Timely cybercrime information sharing between ISPs/Telcos and Banks/Police

BIC Discussion Paper **November 2012**

Barend J E Taute [1]

[1] CSIR Meraka Institute, Pretoria, South Africa

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

The global experience is that cyber crime (theft of money, private details or Intellectual Property, malicious attacks, fraud, money laundering, 419 scams, cyber bullying etc) are becoming more prevalent and more sophisticated – requiring police, banks and other agencies to act fast, often in real time, in order to reduce loss of money, collect evidence and identify perpetrators. Most of the data and activities happen in cyberspace and can easily cross international borders.

Key challenges for investigators include the need for quick identification of the source (IP address, device number, physical location, person) and to gather evidence (SIM swaps, logon details, etc) that can stand up in court or be used to block criminal activity. Criminals can quickly erase their tracks or set up alternative channels / servers / identities.

Much of the information required for criminal investigations resides with the ISPs and Telcos, but sharing this is limited by legislation that includes issues of privacy and freedom of speech.

Research Objective

To develop a legal and technical framework for timely / real-time information sharing between Telcos and ISPs and banks / police to enable reactive and proactive cybercrime investigations. This would study the optimal set of technical data requirements as well as various national and international legal regimes in order to arrive at a useful set of data requirements, means to access them and legal authority to do so.

Expected Outcome

A Framework for Timely Data Sharing to Support Criminal Investigations that takes a global view of the data needs of cybercrime investigators and seeks to define an optimal legal basis that will allow ISPs and Telcos to provide such information. This could then be used to advise international and national legal modernisation initiatives.

Stakeholders – and how best to mobilise them

Cybercrime investigators:

Police and Financial Institutions. They have the challenge to investigate and stop criminal activity. International agencies like InterPol and national/international banking associations could verify the needs and support a project.

Communications network operators

ISPs and Telcos have access to data that can support investigations, together with various national and international associations. They typically need to protect privacy, reputation and revenues and would need a sound and safe solution.

Researchers and regulators

National and international legal academics, legislators and regulators such as the International Telecommunications Union. This is probably already on their agenda and needs to be explored with them.

Benefits and success metrics; the need for INCO

Benefits

Parallel studies in a variety of countries / continents will highlight the spectrum of crime types, legal challenges, technical issues and possibly creative solutions that have already been found.

Success metrics

A Framework that can be adopted internationally and that will guide national legislative modernisation.

Recommended approach

Telcos/ISPs operate nationally and globally and criminal activities know no boundaries. A multi-national approach from the beginning will enhance the benefit for the global community.

Timeline

Q1: Verification of problem statement

- Interaction with national Legislators / Financial Institutions / Police in a number of targeted countries to refine the problem statement and requirements for investigators.
- Contact with international legislators, agencies and regulators to identify current initiatives and to verify the legal limitations / processes.
- Mobilisation of stakeholders to support the project's objectives

Q2, Q3: Analysis

- Multi-pronged approach to gather detailed national and international information

Q4: Design

- Development of a framework

Q5: Validation

- Testing the framework with all stakeholders, updating and refinement

Q6: Promotion and implementation

- Seeking support from stakeholders that can influence implementation.

The full presentation can be found at http://www.bic-trust.eu/files/2012/10/Taute-BIC-27Nov20121.pdf

Dr. Barend J E Taute, Manager: ICT Contract R&D,
CSIR Meraka Institute, Pretoria, South Africa

Barend Taute is an electrical engineer with a PhD in Electromagnetics from the Ohio State University, Ohio, USA. He has been with the CSIR since 1983, involved in research, development, technology management and business development in areas such as radar, antenna design, microwave heating, remote sensing, safety & security technologies, crime prevention, information security and ICT. He is the South African National Contact Point for promoting participation in the European Framework Programme 7, Security Theme, and as such a partner in FP7 project SEREN2 (Network of Security NCPs).
In addition, he is a partner in the FP7 project EuroAfrica-P8 that promotes ICT dialogues, networking and analysis of research priorities between Europe and Africa. He collaborates with the South African Department of Science and Technology on ICT-related bilateral relationships in Africa and Europe, and is a member of the E-Commerce Advisory Committee in South Africa.