Williams, M. L. and Levi, M. 2012. Perceptions of the eCrime controllers: modelling the influence of cooperation and data source factors. *Security Journal* n/a (10.1057/sj.2012.47)

Original Article

Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors

Matthew Williams[a,*] and Michael Levi
[a]School of Social Sciences, Cardiff University, King Edward VII Ave,
Cardiff, CF10 3WT, UK.
E-mail:WilliamsM7@cf.ac.uk

*Corresponding author.

Abstract eCrime is now the typical volume property crime in the United Kingdom impacting more of the public than traditional acquisitive crimes such as burglary and car theft (Anderson *et al,* 2012). It has become increasingly central to the National Security Strategy of several countries; in the United Kingdom becoming a Tier One threat. While it is apparent to some governments that cybercrimes are now as much of a 'problem' as some forms of organised crime, little is known about the perceptions of the broad network of what we call public and private sector 'eCrime controllers' in the United Kingdom. A survey of 104 members of the UK Information Assurance community garnered data on the perceptions of the eCrime problem. The results showed an association of cooperation and consumption of data sources with perceptions. It is likely that perceptions within non-specialist corporate and public domains (non-IT and Finance) will begin to change as new cooperation arrangements are introduced as part of the UK Cyber Security Strategy. These findings call for a more in-depth qualitative understanding of the cooperation between eCrime controllers and their data consumption practices. Ascertaining what shapes this cooperation (and non-cooperation) and how perceptions compare with 'actual' threats and risks is necessary if we are to better understand the 'social construction' of the problem and subsequent policy and operational outcomes.

Keywords: eCrime; information assurance; cooperation; partnership; information sharing

Introduction

eCrime has become increasingly central to the National Security Strategy of the United Kingdom (HM Government, 2010, 2011) and of many other EU countries (for example, France, Germany and the Netherlands). Beyond the EU, it is high on the security agendas of other countries, including the United States, Australia, China, India and Russia (though some of their constructs of 'security' may involve breaching other countries' corporate and governmental cyber defences). In the United Kingdom, eCrime has become a Tier One threat, above organised crime and fraud generally, although it is an extremely broad category

ranging from opportunist thefts (or, as we prefer to express them, 'duplications') of personal data to systematic mass attacks on banks, unauthorised obtaining of key corporate Intellectual Property (IP) and cyberwarfare, at the other extreme. Based on Crime Survey data from England, Wales and Scotland, and from Eurostat, eCrime is now the typical volume property crime in the United Kingdom, impacting more of the public than traditional acquisitive crimes such as burglary and car theft (Anderson *et al*, 2012). However, as with 'organised crime' and other national threats, substantial variations exist in the *perceived* prevalence of eCrime and its constituent components, and there is no simple translation of these strategic judgments into locally felt concerns. These present difficulties for public engagement in interventions, for public scepticisms may have to be overcome or lived with in the course of control strategies. Our study is the first to predict the perceptions of the eCrime controllers[1] within the UK Information Assurance (UKIA)[2] community on the severity of the eCrime problem. Variation in opinions among these controllers, and influences upon them, are mapped via two regression models. The results indicate that perceptions of the eCrime problem are correlated with levels of cooperation and consumption of certain data sources. Acknowledging these associations is important as it is likely that organisational perceptions (including public and private large and SMEs) will begin to change as new cooperation arrangements are introduced as part of the UK Cyber Security Strategy (Cabinet Office, 2011). The following sections provide the context to the article while also illustrating the complex nature of eCrimes information (in this instance definition and prevalence) which is commonly digested by the UKIA community.

Context

There is now a wealth of academic and consultancy research available to eCrime controllers on the rise of the cybercrime problem (see Williams, 2006; Yar, 2006; Wall, 2007; Garlik, 2009; Jewkes and Yar, 2010; PwC, 2012; Symantec, 2012). Recently these sources evidence that the prevalence and severity of cybercrimes are increasing. Governments' fears of nation-state-sponsored cyber attacks, which were often disregarded as scaremongering by sceptical academics, have been shown to contain at least some degree of reality, with the creation of complex malware for targeted attacks such as Stuxnet and most recently (as we write) Flame/sKyWIper (Farwell and Rohozinski, 2011; CrySyS Lab, 2012). Yet there remains ambiguity over the definitions and measurements of prevalence, impacts and costs of eCrime (Anderson *et al*, 2012; Levi and Williams, 2012). Part of the explanation of this lack of agreement rests with the foundation of eCrimes: *technology*. While conventional 'terrestrial' crimes are often rationalised and understood in terms of (a) being static in time, (b) being static in space, (c) being largely universally recognised as 'criminal' (politically, legally and publically), and (d) most frequently perpetrated by individuals from socio-economically marginalised backgrounds, the technology of the Internet disrupts all of these dimensions. As Giddens (1990) puts it, these new forms of networked technologies afford 'distanciated' interactions, meaning that an action in one spatial-temporal boundary may have an effect outside of that jurisdiction. Cyber criminals are able to attack their victims at-a-distance in compressed or expanded periods of time (Williams, 2010). There also remains confusion and misinformation regarding what cybercrimes are in the political, legal and public domains and even more uncertainty regarding the characteristics of the perpetrators of such acts.

The United Nations highlighted the problem of definition in its *Manual on the Prevention and Control of Computer-Related Crime* (1995) stating that while there is consensus among experts, these definitions have been functional and hence too specific. The Council of

Europe took a similar view, and its Committee on Crime Problems decided to leave out any definition of cybercrime in its 2001 Convention on Cybercrime, allowing individual jurisdictions to apply their own definitions based on their specific body of law, an approach that reflected a realistic judgment that preventative action should not await the unlikely event of global legal harmonisation. The EU did however provide a working definition for Europol's initial mandate, though this definition only relates to attacks on automated data-processing systems (Council of the European Union, 2000). This related to Europol's restricted mandate for certain crimes that can be committed over computer networks (drug and arms trafficking, counterfeiting, trafficking in human beings, child pornography, illegal immigration networks, and so on), nullifying the necessity for a more comprehensive definition of eCrimes. The recent establishment of a European Cybercrime Centre (EC3) at Europol, however, will likely see renewed efforts at defining the problem, as well as intelligence sharing and strategic interventions. Perhaps one of the more satisfying classificatory attempts is that of Wall (2007). He maps out cybercrimes in terms of whether the victim groups are individual users, corporate entities or nation states, their level of mediation by technology, and the type of offending behaviour. Wall goes on to specify (a) crimes against the machine (for example, hacking), (b) crimes using machines (for example, frauds) and (c) crimes in the machine (storing illegal materials). Finally, he distinguishes ordinary cybercrimes (those that assist terrestrial crimes), hybrid cybercrimes (global opportunities for 'terrestrial' crimes) and true cybercrimes (new opportunities for new types of crime such as Botnets).

