also a concrete possibility via satellite.

Access to adequate maps is rather more difficult. Outside the developed World there may be no up-to-date maps or access may be restricted through national security concerns. If the disaster is as a result of military action then there will be military maps in plenty but the embargo on dual use makes it difficult if not impossible to transfer these, once the military no longer needs them, to NGOs.

The ESA/CNES initiative to programme the satellite and provide satellite remotely sensed data free of charge to all disaster struck areas or regions – the Charter – has now been adhered to by India, Canada, and NOAA which greatly enhances the chances of a remote sensing satellite being overhead at the time the disaster occurs. It is not however infallible since they are all polar orbiting. They may however have archived data over the area. Before these data are of use to relief workers they need to be transformed into information and this takes time. These data are therefore of smarter use in the reconstruction period. High resolution satellite data are now available and can be used as an alternative to maps but at a cost few NGOs can afford. In flood situations radar data are invaluable but again need time to be transformed to useful information. In post crisis situations satellite derived information is useful for determining suitable sites for refugee camps and can be useful as a means to identify possible mined areas by means of land use change detection and also to give an idea of the type of terrain deminers will have to contend with when demining.

Meteorological satellites provide continuous meteorological data which are directly useful especially to predict further bad weather. These data are widely available at both national and regional level.

How can the situation be resolved? Basically what is needed is a centralised clearing house which can relay user requirements to the satellite providers to programme the satellite and then contact a specialised commercial entity or the military to transform the data into information and send it to the user. The competence exists in Europe. The problem is to get all the actors together and to finance the operations. However, if the clearing house existed it could also pre-collect information on known trouble spot areas and build up a library of disaster information (first European, then global……)

US - Europe Technology Gap

by **Ruurd Lutje Schipholt,** Director
Netherlands Institute of Applied Geoscience, TNO
Delft, The Netherlands

It is well known that the US spends many times more than Europe on defense R&D. It is important to understand the underlying reasons and resulting consequences. Only then can a sensible European reaction be considered. Quite a different problem is if common European action resulting from those considerations will be feasible.

I suggest that the underlying reason for the US to invest so much in defense technology is less a result of being threatened than one of a desire to be winner in a world-wide (technical) industrial competition. Even before 11 September 2001 the defense R&D expenditure in the US was much higher than that in Europe and was not reduced in step with overall defense budget reductions. That did not only create a revolution in military affairs, but also a competitive edge to US defense industry. And as a spin-off growth in other areas of the US economy.

Theoretical studies in the transfer efficiency of defense R&D for growth of economy compared with civilian R&D investment rate the latter higher. But in the US system state subsidy of R&D in defense is much more accepted than other forms of subsidy, especially after 11 September 2001. It will also lead to dominance of the defense industry-market and therefore to foreign military sales, with a levy for R&D investment. No technology transfer to the customer, but a refund to the US Government for their R&D investment.

As an example 1 might give the present Missile Defense program. A technological challenge comparable to putting the first man on the moon. The Missile Defense Agency has been given full authority by the US Government to direct and co-ordinate all efforts for this program (and funding is ample). They have stated as their mission, I quote:

* Innovation: Encourage and sponsor forefront research and development to enhance national security

* Technologies Transition: Find new ways to transition promising technology from the research phase into early development

* Commercialisation: Aggressively move defense technology into the sector to enhance economic security

* Education: Assist the quality training of student scientist and engineers in disciplines critical to national security.

The consequence of this immense investment in defense and its R&D and industries is world dominance. For the European partners in NATO this will have mainly military and political implications. The European defense industries will find ways to create partnerships or subcontracting roles with US defense industries as defense markets in Europe shrink and globalisation progresses.

The European influence on security matters in the world will diminish due to the disparity in defense effort compared to the US. The possibility of having military operations with the US will fade away due to the discrepancies in technology in the material and the unilateral development of US military doctrines. NATO partners on both sides of the Atlantic will drift apart.

