CS 978 – Legal, Ethical, and Professional Issues for the Information Society

Lecture 7 – Cybercrime

Introduction

Last week we discussed the UK legislation related to computer misuse. While computer misuse is one element of cybercrime, it is actually a topic that covers many areas of law.

This lecture will focus on some definitions of cybercrime, before considering the UK's own strategy on cybercrime, and questioning how much we need to take responsibility for cyber security as citizens and computing professionals.

Definitions and Convention on Cybercrime

Cybercrime is the use of any computer network for committing a criminal act. It includes a wide range of potential crimes, including hacking, virus, worm and trojan creation and transmission, phishing, pornography, fraud and intellectual property infringement.

The Council of Europe *Convention on Cybercrime* defines it as, "criminal offences committed against or with the help of computer network". The Convention covers three key issues:

- Computer crimes
- Government access to communications and computer data
- Trans-border cooperation

The C*onvention* was introduced in 2001 with 42 signatories initially, including the USA, and it was ratified by the USA in 2007. The UK finally ratified the document in 2011. It covers a range of offences:

- Illegal access
  - Member states must make illegal the intentional access to the whole of any part of a computer system without any right.
- Illegal interception
  - This conduct penalizes the intentional interception, without a right, made by technical means, of non-public transmission of computer data to, from or within a computer system.
- Data interference

  - Member states were required to criminalize the intentional damaging, deletion, deterioration, alteration, or suppression of computer data without right.

- Systems interference

  - This conduct involves the intentional hindering of a computer system, without a right of the function of the computer system, by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

- Misuse of devices

  - This conduct involves the intentional and without right production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed to commit any other offense described in this convention, or the production of a password, code, or similar data that facilitates some criminal conducts described in this convention.

- Systems interference

  - This conduct involves the intentional hindering of a computer system, without a right of the function of the computer system, by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data

- Misuse of devices

  - This conduct involves the intentional and without right production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed to commit any other offense described in this convention, or the production of a password, code, or similar data that facilitates some criminal conducts described in this convention.

- Computer-related forgery

  - Member states must attach criminal liability to the intentional (intent to defraud must be present) and without right input, alteration, deletion, or suppression of computer data resulting in inauthentic data with the intent to use it as it were authentic

- Computer-related fraud

  - This involves the causing of property loss to another person any input, alteration, deletion or suppression of computer data, and any interference with the functioning of a computer system.

- Offences related to child pornography

  - These offences concretely related to the production, offering, distributing or transmitting, procuring, and possessing sexually explicit material involving children, through the use of computer systems. These offences include real children, a person appearing to be minor, and realistic images depicting a minor.

- Offences related to infringement of copyright and related rights
    - to criminalize the "willful" infringement of **(a) copyrights** by means of a computer system. This is not applicable to moral rights conferred by such conventions, and **(b) copyright-related rights** by means of a computer system. Allows member states to reserve the right not to impose criminal liability for the above infringement conducts if another effective remedy is available in the member state

Subsequently, the European Commission has identified three key risks for internet security:

- Attacks on information systems are increasingly motivated by profit rather than by the desire to create disruption for its own sake. i.e. it is becoming less about hackers doing so for the challenge, and more about organized, targeted criminal activity
- The increasing deployment of mobile devices (including 3G mobile phones, portable videogames, etc.) and mobile-based network services will pose new challenges which could eventually prove to be a more common route for attacks than personal computers - the latter already deploy a significant level of security.
- The advent of “ambient intelligence” in which intelligent devices supported by computing and networking technology will become ubiquitous (for example, through RFID, Internet of Things, or IoT) will create additional security and privacy related risks through the exploitation of shared vulnerabilities.

The UK cyber security strategy

The UK cyber security strategy has a clear focus on both social and economic issues. The strategy can be understood in terms of the 4 key objectives:

Objective 1: The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace

This is clearly a proactive stance aimed to reassure business, and since so much of the modern economy is built on transactions in cyberspace this is a very important focus for any cyber crime strategy.

Objective 2: The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace

Here the focus is on ensuring the country and the organisations within in recognise the dangers of cyber attacks and have the highest possible protection against it.

Objective 3: The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies

The focus here is outlooking and seeks to appear not to be insular, thus alongside the clear focus on protection, we can interpret here an acknowledgement that cyberspace needs to remain the place first envisaged by so many of its progenitors.

Objective 4: The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives

The focus here is on skills and capability, so the development of expertise to ensure the country remains alert to both protection and development of cyberspace expertise is key.