Data on eCrime

A key problem to better understanding and controlling eCrimes is the lack of reliable data on their prevalence and impact on businesses, the national infrastructure and the general public. Several papers provide insightful reasons why existing data are flawed (see Casper, 2007; Anderson *et al*, 2008, 2012; and Sommer and Brown, 2011). The data issues identified include information asymmetries, the lack of data sharing protocols, confidentiality and anonymity of respondents, failure to adopt gold standard data collection practices, and knowledge and perception of victimisation.

Anderson *et al* (2012) identified over one hundred different attempts to collect data on cybercrime to date. The sources most digested include reports of attack trends (for example, from Symantec and McAfee); security breach disclosure reports from the Information Commissioner's Office; reports by trade bodies (for example, from the British Chambers of Commerce, the Federation of Small Businesses and banking trade associations) and surveys (for example, British Crime Survey, Offending Crime and Justice Survey, Commercial Victimisation Survey, Information Security Breaches Survey, Oxford Internet Survey and Eurostat).

By far the most voluminous sources of data on eCrimes are vendor databases of malicious code activity (for example, Symantec's Threat Assessment Report).[3] However, these data understandably focus on breaches such as botnet activity and subsequent spam levels that are technologically measurable by vendor specific software, (that is, they bypass

individuals' awareness levels about breaches). This approach, while valuable in identifying overall trends, does not represent all the populations of interest (for example, public sector organisations, business community and domestic users) or perceptions of harm and insecurity. Essentially they cannot provide the detail required on prevalence of breaches within each sector or region (where the unit of analysis is an organisation or individual), the perceived or actual impact of breaches, and the reaction of business or individuals to attack. Numbers of attacks identified by anti-virus vendors may once have been meaningful, but the growth of server-side polymorphism[4] has led to constant transformations which mean they are no longer a sensible count of malware. Furthermore, the origin of such statistics raises important questions of perceived impartiality. In terrestrial terms, such sources of data would be comparable with data produced by private security companies who provide services to local communities and businesses. Objectivity suffers in the face of economic drivers inherent in such enterprises.

Police data on reported eCrimes is potentially the most impoverished source. An early review of police eCrime recording evidenced that the practices of individual police services varied enormously, with only a few including computer crime markers on crimes committed via computer networks (Hyde-Bales *et al*, 2004). More recent recording practices have been guided by the Association of Chief Police Officers' (ACPO) eCrime strategy (ACPO, 2009), which recommended that the National Fraud Reporting Centre (renamed Action Fraud) become the hub for all recorded eCrimes. While this has the benefit of harmonising recording practices across forces, the criminal justice system as a whole is restrained by the criminal law which is largely technology-neutral. We do not know whether breaches unrelated to fraud are thus reported, and businesses and individuals (and the police themselves) may not know who to turn to. The detail required by analysts (for example, the nature of an electronic attack such as denial of service, distributed denial of service, insider unauthorised access, and so on), common to other eCrime sources, is often missing in police data.

National surveys on eCrime identify the organisation or individual as the unit of analysis. That is to say an employee (usually the person with responsibility for IT security) is asked about security issues and attacks in relation to their organisation, or a member of the general population is asked similar questions in relation to the home. These surveys capture instances of 'known' victimisation where the respondent directly experiences an eCrime attack or has been made aware of the attack by software (for example, virus checker) or by another person (such as a payment card firm who telephones the victim about a transaction suspected by the firm). In contrast to vendor data, these surveys not only identify prevalence of 'known' breaches, but also capture data on impact and response. Impact questions vary by survey, but often include length of system downtime, financial losses, potential reputational damage and anxiety in relation to possible future attack (in relation to surveys of the general public). Response questions include reporting and system upgrade behaviour, among other topics.

The majority of the surveys on business eCrimes adopt non-random sampling. The resulting data pool is biased towards knowledgeable victims from sectors where IT security is well embedded (that is, there is an IT security manager to answer the survey questions). Those respondents who are reluctant to respond, due to a lack of knowledge or interest or fear of reputational damage from notification of a breach, are absent from the data set, leaving a skewed picture of the eCrimes problem. Unlike in some American states, where Security Breach Notification is required by law, creating a near census of breaches

(see Anderson *et al*, 2008), the UK picture from the perspective of surveys adopting non-random samples is partial and biased.

While surveys that adopt random probability approaches to surveying eCrimes produce the most representative data, conceptual issues with question wording and with knowledge assumption can undermine the reliability and validity of data produced. Such problems led the European Commission i2010 High Level Group to conclude many of the questions in the Community Surveys on ICT Usage relating to business eCrimes attacks were unreliable. They also reported similar problems in relation to their domestic surveys (i2010 High Level Group, 2006). A European Commission sponsored review into eCrimes questions in the annual Information Society Surveys found questions relating to businesses were likely to be unreliable because: (i) SMEs lacked the expertise with technical terms; (ii) the outsourcing of security to specialists resulted in the lack of technical details; and (iii) the general reluctance of businesses to admit a problem in their own IT systems. In relation to domestic respondents the review concluded eCrimes questions were possibly unreliable due to: (i) a lack of expertise with the technical terms such as virus, firewall, and so on; (ii) the inability to trace back any incident to a certain cause (virus/adware/spyware/fraud); and (iii) the ambiguous or vague question wording (Empirica, 2007).

Large-scale random probability national surveys, such as the Crime Survey for England and Wales (formerly the British Crime Survey), the Scottish Crime and Justice Survey: the Offending Crime and Justice Survey, and the Commercial Victimisation Survey, have sometimes included questions on eCrimes victimisation and perpetration in their questionnaires. However, surprisingly few respondents reported eCrime experiences,[5] and in the light of other data on anxiety about identity theft and the prevalence of security breaches, response validity is open to question. Furthermore, questions on e-victimisation are sparse, often only focusing on a very limited range of completed e-fraud.[6] Given the problems outlined, it is apparent that the eCrimes data pool is currently unfulfilled, both in terms of quality and quantity, proving a confusing picture of the problem to eCrime controllers within the UKIA community. The largest databases produced by vendors are likely to be partial in their coverage and thus biased, while the best quality data from national surveys adopting random probability sampling techniques, suffer from poor conceptualisation and a paucity of detailed questions on the topic.

