NATO OTAN

perCEPtions Newsletter

Civil Emergency Planning

Plans civils d'urgence

N°8 • September 2009

Supporting NATO Operations - Protecting Civilian Populations

PAGE 3-4
Energy Security:
- Jurgita Bilvaisiene – Lithuania,
- Diether Urban – Chairman of NATO's Industrial Planning Committee

PAGE 5-6
Cyber defence:
- Ligia Ferreira – Chairman, NATO's Civil Communications Planning Committee,
- Suleyman Anil – Head of NATO's Cyber Defence Coordination and Support Centre

PAGE 8
- Piracy: Jim Caponiti – Chairman of NATO's Planing Board

PAGE 9
- Pandemics: Eric Lecarpentier – Chairman of NATO's Joint Medical Committee

PAGE 12
- NATO Science Programme on cyber security in Partner countries – Jayne Clinton

PAGE 13
- Developments in the SCEPC

PAGE 14-15
- EADRCC Update: The AidMatrix - Günter Bretschneider, Head EADRCC

Editorial

by Martin Howard, NATO Assistant Secretary General for Operations

NATO Civil Emergency Planning – New threats and challenges

Contrary to the past, today's security challenges focus almost entirely on protecting people rather than territory. The new threats and challenges featured in this issue illustrate this only too clearly. Energy security, cyber defence, piracy and pandemics all transcend national boundaries and affect people rather than national borders.

This issue aims to raise a number of questions. Is CEP doing enough? Could CEP be more involved and contribute in other areas? Does CEP's pool of civil experts contain the right mix to address these challenges? One topic, not covered in this issue, is that of climate change and its potential to exacerbate existing risks to nations' stability. Should CEP consider enlarging its expertise and contribute more efforts to mitigating the consequences of climate change, such as through greater use of the Euro-Atlantic Disaster Response Coordination Centre?

Recently, in an address to launch the new Strategic Concept, the NATO Secretary General stated that the basis of the debate should not be what **can** NATO do, but rather what **should** NATO do; not how to adapt missions to the capabilities available but rather how to adapt capabilities to meet the challenges we face. The same applies to Civil Emergency Planning. Too often we are concerned about "selling" existing products such as specific expertise already available. Maybe we should look more at seeking ways to adapt to our changing environment and create new innovative products for the future. As the old adage goes: 21st century challenges cannot be addressed with a 20th century mindset. NATO's strength resides in its duality as a civil-military alliance. New challenges will be best addressed if joint civil-military planning and conduct become the norm.

The question is how to strike the right balance. NATO as an organisation must certainly address the most pressing current and future security challenges but it should avoid the danger of becoming a jack of all trades and master of none. Discussions on the new Strategic Concept over the coming months will help identify these priorities and where this balance lies.

CEP Quote

In addition to the most readily identifiable threats, this last decade has seen the emergence of a whole series of challenges that we increasingly see are having security implications. By these I mean energy security or defence against cyber attacks and our awareness of the increasing impact of climate change on the stability of states and the international sharing of precious resources, such as water.

Jaap de Hoop Scheffer, NATO Secretary General on the opening of the new Strategic Concept seminar, 7 July 2009

In addressing new threats and challenges, CEP plays a pivotal role given its intensive and inclusive approach to partnerships. Discussions on practical implementation of NATO policy have, for a long time, been open to Partners in a spirit of openness and solidarity. Furthermore, many Partner countries have considerable expertise in specific areas, and from whom the Alliance can learn a great deal.

Cooperation with international organisations also remains essential when addressing new threats to avoid unnecessary duplication. For example, many of the new threats covered in this issue are also addressed by the EU. There is often a fine line between where one organisation's mandate begins and another's ends.

In conclusion, no country is immune from global threats and there is always a need for cooperation to address common challenges. NATO's civil emergency planning activities continue to provide a forum for efficient sharing of information and best practices. CEP is already taking up these challenges and is prepared to be at the forefront of adopting new mindsets to address them. Undoubtedly, more could be done to better exploit CEP's potential in the field of joint civil-military planning and support to operations, particularly drawing on existing links with Partners where specific expertise could be tapped. One fact is clear. CEP's greatest added value lies in the vast networking possibilities provided by the multitude of interfaces with civilian agencies across sectors as broad as industrial planning to medical matters. These provide an excellent foundation on which to build efficient structures contributing to the protection of populations and limiting the impact of crises when they occur.

DID YOU KNOW ?

To date, 28 nations have subscribed to the MoU on the Facilitation of Vital Cross Border transport : Albania, Armenia, Austria, Bosnia-Herzegovina, Bulgaria, Canada, Croatia, Denmark, Estonia, Finland, Georgia, Germany, Hungary, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Turkey, the former Yugoslav Republic of Macedonia*, the USA, the UK and Ukraine. This MoU improves the speed and efficiency of bringing assistance to victims of humanitarian crises and disasters, including those triggered by a Chemical, Biological, Radiological or Nuclear (CBRN) event within the EAPC area.

* Turkey recognises the Republic of Macedonia with its constitutional name.

Martin Howard together with US Ambassador Ivo Daalder (1), Polish Ambassador Boguslaw Winid (2) and Estonian Ambassador Jüri Luik (3) for the signing of the MoU.

The following national contribution has been provided by Lithuania, a NATO Ally with specific expertise and priorities in the field of energy security. Dieter Urban, the Chairman of NATO's Industrial Planning Committee has contributed a piece on activities in the field of protection of energy critical infrastructure, one of the main focuses of this committee's work.

A Lithuanian perspective on Energy Security

Energy security is an essential component of a functional economy as well as a key element in national security and civil protection. A diversified and reliable supply of energy resources, together with their sustainable, efficient use contribute significantly to the well-being of a particular state. Consequently, energy security contributes to the stability of the international community as a whole. In recent years, it has become apparent that energy security challenges are more than simply national or regional in nature and that the need for global solutions is paramount.