If on the other hand the European nations, through the European Union, pool their effort and increase the volume in civilian R&D investment the growth in economy in our region will be safeguarded. That is a big if… Because at the base of good R&D lies investment in first class education. R&D is not mainly the task of industry as suggested by our European political leaders. The approach and results of those areas in Europe are points of serious concern. Furthermore separating military and civilian R&D investment, as is presently the case in Europe, is getting more and more irrelevant and wasteful. Dual use technology for civilian and military applications is rapidly gaining in importance as we all know.

Pooling of brains and resources in R&D, as the federal US Missile Defense Agency is doing, is up to now in Europe a possibility of Utopian scope. The result of this lack of European vision was not addressed seriously in the recent top meeting in Barcelona. That lack of unified approach to defense R&D will make matters worse.

Having a European say in world security matters without serious increase (and pooling) in defense budgets and defense R&D investment, will not be possible. In that respect a NATO of two speeds is already a fact. We get what we pay for. There is no free lunch.

Not investing enough in making our technological society more robust against terrorist attacks, will make our society more and more vulnerable, with possibly enormous economic consequences.

R.M. Lutje Schipholt March 2002

Information Technology and Crisis Management

Speech by **Jaakko Iloniemi,** Minister
Office of President Ahtisaari
Helsingfors, Finland

Ladies and Gentlemen:

During the recent years a significant effort has been mounted by various actors to make their crisis prevention and response capability more timely and effective. Among the other measures taken, the usage of latest information technology has expanded rapidly within the organisations ensuring the security of citizens. At the same time the crisis situations have grown more complex and whole new types of security threats have emerged, as we have tragically come to notice since last September.

Indeed, - terrorism is a good example of the new security threats that seriously challenge what is still a largely state-centred security system. In addition to terrorism, corruption, organised crime, drug trafficking, spreading of small arms and proliferation of weapons of mass destruction make our societies extremely vulnerable. Societies that are recovering from internal conflicts or where the state authorities are weak or the whole state apparatus has collapsed are the ones threatened most seriously.

Adequate response to different emergency situations require rapid, concerted action of several actors. This applies as well to situations like September IIth as to missions like UNMIK in Kosovo. Both military and civilian actors in the field should join in a shared effort to mitigate and resolve the crisis at hand. Within a single operation the core processes should not be confined separately inside each individual organisation but there should be I flow between all the key players.

Modern, well utilised information technology is a necessary enabler in order to solve this challenge. The technology as such is hardly the driver of the organisational change. It can, however, provide decisive support for the administrative innovation by implementing new kind of thinking into the tools of everyday work.

It is not feasible to expect that different organisation commit to the same products. Different organisations have different needs, and they must be able to address their particular needs with the most suitable products. That is why adoption of common standards will play an important role in enhancing the interagency information flow and cooperation in crisis management.

The deployment of common standards is a long-term project for the crisis management community. While the standardisation will certainly pay off in the long run, the effort needed is difficult to legitimise if one only looks at the short-term spending within a single organisation.

At the moment my employer, the Crisis Management Initiative, is contributing to the positive development in the interagency coordination by participating in the project called Information Technology and Crisis Management. The objective of the ITCM project is to develop and deploy a decision-making support and knowledge management system that meets the specific requirement of modern crisis management. The development is based on close cooperation with crisis management organisations and on the Object Management Group's evolving C4I standard for command, control, communication and intelligence systems.

List of Participants

Aleksi Aaltonon, ITCM Expert
Office of President Ahtisaari
Erottajankatu 11A, 4th floor
00139 Helsinki, Finland
Tel +358 9 6987024
Fax +358 9 6127759
E-mail aleksi.aaltonen@ahtisaari.fi

Marc Acheroy, Professor
Royal Military Academy
Avenue de la Renaissance 30
B-1000 Brussels, Belgium
Tel +32 2 737 6470
Fax +32 2 737 6472
E-mail acheroy@elec.rma.ac.be

Ralph W. Alewine III, Deputy Ass to the Secretary of Defense
Nuclear Treaty Programs
1515 Wilson Boulevard, Suite 720
Arlington, Virginia 22209, USA
Tel +703 588 1983
Fax +1 703 588 1984
E-mail alewinerw@att.net

Bengt Anderberg, Director General
Swedish Defence Research Agency, FOI
SE-172 90 Stockholm, Sweden
Tel +46 8 55 50 3000
Fax +46 8 55 50 3100
E-mail bengt.anderberg@foi.se