The current picture of eCrime

The 'best' data on business eCrime available in the United Kingdom before 2010[7] was the Information Security Breaches Survey (ISBS). The ISBS adopted probability sampling and adhered to standardised and well-conceptualised[8] questions. In the domestic domain, the Oxford Internet Survey (OIS) represents the gold standard. The OIS adopts a random sampling technique and includes a good range of eCrimes questions that the general public understand. Figure 1 shows trends in business eCrimes over the last decade in the United Kingdom and the United States. What is clear in the United Kingdom is that the trend in eCrimes attacks has reversed from a general decline since 2004 to a sharp increase from 2010. This is contrary to trends in the United States where a general decline in eCrimes breaches has been recorded since 2000 by the CSI Computer Crime & Security Survey.[9]

Figure 2 shows ISBS recorded breaches over time disaggregated by eCrime type. Malware attacks show the most marked decrease in breaches between 2004 and 2008, followed by theft

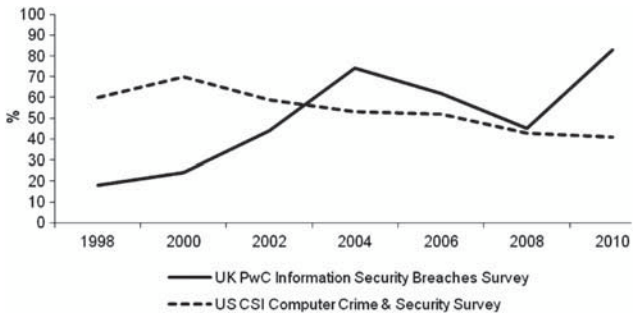

Figure 1: Organisations reporting eCrimes breaches in the United Kingdom and United States (1998–2010).

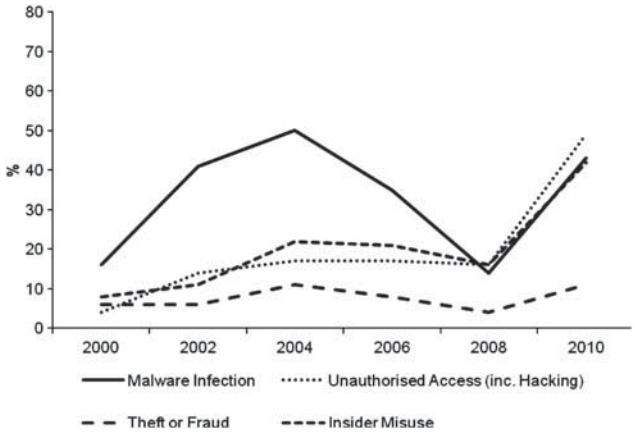

Figure 2: UK organisations reporting breaches by eCrime type (2000–2010).
Source: PwC ISBS.

and fraud and insider misuse. The reported prevalence of unauthorised access (including hacking) remained relatively stable in the same period. Reports in 2010 indicate a sharp increase in prevalence for malware infection, insider misuse and unauthorised access, and a slightly modest increase in reports of theft and fraud. Reports of insider misuse and unauthorised access peak at new all-time highs (42 and 49 per cent, respectively), while malware attacks return to near their peak prevalence in 2004.

Figure 3 details trends over time in domestic eCrimes breaches collected by the Oxford Internet Survey. Given the public's limited understanding of many eCrime types, this survey adopts more colloquial terms to ensure robust data collection. Unfortunately this precludes a forensic comparison with business eCrimes trends. However, the pattern of those members of the public experiencing virus attacks is similar to the patterns of business malware attacks. A decline is evident from 2005 to 2009, with a definite upward trend in 2011 (an increase of 7 per cent compared with 2009). Similarly, there is an upward trend in recorded domestic phishing attempts, indicating, as with business-recorded eCrimes, that eFraud is on the increase.

The British Crime Survey only routinely includes eCrime questions relating to fraud. The last tranche showed 4 per cent had suffered from this type of victimisation, twice the

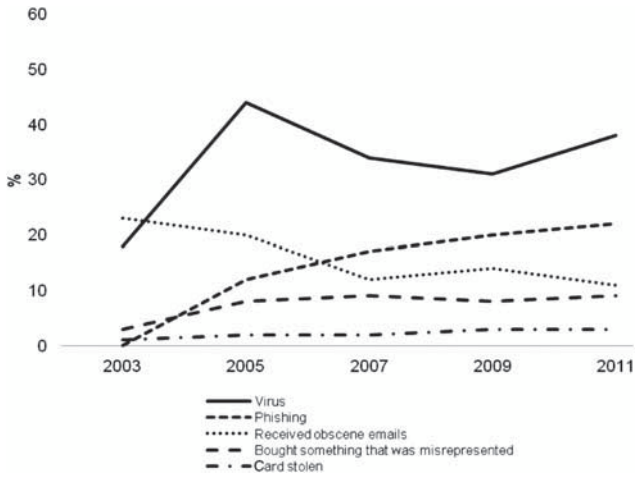

Figure 3: Domestic breaches by eCrimes type (2003–2011).
Source: Oxford Internet Institute Internal Survey.

proportion who experienced burglary or car theft.[10] The 2010 Eurostat ICT survey shows the 5 per cent of respondents from the United Kingdom suffered payment card fraud, placing it first in rank compared with all other European countries in the survey. The United Kingdom placed second for financial losses caused by phishing and pharming attacks (Anderson *et al*, 2012). These domestic eCrimes data add weight to the position that in general eCrime trends are on the rise in the United Kingdom and that online *property* victimisation is now overtaking its terrestrial counterparts.

The UKIA community

The control of eCrime is a networked activity, involving multiple actors from across industry sectors and public departments both nationally and internationally. It is the prime candidate for networked and nodal regulation (Johnston and Shearing, 2003), given the transformative nature of the Internet and its global reach. While the police are a significant actor within this network, their traditional local dominance over the security domain is diluted by the expertise brought by the private sector, especially finance and IT (Wall and Williams, 2007). As Grabosky and Smith (2001, p. 8) note, 'much computer-related illegality lies beyond the capacity of contemporary law enforcement … security in cyberspace will depend on the efforts of a wide range of institutions'. Furthermore, the resource constrains upon governments have forced them to enlist the assistance of the private sector and wider civil society in what is possibly the most significant policing challenge in modern times (Williams, 2006).

Early attempts to delineate the network of eCrime controllers were limited by the primitive development of the governmental architectures of the time (see Walker and Akdeniz, 1998). Since the introduction of the Council of Europe's Convention on Cybercrime in 2001 this architecture has matured, allowing more recent attempts at mapping this structure to

be more forensic. The Information Assurance Collaboration Group's (IACG)[11] UKIA map 2011 (issue 3.1) delineates the community into seven groupings: Regulatory Bodies (OFCOM, ICO, and so on); International Forums (ENISA,[12] ISSF,[13] and so on); Government/ Industry Groups (EURIM,[14] Get Safe Online, and so on), Professional Bodies (The Law Society, BCS,[15] and so on); Government (Home Office, GCHQ, and so on); Trade Associations & Industry Groups (IT Security Forum, Nominet, and so on); and Academic and Research Bodies. Outside of these groupings exist the private actors, such as the finance and IT sectors, who also play a role in providing advice and data on eCrimes to the police, government and public.

