Levi, M. and Williams, M. L. 2013. Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security* 21(5), pp. 420-443. (10.1108/IMCS-04-2013-0027)

IMCS

MULTI-AGENCY PARTNERSHIPS IN CYBERCRIME REDUCTION
Mapping the UK Information Assurance Network Cooperation Space

MICHAEL LEVI and MATTHEW L WILLIAMS

Cardiff University, Cardiff, UK

Abstract

Purpose – This paper maps out multi-agency partnerships in the UK information assurance (UKIA) network in the UK.
Design/methodology/approach – The paper surveyed members of the UKIA community and achieved a 52 percent response rate (n=104). The paper used a multi-dimensional scaling (MDS) technique to map the multi-agency cooperation space and factor analysis and ordinary least squares regression to identify predictive factors of cooperation frequency. Qualitative data were also solicited via the survey and interviews with security managers.
Findings – Via the quantitative measures, the paper locates gaps in the multi-agency cooperation network and identifies predictors of cooperation. The data indicate an over-crowded cybersecurity space, problems in apprehending perpetrators, and poor business case justifications for SMEs as potential inhibitors to cooperation, while concern over certain cybercrimes and perceptions of organisational effectiveness were identified as motivators.
Practical implications – The data suggest that the neo-liberal rationality that has been evoked in other areas of crime control is also evident in the control of cybercrimes. The paper concludes divisions exist between the High Policing rhetoric of the UK's Cyber Security Strategy and the (relatively) Low Policing cooperation outcomes in "on the ground" cyber-policing. If the cooperation outcomes advocated by the UK Cyber Security Strategy are to be realised, UKIA organisations must begin to acknowledge and remedy gaps and barriers in cooperation.
Originality/value – This paper provides the first mixed-methods evidence on the multi-agency cooperation patterns amongst the UKIA community in the UK and highlights significant gaps in the network.

Keywords – Cooperation, Information sharing, Partnership, Cybercrime, Cybersecurity networks Paper type Research paper

Introduction

Activity conducted through the Internet and other networked digital systems represents an increasingly important front for national and international security and crime-fighting. One of the most problematic issues in cyber security is the lack of cooperation and coordination amongst organisations to monitor, detect and react to attacks. Although various software tools (anti-virus, malware and intrusion detection systems) and standards (e.g. ISO 27000 series on security risk assessment) exist, the most recent Information Security Breaches Survey (PwC 2013) identified that 93% of large business and 87% of SME respondents had a security incident in the last year, with the average cost of the worst incident ranging from £450k-£850k for large businesses and £35k-£65k for SMEs. Vendor statistics show an increase on 2011 in new unique malicious

web domains, targeted attacks, mobile vulerabilites, Bot zombies, and virus and phishing attempts (via email) (Symantec 2013). Academic research shows high public concern about identity theft and public-facing consumer cybercrime in a variety of countries, most notably the UK (see Levi and Williams 2012, Williams and Levi 2013). Given time lags in crime reporting and cross-border victim-offender distanciation, full enforcement of crimes reactively reported is impossible, even if it were desirable to spend taxpayer resources in that way. The likely impacts of intelligence led policing strategies depend on the organisation of criminal markets and on their susceptibility to different interventions: but unless the markets are highly concentrated *and* accessible to police with a competence and motivation to act against them, then such criminal justice approaches will also have limited effects. In common with many areas of financial sector policing, data about cybercrimes sometimes comes from the public, but the majority of the data is held in private commercial hands, and often, it is the private sector that has a primary role and interest in defending their businesses from cyber-assisted crimes. More recently cooperation has arisen as the preferred form of defence, facilitating the sharing of cybercrime information between private and criminal justice actors (Cabinet Office 2011). However, there currently exists little evidence on the organisation of these various actors in the 'cybercrime reduction network space'. On the basis of a study carried out in 2011 and 2012, this paper primarily reports and analyses data on the public-private, public-public and private-private policing interfaces in the policing of cybercrimes in the UK, and explores the implications both for the literature on the new security governance and for the regulation of cyber-related harms. Based on a survey of 104 members of the UK Information Assurance community this paper reports on the location of gaps in the network and identifies predictors of cooperation via multi-dimensional scaling and regression techniques. In addition, qualitative data indicate an over-crowded cybersecurity space, problems in apprehending perpetrators, and poor business case justifications for SMEs were potential inhibitors to cooperation; while concern over certain cybercrimes and perceptions of organisational effectiveness were potential motivators to cooperation. Our data suggest that the neo-liberal rationality that has been evoked in other areas of crime control is also evident in the control of cybercrimes. We conclude divisions exist between the High Policing rhetoric of the UK's Cyber Security Strategy and the (relatively) Low Policing cooperation outcomes in 'on the ground' cyber-policing.