The energy security issue is relatively new on NATO's agenda. Taking into consideration that disruptions to energy flows could affect Allies' security, we believe that NATO, as a political-military establishment, should also take its role in the field of energy security. No single existing international organisation has the monopoly on this subject. Therefore, NATO should not limit its role purely to protecting vital energy infrastructure, which is of course an important but not sufficient element of the subject. The political dimension of energy security should also be addressed. We need a coherent and balanced approach between both technical and political dimensions.

In the Lithuanian context, the issue of energy security is of particular importance. Due to historical circumstances, Lithuania has been isolated from EU and NATO countries in the energy sector. Furthermore, the country is totally dependent on Russian gas supply and, to a great extent, on Russian oil exports. The situation could become even more complicated after closure of the Ignalina nuclear power plant which currently meets most of the country's energy demand. Hence, the integration of the Lithuanian energy sector into the EU common energy market and reducing our dependence on a single external supplier are our main objectives for the foreseeable future.

Once dependence on a single energy supplier is recognised as one of the major energy security issues, it follows that diversification of energy supply sources takes on strategic importance. In order to achieve this goal, we need to further intensify dialogue among energy producers, consumers and transit countries. This dialogue should be based on the principles of transparency, non-discrimination, mutual confidence, reciprocity and free access to transit routes, which are enshrined in the Energy Charter Treaty. NATO could be the link between countries that would provide a forum on cooperation in the energy sector.

It should be noted that diversification of energy supply is only one part of the problem. We need to diversify the energy mix as well. Reserves of traditional energy sources are shrinking, prices are fluctuating and growing energy consumption has a negative impact on the global climate. Global warming is one of today's major worldwide problems that can be addressed principally by applying two measures: a) using energy sources more efficiently and b) consuming more renewable and other climate friendly energy sources, including nuclear power.

Security of vital supplies is directly linked to the security of Alliance populations which is a major responsibility for NATO's civil emergency planning (CEP). CEP efforts in this field could be focussed mainly on the role of addressing technical issues in global forums. In the near

Jurgita Bilvaisiene, Energy Security Policy Division, Lithuanian Ministry of Foreign Affairs

future, the Lithuanian Ministry of Foreign Affairs, NATO's Industrial Planning Committee and the Science for Peace Committee are planning to carry out joint projects on energy security to promote mutual dialogue in the energy sector and protection of critical infrastructures.

In conclusion, only our combined efforts, foresight and strategic approach to energy security will allow us to form a more open-minded way of thinking that is capable of responding to the major challenges ahead.

Contributions of NATO's Industrial Planning Committee to Energy Security

In the light of new challenges facing the Alliance and NATO's efforts in the field of energy security, the Industrial Planning Committee (IPC) has been addressing the CEP-related issues of energy security since June 2004 under the Senior Civil Emergency Planning Committee's guidance. From the outset, there has been common political understanding that the IPC should only deal with physical aspects of the protection of critical energy infrastructure. Issues concerning the security of vital energy resources and their supply are not analysed within the IPC. The IPC concentrates its activities on monitoring security related threats, in particular terrorism, which are the responsibility of national governments or require government and private sector industry coordination.

The IPC's priority has been to focus on the protection of critical electricity infrastructure since this has a direct impact on most industries and the main functions of society. Subsequently, oil and gas infrastructures have been examined.

Because energy infrastructure systems go beyond national boundaries, cooperation between NATO member states, especially with partner countries is very important. Therefore, the IPC involves closely Euro-Atlantic Partnership Council (EAPC) states in its work on energy security. It analyses energy infrastructure inside NATO/EAPC territories and in particular focusses on cross border connections. Since energy infrastructures are often owned by private operators, public-private partnerships are considered very important for the IPC's analyses.

The IPC's work aims at raising awareness among governmental planners, at information sharing and at enhancing dialogue and developing bilateral contacts between the IPC's national representatives, industry experts and among other committees within NATO dealing with critical energy infrastructure.

During the IPC's seminars and plenary meetings, the Committee, supported by industrial experts specialised in energy related questions, addresses protection measures, shares experiences and informs on developments in the different energy markets. Because of various protection systems, the IPC considers it more practical to develop a policy of sharing best practices instead of an inventory of protection measures. The IPC does not stipulate binding policies or obligations. These best practices are designed to promote exchange of information, give general advice and coordinate information to governmental authorities who need guidance and who are responsible for the protection of critical energy infrastructures.

As a result, best practices have been developed for critical electricity and critical gas infrastructures. The development of a catalogue of best practices for critical oil infrastructures is currently underway. Relevant authorities can use these policies to ensure that they implement best practices and that operators execute appropriate measures for the protection of critical infrastructure.

Dieter Urban, Chairman of the NATO Industrial Planning Committee

The attacks on Estonia in Spring 2007, conducted through the internet against public websites served as a reminder of the vulnerabilities of key systems in open, modern societies to acts of hostility. Ligia Ferreira, Chair of NATO's Civil Communications Planning Committee explains the risks and challenges of an interconnected information society. Suleyman Anil, Head of NATO's Cyber Defence Coordination and Support Centre, explains NATO measures to enhance protection of its communication and information systems against attempts at disruption an cyber attacks.

Risks and challenges in an interconnected society

Electronic communication networks are the backbone of today's information society. These interconnected and complex "distributed systems" have generated a massive increase across all sectors in the use of computers, infrastructure, electronic services and applications, known collectively as Information Communication Technology, or ICT. Further, the infrastructure necessary to operate these systems on a 24/7 basis around the world is, of necessity, both interconnected and interdependent. All these factors create an extremely challenging – and risk-filled – environment in which nations must operate. Fortunately, NATO has several bodies and mechanisms to address many of the issues arising from this. The Civil Communications Planning Committee (CCPC) is a key body in this effort.