The recent UK Cyber Security Strategy (Cabinet Office, 2011) calls for more partnership working and information sharing among this diverse group of controllers in an attempt to foster a more intelligence-driven strategic fight against the eCrime problem. Partnership 'hubs' were piloted in 2011 in defence, finance, telecommunications, pharmaceutical and energy sectors with an expected national rollout in late 2012. Existing informal partnership working has been scoped in the Nominet eCrime Reduction Partnership Mapping Study (Levi and Williams, 2012), which evidences strengths and gaps in collaboration. The study also showed that the UKIA community perceptions of the eCrime problem were largely symmetrical with the eCrime data outlined in the previous section. However, they were only able to examine ordinal symmetry (the ordering of most to least problematic eCrimes) and were not able to conclude the degree of cardinal symmetry (rises and falls in both perceptions and the amounts of recorded eCrimes). Currently, little is known about how these various controllers digest the eCrime information outlined previously, and what influence this and forms of existing cooperation have on perceptions of the problem.

Hypotheses

Hypothesis 1: Levels of cooperation with domain specialist groups (finance and IT organisations) will impact positively upon the perceptions of the eCrime problem.

This assumption is based on three premises: (a) criminological research that identifies previous victimisation as a strong predictor of perceptions of national and local crime trends (Mohan *et al*, 2011), (b) research that shows organisations with more expertise and resources to detect crime will identify more breaches (Carr-Hill and Stern, 1979), and (c) research that shows that 'controllers' are more likely to perceive that there is a crime problem in their jurisdiction (Blom-Cooper and Drabble, 1982). In reference to (a) we argue that both finance and IT UKIA organisations are more likely to have been subject to more eCrimes (that were detected) than other organisations, given their desirability as targets. In relation to (b) as a result of their desirability as targets, both types of organisation are more likely to have increased levels of security to identify breaches. In relation to (c) we assume those who cooperate with finance organisations will perceive higher levels of eFrauds and those who cooperate with IT organisations will perceive higher levels of Security Breaches. This is likely not only due to the cumulative effect of (a) and (b) but also that these organisations potentially have a vested interest in communicating

their plight in relation to their respective eCrime problems, possibly to vie for more resources.

Hypothesis 2: Consumption of eCrime data sources will impact upon the perceptions of the eCrime problem.

The impact of secondary information sources, such as the media, on shaping perceptions of crime among the general public is well established (Greer and Reiner, 2012). Based on this premise we surmise that secondary eCrime data sources, such as surveys and police-recorded crime statistics, will impact upon perceptions of eCrime among controllers. Given the lack of evidence on the impact of eCrime data on perceptions, we make no assumption on the effect of particular types of sources.

As per conventional scientific methodology *null* hypotheses (H_0) were generated from the two *alternative* hypotheses above indicating the absence of an effect in each case. The models reported later provide evidence to reject the null hypotheses, lending support for our alternative hypotheses (Tabachnick and Fidell, 2013).

Methods and Research Design

Data generation

While data exist on eCrime patterns (via law enforcement and private channels) there are currently no publicly available data on the perceptions of eCrime controllers. The Information Security Breaches Survey generates the most robust data set on the experiences of eCrime and security, but it does not ask specific questions regarding perceptions of eCrime from the organisations it surveys. Furthermore, the sampling frame includes *all* organisations (public and private) in the United Kingdom and the results do not disaggregate the UKIA community from the overall sample. The primary data used in this analysis were derived from a cross-sectional study of UKIA community perceptions of the eCrime problem. Cross-sectional designs allow for researchers to observe a subset of a population providing a 'snap-shot' of activity or perception in a specific timeframe. We used an online survey as our research instrument to collect quantitative data on demographic, activity and perception-based characteristics on 104 Information Assurance organisations in the United Kingdom in 2011. The IACG UKIA map 2011 (issue 3.1) was used to draw a sample.[16] The Bristol Online Survey tool[17] was used to design and distribute the survey via email to CEOs and senior security managers. All listed organisations in the UKIA map were contacted where possible, amounting to a target population of 200 organisations. Nonprobability sampling was employed to derive the sample of organisations. While sample bias is a fundamental shortcoming of nonprobability sampling, Dorofeev and Grant (2006) note that this is often the only option available to researchers embarking on exploratory research. Furthermore, as the hypotheses tested in this analysis are concerned more with the existence of inter-variable relations and strengths of association than estimating population prevalence,[18] the use of nonprobability sampling does not fundamentally weaken the design of the study (Dorofeev and Grant, 2006). Moreover, our study is principally concerned with 'soft' measures (perceptions), which have no absolute validity (they cannot be compared with any authoritative

external measure). However, Tabachnick and Fidell (2013) caution that sampling bias can still affect hypothesis testing if a sample is significantly uncharacteristic of the target population. Selective targeting was employed during survey recruitment to mitigate this potential problem. We achieved a 52 per cent response rate with good coverage within all sectors (public, private, criminal justice, voluntary, regulatory bodies and groups).

The research was conducted in line with the ethical guidance established by the Association of Internet Researchers[19] and the British Society of Criminology. Given the nature of the research topic the authors made efforts to establish informed consent via the introduction page to the online survey. The research aims and objectives were clearly expressed and all respondents were informed that the data produced would be anonymised and would remain confidential.

Methods and Measures

Dependent variables

The survey included five items that measured UKIA organisational perceptions of the eCrime problem in the United Kingdom on a four-point ordinal scale ('not a problem' through to 'a very serious problem'). Factor Analysis was used as a data reduction method to identify the underlying components of the five items (inter-correlations of a set of variables). Principal components factor analysis, where each variable is standardised to have a mean of 0.0 and a standard deviation of 1.0, was used with orthogonal rotation (varimax). Two components (Security Breaches and eFrauds) were extracted based on an inspection of the scree plot and rotated factor loadings (see results).

Both components were included in separate Ordinary Least Squares (OLS) regression models as dependent variables. The results from correlational analyses (not shown), and tolerance statistics and variance inflation factors showed there were no problems with multicollinearity among the predictor variables. Diagnostics indicated a robust fit to the data in both models with both R^2 statistics exceeding the social science benchmark of a 'good' fit: 0.30 (Cohen, 1988).[20]

Predictor variables

Organisation type
UKIA community respondents were asked to identify their organisation from a list of types. These types were then recoded into eight categories reflecting the diverse nature of the UKIA community. These variables were entered as into the regression models to control for organisational influences over the dependent measures.

Cooperation
Respondents were asked to indicate their frequency of cooperation with other eCrime controllers in their network on a four-point ordinal scale (ranging from 'no cooperation' to 'a lot of cooperation'). These variables were entered as predictors in the regression models.

eCrime data sources

Six eCrimes data sources were identified, ranging from national Government surveys to bespoke financial data sets on security breach detection. Respondents were asked which, if any, they consulted as an organisation. Responses were included as binary variables in the regression models.