Partnerships in Cybercrime Reduction

There exists a significant body of academic work on the emergence and maturation of the 'preventive turn' and community safety in late-modern times (see Crawford 1997; Garland 2001; Gilling 2007; Hughes 2007; Hughes and Edwards 2009). The Crime and Disorder Act (1998) formalised partnership arrangements and began 'a long overdue recognition that the levers and causes of crime lie far from the traditional reach of the criminal justice system… drawing together a variety of organisations and stakeholders, in the public, voluntary and private sectors as well as from among relevant community groups' (Crawford 2002: 31). The recognition of the limits of policing and of other state agencies promotes governing strategies that rely on 'responsibilising' private actors and civil society to govern their own spaces in crime and disorder reduction efforts (Garland 2001). A certain neo-liberal rationality has been evoked where state intervention is rolled back as private actors adopt individualized, responsibilised and practical roles in community networked governance (Edwards and Hughes 2009; Johnston and Shearing 2003). Where the old paradigm of criminal justice marshalled police-based expertise, the new networks of security mobilise diverse resources, placing importance upon specialist knowledge and capacity (Johnston and Shearing 2003). This interpretation is specifically applicable to the domain of cybercrime and cyber-security – the technical challenge posed by cybercrime cannot be met by the police alone and the expertise required must be brought in from outside the police service. This has always

been the case in dealing with frauds of different types (Williams 2006; Doig and Levi 2009; Levi 2010).

Many areas of the policing crime diet have been addressed by the application of multi-agency crime reduction partnerships. It has been argued by many authors that cybercrime is the ideal candidate for such arrangements (Williams 2006; Wall 2007; 2011; Sulek 2011; Irion 2012; Levi and Williams 2012; Williams and Levi 2012). In particular, the theoretical constructs of plural policing and nodal governance have been applied to understand the arrangements and practices of networks of actors in the information assurance domain (Dupont 2004; Wall 2007; Wall and Williams 2007; Nhan and Huey 2008; Huey et al. 2012). The main thrust of these positions is that late-modern forms of policing are characterised by a diffusion of responsibilities related to the governance of cybercrime to actors that have traditionally not had an official or non-official regulatory mandate. The 'networked and nodal architecture' of the internet inherently makes it a prime candidate for a partnership approach to regulation and governance (Wall 2007). Nhan and Huey (2008) categorise 'nodal clusters' that form the cybercrime reduction network: *government* (including international and national criminal justice, non-criminal justice and local); *law enforcement* (from international to the local); *private industry* (across all sectors, large, medium, small and micro) and the *general public* (civil society groupings both on and offline)[i]. Dupont delineates five forms of capital that shape nodal networks. Nodes with high degrees of *social capital* can foster and sustain mutually beneficial social relations with other nodes. *Cultural capital* relates to knowledge possessed by a node that can be used and offered up to other nodes for cybersecurity. Nodes with *political capital* have a strong theoretical and/or working knowledge of local, national and international political structures and may have the power to shape legislation and marshal public resources. *Economic capital* relates to knowledge of international markets as they relate to cybersecurity and beyond and the purchasing power of a node. *Symbolic capital* is the final overarching and linking form that underpins all others – a less manifest form of capital that affords organisational legitimacy. Access to these forms of capital vary by node and an efficient and resilient cybersecurity network must be in a position to assemble sufficient degrees of each though its nodes. Therefore, collaboration and partnership in the arena of cybercrime reduction is becoming commonplace as actors within nodes recognise the limitations of the Peelian paradigm of policing that frames the police–public mandate (Wall and Williams 2007).

There exist several high-profile multi-agency cybercrime reduction partnerships. Wall (2007) highlights several international partnerships, including POLCYB (Society for the Policing of Cyberspace) and the High Tech Crime Consortium (HTCC). POLCYB is a multi-agency, cross-sectoral partnership that facilitates cooperation between members and the sharing of information on cybersecurity risks and issues that relate to policy. HTCC is an Internet based closed forum for law enforcement and security professionals that is more operational in orientation. The Virtual Global Task Force represents an international partnership between law enforcement, non-government organisations and industry groups with the aim of protecting children online. In the United States (US) public-private partnerships exist between the government and several commercial nodes including ISPs (the Defense Industrial Base) and the Industry Botnet Group (Butler and Lachow 2012). US and European Union partnerships include the Working Group on Cybersecurity, and within Europe, the Public-Private Partnership for Resilience programme (EP3R) has a mandate to foster cooperation between public and private stakeholders to strengthen resilience in relation to pan-European critical infrastructure (Irion 2012).