Established over 50 years ago, the CCPC is tasked to provide advice to NATO and EAPC nations on all matters related to civil communications aspects of civil emergency preparedness. The Committee is responsible to develop and co-ordinate the arrangements necessary to ensure, to the maximum practical extent, the continued availability of civil communication in times of crisis. This involves, **inter alia**, developing and providing to the nations, recommendations regarding new and emerging technologies, including with respect to cyber security and cyber defence.

Cyber security, which involves protecting information by preventing, detecting and responding to attacks, is essential at all levels. Governments need to secure their electronic information networks and systems to protect all public activities, such as military defence, logistics, transportation and financial systems, infrastructure, and citizens' personal information. Very worrisome to governments is the fact that a cyber attack on one governmental system or sector could well have serious impacts on others.

Cyber attackers can be individuals, criminal elements, adventurers, or they could be sponsored by unfriendly governments or transnational organisations. Their capacity, motivation and willingness to exploit weaknesses seem unlimited. Furthermore, sophisticated attacks are almost impossible to trace to their true source, and the resultant anonymity enjoyed by today's cyber attackers creates substantial problems for stricken nations trying to respond to attacks.

The potential results of cyber attacks during natural or technological disasters or other crises such as terrorist attacks, could be catastrophic to a nation's viability. Such attacks could seriously disrupt normal information flow between different government ministries or agencies. They could prevent communication to the affected portions of the population. Also, they could hinder the efforts of disaster response agencies to quickly and appropriately respond to the afflicted area. Finally, they could hamper one nation's ability to cooperate with neighbours or regionally in response to a multinational crisis or disaster.

Ms. Ligia Ferreira, Chair of the NATO Civil Communications Planning Committee

The CCPC has been directly involved with cyber security since 2003. Under its current Work Programme, the Committee is evaluating national-level existing and potential vulnerabilities on electronic communications networks from cyber attacks. Other threats such as those caused by passive leakage of information from electronic components or systems, are also being researched. At the request of nations, CCPC has previously analysed other cyber security issues such as consequences of cyber attacks, critical information infrastructure protection, and the possible use of prioritisation schemes to mitigate system overload or failures.

A group of cyber defense experts, located in nations but responsive to NATO requirements through the Civil Emergency Planning Crisis Management Arrangements, supplement the Committee. These experts can respond to requests for support and advice from EAPC, Mediterranean Dialogue, and Istanbul Cooperative Initiative nations as well as from the NATO military. Nations have requested such support in response to actual crisis situations as well as in order to address needs to establish cyber defence-related programs. These same experts are available to assist NATO's other cyber security bodies such as the NATO Computer Incident Response Centre (see Mr. Anil's article), the NATO C3 Board, and other structures.

Of course, the CCPC does not work in isolation. The Committee membership comprises senior representatives from national ministries of communication, many of whom also participate as national representatives to the ICT sectors of international organisations such as the UN's International Telecommunications Union, and the European Union. Hence, there is a good informal crossflow of information between the organisations, which helps prevent unnecessary duplication.

Today's interconnected information society both reflects current needs and indicates the future environment. Individuals', nations', and international alliances' dependence on electronic services, infrastructures and applications will surely grow, as will the corresponding requirements for improved cyber security. Alliance nations have identified a clear role for NATO in this arena, and the Civil Communications Planning Committee will continue to accomplish its responsibilities

Defending against cyber attacks

The first cases of cyber attacks against NATO information systems were reported in the late 1990s during NATO's operations in the Balkans. Some of these attacks resulted in NATO communications and information systems being compromised, causing interruptions to operational NATO services. Building on lessons-learned from operations in the Balkans, at the 2002 Riga NATO Summit, Governments called for "improving the protection of key information systems against cyber attacks". This declaration initiated several internal NATO actions to improve the Alliance's cyber security posture. The most significant and comprehensive initiative was the NATO Computer Incident Response Capability (NCIRC) Project launched in 2003. The NCIRC has been operational since the end of 2005 and responds to security incidents reported on NATO networks.

In May 2007, the world watched as a NATO member, Estonia, fell victim to cyber attacks on its Information Technology (IT) infrastructures and online services following a political conflict. This was the first example of such attacks which lasted about three weeks and demonstrated the chaos and disruptions to public, financial, and media services caused by targeting national cyber space. In the aftermath of the cyber attacks, NATO nations agreed to take further actions to increase NATO's Cyber Defence Capabilities, including provision of technical and operational assistance to a member nation should such assistance be requested.

Süleyman Anıl, Head of NATO's Cyber Defence Coordination and Support Centre, NATO HQ, Brussels

Cyber Security

NATO's Cyber Defence Policy is detailed in a series of high level documents which define the principles, decision-making processes and the procedures in order to ensure a common and coordinated NATO approach to cyber defence and the response to cyber attacks. NATO's Cyber Defence Management Agency (CDMA) is responsible for initiating and coordinating the immediate and effective cyber defence actions within NATO and between nations when required. As one of the NATO CDMA's stakeholders, CEP plays an important role in assisting Alliance and partner nations through established procedures and facilitates contacts within NATO.

Threats that concern NATO are the state-sponsored cyber attacks to target NATO and member nations during a political or military conflict. Such cyber attacks are the most difficult to respond to and can have significant effects, especially on nations with poor or small national IT infrastructures. Such attacks can destabilise national security, cause significant economic loss and disrupt public and commercial services for days or weeks. State-sponsored cyber attacks are also frequently used for espionage and information gathering. The current assessment of cyber threats from terrorist groups is considered low, however this is expected to increase in the short term.