Ian Anthony
Stockholm International Peace Research Institute, SIPRI
Signalistgatan 9
SE-169 70 Solna, Sweden
Tel +46 8 655 97 59
Fax +46 8 655 97 33
E-mail anthony@sipri.org

Peter Bröms, Senior Analyst
Europol
PO Box 90850
NL-2509 LW The Hague, The Netherlands
Tel +31 70 302 5197
Fax +31 70 345 5896 or +31 70 302 5450
E-mail BromsP@europol.eu.int

Martin Dahinden, Director
Geneva International Center for Humanitarian Demining, GICHD
P.O. Box 1300
CH-1211 Geneva 1, Switzerland
Tel +41 22 9061660
Fax +41 22 906 1690
E-mail m.dahinden@gichd.ch

Ola Dahlman, Director
OD Science Application AB
Fredrikshovsgatan 8
SE-115 23 Stockholm, Sweden
Tel +46 8 6628575
Fax +46 8 6675617
E-mail ola.dahlman@scienceapplication.com

Thérèse Delpeche, Director
French Atomic Energy Commissariat, CEA
31-33, rue de la Fédération
75752 Paris cedex 15, France
Tel +33 1 40 45 10 00
Fax +33 1 40 56 15 16
E-mail ROHRMAIER@aramis.cea.fr

Also:
Senior Research Fellow
CERI
56, Rue Jacob
75006 Paris, France

Mona Dreicer, Office Director
Bureau of Verification and Compliance
Office of Nuclear Affairs (VC/NA)
2201 C Street NW
Washington DC 20520, USA
Tel +1 202 647 6405
Fax +1 202 736 7634
E-mail DreicerMo@T.state.gov

Rolf Ekeus, Chairman of Board
Stockholm International Peace Research Institute, SIPRI
Signalistgatan 9
SE-169 70 Solna, Sweden
Tel +46 8 655 97 00
Fax +46 8 655 97 33
E-mail ekeus@sipri.se

Richard Escritt
Director European Commission Research
Rue de la Loi 200
SDME 05/62
B-1049 Brussels, Belgium
Tel +32 2 2950725
Fax +32 2 2991605
E-mail richard.escritt@cec.eu.int

Jan Foghelin, Director
FOI, Division of Defence Analysis
SE- 172 90 Stockholm, Sweden
Tel +46 8 55 50 3745
Fax +46 8 55 50 3866
E-mail jan.foghelin@foi.se

David Heyman, Director and Senior Fellow
Science and Security Programs
Center for Strategic & International Studies, CSIS
1800 K Street N.W
Washington, DC 20006, USA
Tel +1 202 775 3293
Fax +1 202 775 3199
E-mail dheyman@csis.org

Valerie A Hood
Secretary General
EURISY Association
3 – 5 Mario Nikis
75015 Paris, France
Tel +33 1 47 34 00 79
Fax +33 1 47 34 01 59
E-mail eurisy@micronet.fr

Jaakko Iloniemi, Minister
Office of President Ahtisaari
Erottajankatu 11A, 4th floor
00139 Helsinki, Finland
Tel +358 9 6987000
Fax +358 9 6127759
E-mail jakko.iloniemi@ahtisaari.fi

Arne Jernelöv, Acting director
International Institute for Applied Systems Analysis, IIASA
Schlossplatz 1
A-2361 Laxenburg, Austria
Tel +43 2236 807 653 or +43 2236 807 477
Fax +43 2236 807 201 or +43 2236 807 366
E-mail jernelov@iiasa.ac.at

Erik van de Linde
RAND Europe
Newtonweg 1
2333 CP Leiden, The Netherlands
Tel +31 71 524 5151
Fax +31 71 524 5191
E-mail vandelinde@rand.org

Rolf Linkohr
Member of European Parliament
Rue Wiertz
B-1047 Brussels, Belgium
Tel +32 2 284 5452
Fax +32 2 284 9452
E-mail rolf.linkohr@europarl.eu.int

