

**Title: Crime mapping and analysis for community safety and the prevention and detection of crime**

**Acronym:** Crime mapping

**Submitted by:**

Antony Cooper (acooper@csir.co.za)

Tel: 012 841 4121 Mobile: 082 497 3812

Postal Address: PO Box 395 Pretoria 0001

**Theme:** Security and Space

**Focus Area:** Protection against terrorism and crime

**Type of project:** R&D project (small scale)

**Summary:** Traditional crime mapping in police stations consists of using coloured pins stuck into wall maps to denote the occurrences of crimes - pin mapping. Unfortunately, such manual mapping is cumbersome, time-consuming, and not reproducible and provides limited visual analysis - and the many pins stuck into the map at "hot spots" of crime tend to shred map! Geographical information systems (GIS) allow one to do such pin mapping on a computer, providing data that can be used to produce a variety of maps whenever and wherever needed, and that can then be used for analysis. Besides crime scenes, one could pin map calls for service, encounter sites and the deployment of resources. These data can be combined with many different types of external data to provide backgrounds for the maps or for analysis: street networks, aerial photography, demographics, alcohol retail outlets, satellite imagery, transport nodes, buildings, traffic densities, topography, jurisdictional boundaries, barriers, victimisation surveys, etc. Crime mapping and analysis can support all levels of combating crime: strategic, operational and tactical. The analysis of crime data has been driven by key breakthroughs in the theory of environmental criminology, such as routine activity, criminal opportunity, repeat victimisation, activity spaces, distance decay, and geographic profiling. Using a GIS and other tools, the analysis can identify crime hot spots, patterns and trends (both spatially and temporally), linkages, vulnerable targets, suspects, syndicates, criminal resources and the causes of crime. It can be used for deploying resources, through determining where the gaps are, and simulating interventions or routine patrolling. Such crime mapping and analysis can be used to empower communities to understand the real crime situation in their neighbourhoods, for leading courts through complex cases, for policy development and for the strategic, tactical and operational management of resources in the justice system.

**Expertise offered:** The CSIR has expertise in the following: o Geographical information science; o Crime mapping and analysis, including developing innovative techniques such as crime clocks, target performance maps, and mapping the use of cellular telephones by criminals; o Statistics; o Operations research; o Information management; o Decision support systems; o Software development.

**Previous FP involvement:** No

**Consortium status:** No consortium yet, though we have started talking to possible partners

**Expertise sought:**

**Related projects:** South African national R&D programmes

**Title:** High temperature structural alloys for aerospace and space applications

**Acronym:** HTAlloy

**Submitted by:**

Sara Prins (sprins@csir.co.za)

Tel: +27128414806 Mobile: +27833816516

Postal Address: PO Box 395 Pretoria 0001 South Africa

**Theme:** Security and Space

**Focus Area:** Space-based applications at the service of the European Society

**Type of project:** R&D project (small scale)

**Summary:** Investigate new high temperature structural alloys for space and aerospace industry, specifically for jet turbine engines and rockets for satellites and space craft

**Expertise offered:** Experimental design and testing first-principles calculations of properties thermodynamic modelling of phase equilibria mechanical testing and properties

**Previous FP involvement:** No

**Consortium status:** not existing yet, but collaborating informally with U Bayreuth, Germany, and informal talks to German Space Agency and MTU Aero Engines

**Expertise sought:**

**Related projects:** South African national R&D programmes

**Title: Recognizing and preparing loss estimates from cyber-attacks on SMEs**

**Acronym:** RPLECA

**Submitted by:**

michael Kyobe (mkyobe@commerce.uct.ac.za)