In the UK several nodes form the complex network of cybersecurity. The Information Assurance Collaboration Group's (IACG)[ii] UK Information Assurance (UKIA) map 2012 (issue 4.0) delineates this network into eight clusters: Regulatory Bodies (OFCOM, ICO etc.); International Forums (ENISA[iii], ISSF[iv] etc.); Government/Industry Groups (EURIM[v], Get Safe Online etc.), Professional Bodies (The Law Society, BCS[vi] etc.); Government (criminal justice related - Home Office, GCHQ, and non criminal justice related - Cabinet Office, HMRC etc.); Trade Associations & Industry Groups (IT Security Forum, Nominet etc.); Academic and Research Bodies, and Other (e.g. Liberty). In addition IT, finance and other large, medium, small and micro commercial organisations, can be said to form a private cluster. In relation to illegal online content, collaborative arrangements exist between the Internet Watch Foundation (IWF), the Association of Chief Police Officers (ACPO), the Crown Prosecution Service (CPS), the Child Exploitation Online Protection Centre (CEOP) and the Serious Organised Crime Agency (SOCA). In the area of fraud, cooperative arrangements exist between Action Fraud, the National Fraud Intelligence Bureau (NFIB), SOCA, the Serious Fraud Office (SFO), Her Majesty's Revenue and Customs (HMRC) and the National Police Central cybercrime Unit (PCeU). Cooperation with private nodes within these partnerships is ad hoc and largely informal. To address this deficit the UK Cyber Security Strategy (Cabinet Office 2011) promoted public-private partnership working amongst the various nodes and outlined the piloting of partnership 'hubs' in defence, finance, telecommunications, pharmaceutical and energy sectors. A year on from the publication of the Cyber Security Strategy, the Cabinet Office (2012) announced the creation of a dedicated UK national Computer Emergency Response Team (UK CERT) to improve the national coordination of cyber incidents and to act as a focal point for international sharing of technical information on cyber security. In addition, a permanent information sharing environment – the Cyber Security Information Sharing Partnership (CISP) – was announced. The formation of the National Cybercrime Unit (NCCU) as an integral part of the National Crime Agency promises to further integrate commercial voices into the regulatory sphere by dedicating a 'pillar' of its remit to building and sustaining public-private partnerships (Home Office 2010).

The effectiveness of these partnerships in achieving their objectives is difficult to determine (Wall 2007). Some authors argue that partnership working, especially between public and private partners, can be 'an unreliable and unpredictable solution…in the areas of national emergency preparedness and crisis management' (Andersson and Malm 2006: 140). Reasons for this include that the interests of private corporations and the state are often not easily reconcilable, resulting in a lack of a clear business case for industry (especially for SMEs and in times or austerity); a lack of trust between parties, including tensions between hierarchical reporting and horizontal information sharing; failures to effectively and fully engage with civil society and the various 'publics' (both on and offline); and the existing limitations of national and international cooperation arrangements (Dunn-Cavelty and Suter 2009; Huey et al. 2012; Sulek & Doscher 2011; Wall 2007). Contrariwise, where partnerships between the police and private industry are successful, concerns have been expressed over the 'transformation' thesis (Jones and Newburn 2002), that contends as the ratio of private actors to police actors increases in any given policing system, the overall orientation of the system shifts from the logic of the public good to the logic of the market. However, White and Gill have shown that this is short-sighted, and that existing partnerships in the UK have seen a 'complex blurring of relations and rationalities, with both private and police actors drawing upon a mix of public and private scripts to inform their actions' (2013: 74). These concerns remind us of Crawford's (2002) recognition that the pluralisation of security and safety has created sites of contradiction, ambiguity and ambivalence. Edwards and Hughes' (2009) research into partnership working in

England and Wales has them concluding like Crawford that the field is marked by contradictory and unstable forces. In particular, they note there are often schisms between security talk, decisions and actions resulting in gaps between intended governmental projects and their actual outcomes. We now turn to our hypotheses that draw upon this conceptual and empirical work, which we then return to in the discussion to make sense of our findings.

Hypotheses

H_1: Intra-sector cooperation around cybercrime reduction will be evident in the multi-dimensional scaling, but inter-sector cooperation will not.

This assumption is based on the nascence of inter-sector cooperation initiatives developed in the recent Cyber Security Strategy (Cabinet Office 2011) and previous research that demonstrates the tensions evident in inter-sector security partnerships and the negative impact these have on open cooperation channels, especially between public and private nodes (Dunn-Cavelty and Suter 2009; Huey et al. 2012; Sulek & Doscher 2011; Wall 2007).

H_2: Perceptions about cybercrimes, both in terms of the seriousness of the problems and the difficulty of their control, will be significantly associated with levels of cooperation. In particular, (i) perceptions that cybercrimes are a serious problem will be positively associated with cooperation; and (ii) perceptions that cybercrimes are difficult to control will be positively associated with cooperation.