Results

Descriptive statistics

All responding organisations that took part in the study belonged to the UKIA community. Table 1 provides details of the organisations who responded to the online survey. The largest group of responding organisations were the private sector (37.6 percent), with IT security suppliers making up the majority, followed by 'other' private organisations and financial services. Just under one-fifth of respondents (18.3 percent) originated from government and public sector organisations and just over 13 per cent came from groups and regulatory bodies. Just over 10 per cent of respondents originated from the police and 12.5 per cent from

Table 1: Descriptive statistics of UKIA organisations *N*=104

Independent variables	*Coding*	*Sample*	
		M	*SD*
Organisation type	Gov. CJ	0.06	0.23
	Gov. non-CJ	0.13	0.33
	Private – Finance	0.09	0.28
	Private – IT	0.15	0.36
	Private – Other	0.14	0.34
	Group/Reg. body	0.14	0.34
	Charity/NfP	0.13	0.33
	Academic/Research	0.08	0.27
	Police	0.11	0.30
Cooperation	with Gov. CJ (0–3)	1.87	1.24
	with Gov. non-CJ (0–6)	2.77	2.09
	with Private – Finance (0–3)	1.58	1.21
	with Private – IT (0–3)	1.67	1.23
	with Private – Other (0–3)	1.16	1.08
	with Group/Reg. bodies (0–15)	7.52	5.09
	with Charity/NfPs (0–3)	0.90	1.07
	with Academia (0–3)	1.44	1.13
	with Police (0–3)	1.85	1.24
Data sources consulted	Gov. surveys	0.54	0.50
	Recorded (non-police)	0.65	0.48
	Recorded (police)	0.52	0.50
	Private security surveys	0.67	0.47
	Vertical market sources	0.39	0.49
	Academic research	0.71	0.46

charities/non-profit organisations. Half of responding organisations had 250 employees or more (48.1 per cent) and had been in operation for over 20 years (52.9 per cent). Small (between 1 and 9 employees) and young (5 years or less) organisations represented just over one-fifth of the sample (20.2 and 19.2 per cent, respectively).

Factor Analysis

The five eCrime items that measured organisational perceptions of the eCrime problem were subjected to principal components analysis. Table 2 shows the correlation matrix of the items revealing the presence of multiple coefficients at 0.3 and above. Factor analysis would not reduce variables to underlying components if perceptions of all five eCrimes were very highly correlated ($r \Rightarrow 0.9$). Equally, if no strong correlations were present, all eCrime items would reduce to five underlying factors, mitigating the need for reduction. In our factor analysis, organisational perceptions of the seriousness of the malware problem strongly correlated with perceptions of the seriousness of the Denial of Service problem ($r = 0.56$) and Hacking problem ($r = 0.66$); and organisational perceptions of the seriousness of the Customer ID theft problem strongly correlated with perceptions of the Corporate ID theft problem ($r = 0.67$). This matrix therefore provides evidence that the eCrime items reduce to two or more components. Furthermore, the Kaiser-Meyer-Oklin value was 0.787, exceeding the recommended value of 0.6 (Kaiser, 1974), and Bartlett's Test of Sphericity reached statistical significance, supporting the factorability of the correlation matrix. Both associations between sets of variables and Cronbach's α (0.870) indicated that reduction to underlying factors was possible.

Table 3 presents the factor loadings for responses (major loadings for each item in bold). The two component solutions explained 79 per cent of the variance, with component one contributing 65.19 per cent and component two contributing 13.81 per cent. To aid interpretation, orthogonal (varimax) rotation was performed. The rotated solution revealed the presence of a relatively simple structure, with both components showing a number of strong loadings, and the majority of variables loading substantially on only one component. Responses that are loaded heavily on component one are specific to Security Breaches (for example, Malware, Denial of Service and Hacking) but not eFrauds; responses that are loaded heavily on component two are specific to eFrauds (Personal and Corporate Identity Theft) but not Security Breaches. Therefore, component one was designated Security Breaches and component two was designated eFrauds. These components represent measures of the

Table 2: Spearman correlation coefficients among the perceptions of the five eCrime types

	1	*2*	*3*	*4*	*5*
1 Malware	1.00	—	—	—	—
2 Denial of service	0.560	1.00	—	—	—
3 Hacking	0.658	0.677	1.00	—	—
4 Customer ID theft	0.491	0.537	0.546	1.00	—
5 Corporate ID theft	0.548	0.387	0.569	0.677	1.00

All correlations significant at $p < 0.01$.

Table 3: Factor loadings with Kaiser–Meyer–Olkin (KMO) measures of sampling adequacy

Item	*Rotated factor loadings*	
To what extent does your organisation perceive the following as a problem within the United Kingdom today?	*Component 1*	*Component 2*
Malware	**0.887**	0.177
Denial of service	**0.801**	0.392
Hacking	**0.721**	0.404
Customer ID theft	0.248	**0.904**
Corporate ID theft	0.358	**0.805**

$\chi^2(10)=206.32$, $p<0.00$; Kaiser–Meyer–Olkin measure of sampling adequacy (overall)=0.787.

perceived *seriousness* of the two *reduced* eCrime types by the respondents in the UKIA community sample.

Regression Models

The predictor variables were regressed onto the outcome variables, perceptions of the problem of Security Breaches and eFrauds, using two OLS regression models (Table 4). Three sub-models containing only the predictor variables for (i) Organisational Type, (ii) Cooperation and (iii) eCrime Data Source were also run separately to identify the total variance explained in the dependent measures by each set of predictor variables.[21]

Cooperation

Several significant associations emerged between the cooperation predictors and the outcome measures. Holding all other factors constant, cooperating with private IT organisations significantly predicted perceptions that Security Breaches were a serious problem, as did cooperation with Government non-Criminal Justice Departments and Charities/Not-for-Profit organisations. Conversely cooperating with Groups/Regulatory Bodies and Government Criminal Justice related departments significantly predicted the perception that security beaches were not so much of a serious problem. Only one cooperation type emerged as a significant predictor in relation to eFrauds. Cooperating with finance organisations significantly predicted perceptions that eFrauds are a serious problem, while a slight negative association (only approaching significance) emerged between cooperating with IT organisations and perceptions that eFrauds are a serious problem.[22]

eCrime data sources

Significant associations emerged between the eCrime data sources predictor and both outcome measures. Holding all other factors constant, organisations that consulted non-police recorded data (from UKPA, CIFAS, NFA) were significantly more likely to perceive both

Table 4: Ordinary least squares regression models for perceptions of Security Breaches and eFrauds

