PROJECT PERIODIC REPORT

1. Publishable summary

SECURENV supports the development of knowledge base needed to ensure the security of citizens from future threats associated with possible deliberate attacks on the environment. The cornerstone in assessing the emerging threats is a foresight exercise well-suited to identify emerging threats to the environment from deliberate action. Results will be theoretical and practical insights into potential emerging elements of environmental terrorism including understanding how either the deliberate destruction or the use of environmental factors to enhance the effect of conventional attacks may affect societies. These key results will be converted to specific recommendations for adjusting European policies to address threats of environmental terrorism. The long-term objective of SECURENV is to support the development of appropriate counter measures and mitigation strategies.

The first year of the project has been dedicated to a focused assessment of the background issues including emerging factors and to the development of the tools and methods to be used during the second year of the project. The work started with a review and assessment of past environmental accidents, catastrophes and examples of deliberate attacks on the environment. For the structured assessment of these incidents a MySql database was created that hosts over 330 records with qualitative and quantitative parameters used to categorise the entries. While there is substantial anecdotal evidence of deliberate destruction throughout history, the actual amount of incidents related to environmental terrorism in the recent past is limited. However, organised crime appears to be an emerging phenomenon in this domain and the number of incidents is increasing, not least because of increasingly strict environmental regulations. Several examples of environmental warfare have also been identified and also special attention has been given to incidents related to invasive species, as investigations by the project revealed the scale of the potential economic and environmental damage some of these species can cause.

Parallel to the assessment work on previous incidents work on developing a suitable foresight methodology has also started. The objective was to develop a systematic security foresight approach tailored to suit the specific needs of the objectives of SECURENV. For this purpose, existing foresight approaches in the area of environment and security have been reviewed and synthesised and tailored to the approach of SECURENV. The resulting methodology is a combination of well-established methods that utilises both the expertise in the consortium (such as Brainstorming, Trend-spotting, Mind-mapping and SWOT analyses) and expertise outside the consortium, in particular a Delphi survey addressing more than 600 experts in Europe and beyond, as well as scenario-building workshops involving 15-20 experts. Furthermore, backcasting would be used at the end of the scenario workshops and during the final workshop to arrive at relevant policy recommendations.

Parallel to these thematic activities SECURENV has developed a strong dissemination and end-user involvement strategy. In this case a particular challenge was to find a compromise between the need to publicly disseminate project results and to make sure that potentially sensitive results are distributed adequately.. In order to meet this challenge a security-sensitive approach has been developed throughout the implementation of the project. Accordingly a strategy has been devised that divided end-users according to three main groups depending on their degree of engagement in

the project and the type of restricted information they can receive. The first group consists of end-users from intelligence, security and the counter-terrorism community. This group is small and restricted and they will receive information the sensitive concepts developed in the project. The second group consists of those responsible for or related to civil protection and environmental protection. This group is larger and has access only to non-classified results. The third group consists of end-users outside the EU such as U.N. organisations and others internationally involved in environmental protection and/or counter-terrorism security affairs. Depending on their classification status, some members may receive classified results while others will only receive public deliverables.

In terms of dissemination towards the greater public, a non-compromising dissemination approach has been developed throughout the implementation of the project in order to avoid any unwanted interest. Separate public and confidential project profiles have been defined. The "Public profile" is that the project investigates serious environmental accidents and catastrophes and formulates recommendations for civil defence use and for increasing public security from accidents. The "Confidential profile" and the project's mainstream activity is to implement foresight methods and scenario building techniques for the investigation of threats associated with possible deliberate attacks on the natural environment by terrorists and other organised groups or individuals. In order to make sure that a careful treatment of results is maintained and in order to avoid the dual use (and any other form of potential abuse) of project results, a Dual Use Advisory Board (DUAB) has been set up that continuously screens project results. The DUAB consists of two retired intelligence officers, who review the deliverables and give the project consortium advice on the appropriate manner of dissemination and communication.

All the results that were produced during the first year of the project will be used during the second year with the purpose of identifying novel and emerging threats on the environment by terrorists and possibly other organised groups. The objective is to identify novel and emerging threats of environmental terrorism and also the technological opportunities via the developed foresight methodology and using the results of the review of past incidents during the first year. Scenario building techniques will be applied for systemic risk analysis that will address environmental security/environmental threat as an evolving concept. Based on the outcomes of the exercise key findings will be identified, which will serve as main input for policy measure developments. The boundary objectives set up for the foresight exercise will also be evaluated against the achieved results, including the quantity and quality of outputs, impact of outputs, potential effects on policy and future security research. Based on the outcomes, additional complex factors and uncertainties will be analysed where appropriate. This includes among others, how climate change may potentially affect the risk of environmental terrorism, such as making the environment more vulnerable and thus a more attractive target.

As a final step SECURENV will provide policy recommendations to European policy-makers and the intelligence community taking into account ethical, cultural and organisational challenges. The objective is the targeted development of policy recommendations for European policy-makers and the security community based on the results acquired during the course of the project. This will on the one hand identify how the current structure of the EU may cope with the challenges identified in SECURENV. The project will also help to identify the critical gaps that need to be filled within the European security research efforts in the environment domain. Finally, SECURENV will provide a broad outlook from a global perspective, to what extent the threats identified may have implications for farther regional and global structures (such as UN and other international agencies) against the backdrop of global trends. Work will also contribute on the elaboration of the security-research roadmap for Theme 10 of FP7.

General information about the project is available at www.securenv.eu. This secure website has a variety of access levels available, given the different user groups. It is also used by the Consortium members to exchange ideas, data, and for everyday communications (e.g. availability/absence of project partners and staff members, identifying suitable meeting dates, etc). The DUAB has the highest level of access to the website where they can directly remove items from the database and they can also use internal messaging to propose other changes.

Figure 1 – The project website and the project logo

The project has also developed a logo and established a Power Point and Word template for uniform representation at conferences and other public events, and throughout project publications. A project brochure has been printed and it is also downloadable in electronic format from the project website. The brochure will be updated for the second year and it will include results from the first year's investigations.	SECURENV