These assumptions are based on the partnership literature that suggests networks of security arrange around significant and complex crime problems (Crawford 1997; Garland 2001; Hughes 2007). In relation to (i) we assume those who perceive that cybercrimes are more of a serious problem will seek out cooperation with nodes, especially those who have expertise in a given area. In relation to (ii) we assume perceptions that cybercrimes are difficult to control will promote a cooperative approach given that cooperative arrangements in crime reduction are associated with complex social problems and hard-to-control crimes.

H_3: Perceptions of the effectiveness and importance of nodes will be associated with levels of cooperation. In particular (i) perceptions that private, government and non-government nodes are effective in combating cybercrime will be positively associated with frequency of cooperation with these respective nodes; (ii) perceptions that private, government and non-government nodes are important in the cybersecurity network will be positively associated with frequency of cooperation with these respective nodes.

These assumptions are based on research that shows nodes will seek to cooperate with other nodes who demonstrate they can assemble certain forms of network capital to achieve effective outcomes, which increases their importance in cybersecurity networks (Nhan and Huey 2008; Huey et al. 2012; Dupont 2004).

As is recommended by Tabachnick and Fidell (2013) the three *alternative* hypotheses above were transformed into *null* hypotheses (H_0), each indicating the absence of the specified associations. Evidence in the regression models detailed in the results section of the paper lend support for our alternative hypotheses, allowing us to reject the null hypotheses.

Data & Methods

Data

Currently no accessible sources of data exist on the frequency of cooperation in the multi-agency partnership cybercrime reduction network (the UKIA network). The data used in this paper were collected as part of the Nominet funded project 'Mapping Cybercrime and its Control'. This study aimed to map the cooperation space in the UKIA network to identify gaps in collaboration and opportunities for the development of a formal partnership approach. The population of interest was the UKIA network which includes members from the public, private and voluntary sectors. The Information Assurance Collaboration Group's (IACG) UKIA map 2011 (issue 3.1) was used to draw a sample[vii] and all listed organisations (approximately 200) were invited to participate in the study. A mixed methods approach was adopted, including an online survey instrument[viii] and online and offline interviews with node representatives[ix]. As the respondents were self-selecting we were not able to establish a randomised probability survey sample. Dorofeev & Grant (2006) state that studies that are concerned more with interrelationships between variables and less with hard measures of prevalence are likely to suffer less from the use of nonprobability sampling. The results reported later in this paper relate to inter-relations between variables and not measures of prevalence. Moreover, our study is principally concerned with 'soft' measures (perceptions), which have no absolute validity (they cannot be compared with any authoritative external measure). To mitigate sampling bias, a potential drawback of self-selecting sampling techniques (Tabachnick and Fidell 2013), we selectively targeted the various sectors within the UKIA network to achieve a balanced representation. Overall we achieved a 52 percent response rate with good coverage within all sectors.

Methods

Multi-Dimensional Scaling Procedure

The online survey included several questions that invited respondents to detail cooperation frequency with other nodes in the UKIA network. Multi-dimensional scaling (MDS) was used to make sense of this data. MDS models take sets of quantitative proximity data (distances and similarities between objects) and represent them visually by a set of points in a space. These points are plotted in such a way that geometrical relationships such as distance between the points reflect the empirical relationships in the data. The resulting picture of the data is much more simple to interpret than the matrix of quantitative measures it represents (Coxon 1982). The most widely understood example of MDS is based on literal geographic proximities (Kruskal and Wish 1978). A dataset consisting of distances in miles between pairs of cities in the US can be visually plotted in two dimensions (See Figure 1). Small and large distances between points in the visualisation relate to the small and large distances in miles between cities in the dataset. Furthermore, the two dimensions produced by the MDS procedure relate to North-South and West-East geography in real space. In criminology, MDS and its derivatives (e.g. Smallest Space Analysis) have been used widely in the fields of offender profiling and crime scene analysis (see Salfati 2000; Santtila 2003). The key difference between studies like these and the example used above is that social science measures of 'distance' between the objects of study are often less manifest than miles. Typically social science distance data are non-metric (such as ordinal data) and can relate to *perceptions* of similarities or dissimilarities between objects. Resulting MDS visualisations of these kinds of data are often more difficult to interpret compared to the above example, as researchers are left to infer the nature of dimensions that are calculated on more abstract measures (e.g. perceptions of distance). Furthermore, more than two dimensions are also possible in a MDS solution, further complicating interpretation (although two dimensional solutions are most common).