	Model 1: Security Breaches			*Model 2: eFrauds*		
	B	*SE*	β	*B*	*SE*	β
Organisation type						
Gov. non-CJ	−0.34	0.60	−0.09	−0.02	0.53	−0.01
Private – Finance	−0.84	0.62	−0.26*	0.57	0.55	0.19
Private – IT	−0.20	0.61	−0.07	0.12	0.54	0.05
Private – Other	0.38	0.60	0.13	−0.67	0.53	−0.26
Group/Reg. body	−0.17	0.65	−0.05	−0.91	0.58	−0.27*
Charity/NfP	−0.97	0.60	−0.31*	−0.68	0.53	−0.24
Academic/Research	0.50	0.64	0.13	0.07	0.56	0.02
Police	0.34	0.57	0.11	−0.82	0.50	−0.30*
(Ref: Gov. CJ)	—	—	—	—	—	—
Cooperation						
with Gov. CJ	−0.40	0.20	**−0.50****	0.15	0.18	0.21
with Gov. non-CJ	0.28	0.13	**0.57****	−0.05	0.11	−0.11
with Private – Finance	−0.07	0.26	−0.09	0.41	0.23	**0.54****
with Private – IT	0.62	0.20	**0.73*****	−0.27	0.18	−0.35*
with Private – Other	0.38	0.26	0.39*	−0.17	0.23	−0.20
with Group/Reg. bodies	−0.13	0.07	**−0.67****	−0.06	0.06	−0.35
with Charity/NfPs	0.38	0.17	**0.39****	−0.06	0.15	−0.07
with Academia	−0.40	0.25	−0.43*	0.25	0.22	0.30
with Police	−0.09	0.18	−0.12	−0.14	0.16	−0.19
Data sources consulted						
Gov. surveys	0.20	0.29	0.09	−0.04	0.26	−0.02
Recorded (non-police)	1.01	0.39	**0.44*****	1.02	0.35	**0.49*****
Recorded (police)	−0.81	0.34	**−0.38****	−0.29	0.31	−0.15
Private security surveys	−0.30	0.37	−0.12	−0.37	0.33	−0.17
Vertical market sources	0.09	0.36	0.04	−0.53	0.32	−0.28*
Academic research	0.36	0.45	0.13	0.63	0.40	0.26*
Constant	−0.35	0.64	—	0.20	0.57	—
Model fit						
sig.	0.017		—	0.010		—
R^2	0.45		—	0.48		—
N[a]=	80		—	80		—

*p<0.10; **p<0.05; ***p<0.01.

[a]Reduction in sample size due to listwise deletion of cases necessary for regression requirements.

Security Breaches and eFrauds as serious problems, compared with organisations that consulted other sources. As both models controlled for organisation type, this association is not explained by the assumption that financial organisations are more likely to consult these data sources, who are themselves more likely to perceive these eCrimes as more of a serious problem. To the contrary, the organisation type predictor shows that finance organisations were less likely[23] to think security breaches were a problem (compared with the reference category Government Criminal Justice Related); and there was no significant association

with perceptions of the eFrauds problem. The first model also showed that organisations that consulted police eCrimes data were less likely to think there was a problem with security breaches compared with organisations that consulted other types of data. In the second model, a negative association between consulting vertical market sources and perceptions the eFrauds problem was present, while consulting academic sources increased the likelihood of perceiving a problem with eFrauds. However, both associations only approached conventional levels of significance.

Sub-model analysis

In order to ascertain which *sets* of variables (cooperation or sources) were most influential in forming the perceptions of UKIA organisations in regard to the eCrime problem, we conducted sub-model analyses. By isolating cooperation and sources variables in separate regression models we were able to determine how much variance these explained in the dependent measures independently. We examined the R^2 statistic which is the coefficient of determination in the models that indicates how well the model predicts the observed data (model fit). An R^2 of 1 indicates a perfect fit to the data, meaning the independent variables in the model explain 100 per cent of the variance in the dependent. The most widely applied guidelines are those developed by Cohen (1988). These criteria specify that $r=0.10$ is 'small', $r=0.30$ is 'medium' and $r=0.50$ is 'large'. As stated earlier in the article, the social science standard for a 'good' fit is R^2: 0.30. With all predictor variables included (cooperation, sources and controls) the Security Breaches model fit was R^2: 0.45, while the model fit for eFrauds was R^2: 0.48 (both far in excess of the social science standard for a 'good' fit). Sub-model analysis revealed that independently the set of cooperation predictors accounted for 24 per cent (R^2: 0.24) and 20 per cent (R^2: 0.20) of the variance for perceptions that Security Breaches and eFrauds were a serious problem, respectively. Independently the set of eCrime data sources predictors accounted for 10 per cent (R^2: 0.10) and 20 per cent (R^2: 0.20) of the variance for perceptions of Security Breaches and eFrauds, respectively. In summary, cooperation with organisations was most predictive of perceptions of Security Breaches, whereas data sources consulted and cooperation were equally predictive of perceptions of eFrauds.

Discussion

Both cooperation and consumption of eCrime data sources had significant influences on the formation of eCrimes perceptions among controllers within the UKIA community. Both models provide evidence in support of the first hypothesis, that cooperation with domain specialists (finance and IT organisations) will positively predict perceptions that eCrimes pose a serious problem. However, these influences were not symmetrical. Organisations that had higher levels of cooperation with private IT companies, non-criminal justice government departments and charities were significantly more likely to perceive Security Breaches as a serious problem. These patterns were not mirrored in relation to perceptions of eFrauds, where only cooperation with the finance sector was greatly predictive. Curiously cooperation with groups and regulatory bodies, and criminal justice-related government

departments was negatively associated with perceptions that Security Breaches constituted a serious problem.

A possible explanation for these patterns is the higher victimisation and detection levels in the domain-specific organisations, which are subsequently communicated to partners (cooperation with IT organisations was the greatest predictor, 0.73 in relation to Security Breaches, as was cooperation with finance in relation to eFrauds, 0.54). The cumulative knock-on effects of high victimisation, including increased investment in detection and demand for resources furthers the zeal with which these organisations communicate their domain-specific problem, causing a ripple effect throughout the wider UKIA community.[24] This is further supported by the sub-model analysis which revealed cooperation was most predictive, compared with eCrime data sources, of perceptions that Security Breaches are a serious problem. However, this did not stand for perceptions of the eFrauds problem, where eCrime data sources consulted shaped perception just as much. The negative associations between cooperation and perceptions of the Security Breach problem are more difficult to explain. Further qualitative work into the nature of the cooperation of criminal justice-related government departments and groups and regulatory bodies is necessary to understand why it is associated with the perception that Security Breaches are less of a problem.

Evidence in the models that showed consumption of non-police eCrimes data was greatly predictive of perceptions that both Security Breaches and eFrauds were more of a problem supports the second hypothesis. Why domain specialist data on breaches and frauds (CIFAS, UKPA, NFA) increases perceptions that these eCrimes are serious problems is unclear, especially when it is the only positive predictive source of information. Research by Levi and Williams (2012) shows that this type of source is most highly regarded in terms of quality by UKIA community members, but why consultation with it results in the perception that both types of eCrime are more of a problem is unclear. Of course, the direction of causality may reverse – those who think that these eCrimes problems are serious use data that are 'good' and 'useful' in helping address the problems. Further qualitative research is required to investigate this association.

