The EU ECENTRE Project: Education as a Defensive Weapon in the War Against Cybercrime

Denis Edgar-Nevill, Centre for Cybercrime Forensics, Canterbury Christ Church University, Canterbury, United Kingdom

ABSTRACT

Since the EU Cybercrime Convention in 2000 (EU 2001), there has been a clear recognition of the accelerating threats to society posed by those who would exploit computers for crime and the logical progression to cyber-terrorism and cyberwarfare. Since that time the capacity to deal with cybercrime (crimes involving the use of computers) has improved but the problem has grown alarmingly. The European Commission recognises the increasing threat of cybercrime and has committed significant research and development funding in seeking to protect the community from cybercrime and cyberwar. This paper discusses a new European Commission funded project ECENTRE – England’s Cybercrime Centre of Excellence Network for Training, Research and Education. On 20th December 2012 the European Commission signed the €0.935million (£760,000) contract for the project. The contract is awarded under the Programme Prevention of and Fight against Internet Crime Targeted Call – ISEC 2011 Action Grants – Project Number HOME/2011/ISEC/AG/INT/4000002226. The author is the Project Manager and Principal Investigator for the project. ECENTRE forms part of a wider European network of centres of excellence to share expertise, promote best practice and provide training opportunities for law enforcement across the EU. The challenges in establishing effective cooperation and sharing are discussed. The considerable problem of keeping pace with the fast-developing, complex, problem posed by threats to national infrastructure, organisations and individuals is examined; highlighting the role of education as a fundamental weapon in the fight. The more we know about a threat (real or potential) – the better protected against it we become.

Keywords: Cybercrime, Cyberwar, Defence, Education, England’s Cybercrime Centre of Excellence Network for Training, European Union (EU), Research and Education (ECENTRE)

1. CYBERCRIME, CYBERWAR AND CYBER TERRORISM

Cybercrime and Cyberwar are inextricably linked. Given Cyberwar is usually covert in nature, it’s not really clear who is being attacked by whom, or if the aggressor is a national government, organisation, private group or individual.

For example, major attacks were launched on US military installations by a British lone hacker, Gary McKinnon, shortly after the 9/11 attacks in New York. Amongst a number of attacks on NASA and military targets he deleted military armaments logs at the US Earle Naval Station; bringing down the network of over 300 computers used to resupply the US.
Navy Atlantic Fleet (Law Lords Department 2008). Because the Internet makes hiding your identity possible, we cannot be sure who is on the other end of the line. Even if an attacker declares who they are we cannot be sure. This also allowed governments to conduct operations against enemies and espionage hiding behind a cloak of anonymity. In some cases we can infer the culprits by the level of sophistication of the attack. The release of the Stuxnet Worm, for example, has been considered to be the product of a nation state simply because of the complexity of ideas the software makes use of (WikiDot 2013). When considering the attacks by groups calling themselves the “Iranian Cyber Army”, “Pakistan Cyber Army”, “Indian Cyber Army”, “Indian Cyber Warriors”, “China’s Cyber Army” we cannot be sure if any or all are state sponsored or how many individuals are involved.

All attacks can be considered as manifestations of cybercrime with different levels of severity (Figure 1).

The recorded rates of computer crime and in particular, Internet-based Cybercrime, is growing at a staggering rate in the European Union and across the rest of the World (SDI 2012; Paganini 2012). The ability of governments, intelligence agencies and police forces to cope with this tidal wave is very limited. In the last few years we have seen a lot of money being committed to establishing national, CERT teams (Cyber Emergency Response Teams; EU 2011; AMEinfo 2012; TTOI 2012; CERT Australia 2013), Cyber Commands (US 2013; Gilad 2012; Segal 2011; Leyden 2011) or Cyber Militias (Arsene 2012; Segal 2012). The scale of financing, running into many billions of dollars, sounds impressive but must be countered with the scale of the problems being faced. Where such expenditure is strictly for defensive measures it’s difficult to test value-for-money unless attacks occur.

The readiness of governments to spend in this area has led to the development of proactive warfare weapons where something directly tangible is produced. Certainly the revelations about the nature and extent of information surveillance by intelligence agencies, revealed by whistle-blowers such as Edward Snowden, continue to draw criticism from prominent figures (BBC 2013). The readiness of the General Public to allow such intrusions has an important effect. The 9/11 attacks caused the population to accept a greater level of intrusion as a price of achieving greater security. However, the extent to which this has been progressed by some governments in the last decade has shocked many and the recent revelations have required explanations and justifications. The recent tele-

---

Figure 1. Levels of cybercrime

![Figure 1. Levels of cybercrime](image_url)
Understanding Optimal Investment in Cyber Terrorism: A Decision Theoretic Approach
www.igi-global.com/article/understanding-optimal-investment-cyber-terrorism/64311?camid=4v1a