The Threat of Cyber-Crime to the UK
RUSI Threat Assessment

Calum Jeffray

This is the first in a series of threat assessments produced by the National Security & Resilience Studies department at the Royal United Services Institute (RUSI). These assessments are designed to raise awareness, and inform public debate, on key threats to UK national security. The assessments are based on open-source analysis and expert insight, and have been through a rigorous process of validation.

Cyber threats to the UK remain a Tier-One national security risk, and the Cyber Security Strategy identifies criminal use of cyberspace as one of the three principal threats to UK cyber-security alongside state and terrorist use.

As the number of internet users and ease of access increases, and more and more of the nation’s public and private assets are stored electronically rather than physically (often outside UK jurisdiction), so too do opportunities grow for individuals to exploit the internet for criminal ends. According to the National Crime Agency, ‘If there is a single cross-cutting issue that has changed the landscape for serious and organised crime and our response against it, it is the growth in scale and speed of internet communication technologies.’

Open-source analysis reveals that the scale and reach of cyber-crime are perceived to be increasing. Cyber-criminals rapidly identify potential vulnerabilities in new and evolving technology, exploiting them to unlawfully acquire data or disrupt systems, typically for financial gain. Like all types of crime, cyber-crimes are committed by both opportunistic individuals and organised crime groups (OCGs), and the public, businesses and government are all at risk.

Understanding the scale of cyber-crime, how it is changing over time and the impact of interventions to tackle it are key priorities for policy-makers. However, the scale of such crime in the UK and its cost to the economy have proved challenging to quantify with any degree of confidence. This is largely because of the unclear methodologies or metrics used to measure online criminal activity, as well as the challenges of cross-border activity and confusion and ambiguity over much of the terminology associated with cyber-crime. Under-reporting and inadequate recording of such crimes represent further challenges.

This assessment elucidates some of the characteristics of the threat to the UK, as well as the perpetrators, targets and likely future trajectory of cyber-crime. It does not address its scale or cost. The analysis revolves around five main questions:

- Who is stealing the most money from UK citizens?
- How are they doing it?
- Which UK entities are most affected?
- What are the links between cyber-thieves and states?
- What is the likely trajectory for the cyber-crime threat over the next two years?

Key Judgements

1. Data, rather than financial assets, is now the most lucrative and common target for cyber-criminals
The scale of cyber-crime is often framed in terms of the sum of money stolen online, but stolen personal information and identification-related data (and, to an extent, intellectual property) is often more lucrative than stolen money as it can be rapidly and repeatedly sold on via online criminal networks. The value of data and confidential information is typically subjective and the scale of losses hard to quantify in monetary terms; large-scale data losses also entail unquantifiable costs such as damage to brands, reputation and consumer confidence.

2. The number of cyber-crimes is a less useful gauge of the scale of the issue than the impact of each individual attack. Criminals focus on high-value targets, based on intelligence obtained through long-term online espionage or from insider sources, which can yield greater returns than multiple small-scale attacks
The current trend indicates that the scale and impact of individual cyber-attacks will increase. While mass online scams may continue, their effectiveness

will decline and criminals will increasingly seek detailed information on specific targets. This intelligence allows them to both understand businesses processes and practices in order to exploit vulnerabilities, as well as acquire data on the customer base in order to increase the sophistication of social engineering tactics.

3. A lack of specialised technical expertise is no longer an obstacle to committing cyber-crimes. Purchasing specialist services – such as coding, equipment or bespoke malware kits – offers opportunities for criminals with limited technical competence to commit crimes online. With the increased availability of technical skills and tools through online ‘marketplaces’, the cyber-criminal environment has become more accessible to non-experts and those without expertise in computer programming. These online marketplaces operate an ‘as-a-service’ business model, in which membership of online OCGs is more fluid and less structured than in traditional OCG structures.

4. There has been a rise in high-frequency, low-level cyber-crime comprising ‘old-fashioned’ criminality such as extortion, with criminals employing relatively uncomplicated techniques. Cyber-enabled crime is growing as criminals return to old-fashioned techniques while using new technology. An example is the use of ‘ransomware’, a type of malware which prevents users from accessing their system or files until a ransom payment is made to restore the system. The amount of high-volume, low-end cyber-crime is likely to increase as a result.