Consulting police eCrimes data was negatively associated with the perception that Security Breaches (but not eFrauds) are a serious problem. This source of eCrime data may suffer from the lack of granularity in existing crime codes for these types of offences. Historically, reports of eCrime to the police have been faced with inconsistent record keeping and recording practices, which often precluded the identification of an electronic element in the *modus operandi* (Hyde-Bales *et al*, 2004). Thus it becomes impossible even to conduct any detailed analysis of *official* sources on the prevalence of eCrime in England and Wales. The law generally takes a technology neutral stance to offences (for example, fraud is fraud whatever the *modus operandi*). This flexible approach ensures the law does not fall behind the rapidly changing technological landscape, but it means that we cannot track the *techniques* of crime. In an attempt to combat this shortfall, some local forces attach a computer crime marker to command and control incident records, crime desk records and crime-related intelligence logs. These practices however are far from systematic, and significant gaps still remain in the recording process. Therefore, denial of service attacks, hacking, malware infection and the like are unlikely to be easily identifiable from police crime digests, potentially resulting in the perception that they are less of a problem. Over time however, the police eCrime data pool may become fuller and more forensic given existing cyber priorities. The ACPO (2009) Strategy is under review and is likely to change

in light of the establishment of the National Crime Agency (late 2013) which will take a strategic lead on eCrime.

Conclusion

The models presented in this article provide the first quantitative evidence on which factors best and least predict controllers' perceptions of the eCrime problem. While the UKIA community perceptions of the eCrime problem are largely symmetrical with the best eCrime data available (Levi and Williams, 2012), until now there have been no data to suggest what influences these perceptions. The predictive power of cooperation with other organisations is not counter-intuitive. Partnership working, whether formal or informal, will always influence the perceptions of actors in a network. This study has shown that cooperation with IT and finance organisations is associated with perceptions that both Security Breaches and eFrauds are more of a problem. The question remains whether partnership working with these organisations increased the perception of severity of both eCrimes within the UKIA community, or whether members of the community were attracted to cooperating with these organisations due to their *pre-existing* perception that these eCrimes were a problem, in order to help mitigate them. In either case, the partnership drive pushed forward by the UK Cyber Security Strategy (Cabinet Office, 2011) will forge more formal links between UKIA community members, potentially widening the net to traditionally less cooperative organisations (such as local government, see Levi and Williams, 2012). Who they cooperate with may alter their existing perceptions of the eCrime problem, potentially heightening awareness and enhancing risk perception.[25]

The influence on perceptions of prevalence and seriousness of crime representations, be they from the media or primary data sources, is well documented. This study shows that certain eCrimes primary data sources, chiefly non-police domain-specific sources, are positively associated with perceptions of the problem of both eCrime types examined. Conversely, those who use police data are less likely to think that eCrimes are a serious problem. These patterns may have something to do with the 'fidelity' of the data recorded as mentioned previously. Further qualitative work is needed to understand the nuances of these influences, for example, are perceptions brought into line with the current level of risk or reduced/raised, especially if the network of eCrime controllers is to expand to include non-specialists (that is, non-finance and IT). Or might it be the case, as we suspect, that pre-existing perceptions that these eCrimes are a serious problem motivate consultation with specific sources, that is, those who are worried want to find out more.

The National Statistician (National Statistician, 2011) was critical of the Home Office for its failure to address statistics on fraud in general and eCrimes in particular. In our view, attempts to measure *all* cybercrimes and their direct and indirect costs *precisely* are doomed to failure. However, better statistics than we have at present on their costs to and impact on individuals, businesses of different types, and government are important and are possible. In addition to their inherent value in helping us understand the risks that we face, these data would help the UKIA community to more rationally direct prevention efforts and assess their impact. This assessment is much more difficult where estimates are speculative, because if the estimates fall or rise, we seldom know whether this is due to measurement error or to real changes in the phenomenon. However for some components that are inherently

difficult to define and identify as eCrime, and/or where the survey instruments do not exist or are distrusted, there will always be an element of uncertainty. Besides, some organisations will always want more real-time 'close to market' data to address rapidly changing or unchanging threats.

This article has shown the association of cooperation and consumption of data sources with perceptions of the eCrime problem. Knowing these associations exist is important given that the recent UK Cyber Security Strategy has called for more cooperation and more robust sources of evidence. It is likely that perceptions within non-specialist corporate and public domains (non-IT and Finance) will begin to change as new cooperation arrangements are introduced. These quantitative findings call for a more in-depth qualitative understanding of the cooperation between eCrime controllers and their data consumption practices. Ascertaining why these factors have an influence and how perceptions compare with 'actual' threats and risks is necessary if we are to better understand the 'social construction' of the problem and subsequent policy and operational outcomes.

Acknowledgement

This work was supported by Nominet Trust under the grant 'Mapping Cybercrime and its Control'.

Notes

1 The term eCrime Controllers is preferred to other terms, such as eCrime Policing or eCrime Regulators: it indicates that a broader range of relevant parties are involved in controlling eCrime, beyond just law enforcement and government regulators.
2 In this article we define the UKIA community in the broadest sense, including criminal justice agencies, private sector (IT, Finance and SMEs), public sector (criminal justice and non-criminal justice departments), academia, voluntary sector and industry groups and forums. A fuller description is provided in the methods section of the article.
3 Symantec gathers malicious code intelligence from more than 133 million client, server and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks that provide valuable insight into attacker methods.
4 A process where the engine responsible to altering the behaviour of malware resides outside of the malware itself, usually on a website. By extracting this function from within malware, analysts find it more difficult to identify and eradicate infection.
5 The Scottish Crime and Justice Survey 2010/11 estimated that 4.5 per cent of adults had experienced card fraud in the 12 months before interview and 0.5 per cent of adults had been a victim of identity theft, where someone had pretended to be them or used their personal details fraudulently. For card fraud, there were roughly the same instances of cards themselves being used without permission (2.4 per cent) and just the card details being used (2.2 per cent).
6 The BCS included a technology crimes module in 03/04 but it has not since been repeated. The only consistent question in this survey on eCrime relates to identity fraud (since 05/06).
7 The 2010 ISBS adopted a self-selecting sample framework that reduced the representativeness of the findings and therefore precluded a robust basis for comparison with previous ISBS surveys.
8 PricewaterhouseCoopers' research team ensured that questions asked in the first survey (1998) became standard for all subsequent surveys. This ensured that (to the extent that they were the same individuals) respondents became familiar with the terms expressed, resulting in plausibly sounder answers over time.