Implementing an effective national cyber defence capability is technically challenging but feasible if well planned and politically supported. Assuming that a national cyber defence strategy is developed and made effective though supporting legislations, implementation of a national cyber defence capability would require (1) an operational centre where technical and operational services are resourced, (2) a coordination centre where strategy and concepts are developed and coordinated, legal aspects are addressed, relations with industry and international organisations are maintained, (3) an executive body where strategic decisions are presented, discussed and endorsed for implementation. The Cyber Defence Operations Centre would require most of the funding and human resources. The cost depends on the volume of cyber space protected (i.e. computer networks and infrastructures) and the type of services that are centrally offered by the CD Ops Centre.

The current NATO Computer Incident Response Capability handles hundreds of thousands of electronic events daily to detect malicious activity and to respond appropriately. To date, more than 800 cyber security incidents have been formally pursued, some which could have had significant consequences. Such incidents vary from web defacements to cyber espionage and to major network penetrations.

For the near future, NATO has plans in place to enhance its current cyber defence capabilities further, to improve assistance to nations and collaboration with industry and international organisations.

NATO Cyber Defence Capability (NCIRC) - Operations Centre

The growing challenge of piracy in the Gulf of Aden and off the Horn of Africa is threatening international humanitarian efforts, as well as safety of commercial maritime routes. At the request of the UN, NATO is actively helping to increase security by conducting counter-piracy operations in the area. This article by Jim Caponiti, Chairman of NATO's Planning Board for Ocean Shipping describes this committee's role in deterring piracy. He also covers other international coordination efforts.

Assisting in deterring piracy

The Planning Board for Ocean Shipping (PBOS), one of eight Planning Boards and Committees subordinate to the Senior Civil Emergency Planning Committee (SCEPC), provides advice to NATO on anti-terrorism measures concerning the protection of civil maritime assets and monitors any related security development that impacts commercial shipping. Piracy is currently an issue that is affecting commercial shipping especially off the coast of Somalia.

PBOS through its National Representatives and Civil Shipping Experts has been focused on piracy and the identification of practices necessary to deter piracy. The original area of concern was in and around the Straits of Malacca and more recently has been the Gulf of Aden and the waters off the coast of Somalia. Acts of piracy are crimes that threaten freedom of navigation, crew safety, and the flow of commerce.

PBOS continues to exchange information on piracy, analyse efforts to address piracy, provide shipping advice to the NATO Military Authorities (NMAs) and National Authorities, provide input on best practices to deter piracy and to disseminate best practices. PBOS is well positioned to provide binding or non-binding guidance to deter piracy to Alliance and Partner flag states.

Many actions are currently being taken to deter piracy and PBOS applauds these actions. Continued cooperation between governments and industry will help reduce the incidence and success of piracy attacks.

A group closely aligned with PBOS that is addressing anti piracy efforts is the Contact Group on Piracy Off the Coast of Somalia (CGPCS) established by UN Security Council Resolution 1851. The CGPCS is comprised of 28 nations and six international organisations, including NATO, and acts as a common point of contact between and among states, regional, and international organisations on all aspects of combating piracy and armed robbery at sea off Somalia's coast. The CGPCS has four working groups (WGs) that meet periodically and provide recommendations to deter piracy.

WG-1 is led by the United Kingdom and is the group principally focused on the military and is concerned with operational coordination and regional capability development. WG-2 is led by Denmark and is concerned with identifying practical and legally sound solutions to ensure prosecution of persons suspected of piracy. WG-3 is led by the United States and is focused on industry self-awareness and protection. WG-4 is led by Egypt and is concerned with public diplomacy and communications.

In conclusion, progress is being made to address the piracy threat but challenges remain. PBOS will continue working with appropriate organisations to address piracy and to help identify measures and processes that will assist commercial carriers in avoiding, deterring, and preventing successful pirate attacks.

James E. Caponiti, Chairman of NATO's Planning Board on Ocean Shipping

Public health challenges like pandemics (HIV, flu, etc) transcend national borders. Risks to social order can be great and traditional public health approaches may be inadequate. Furthermore, states cannot tackle such problems in isolation and international cooperation is essential. Eric Lecarpentier, Chairman of NATO's Joint Medical Committee, provides an overview of the current H1N1 flu epidemic and appropriate preventive measures.

Flu A(H1N1)

Flu is a very contagious acute respiratory infection caused by the influenza viruses. There were three flu pandemics in the 20th century. The Spanish flu of 1918–1919 (influenza A virus subtype H1N1) affected the whole planet. At least 40 million people died from it, according to estimates from the World Health Organization (WHO) website. Later there were much less severe pandemics: the Asian flu (influenza A virus subtype H2N2) in 1957-1958, and the Hong Kong flu (influenza A virus subtype H3N2) in 1968–69.

Each year in autumn and winter there are flu epidemics in temperate regions. As a result some people require hospital treatment and there are deaths, mainly among high-risk groups (the very young, the elderly and those with chronic diseases). World-wide these annual epidemics bring some three to five million serious cases and 250,000 to 500,000 deaths. Most of those who die as a result of flu in industrialized countries are aged 65 or more. In some tropical countries flu viruses are active throughout the year, with one or two peaks in the rainy seasons.

Influenza viruses are of three different types, designated A, B and C. The seasonal epidemics result from A and B viruses, but only an A virus can cause a pandemic. C viruses cause sporadic cases. Flu viruses are characterized by frequent mutations. This genetic evolution occurs:

- either by drift during seasonal epidemics,
- or by shift. This only affects type A viruses. It is responsible for the appearance of new viruses from which the population is not protected, leading to flu pandemics.

Influenza type A viruses are divided into subtypes distinguished by their particular combinations of the different sorts of surface protein. The virus subtypes are accordingly designated A(HxNx). The current epidemic involves a new strain of the A(H1N1) family which spreads from person to person. It results from genetic reassortment among pig, human and bird viruses. This virus is different from the H1N1 seasonal flu virus of human origin which usually circulates in the winter.