5. Malware that specifically targets and affects mobile devices and/or social media is likely to pose a significant threat in future. Cyber-criminals demonstrate a particularly responsive form of criminality by rapidly exploiting vulnerabilities. Access to the internet from the UK using a mobile device more than doubled between 2010 and 2012 from 24 per cent to 51 per cent of the total, making mobile devices an increasingly attractive target for criminals (as is beginning to manifest in many parts of Asia). The increase in social media use will also give rise to innovative social engineering techniques.

Threat Analysis

Who is Stealing the Most Money from UK Citizens?
The amount of money stolen from UK entities is not systematically calculated, and may not in reality provide a valuable indicator of either damage inflicted on individuals and organisations, or the total proceeds of cyber-crimes. This is particularly true given the appeal of stealing data rather than money directly. An OCG can sell on stolen data, which in the long term may prove more cost-effective and profitable than targeting financial accounts directly. The value of data is subjective, and may be of particular worth to a company's competitor, for example.

There are other limitations to calculating the amounts of money stolen online. Businesses in particular are reticent to report cyber-crimes and subsequent losses through fear of reputational damage. Police recorded crimes do not distinguish online from offline offences, making it difficult to delineate the amount of money acquired solely through cyber-crime. Finally, cyber-attacks often entail 'indirect' financial costs such as repairing damaged systems or increased spending on cyber-defences. The true financial impact of cyber-crimes is thus unlikely ever to be measured accurately.

Few efforts have been made to conduct criminal profiling and comparatively little is thus known about the individuals committing cyber-crimes. For example, there is limited evidence about the characteristics of offenders, their backgrounds and career pathways, the links between online and offline offending, progression into other criminal roles, and interventions to prevent (re-)offending. The problem is compounded by the degree of anonymity offered online and the limited information available on offenders located in foreign jurisdictions.

That said, over the past year or so more has become known about how cyber-criminals operate and interact. It has become easier to commit cyber-crimes, and cyber-techniques have proliferated among criminals without technical expertise. An estimated 1 per cent of large data breaches are rated as 'highly' difficult, requiring advanced skills; 78 per cent of breaches are estimated to be in the 'low' or 'very low' (average user capability) difficulty category, indicating that many cyber-criminals may in fact be non-specialists with limited technical knowledge or expertise.

This is in large part thanks to the existence of a global online 'marketplace' where criminals can buy and sell the technical tools or services used for,

---

5. Ibid.
6. Ibid.
or products derived from, cyber-crime attacks. Rather than ‘traditional’ hierarchical organised crime groups, criminals therefore tend to operate in atypical group structures, forming looser online networks with limited centralised control. Allegiances to groups is rare; membership is transient depending on the skills and expertise needed, and members rarely meet in person or even know each other’s true identities.

How are They Doing It?
Cyber-criminals are able to gain financial rewards through both cyber-dependent crimes, including spreading viruses and other malware, hacking into systems and launching distributed denial of service (DDoS) attacks, and cyber-enabled crimes (traditional crimes such as fraud and money laundering, which can be increased in their scale or reach by use of computers, networks or other forms of ICT). These are some of the most common ways in which criminals can profit from online criminal activity:

**Online financial fraud**: the defrauding of legitimate businesses, using forged or fraudulent credit cards, or fraudulent applications for government services such as benefits.

**Data or revenue theft**: typically achieved through directly hacking into an organisation’s system by exploiting vulnerabilities or implanting malware to acquire valuable data. Revenue theft is often achieved through employing social engineering techniques and ‘tricking’ customers into revealing personal data such as bank account details or login information.

**Industrial espionage or theft of intellectual property**: criminals hack into an organisation’s system in order to acquire confidential commercial information or product details, selling them on to competitors or directly to customers. Crimes such as selling and distributing pirated music, films and games without due rights also fall into this category.