Lars–Erik Lundin, Head of Unit Security Policy
European Commission
External Relations Directorate-General
Rue de la Loi/Wetstraat 200
B-1049 Brussels, Belgium
Tel +32 2 296 5081
Fax + 32 2 295 0580
E-mail lars.lundin@cec.eu.int

Ruurd Lutje Schipholt, Director
Netherlands Institute of Applied Geoscience, TNO
P.O. Box 6000
NL – 2600 JA Delft, The Netherlands
Tel +31 15 2696716
Fax +31 15 269 6699
E-mail schipholt@rvb.tno.nl

Jenifer Mackby, Fellow
The Center for Strategic and International Studies, CSIS
126 rue des Gelinottes
01710 Thoiry, France
Tel +33 450 412 837
Fax +33 450 412 891
E-mail jmackby@csis.org

Gordon McBean, professor
Department of Geography and political Sciences
University of Western Ontario
1389 Western Road, London, ON Canada
Tel +1 519 661 4274
Fax +1 519 661 4273
E-mail gmcbean@eng.uwo.ca

Ken Peebles, Director
RTA (Research and Technology Agency) NATO
7 rue Ancelle
92200 Neuilly sur Seine, France
Tel +33 1 55612204
Fax +33 1 55612299
E-mail peeblesk@rta.nato.int

Alexander Pikayev, Co-chairman
Nuclear Non-Proliferation Programme
Carnegie Moscow Centre
16/2 Tverskaya str.
Moscow, 103009, Russia
Tel +7(095) 935 89 04
Fax +7(095) 935 89 06
E-mail alexp@carnegie.ru

Jean-Pol Poncelet, Director of Strategy and External Relations
European Space Agency
8, 10 rue Mario-Nikis
F–75738 Paris Cedex 15, France
Tel +33 1 5369 7183
Fax +33 1 5369 7181
E-mail jean-pol.poncelet@esa.int

Gary Samore, Senior Fellow for Non-Proliferation
The International Institute for Strategic Studies
Arundel House
13 – 15 Arundel Street
Temple Place
London WC2R 3DX , UK
Tel +44 20 73959106
Fax +44 20 7395 9192
E-mail samore@iiss.org

Alois Sieber, Head of Humanitarian Security Unit
Institute for the Protection and the Security of Citizen
I-21020 ISPRA (Varese), Italy
Tel +39 0332789089
E-mail alois.sieber@jrc.it

Bernard Sitt, Director International Cooperation
CEA/DAM-Ile De France
BP no 12
91680 Bruyères-le-Chatel, France
Tel +33 1 69267505
Fax +33 1 69267001
E-mail Bernard.sitt@cea.fr

Lena Torell, Director
Royal Academy of Engineering Sciences (IVA)
Grev Turegatan 14
Box 5073
SE-102 42 Stockholm, Sweden
Tel +46 8 791 29 00
Fax +46 8 611 56 23
E-mail lena.torell@iva.se

David R. Wilkinson, IPSC Director
European Commission - Joint Research Centre
Via E. Fermi, T.P. 361
I-21020 Ispra VA, Italy
Tel +39 0332 789947
Fax +39 0332 789923
E-mail david.wilkinson@jrc.it

Pia Övelius
Statsrådsberedningen
Regeringskansliet
SE-103 33 Stockholm, Sweden
Tel +46 8 405 10 00
Fax +46 8 723 11 71
E-mail pia.ovelius@primeminister.ministry.se

Marie Lindersjö, Secretary
Swedish Defence Research Agency, FOI
Box 1165
SE- 581 11 Linköping, Sweden
Tel +46 13 378347
Fax +46 13 378039
E-mail marie.lindersjo@foi.se

Agenda for Workshop on

Science and Technology in Support of European Security

April 24, 2002

19.30

Dinner

Hosted by the Ministry of Foreign Affairs

April 25, 2002

09.00 – 12.00

Welcome

- **Sven-Olof Petersson**, DG for Political Affairs, Ministry of Foreign Affairs, Stockholm, Sweden: *Intrductory Address - Issue to include".*

Introductory Address

- **Richard Escritt,** Director, Research Directorate-General European Commission: *"Science and Technology in support of European Security: A European ResearchArea Perspective".*