In the northern hemisphere the seasonal flu epidemic comes each year between November and April. On average it lasts 9 weeks. Mortality from seasonal flu chiefly affects older people (more than 90% of those who die are aged 65 or more).

A pandemic and an epidemic both involve a serious increase in cases of a disease at a given moment. The difference lies in the extent of the phenomenon: a pandemic is characterized by the very wide geographical spread of a new virus subtype resulting from genetic modification, covering several or all of the continents. Because the virus has new characteristics the population has little or no immunity. There may be many serious cases or deaths. Because most persons have low immunity, more are likely to be infected than by seasonal flu. The majority who contract the virus have the benign form and recover without antiviral treatment or medical care. Of the more serious cases, more than half of those hospitalized have suffered from underlying pathologies or an impaired immune system. We define:

Virulence as the ability of a virus or an infectious agent to cause a serious disease;

Contagiousness as the ability of a virus or an infectious agent to pass from one person to another.

Because of the worldwide extent of the flu epidemic caused by the novel A(H1N1) virus, on 11 June 2009 the WHO announced that it was going over to phase 6 of its plan and confirmed that there was a world pandemic. The virus spreads from person to person as easily as the normal seasonal flu. To prevent the propagation of the disease those affected should cover their nose and mouth when they cough or sneeze, stay at home if they do not feel well, wash

Eric Lecarpentier MD, Chairman of the NATO Joint Medical Committee

their hands frequently and keep apart from healthy persons as far as possible. There are no known cases of persons being infected by contact with pigs or other animals. The first signs of an A(H1N1) infection are of the normal flu type: temperature above 38°, body aches, extreme tiredness and coughing or respiratory problems, headaches, sore throat and running nose, sometimes accompanied by vomiting and diarrhoea.

In the current epidemic, transmission is like that of the seasonal flu:

- through the air, that is when the virus is spread in the air by coughing, sneezing or spitting;
- by close contact with an infected person (kissing or shaking hands);
- by contact with objects touched and thus contaminated by a sick person (for example, a door handle).

A sick person is contagious from the first symptoms and for about 7 days, and the incubation period can be up to 7 days. He or she should thus be isolated and wear a surgical mask when in the presence of others throughout this period to avoid contamination of his/her close circle.

To reduce the spread of the virus as much as possible you should:

- avoid all contact with any sick person
- regularly wash your hands with soap or disinfect them with an alcohol solution (available in pharmacies and large stores), particularly after coughing or blowing your nose
- when you cough or sneeze, cover your mouth and nose with a disposable handkerchief (to be thrown away as soon as it has been used, preferably in a bin closed by a lid and lined with a plastic bag), or with your arm or sleeve or with your hands if it is possible to wash them immediately afterwards.

There are two types of mask:

- The surgical mask intended to reduce the projection of droplets by those who are ill, to be worn from the onset of symptoms to lessen infection of other persons/family and friends by coughing or sneezing. The virus spreads through the air. There is a risk of contamination when you are less than a metre from an ill person, face to face.
- The respirator mask (FFP2 standard) for professionals who have a vital role in a pandemic and are in regular close contact with the sick (health professionals, emergency services etc). This is a disposable respiratory mask which protects the wearer from inhaling infectious agents that spread through the air.

If flu symptoms appear, each country has its own special arrangements in place. In France you are currently recommended to go to your family doctor, or to call the local (departmental) medical emergency coordination centre, the 15 centre. In England a national call centre and health coordination service has been set up. There is general agreement that patients should be isolated and encouraged to stay at home. Only serious cases or persons at risk (pregnant women, young

children, immunocompromised persons, those in a weakened condition etc) are likely to be hospitalized.
During the voluntary isolation of a close relation who is sick, medical supervision and regular monitoring will be provided by doctors. You must limit close contact with this person. If some contact is unavoidable during the voluntary isolation, take care that the patient wears a mask and that hygiene barrier precautions are strictly observed to avoid being infected yourself:

- Do not kiss or touch hands with the patient
- Reduce visits to a strict minimum
- Have the patient wear a surgical mask to avoid spreading aerosols
- Observe strict hand hygiene: at home, wash hands with ordinary soap (not the piece used by the patient) or disinfect with an alcohol-based cleaner, in particular after each contact:
  - with the patient
  - with things the patient has used
  - with the patient's personal effects
  - with any surfaces touched by the patient (door handles, furniture, taps etc)
- Properly ventilate the living space by opening windows
- Wash everyday things used by the patient (towels, cutlery, linen etc) with hot water and soap or ordinary cleaning products
- Clean surfaces touched by the patient (door handles, lavatory flush, remote control, telephone etc) with hot water and soap or ordinary cleaning products

If you don't feel well, have a high fever, a cough and/or a sore throat:

- Stay at home and don't go to work, school or public places
- Rest and drink large amounts
- Cover your nose and mouth with paper tissues when you cough and sneeze, and then dispose of them correctly. Thereafter wash your hands carefully with soap or an alcohol solution
- If you have no paper handkerchiefs to blow your nose or cough, do it in the hollow of your elbow
- Wash your hands frequently and carefully with soap and water, particularly after coughing or sneezing
- Inform your family and friends of your illness, and seek help for everyday tasks which involve contacts with others, such as shopping.

WHAT TREATMENTS ARE AVAILABLE?

Only a doctor can decide what treatment to prescribe, according to the particular situation of the patient. This treatment may be simply to prescribe medicine against fever and give hygiene advice, or to prescribe antiviral treatment. The sick person must wear surgical masks from the very first symptoms, to avoid infecting family and close circle.