**Deploying botnets**: these are designed to infect and gain control of tens of thousands of personal computers at a time, primarily to allow criminals to harvest identities for financial gain (but also used as a method to launch large-scale attacks on industry or infrastructure).

**Extortion**: ransomware (also termed scareware when referring specifically to false security software) is increasingly common, where criminals trick individuals into downloading software which prevents users from accessing their system or files. Alternatively, criminals can launch deliberate denial of service attacks on companies or deface their websites. Victims must pay the

---

hacker to remove the malware or stop the attack, and return the system to normal function.

**Distributed denial of service attack:** although they may not directly generate profit for criminals (though may result in revenue losses for the victim organisation), DDoS attacks can be used to divert the attention of IT staff while hackers attempt to break into the company’s network, using methods that may go unnoticed as the DDoS attack continues in the background.

**Which UK Entities are Most Affected?**
The difference between ‘traditional crime’ and ‘cyber-crime’ is one of scope; traditional crime generally occurs in one place and has an impact on one set of victims, while cyber-crime often does not distinguish between victims and can have an impact across multiple jurisdictions.

UK citizens are primarily targeted through social engineering techniques (phishing and malware) by criminals in order to commit identity theft and online fraud. While such crimes may be common, the scale of crimes to individuals is relatively small. The government is targeted owing to the increased availability of government services online; fraudulent applications for services such as benefits, VAT and income tax returns online may be perceived by criminals to offer more anonymity and less human interaction than offline services would require.

**Figure 1:** Malware events per hour across US industries, Jul-Dec 2012.


However, businesses and the private sector are the most profitable target for cyber-criminals, though the sectors targeted may not be the most obvious. In the US the technology, logistics, manufacturing and telecommunications sectors experience the most malware events per hour, with the finance, banking and business services sectors experiencing a below-average number of events (Figure 1).

Using different metrics, Figure 2 below shows that a similar situation exists in the UK, with the manufacturing sector thought to experience the most number of cyber-attacks (though as noted above, this may not be a useful indicator of the impact of cyber-crime in each of these sectors).

**Figure 2:** Top 10 UK industries attacked in 2012.

Bulk business data, required for large-scale scams, has been stolen from many large corporations, such as Adobe in 2013 or Barclays in 2014. As noted above, data security is now a mainstream concern for large business and organisations. Data is particularly vulnerable when held by individual internet users, stored centrally, or in transit between individual and organisation – e.g. using laptops or USB devices – and many organisations have introduced policies to try and prevent this.

However, increasingly it is small and medium enterprises (SMEs) which offer the path of least resistance for criminals. While it can be argued that the rewards of attacking a small business are less than what can be gained from attacking a large enterprise, this is more than compensated by the fact that many small companies do not possess adequate capabilities or invest in...
cyber-defences to the same extent as large corporations. They are therefore less likely to detect and respond to an attack, or to recover as quickly.

Given the nature of modern commerce, attacks on SMEs can generate problems for larger companies as well since they depend on supply chains which may feed into the networks of the bigger enterprises. With each new link, there is a greater likelihood that a cyber-criminal will find a route into not just one company’s system, but a whole network of businesses.\(^\text{10}\)

**What Are the Links Between Cyber-Thieves and States?**

The line between cyber-criminals and state authorities may often be blurred in large part because some states see criminal organisations as useful allies. Even in 2009, it was noted that certain states have demonstrated their willingness to tolerate, encourage or even direct criminal organisations and private citizens to attack enemy targets.\(^\text{11}\)

The degree of state collusion can vary enormously, while attributing criminal acts online to state authorities is notoriously difficult. Evidence is often circumstantial; for example, if the attack was noticeably in a state’s interest, or if the attack was so complex as to necessitate a level of resources only reasonably possessed by state authorities.