Despite these complexities, MDS affords researchers with an intuitive visual way of interpreting empirical relationships in data that may otherwise remain in obscurity. However, its use in criminological research beyond psychological disciplines is limited, and there is no reference in the literature made to MDS being used to analyse the cooperation space in multi-agency partnerships in crime reduction. Outside of criminology Naurin and Lindahl (2007) used the procedure to successfully map the cooperation patterns in the working groups of the council of the European Union using frequency of contact scores. In this study we adopted a similar method by asking responding UKIA nodes to score their frequency of cooperation with other UKIA nodes on an ordinal scale of 1 (no cooperation) to 4 (a lot of cooperation). These nodes fell into 12 clusters (see dependent measures for a description). We then used the PROXSCAL (PROXimity SCALing) procedure in SPSS to map the frequency of cooperation between these types of nodes, where frequencies were converted into measures of distance between points in a plot. Points that are close in proximity reflect high frequency of cooperation, where points that are distant reflect low frequency of cooperation. The dimensions on the plot represent underlying features of the cooperation space between clusters in the multi-agency partnerships (see results section for our interpretation of these dimensions).

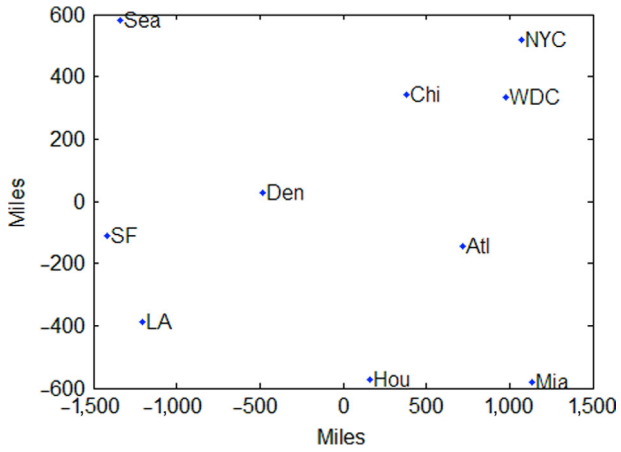

Figure 1: Multidimensional scaling model of flying distances between US cities

Factor Analysis Procedure

MDS enabled the empirically informed visualization of the UKIA cooperation space, but it said little about the organizational characteristics that are associated with high or low cooperation levels. For this regression models were used (see description below). As a precursor to building predictive regression models of cooperation, dependent measures of frequency were derived via the factor analysis procedure principal components analysis (PCA). This procedure reduces a large set of variables to a smaller set of components that have an underlying commonality. These components are derived by calculating inter-correlations and grouping together variables that are highly correlated. The same 12 cluster variables that were entered into the MDS were subjected to PCA and the resulting three components, which we term *meta-clusters*, were entered into the OLS regression models as composite dependent measures of cooperation frequency (see dependent variables and factor analysis results section for a description of extracted components).

Ordinary Least Squares Regression

The three components, *or meta-clusters*, extracted from the PCA were included in three separate OLS regression models as dependent measures. Given the relative small sample size and the violation of the normality assumption of OLS regression the *bias*

corrected and accelerated (BCa) bootstrapping technique was used. Bootstrapping is a nonparametric resampling procedure used to empirically estimate the sampling distribution of the indirect effect, thus reducing problems with type I errors and low statistical power endemic to analyses that rely on assumptions of sampling distribution normality (Efron and Tibshirani 1993). Results from correlational analyses (not shown), and tolerance statistics and variance inflation factors showed there were no problems with multicollinearity among the predictor variables. Statistics indicated a robust fit to the data in all three models[x].

Dependent Variables & Factor Analysis Results

Online survey items measured the frequency of cooperation amongst respondents from within the UKIA network. Respondents were asked to indicate their level of cooperation with 12 types of clusters on a four point likert scale ('no cooperation' through to 'a lot of cooperation'). The list of clusters included: Government Criminal Justice related; Government non-Criminal Justice related; Local Government; Private-IT; Private-Financial; Private-Other; Professional Bodies; Industry Groups; Academic Organisations; Regulatory Bodies; Charities/Not-for-Profit Organisations; and Police. PCA with orthogonal rotation (varimax) was used as a data reduction method to identify the underlying components of the 12 clusters (inter-correlations of a set of variables).

The correlation matrix of the 12 clusters revealed the presence of numerous correlation coefficients at .3 and above[xi]. For example, cooperation with the government departments – criminal justice cluster and cooperation with government departments – non-criminal justice cluster, were strongly correlated (r = .83). Similarly, cooperation with the Police cluster and cooperation with the Private Finance cluster, were also strongly correlated (r = .69). Conversely, cooperation with the charities cluster and cooperation with private sector finance cluster, were poorly correlated (r = .31). The matrix therefore provided evidence that the 12 cooperation clusters were reducible to two or more components[xii]. Based on an inspection of the eigenvalues, screeplot and rotated factor loadings three components were extracted. Table I details the rotated component loadings for the 12 clusters. The three component solution explained 81.12 percent of the variance, with component one contributing 65.65 percent, component two 9.19 percent and component three 6.27 percent. Not surprisingly the rotated solution revealed the presence of a structure similar to the MDS solution (see MDS results), albeit with an additional component/dimension. Each component showed a number of high loadings, with the majority of variables loading substantially on only one component. Items that are loaded heavily on component one were strongly associated with cooperation with a 'front line' *meta-cluster* (private sector finance, IT and other and

