**A Public Health Approach to Cybersecurity**

Huw Fryer (ECS) Supervisors: Tim Chown (ECS), Roksana Moore (ILAWS)
Cyber Security Centre
University of Southampton

**Botnets**
- A Botnet is a network of infected machines (bots) under the control of a remote [criminal] operator
- Botnets are the tool of choice for cybercriminals
  - Make crimes harder to detect eg. DDoS, Fast Flux DNS
  - Makes it considerably harder to trace the real criminals

**Real Criminal Is Protected**

**Phishing Malware DDoS Child Porn Spam**

**Bot Remediation**
- Takedowns are expensive, time-consuming and require international co-operation
- A botmaster can simply purchase more infected machines for a small amount of money
- Remediated machines are no longer committing crimes
- User awareness of the problem should decrease infection rate making the problem easier to manage
- Fewer available machines should increase the cost of cybercrime therefore making it less worthwhile

**Security Economics**
Good security is of benefit to Internet users as a whole, but without appropriate incentives security won’t improve.
- An infected machine sending spam suffers minimal effects in comparison to Internet users as a whole
- Releasing only secure software reduces profits and goes against customer wishes for a quick release cycle
- Bot remediation by ISPs costs money and inconveniences customers

**Aims**
- Identify legal mechanisms which allow a state where positive behaviour is incentivised or negative behaviour is disincentivised
- Discover to what degree these are enforceable through technological methods
- Identify which parties are best targeted to ensure optimal cybersecurity
- Make cybercrime more difficult by reducing available hosts for botnet activity
- Develop principles for a new tort for cybersecurity

**The Public Health Analogy**
There are three levels of a successful public health policy: education (eg. About washing hands), prevention (eg. Vaccinations) and management (eg. quarantine)

- **Education**
  - Teach developers to write secure code;
  - Teach users not to click on the links.

- **Prevention**
  - Appropriate security software should be installed;
  - Systems should be kept up to date with the latest patches.

- **Management**
  - Isolate and remediate infected machines;
  - Quickly patch security holes to minimise the damage.

**Tort of Cybersecurity**
- During the industrial revolution, a new tort of private nuisance was developed which balanced the rights of an individual against the need for society to develop.
- The information revolution has had a similarly dramatic effect on society. Once again, what is in an individual’s interests is not necessarily best for society.
- A tort of cybersecurity should be developed based on similar principles to that of private nuisance to enforce security economics.
- Some manner of regulation will probably be required as well to ensure compliance before security breaches occur

**Future Work**
- Comparative legal study into the approaches taken to protect users and enforce cybersecurity in different jurisdictions.
- Comparison of the regulation and economics of previous technologies with that of Internet technology.
- Empirical study into the use of the Domain Name System by both criminals and normal users.