Overall the UK strategy seems to tread a good balance between understanding the importance of the challenges faced while also focusing on the opportunities cyberspace still presents for development.

Cybersecurity and expanding liability?

Earlier in the semester, we discussed some of the ethical issues that computer scientists need to consider around the software they produce. There have been calls to consider responsibility around companies that provide software services and access to the Internet, as well as the responsibility of users themselves to be more aware of the damage poor computer security can do to themselves and others.

The onus being placed on Internet Service Providers (ISPs) and software vendors with regards to large part of internet user security has a great deal of logic as a concept. There is little doubt that one of the key challenges to a secure Internet is the naivety, and often stupidity, of users themselves. For instance, MacEwan cites a study from the Information Commissioner in the UK that found, "40 percent of people who had Wi-Fi at home did not understand how to change the security settings on their Wi-Fi networks, and 16 percent of people were either unsure whether their network was secure or knew that it was insecure, but had no qualms about that fact." The old adage that you are as strong as your weakest link has elements of truth to with regard Internet security. MacEwan takes the stance in the article that we must place more onus on the users themselves to be more secure. Is this sustainable, however?

The case in Germany where a musician sued a citizen who had allowed his unsecured Wi-Fi to be used by someone who downloaded a lot of his music illegally highlights the issues even more starkly (BBC News, 2010). Whether it is incompetence or naivety, many people find technology complex, but the technology remains a crucial element of modernity, therefore can we rely on users to ensure security? There is a clear argument, then, for financial services, ISPs and software vendors to take on the responsibility of personal security.

Legally we could argue that a system should be fit for purpose with the minimum possible care needing to be taken by a user. Yet computers can still be complex to people, and asking the average person to understand the security of routers and the like is arguably asking too much of them. Equally, vendors should also sell software that is fit for use, and we could argue that a requirement of this fitness for use is that it should be as secure as possible at the most basic setting. Financial services pose significant risks to the privacy and security of users, and the balance between complexity in terms of accessing, and security are vital if users are able to use them efficiently. Banks have no less of a responsibility to a client's money online than they did when the money was locked behind a steel door.

From a financial perspective, there are of course significant barriers. Making financial services secure is clearly possible, but the more security layers added, the more expensive and time-consuming it will be. We use accounts with banks that use a mix of passwords, and others who make you use machines that generate unique codes each time you log on. There is no one size fits all approaches that are used by all banks, but legally there clearly could be. Should we advocate, for instance, the use of biometric data for all financial transactions? Would the cost be prohibitive in doing so? Would users themselves rebel against it?

The expertise to manage security risks exists within the companies who deliver modern Internet services, and if it doesn't, it arguably should. Clearly, there is a great expense in hiring such skilled employees, but the dangers of not doing so include damaged reputation, as well as the loss of data integrity that may occur if targeted by cyber criminals.

Passing liability to vendors, ISPs, and financial institutions may seem like an indemnity too far, but the reality is the world of internet services remains relatively new, and we must attempt to safeguard both the efficacy of the services and the trust placed on them by users. The newness of the area may lead some to argue that we need novel solutions with regards liability, but we should build on existing best practice when it comes to the provision of services that can place people in danger. The Internet is a modern service paradigm, but we have areas of service delivery where security of product and user has been central for decades, such as pharmaceuticals, and public utilities like water services. We could arguably take our inspiration from these areas.

A wired world is one where many of the netizens in it do not understand the infrastructure and their role in its integrity. Passing the onus to those who *provide* the services does not seem to be an unreasonable position for something that can be immensely lucrative for them, and dangerous for their customers if not done properly.

Conclusions

Overall, the expansion of cybercrime in the modern era is inevitable, however, the exponential growth of Internet-enabled technologies in our daily lives raises the stakes significantly.

Future concerns may see us focusing on better security for our systems, and developing a more informed citizenry in terms of using them.

Further reading

Adams, Andrew A. and McCrindle, Rachel J. (2008) *Pandora's Box: social and professional issues of the information age*. Chs. 11 and 13

BBC News (2010), 'Wi-fi owner fined for lax security in Germany' (BBC, 14 May 2010) <http://www.bbc.co.uk/news/10116606> accessed 05 November 2015

Council of Europe (2001) *Convention on Cybercrime*. Budapest: Council of Europe. Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

MacEwan N, (2013) 'A Tricky Situation: Deception in Cyberspace' (2013) 77 *Journal of Criminal Law* 417

UK Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. London: Cabinet Office. Available from:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

DMcM/10-2017