Given the ease of acquiring online criminal tools and expertise from the global ‘marketplace’, it is increasingly difficult to assign particular criminality to a geographical location, or to identify geographic regions as posing a particular cyber-threat. That said, trends in four regions are outlined below. The level of criminality in each case may not necessarily point to direct state involvement; there is a risk, however, that states may not properly investigate (and may even tolerate) these criminal activities, particularly if they align with state interests:

- **Nigeria and Southern Africa** are often the source of phishing emails and other scams to acquire users’ private data.
- **Russia**: The perceived role of government-backed ‘hacktivists’ during the 2007 Estonian and 2008 Georgian cyber-attacks is well documented, but the risk of intellectual property theft by Russian-speaking criminals remains significant.
- **Eastern Europe**: The growth in activity from Eastern European OCGs, particularly in the UK, is carried over into the cyberspace environment, especially within the online banking and finance sectors.
- **China**: Chinese cyber-criminals are thought to be behind many cyber-

\(^{10}\) Sean Hargrave, ‘How to Protect Your Supply Chain from Cybercrime’, *Guardian*, 28 April 2014.

\(^{11}\) McAfee, ‘Virtual Criminology Report 2009; Virtually Here: The Age of Cyber Warfare’, p. 11.
crimes involving illicit pharmaceuticals and intellectual property theft, but economic espionage of Chinese origin appears to have the most state complicity. Particularly in the US, economic cyber-espionage is thought to be Chinese government policy, and the Chinese the most active and persistent practitioners of cyber-espionage in the world. The evidence against groups linked to the Chinese military is increasing, and the US Justice Department recently filed criminal charges against five Chinese military officers for the alleged hacking of five US companies

It is important to dispel the myth that the cyber-crime threat to the UK only comes from overseas. Just as the UK is an attractive place to conduct legitimate business online, so too is it a good environment for cyber-crime. The UK’s highly sophisticated IT infrastructure – which is both cheap and easy to use – as well as London’s reputation as one of the biggest global financial and logistical hubs, makes the country an increasingly popular place from which to launch cyber-attacks.

What Is the Likely Trajectory for the Cyber-Crime Threat Over the Next Two Years?
Changes in the threat from cyber-crime are likely to mirror developments in new technology and shifting patterns of public behaviour. Money can be made in exploiting vulnerabilities in each before the weakness is discovered. The rise of social media and mobile technology use is already generating opportunities for cyber-criminals and will continue to do so.

Social media websites are already attractive for cyber-criminals, as they possess less stringent anti-spam security measures than e-mail and users tend to trust links sent to them from friends and followers on the network. As social media sites go mobile and payment mechanisms become more common, opportunities for malware, phishing and spam will increase, attracting even more attention from criminals.

As tablet and smartphone market penetration continues, specific vulnerabilities in these devices and ‘mobile malware’ will become a significant issue, as is already the case in many parts of Asia. In 2013 over 143,000 new modifications of malicious programs targeting mobile devices were detected, demonstrating there has been a rapid increase in the number of such programs. Android continues to be the most targeted mobile

operating system, accounting for 97 per cent of the new threats discovered in 2013.\(^{15}\) Criminals deploying the ransomware and other malware currently infecting computers are likely to begin targeting mobile platforms in the next two years.

While the frequency of cyber-crime attacks may not necessarily increase, each attack is likely to inflict greater damage. Criminals are likely to conduct more targeted attacks through exploiting better intelligence, given the higher conversion rates of these attacks and their lower risk of exposure than large-scale attacks.

The cyber-crime environment will continue to operate as a sophisticated marketplace and, just like commercial markets, will strive for operational efficiencies, increased profit and return on investments, while also remaining susceptible to market forces and external interventions.

In this same vein, the trend of criminal professionalisation is expected to continue, with OCGs acquiring the ‘services-for-hire’ of technically advanced individuals for specialised tasks, software and techniques. The tools required to penetrate systems and obtain data are likely to be sold, distributed and available more widely, lowering the bar of entry into cyber-crime. Given this likely increased ease of access and growth in the number of individuals and groups committing sophisticated crimes online, conflict arising from competition between OCGs online is a further possibility.

*Calum Jeffray is a Research Analyst in the National Security and Resilience Department at RUSI.*

---

\(^{15}\) F-Secure Labs, ‘Threat Report H2 2013’. 