A vaccine will be available from autumn 2009. Antiviral drugs – oseltamivir (Tamiflu ®) and zanamivir (Relenza ®) – are effective against this virus. They are only given on medical prescription after consultation and diagnosis by a doctor, and from appearance of the first symptoms. They in no way constitute preventive treatment. Antivirals are used for early treatment of flu. If taken rapidly at the onset of the disease they can mitigate flu symptoms, shorten the duration of the illness and probably prevent complications. These treatments reduce the virus's ability to reproduce, but they provide no immunization against the disease. Vaccines are the main means of preventing flu from causing illness, as with other infections. They help to immunize the recipients by stimulating their production of antibodies against the virus. The vaccine is not expected to be available for several weeks. Depending on clinical testing, approval for the market and production yields, delivery of the vaccine could take about four months starting in the autumn.

As regards international travel, caution is advised when visiting countries where it is confirmed that the virus is circulating in the community. At this time the World Health Organization (WHO) is not recommending travel restrictions because of the new A(H1N1) flu. Europe has not made any particular recommendation.
You are advised to:

- follow the instructions issued by the local health authorities
- observe basic hygiene precautions (wash hands frequently, ventilate living spaces) and avoid contact with sick persons
- in case of fever or flu symptoms, consult a doctor locally.

The NATO Science for Peace Programme brings together scientists and experts from NATO and Partner countries on a regular basis to work on programmes of common concern. It aims to contribute to security, stability and solidarity among countries by applying science to problem solving. The project below is of relevance to CEP's activities in the field of cyber defence capacity building in Partner countries.

NATO Science Programme Boosts Cyber Security in Partner countries

Keeping computer infrastructures and systems safe is a challenging task. Whenever computer security incidents occur, organisations must be able to react swiftly and effectively in order to limit the potential damage.

Having a *Computer Security Incident Response Team (CSIRT)* in place is an effective way to improve rapid response capability as well as mitigating future attacks. CSIRTs are small teams of 1-3 people, equipped and trained to react swiftly, 24/7, in order to distribute critical security-related news in an effective manner.

In 2006, the NATO Science for Peace and Security (SPS) programme launched a project to establish CSIRTs in 15 countries with no previous computer security systems in place: Afghanistan, Albania, Azerbaijan, Armenia, Belarus, Bulgaria, Georgia, Kazakhstan, Kyrgyzstan, the former Yugoslav Republic of Macedonia*, Moldova, Tajikistan, Turkmenistan, Ukraine and Uzbekistan.

The project provided a "starting kit" to help get the CSIRTs up and running in each country. The kit included a dedicated server with a system of incident handling software, staff working station, router, switch, software, multi-function printer, shredder and manuals. NATO ensured that the equipment was delivered to each country and helped with the installation and initial operation. In addition, NATO funding was able to train up to three CSIRT operators to well defined global standards per country.

Although the NATO SPS programme retains overall supervision for the project and the implementation phase, other key players were involved. National Research and Education Networks (NRENs) in each country were responsible for securing personnel and the office space needed for them. The Central and Eastern European Networking Association (CEENet), an association of national academic, research and educational networks (NRENs) from Central and South Eastern Europe, Caucasus and Central Asian countries, coordinated the procurement and delivery of the equipment as well as providing technical assistance for its installation.

In addition, all aspects of the projects were closely coordinated with the European Network and Information Security Agency (ENISA).

So far the results are very encouraging. The CSIRTS are functioning well in most of the countries and progress is carefully monitored on a regular basis.

It is expected that the NATO SPS programme will continue this kind of activity in the future, with the goal of developing Security Audit Certification capabilities. Furthermore, the project will help to prepare the NRENs and the CSIRTs for participation in a global series of computer security rapid response exercises planned for 2010/2011. Participation in such exercises on a global scale is tribute indeed to the work that has been carried out by Partner country teams since 2006.

This project is also an excellent example of NATO's practical cooperation that delivers concrete results with its Partners in the field of cyber defence.

* Turkey recognises Macedonia by its constitutional name

Jayne Clinton, Science Publishing and Marketing Projects, NATO Public Diplomacy Division

DEVELOPMENTS IN THE SENIOR CIVIL EMERGENCY PLANNING COMMITTEE

This Autumn, SCEPC and the PB&Cs will address several important policy issues. Following the CEP Afghanistan Support Workshop, held at NATO HQ on 1-2 July 2009, SCEPC will discuss the workshop's recommendations and decide how best to take these forward. For information, the goal of the workshop was, on a demand-driven basis, to determine how NATO CEP actors in synergy with national and international civilian actors could help meet the needs for civilian support to the Afghan authorities and ISAF.

Taking into account the wider NATO context as well as the results of the CEP Review, the next Ministerial Guidance for CEP will be developed over the coming weeks. As agreed in the CEP Planning and Review Cycle, the Ministerial Guidance as well as the PB&C Work Programmes will now cover a four year period. The Work Programme 2010-2013 will be reviewed and approved by the SCEPC during the first quarter of 2010. Development of the Ministerial Guidance involves all stakeholders and sets the objective for NATO/CEP for the next four years. To this end, NATO's Partners are involved to the maximum extent possible.

Several practical activities and seminars will take CEP projects forward. Among these, the EADRCC's disaster relief exercise, "Zhetysu 2009", will take place from 5-11 September 2009. The aim of the exercise is to enhance interoperability among first responders and to build capacity in NATO and Partner countries in dealing with complex emergency situations. A further important event will be the Transport Seminar, taking place in Belgium on 26-28 October 2009 and involves primarily the transport PB&Cs (Civil Aviation Planning Committee, Planning Board for Ocean Shipping and the Planning Board for Inland Surface Transport). This multi-modal event will examine the impact of the current economic situation on the transportation industry and its support to NATO operations.

