THEME: Debordering and Rebordering in Cyberspace: Technological, Legal and Political Aspects

PROJECT: Emerging Cyber Bordering Technologies

Lead Supervisor: Professor Sakir Sezer

Supervisory Team: Professor Sakir Sezer, Professor Cathal McCall

Primary Location: CSIT

Securing cyberspace borders is a rapidly evolving and crucial area of interest for governments, private sector interests, and individual citizens. Defending cyberspace borders for the protection of critical infrastructure, key resources and sensitive information is a key concern for governments. Yet, as the Edward Snowden case revealed, governments are also deeply implicated in penetrating cyberspace borders for the purpose of information-gathering on friend and foe alike. Similarly, international corporations have a vital interest in securing internal networks, as well as a research and development compulsion to penetrate the cyberspace borders of competitors in the name of innovation.

Firewalls, network-based application and user detection technologies and URL black and white lists present essential technological tools for building borders in cyberspace and preventing cross-border access to web-content. For example, large scale filtering of URLs in China restricts the access of its citizens to many US and European websites. On the other hand, service providers of streamed content (e.g. live football matches, movies, shows etc.) restrict international cross-border access due to broadcast restrictions of licensed content. For example, except BBC News, all Internet-based access to UK TV programmes are restricted by a firewall, ensuring that access is permitted to users within UK jurisdictions only. However, new technologies, based on well-established Virtual Private Networks (VPNs), and new VPN service providers (CyberGhost, Spotflux, Private Internet Access, Hotspot Shield, ProXPN, etc.) have evolved, providing encrypted anonymous tunnels, capable of penetrating virtual borders and providing anonymous access and hosting of unrestricted content via a country specific proxy server. The majority of these services are used for accessing terrorist or organised-crime related, copyright protected or illegal (offensive, abusive, sexual) content, stored or hosted in states with limited data protection and copyright laws.

The aim of this project is to explore various security, firewall and access control technologies that can be effectively used for policing and enforcing of cyber border policies. Many IT security technologies are developed for the Enterprise market and impose privacy and ethical concerns when they are used for bordering public cyber space. Scalability and global deployment pose technological challenges and potential misuse of intercepted and/or logged information as part of the policing process.
Project Objectives:

- Investigate and evaluate various security technologies that are suitable for cyber bordering and cyber border enforcements.
- In collaboration with AHSS, derive feature specification for cyber bordering technology for national cyber space and national cyber border protection.
- Explore technologies for policing encrypted VPN tunnels without violating user privacy or exposing intellectual property or trade secrets.
- Develop traffic analytics algorithms for cyber border policy enforcement.
- Prototype and validate traffic analytics algorithms and assess their suitability for cyber bordering.
- Assess the proposed analytics algorithms and developed bordering technology in terms of potential misuse for user privacy violation and ethical concerns.

Primary Academic Discipline: Computer Science (Social Science)