Item When tackling the cybercrime problem in the UK, to what extent does your organisation cooperate with any of the following?	Rotated factor loadings		
	Component 1	Component 2	Component 3
Private sector – financial	0.874		
Private sector – IT	0.861		
Private sector – other	0.756		
Police	0.637		
Professional bodies		0.763	
Industry groups		0.752	
Academic/research bodies		0.676	
Regulatory bodies		0.656	
Charities/NfPs		0.641	
Gov. depts – criminal justice			0.809
Gov. depts – non-criminal justice			0.796

Notes: χ^2 (55) = 1,043.59; $p < 0.00$; KMO measure of sampling adequacy (overall) = 0.887; local government were removed from the factor analysis due to poor loadings on each component (<0.300)
Source: Tabachnick and Fidell (2013)

Table I.
Factor loadings with Kaiser-Meyer-Olkin (KMO) measures of sampling adequacy

police) but have weak loadings (<.4) with components two and three; items that are loaded heavily on component two are strongly associated with cooperation with a 'backstage non-criminal justice' *meta-cluster* (professional bodies, industry groups, academic organisations, regulatory bodies and charities) but have weak loadings with components one and three; finally items that are loaded heavily on component three are strongly associated with cooperation with a 'backstage government' *meta-cluster* (government-criminal justice related and government non-criminal justice related) but have weak loadings with components one and two. Based on these distinct loadings we surmised there was a clear distinction between all three components. We labelled component one as *frequency of cooperation with the front-line meta-cluster*, component two as *frequency of cooperation with the backstage non-government meta-cluster*, and component three as *frequency of cooperation with the backstage government meta-cluster*. The component scores were extracted from the PCA and were used as continuous dependent variables in the regression analysis.

Predictor Variables

Perceptions of cybercrime – Two sets of items in the survey elicited perceptions data from respondents. The first set of items elicited data on respondents' perceptions of the severity of cybercrimes including malware attacks, denial of service attacks, hacking, insider unauthorised access and personal identity duplication/theft. The second set of items elected data on respondents' perceptions of the ease of control of the various cybercrimes above. Response options for both sets of items took the form of a four point likert scale ('not at all a problem' through to 'a very serious problem'; 'very easy to control' through to 'very difficult to control'). Both sets of items were entered as ordinal predictor variables in the regression models.

Perceptions of Clusters – Several items measured respondents' perceptions of the effectiveness and importance of clusters in their fight against cybercrime in the UK. On a likert scale of 1 (not at all effective/not at all important) to 4 (highly effective/very important) respondents were asked to rate their perceived effectiveness and importance of the 12 clusters. It is likely that these perceptions emerge through cooperation experience with the clusters being judged, or through the communication of the experience of other nodes. Reliability analysis was conducted on responses that indicated data reduction was possible via the development of scales for front line, back stage government and back stage non-government (directly mirroring the factor analysis reduction). The perceived front line, back stage government and back stage non-government effectiveness and importance scales were entered into the regression models as continuous predictor variables[xiii]. Tolerance statistics and variance inflation factors in the regression analyses reported later in the paper showed there were no issues with multicollinearity between these two sets of variables, indicating they were measuring independent constructs.

Controls – Several variables were included in the models to control for internal organisational and personal respondent characteristics. These include number of employees (categorised micro, small, medium and large organisations), age of node and personal length of tenure of the employee responding to the survey.

Results

Description of Survey Respondents

A breakdown of survey respondents is provided in Table II. UKIA members from the private sector formed the largest cluster of respondents (38 percent), made up of IT (16 percent), 'other' (14 percent) and financial (9 percent) nodes. Just under a third of responding UKIA members originated from non-government organisations, including Charities/Not-for-Profit (13 percent), academic/research (8 percent), and industry

nodes (7 percent) amongst others. Government members made up one fifth of respondents, including government criminal justice related (6 percent), non-criminal justice related (3 percent), local (3 percent) and 'other' (7 percent). Near fifty percent of respondents were deemed as 'large' nodes (>250 employees), with the remainder falling into the Small to Medium Sized Enterprise and Micro Enterprise categories. The majority of responding nodes had been in existence for over 20 years, with just over a quarter reporting less than 10 years of incorporation.