Tel: +27 21 6502597 Mobile: +27 839493011

Postal Address: P.O.Box 34240 Rhodes Gift Cape town 7707 South Africa

**Theme:** Security and Space

**Focus Area:** Security and society

**Type of project:** R&D project (small scale)

**Summary:** Recognizing and preparing loss estimates from cyber-attacks on Small & Medium sized firms (SMEs) **OBJECTIVES** This study will investigate factors inhibiting SMEs from preparing loss estimates from cyber-attacks. It will examine existing cyber loss estimation techniques and explore appropriate measures to ensure disciplined and diligent record keeping of security incidents in SMEs. The key deliverable will be an effective framework, incorporating useful measurement concepts from various disciplines which SMEs may use to produce accurate loss estimates. **MOTIVATION** Technological advances have been phenomenal but have also created a multitude of problems for SMEs. According to Leyden (2000), more than 60% of the small businesses fall victim to such attacks a year and in many cases they are unaware of the problem. A recent survey by a leading South African IT law firm shows that many web-sites don't comply with the Electronic Communications & Transactions Act No 25 of 2002 and numerous SMEs are unaware of the implications. This is of great concern since these firms are the major source of job opportunity and income generation. One important step in solving security problems is proper identification and recording of security breaches (Solms and Solms, 2004). Unfortunately, small organizations do not keep formal records (Rwigema and Karungu, 1999; Kyobe, 2004). SME managers are often unaware of the costs of security breaches and as such have no clue how much money is being lost. Failure to estimate the costs of cyber-attacks translates to inappropriate allocation of resources as the optimal amount to spend on information security cannot be determined and the effectiveness of that spending cannot be measured. In addition, companies cannot even file civil suits because of difficulties in determining the financial impact of such incidents. Some evidence shows that cyber-loss estimates are sometimes compiled in an apparent information vacuum and the underlying methodologies are basically anecdotal and inconsistent. This study will investigate these problems and develop an appropriate tool SMEs can use to prepare accurate estimates.

**Expertise offered:** Information systems management, computer auditing and forensics, Systems evaluation.

**Previous FP involvement:** No

**Consortium status:** knowledge of computer forensics or have conducted e-crime investigations. Experts in electronic law, accounting, auditing & IS. Any one else willing to contribute.

**Expertise sought:**

**Related projects:** South African national R&D programmes

**Title: THz Photonics for Automated Security Scanning**

**Acronym:** TerraScan

**Submitted by:**

Christoph Bollig (cbollig@csir.co.za)

Tel: +27128412707 Mobile: +27724026006

Postal Address: CSIR-NLC PO Box 395 Pretoria 0001 South Africa

**Theme:** Security and Space

**Focus Area:** Protection against terrorism and crime

**Type of project:** R&D project, including technology demonstration (large scale)

**Summary:** Terra-Hertz (THz) radiation is in the electromagnetic spectrum between the far-infrared optical region and the RF microwave region. Many common materials are transparent in this region, e.g. fabrics, paper, plastics. In addition, many substances of interest have a unique spectral signature in this region, e.g. explosives and drugs. Potentially, THz systems can be used to automatically scan packages and envelopes in postal and courier sorting stations for drugs, explosives and other illegal substances. In contrast to x-ray scanning, it can be automated and does not rely on human supervision, which makes mass-scanning feasible. The same technology could also be used to scan luggage on airports and possibly even cars at border stations and security check points. At this time, the main obstacle is the lack of compact and efficient high-power THz sources. In addition, there is still work required in THz optics (delivery and shaping of the radiation), detection and analysis algorithms. In addition to the security field, there are potential applications for THz systems in the medical and biological field. The aim of this project would be research in the following areas: - Novel compact and efficient high-power THz sources - THz optics (including delivery, shaping and scanning) - THz detection and imaging - Detection systems for explosives of various types - Detection systems for drugs of various types - Detection and imaging systems for other threats (e.g. ceramic weapons, powders, etc.) - Systems and algorithms for automatic detection of threats. - Integration into mail and parcel sorting stations

**Expertise offered:** - Efficient high-power mid-IR laser sources as pump lasers for THz generation - Short-pulse operation of lasers - Electronic control of lasers

**Previous FP involvement:** No

**Consortium status:** We are currently discussing the project with the Nonlinear Optics Group of the Physics department, University of St. Andrews, UK.

**Expertise sought:** Non-linear materials for THz generation (e.g. GaAs); THz optics; THz detection and imaging; Experts in the security industry who would potentially utilise this technology; Experts in computer algorithms for automatic detection; Experts from the mail and courier industry

**Related projects:** None