Threat Intelligence and Situational Awareness

The Cyber Security Centre at UH is interested at the issue of collecting and analysing threat intelligence from the cyber domain (including virtualisation and IoT technologies) under the context of situational awareness and how it can assist organisations to proactively defend their information environment.

The information environment is the aggregate of individuals, organizations and systems (resources) that collect, process, disseminate, or act on information. The Information Environment can be broken down into three distinct domains: Physical, Information, and Cognitive. The physical domain is the place where the situation we seek to influence exists. The information domain is where information is collected, processed, stored, disseminated, displayed and protected. Finally the cognitive domain exists within the minds of the decision makers.

Situational awareness is simply knowing what is going on in your environment.

Combining the aforementioned concepts, we suggest that the best method for situational awareness is through the collection and analysis of threat intelligence. Intelligence is the timely, accurate and usable product of logically processed information. Threat intelligence is the timely, accurate and usable product of logically processed information on which threat agents will have what opportunities for exploiting which vulnerabilities of which assets that are within our information environment.

We think that threat intelligence collection and analysis must form part of a modern risk management strategy. Therefore, we are looking for candidates to join our group in designing new methodologies and developing tools to allow for the development of the aforementioned capability.

The prospective candidates should have a strong background in Computer Science or another relevant discipline. In particular, they should demonstrate very strong programming skills in one or more major programming languages. Ideally, they should have some background in the areas of risk and threat assessment, computer networks and security. Active civil servants are particularly welcome.

For informal inquiries please contact Professor Andy Jones (a.jones26@herts.ac.uk).