SCEPC
Currently on the table

- Ministerial Guidance for 2010-2013
- Follow up to the CEP Workshop on Civil Support to Afghanistan

LOOKING AHEAD

SCEPC and PB&Cs Calendar

1-3 September	CPC Seminar and Plenary	Krakow, Poland
9-10 September	Civil Aviation Planning Committee (CAPC) Plenary	NATO HQ, Belgium
14-15 September	Planning Board for Ocean Shipping (PBOS) Plenary	NATO HQ, Belgium
30 Sept – 2 Oct	NATO Medical Conference	Lisbon, Portugal
26-27 October	CCPC Plenary	NATO HQ, Belgium
26-28 October	Transport Seminar	Antwerp, Belgium
5-6 November	Joint Medical Committee Plenary	NATO HQ, Belgium
11-12 November	Energy Critical Infrastructure Seminar	Vilnius, Lithuania
12-13 November	IPC Plenary	Vilnius, Lithuania
17-18 November	FAPC Plenary	NATO HQ, Belgium
23-24 Nov (tobc)	PBIST Plenary	NATO HQ, Belgium
24-25 November	SCEPC Plenary	NATO HQ, Belgium
3-4 December	NATO Foreign Ministers meeting	NATO HQ, Belgium

The Euro-Atlantic Disaster Response Coordination Centre

The Euro Atlantic Disaster Response Coordination Centre (EADRCC) is a Partnership body where Partners and Allies are equal stakeholders. The EADRCC is the focal point for information sharing on disasters in the EAPC. This article describes a new project called the AidMatrix, a tool designed to facilitate dissemination of disaster relief information

The Aidmatrix Tool

The EADRCC has been striving for some time to find a modern solution for disseminating disaster relief information. Traditionally, the Centre prepares reports in 12 to 24 hour cycles which are then sent to EAPC nations by means of e-mail and by fax. This is the proven way of "pushing" information to the recipient, and the Centre will of course continue this practice. However, more advanced methods are available whereby information can be posted continuously on a virtual bulletin board and be "pulled" when demanded.

Thanks to the US Delegation at NATO, which facilitated contacts between the EADRCC and the Aidmatrix Foundation, the Centre has been able to find a modern tool for the dissemination of disaster relief information. Aidmatrix is a state of the art tool which makes reporting on disaster relief faster, more transparent and more efficient.

The Aidmatrix trademark is to get the "Right Aid to the Right People at the Right Time". Aidmatrix is a non-profit organisation that connects donors with people needing aid through their network. This network is used by 38 US states, the US federal agency FEMA, Honduras and Romania. The network is used for most charitable food donations in the United States and for the distribution of donated medical products.

In the area of disaster relief, one of the main challenges addressed by Aidmatrix has been to create a "Disaster Relief Matrix", which improves the flow of humanitarian aid in times of disaster response and recovery. It automates much of the cumbersome process that is performed manually. In particular, the Aidmatrix network provides a single location to capture and report the full picture of need, donations and delivery in real time, making requirements from the field available to potential donors and vice versa.

Günter Bretschneider, Head, Euro Atlantic Disaster Response Coordination Centre (EADRCC)

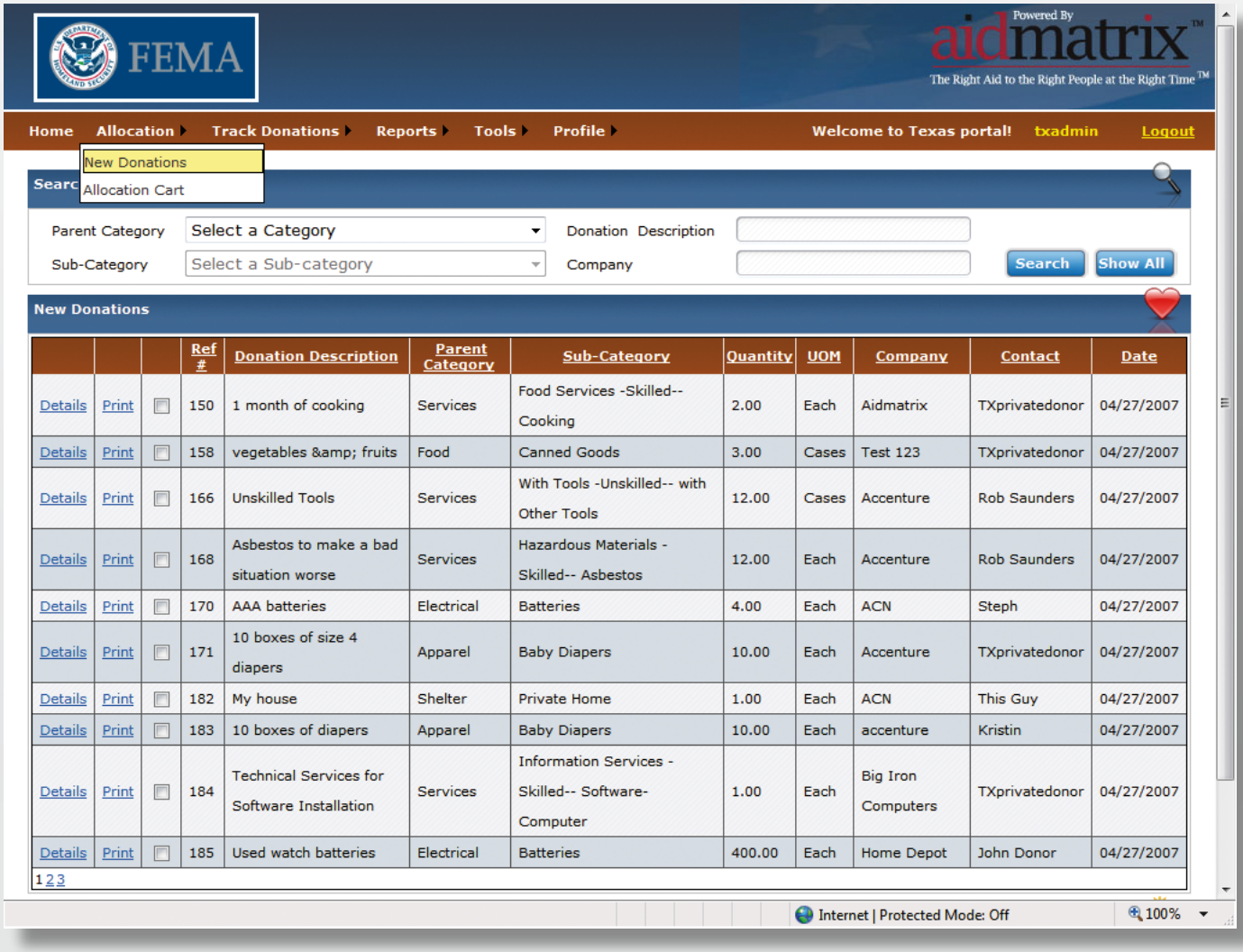
In terms of donation management, Aidmatrix links nonprofit, government and business sectors to improve disaster relief. This solution is used in time of disaster and also as part of the day to day donations management function within participating Federal States.