Independent variables	Coding	Sample *n*/M	Sample %/SD
Organisation type			
Private sector – financial	–	9	8.7
Private sector – IT	–	16	15.5
Private sector – other	–	14	13.6
Police	–	11	10.7
Professional bodies	–	4	3.9
Industry groups	–	7	6.8
Academic/research bodies	–	8	7.8
Regulatory bodies	–	2	1.9
Charities/NfPs	–	13	12.6
Gov. depts – criminal justice	–	6	5.8
Gov. depts – non-criminal justice	–	3	2.9
Public sector – other	–	7	6.8
Local government	–	3	2.9
Controls			
No. of employees	1-9	21	20.4
	10-49	7	6.8
	50-249	25	24.3
	250 or more	50	48.5
Age of org.	<1 year	3	2.9
	1-5 years	17	16.3
	6-10 years	9	8.7
	11-15 years	12	11.5
	16-20 years	8	7.7
	>20 years	55	52.9
Personal length of tenure	0-5 years	19	18.3
	6-11 years	36	34.6
	12 years and above	49	47.2
Perceptions of cybercrime			
Problem of malware attacks	Scale range 1-4	3.25	0.76
Problem of DoS attacks	Scale range 1-4	2.71	0.80
Problem of hacking	Scale range 1-4	2.80	0.91
Problem of insider unauthorised access	Scale range 1-4	2.95	0.99
Problem of personal ID theft	Scale range 1-4	3.20	0.90
Control of malware attacks	Scale range 1-4	2.83	0.85
Control of DoS attacks	Scale range 1-4	2.96	0.75
Control of hacking	Scale range 1-4	2.76	0.76
Control of insider unauthorised access	Scale range 1-4	2.88	0.75
Control of personal ID theft	Scale range 1-4	2.89	0.91
Perceptions of clusters			
Front line effectiveness scale	Scale range 4-16	10.24	2.10
Back stage gov. effectiveness scale	Scale range 2-8	4.63	1.50
Back stage non-gov. effectiveness scale	Scale range 5-18	10.59	2.94
Front line importance scale	Scale range 8-16	14.42	1.70
Back stage gov. importance scale	Scale range 4-8	7.21	1.02
Back stage non-gov. importance scale	Scale range 7-20	15.61	2.78

Table II.
Descriptive statistics of UKIA organisations

Note: $n = 103$

As a whole, the sample of UKIA nodes perceived malware attacks and personal identity theft as the most serious cybercrime problems facing the UK. Perceived as least problematic were denial of service attacks (DoS). Conversely, respondents perceived DoS attacks as most difficult to control, while perceiving hacking as most easy to control (see Williams & Levi 2012 for a sub-group analysis of these perceptions). Respondents perceived front line responses to cybercrime reduction as most effective, followed by back stage non-government and back stage government responses. In relation to perceived importance, respondents rated front line and back stage government as equally important, followed by back stage non-government.

MDS Results

Figure 2 shows the PROXSCAL procedure produced a two dimensional MDS solution of the frequency of cooperation data provided by the UKIA network respondents. The output also generated the stress value, which is a measure of the goodness of fit between the raw cooperation frequency data and the visualisation. A test of statistical significance was applied to the stress value to determine if the match between the data and the visualization was statistically significant. As is convention in the social sciences the threshold of significance for the stress value is .05. The normalised raw stress value for the MDS solution reported here was .042, indicating the relationships among the clusters in the visualisation were statistically significant. The Tucker's φ coefficient of congruence equaled 0.98 and decompositions of normalized raw stress ranged from .02 to .06. Based on these measures we concluded the solution identified was robust and provided a good fit to the data.