9 The data for the ISBS 2010 presented in Graph 1 are derived from the responses from small- to medium-sized firms as they represented the largest group of respondents. It is important to note reports of eCrimes breaches from large firms were far in excess of those reported by SMEs, making the sharp increase in eCrimes attacks in Graph 1 a conservative estimate.
10 The BCS does not distinguish online from offline frauds, but the former is likely to have accounted for the majority of fraud.
11 IACG is an initiative within the Government Communications Headquarters (GCHQ) Communications–Electronics Security Group (CESG).
12 European Network & Information Security Agency
13 Information Security Forum.
14 The Information Security Alliance.
15 The Chartered Institute for IT.
16 IACG is an initiative within the Government Communications Headquarters (GCHQ) Communications–Electronics Security Group (CESG). See http://www.cesg.gov.uk/Publications/Documents/uk_ia_community.pdf.
17 See http://www.survey.bris.ac.uk/.
18 Where population estimates are provided they should be interpreted with a degree of caution.
19 See: https://aoir.org/documents/ethics-guide/.
20 Model fit statistics are presented in Table 4.
21 The results of sub-models not presented here, aside from the R^2 statistic. More detailed results available upon request.
22 Ascertaining 'causality' or direction of association is problematic in cross-sectional designs. We address this problem in relation to our data in the discussion section.
23 This association only approaches conventional levels of significance.
24 Conversely it could also be argued these organisations had an incentive to develop relationships with their 'community' because of their higher risks.
25 Of course, the inverse is also a possibility.

References

ACPO. (2009) *ACPO e-Crime Strategy*. London: ACPO, www.acpo.police.uk/documents/crime/2009/200908CRIECS01.pdf, accessed 9 October 2012.

Anderson, R., Boehme, R., Clayton, R. and Moore, T. (2008) *Security Economics and the Internal Market*. Heraklion, Greece: ENISA.

Anderson, R. *et al* (2012) *Measuring the Cost of Cybercrime*. London: Ministry of Defence.

Blom-Cooper, L. and Drabble, R. (1982) Police perception of crime: Brixton and the operational response. *British Journal of Criminology* 22(2): 184–187.

Cabinet Office. (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. London: Cabinet Office.

Carr-Hill, R.A. and Stern, N. (1979) *Crime, the Police and Criminal Statistics: An Analysis of Official Statistics for England and Wales Using Econometric Methods, Quantitative Studies in Social Relations*. London: Academic Press.

Casper, C. (2007) *Examining the Feasibility of a Data Collection Framework.* Heraklion, Greece: ENISA.

Cohen, J. (1988) *Statistical Power Analysis for the Behavioral Sciences*, 2nd edn. Hillsdale, NJ: Lawrence Erlbaum.

Council of the European Union. (2000) Proposal for the extension of Europol's mandate to the fight against cyber-crime. Note from Presidency to Article 36 Committee. http://www.statewatch.org/semdoc/assets/files/council/12224-00.pdf, accessed 5 October 2012.

CrySyS Lab. (2012) sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex Malware for targeted attacks. Laboratory of Cryptography and Systems Security: Budapest University of Technology and Economics. http://www.crysys.hu/skywiper/skywiper.pdf.

Dorofeev, S. and Grant, P. (2006) *Statistics for Real-Life Sample Surveys: Non-simple random Samples and Weighted Data*. Cambridge, UK: Cambridge University Press.

Empirica. (2007) Benchmarking in a Policy Perspective: Security and Confidence. Report No.8. Brussels: Empirica.
Farwell, J. and Rohozinski, R. (2011) Stuxnet and the future of cyber war. *Survival* 53(1): 23–40.
Garlik. (2009) *UK Cybercrime Report 2009*. London: Experian.
Giddens, A. (1990) *The Consequences of Modernity*. Oxford, UK: Polity Press.
Grabosky, P. and Smith, R. (2001) Digital crime in the twenty-first century. *Journal of Information Ethics* 10(1): 8–26.
Greer, C. and Reiner, R. (2012) Mediated Mayhem: Media, crime and criminal justice. In: M. Maguire, R. Morgan and R. Reiner (eds.) *The Oxford Handbook of Criminology*, 5th edn. Oxford, UK: Oxford University Press, pp. 245–278.
HM Government. (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The Stationery Office.
HM Government. (2011) *Strategic Defence and Security Review: The First Annual Report*. London: The Stationery Office.
Hyde-Bales, K., Morris, S. and Charlton, A. (2004) *The Police Recording of Computer Crime*. London: The Stationery Office.
i2010 High Level Group. (2006) *Benchmarking Framework*. Brussels, Belgium: European Commission.
Jewkes, Y. and Yar, M. (2010) *Handbook of Internet Crime*. Cullompton, UK: Willan.
Johnston, L. and Shearing, C. (2003) *Governing Security: Explorations in Policing and Justice*. London: Routledge.
Kaiser, P. (1974) An index of factorial simplicity. *Psychometrika* 39(1): 31–36.
Levi, M. and Williams, M. (2012) *eCrime Reduction Partnership Mapping Study*. London: Nomient Trust.
Mohan, J., Twigg, L. and Taylor, J. (2011) Mind the double gap: Using multivariate multilevel modelling to investigate public perceptions of crime trends. *British Journal of Criminology* 51(6): 1035–1053.
National Statistician. (2011) *National Statistician's Review of Crime Statistics: England and Wales*. London: Government Statistical Service.
PriceWaterhouseCoopers. (2012) *Information Security Breaches Survey*. London: PwC.
Sommer and Brown. (2011) *Reducing Systemic Cybersecurity Risk*. London: OECD.
Symantec. (2012) *Internet Security Threat Report, Volume 17*. Mountain View, CA: Symantec.
Tabachnick, B.G. and Fidell, L.S. (2013) *Using Multivariate Statistics*, 6th edn. Boston, MA: Allyn and Bacon.
U.N. Commission on Crime and Criminal Justice. (1995) *United Nations Manual on the Prevention and Control of Computer-related Crime*. New York: United Nations.
Walker, C. and Akdeniz, Y. (1998) The governance of the internet in Europe with special reference to illegal and harmful content. *The Criminal Law Review*, Special Edition on Crime, Criminal Justice and the Internet, 5–18.
Wall, D.S. (2007) *Cybercrimes: The Transformation of Crime in the Information Age*. Cambridge: Polity.
Wall, D.S. and Williams, M. (2007) Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice* 7(4): 391–415.
Williams, M. (2006) Policing & cyber-society: The maturation of regulation within an online community. *Policing & Society* 17(1): 59–82.
Williams, M. (2010) Cybercrime. In: F. Brookman, M. Maguire, H. Pierpoint and T. Bennett (eds.) *Handbook of Crime*. Cullompton, UK: Willan.
Yar, M. (2006) *Cybercrime and Society*. London: Sage.