The table below depicts how the cental clearing house mechanism works:

The entry at the bottom shows a donation of 400 watch batteries by Home Depot. This one and other donations are reviewed and administered by a disaster agency and can be requested by a registered recipient in need of assistance. How does this transpose to the EADRCC and its clearinghouse function ?

The people in need are the ones in a stricken nation requesting assistance through a government agency that is in charge of the emergency situation. The donors are the EAPC nations responding to a request for assistance. The EADRCC coordinates, reviews and administers the process.

Aidmatrix has made its “Disaster Relief Matrix” available for use by the EADRCC, the EAPC and other Partner nations after a Memorandum of Understanding was signed in June 2008. Since September 2008, the EADRCC has used Aidmatrix’s “Disaster Relief Matrix” as a complement to its traditional reporting tools.



			Ref #	Donation Description	Parent Category	Sub-Category	Quantity	UOM	Company	Contact	Date
Details	Print		150	1 month of cooking	Services	Food Services -Skilled-- Cooking	2.00	Each	Aidmatrix	TXprivatedonor	04/27/2007
Details	Print		158	vegetables & fruits	Food	Canned Goods	3.00	Cases	Test 123	TXprivatedonor	04/27/2007
Details	Print		166	Unskilled Tools	Services	With Tools -Unskilled-- with Other Tools	12.00	Cases	Accenture	Rob Saunders	04/27/2007
Details	Print		168	Asbestos to make a bad situation worse	Services	Hazardous Materials - Skilled-- Asbestos	12.00	Each	Accenture	Rob Saunders	04/27/2007
Details	Print		170	AAA batteries	Electrical	Batteries	4.00	Each	ACN	Steph	04/27/2007
Details	Print		171	10 boxes of size 4 diapers	Apparel	Baby Diapers	10.00	Each	Accenture	TXprivatedonor	04/27/2007
Details	Print		182	My house	Shelter	Private Home	1.00	Each	ACN	This Guy	04/27/2007
Details	Print		183	10 boxes of diapers	Apparel	Baby Diapers	10.00	Each	accenture	Kristin	04/27/2007
Details	Print		184	Technical Services for Software Installation	Services	Information Services - Skilled-- Software-Computer	1.00	Each	Big Iron Computers	TXprivatedonor	04/27/2007
Details	Print		185	Used watch batteries	Electrical	Batteries	400.00	Each	Home Depot	John Donor	04/27/2007

1 2 3

CEP in other international organisations

As NATO's Civil Emergency Planning activities do not take place in a vacuum, this table provides an overview of useful links to other organisations also active in the field of Civil Emergency Planning.

ORGANISATION	WEB SITE
European Commission	http://ec.europa.eu/environment/civil
	http://ec.europa.eu/dgs/justice_home/terrorism/dg_terrorism_en.htm
EU Monitoring and Information Centre (MIC)	http://ec.europa.eu/environment /civil/prote/mic.htm
EU Commission Human Aid Office (ECHO)	http://ec.europa.eu/echo/index_en.htm
United Nations Office of the Coordination of Humanitarian Affairs (UN-OCHA)	http://ochaonline.un.org
The Organization for Security and Co-Operation in Europe (OSCE)	http://osce.org
International Atomic Energy Agency (IAEA)	http://iaea.org
IAEA Incident and Emergency Centre (IEC)	http://www-ns.iaea.org/tech-areas/emergency/incident-emergency-centre.htm
IAEA Guidance for First Responders to Radiological Emergencies	http://www-ns.iaea.org/tech-areas/emergency/emergency-response-actions.asp
Organization for the Prohibition of Chemical Weapons (OPCW)	http://www.opcw.org

CEP COURSES AND EVENTS

Below is a list of upcoming events in other international organisations:

ORGANISATION	EVENT	DATE	PLACE
OPCW	Course on Assistance and Protection	7-11 September	Kuopio, Finland
Swedish Rescue Service	Course on international environmental disasters	7 September	TBD, Sweden
BBK, Germany	5th European Congress on Civil Protection and Disaster Management	5-6 November	Bonn, Germany
NATO School	NATO Civil Emergency Planning Course	16-21 November	Oberammergau, Germany
NATO School	NATO Defence Against Terrorism Course	23 November	Oberammergau, Germany
European Commission	3rd Civil Protection Forum	25-26 November	Brussels
IAEA	Enhancing the Global Nuclear Safety and Security Regime	14-18 December	Cape Town, South Africa
Wilton Park	A Smart EU Energy Policy	3-12 December	Wilton park, UK

Further information is available on e- Prime, the Partnership Real-time Information Management and Exchange System.

1420-09 NATO PRINTING & GRAPHICS STUDIO

If you would like to contribute to "perCEPtions", the CEP newsletter, please contact **Clare Roberts, CEP, NATO HQ** **cepd@hq.nato.int**