The New Security Agenda

Introductory presentations:

- **Mona Dreicer**, Director, US State Department, Washington: *"Science and Technology Support for U.S. Homeland Security".*
- **Lars–Erik Lundin**, Head of Security Policy Unit, European Commission, Brussels: *Brief points from an EU perspective on the New Security Agenda".*
- **Thérèse Delpeche**, Director, CEA, Paris: *"International Security after September 11".*

Short Presentation:

- **Jan Foghelin**, Head of Division of Defence Analysis, FOI, Stockholm: *"A Complex World Needs Complex Security Strategies".*

Discussion

12.00 – 13.30 **LUNCH**

13.30 – 15.30

Arms Control and Disarmament

Introductory Presentation:

- **Bernard Sitt**, Director, International Affairs, Atomic Energy Agency, Paris: "*What Role for Arms Control in the International Security Context of the New Century*".

Short Presentations:

- **Martin Dahinden**, Director, GICHD: "*Use of Modern Technology in Humanitarian Crisis*".
- **Ian Anthony**, Dr., SIPRI: "*The European Union Dual-Use Export Control System after 11 September: Is There a Need for Reform?*".

Discussion

16.00 – 18.00

Non-Proliferation

Introductory Presentations:

- **Rolf Ekeus**, Chairman, SIPRI, Stockholm: "*Non-Proliferation and the International Security*"
- **Gary Samore**, Senior Fellow for Non-Proliferation, IISS, London: "*Impact of September 11 on U.S. Nonproliferation Policy*".
- **Alexander Pikayev**, Co-chairman Nuclear Non-Proliferation Program, Carnegie Moscow Centre: "*Science and Technology: Versus or For Non-Proliferation*".

Short Presentation:

- **Ian Anthony**, Dr., SIPRI: "*Using technology in risk assessment*".

Discussion

April 26, 2002

09.00 – 12.00

The Vulnerability of the Society

Introductory presentations:

- **Peter Bröms**, Senior Analyst, Europol, The Hague: "*Organised crime in the European Union: The need for common action".*
- **David Heyman**, Senior Fellow and Director of Sience and Security Initiatives, CSIS, Washington: *"Bioterrorism and the Vulnerability of Society".*
- **Erik van de Linde**, RAND Europe, Leiden: *"Critical Infrastructure Protection".*

Short Presentations:

- **Gordon McBean,** Professor, Institute for Catastrophic Loss Reduction, The University of Western Ontario London, ON, Canada*: "Vulnerability from Natural Hazards and Implications for Security".*
- **Arne Jernelöv,** Acting director, IIASA, Laxenburg, Austria: *"What makes systems vulnerable".*

Discussion

13.30 – 17.00

Science for Security

Introductory Presentations:

- **Rolf Linkohr**, Dr.,European Parliament, Brussels: *"Science for Security".*
- **David Wilkinson**, Director, Joint Research Centre, European Commission, Italy: *"Technology for Stability and Security - Implications for the Euopean Union".*
- **Ken Peebles**, Director, RTA, NATO, Paris: "*Defence Research: Part of the Answer to Terrorism".*
- **Ralph W. Alewine III,** Dep Ass to the Secretary of Defense Answer, Nuclear Treaty Programs, Arlington, USA: *"The DARPA Example".*

Short presentations:

- **Valerie A Hood,** Secretary General, EURISY Association, Paris, France: *"Humanitarian Aspects of Security".*
- **Ruud Lutje Schipholt**, Director, TNO, JA Delft, The Netherlands:*:"Us-European Technology Gap".*
- **Gordon McBean**, Professor, Dept of Geography and Political Sciences, Univ of Western Ontario, London, ON Canada*: "Examples from Meteorological Services".*

- **Arne Jernelöv**, Acting director, IIASA, Laxenburg, Austria: *"Systems Analysis".*
- **Jaakko Iloniemi**, Minister, Office of President Ahtisaari, Helsinki, Finland: "*Information Technology and Crisis Management".*

Discussion

Concluding Remarks

- **Bengt Anderberg**, DG, Swedish Defence Research Agency (FOI), Stockholm, Sweden.