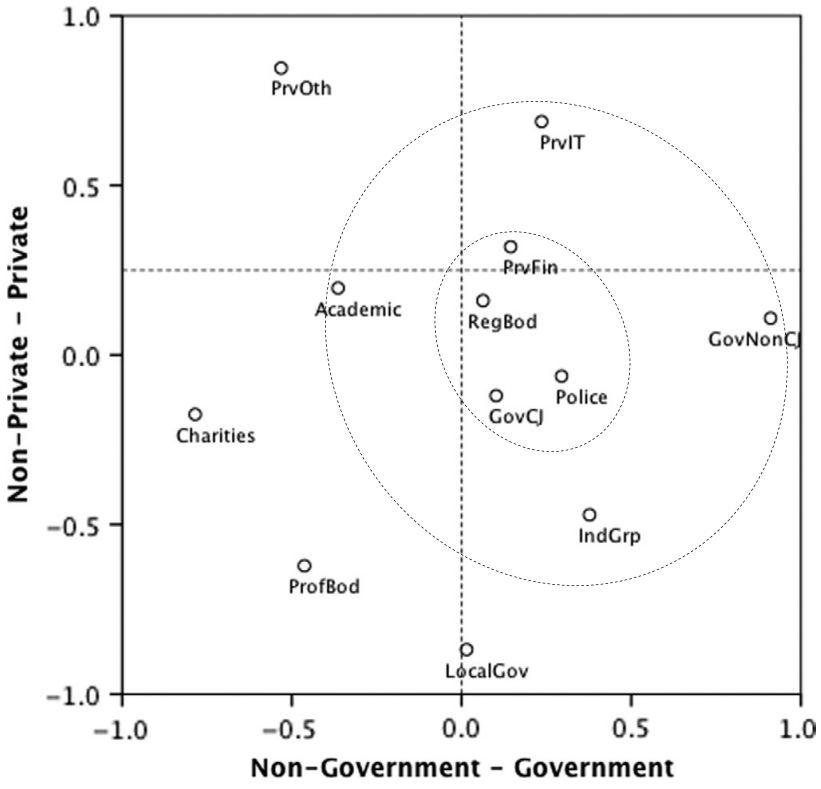

Figure 2. UKIA frequency of cooperation space

Interpreting the dimensions of non-metric MDS solutions is not a precise science as the underlying data may not relate to any externally valid hard measure (Kruskal and Wish 1978). In our case we asked respondents to rate their perceived level of cooperation on a four point Likert scale. The resulting dimensions therefore represent some underlying features of the 'perceived' cooperation space. An inspection of the plot does reveal variability in the distances between points that represent clusters. Some are close in

proximity, such as government criminal justice and police, while some are distant, such as local government and private sector – other. An inspection of the original data matrix shows that in the former coupling both clusters scored their cooperation with each other as high (the mean score for government criminal justice cooperation with the police was 3.0 out of 4, while the mean score for police cooperation with government criminal justice was 2.1 out of 4), while in the latter coupling the clusters scored their cooperation with each other as low (the mean score for private sector – other cooperation with the local government was 0.1 out of 4, while the mean score for local government cooperation private – other was 0.3 out of 4). This check further confirms the MDS visualisation accurately represents the underlying cooperation data. We can therefore infer that the dimensions are a reflection of some underlying 'nature' of this cooperation space. On the *y* axis, private clusters dominate the high end, while non-private clusters dominate the lower end. On the *x* axis, government clusters dominate the high end, while non government dominate the lower end. We therefore inferred that the *y* dimension reflected non-private – private cooperation showing that private clusters tend to cooperate more frequency with each other than with non-private clusters, and vice versa. The *x* axis reflected non-government – government cooperation, showing that government clusters tend to cooperate more with each other than with non-government clusters (with the exception of regulatory bodies) and vice versa. Along these dimensions some clusters organise into dense cooperation 'cliques'. The most apparent is at the rough intersection of the axes as indicated. The regulatory bodies cluster takes centre stage in the cooperation space, in close proximity to private finance, government criminal justice, and police clusters. This might be considered the inner-circle of cooperation. Private sector IT, government non-criminal justice, industry groups and academic clusters occupy an outer circle that cooperates less frequently with the clusters within the inner circle and with each other. On the periphery are private sector – other, charities, professional bodies and local government clusters – these have the lowest cooperation frequencies and are largely excluded from the inner cooperation spaces.

Regression Models

The sets of predictor variables (perceptions of cybercrime and perceptions of nodes) and controls were regressed onto the outcome variables derived from the PCA generating three models: Model 1 – *frequency of cooperation with the front-line meta-cluster*; Model 2 – *frequency of cooperation with the backstage non-government meta-cluster*; and Model 3 – *frequency of cooperation with the backstage government meta-cluster* (see Table III).

Perceptions of cybercrime – Holding all other factors constant several of the perceptions of cybercrimes variables emerged as having significant associations with frequency of cooperation in all three models. In relation the front line meta-cluster (private companies and the police) respondents who perceived that malware attacks were a serious problem and that DoS attacks were easy to control were significantly more likely to report a higher frequency of cooperation. In relation to the back stage non-government meta-cluster (e.g. charities, regulatory bodies, forums etc.), respondents who perceived DoS attacks as less of a problem, malware attacks as easy to control, and insider unauthorised access as difficult to control, were more likely to report higher levels of cooperation; although all these associations only approached conventional levels of significance. Finally, in relation to the back stage government meta-cluster (e.g. Home Office, Cabinet Office, HMRC etc.) respondents who perceived personal insider unauthorised access as easy to control and ID theft as less of a problem were more likely to report higher cooperation rates; although both of these association only approached conventional levels of significance.

Perceptions of Clusters – Holding all other factors constant the perceptions of organisations scales were significantly associated with cooperation in all models. In relation to the front line meta-cluster, a positive association emerged between cooperation frequency and the front line effectiveness scale; although this association only approached conventional levels of significance. Conversely, the back stage non-government importance scale was negatively associated with cooperation with the front line meta-cluster. In relation to the non-government meta-cluster, the back stage government importance scale was negatively correlated with cooperation, while the reverse was observed with the back stage non-government importance scale. Finally, in relation to the government meta-cluster, the back stage non-government effectiveness scale was negatively associated with cooperation frequency.

Controls – Only two control variables emerged as holding significant associations with cooperation frequency. In relation to cooperation with the non-government meta-cluster, organisations that had been incorporated for longer and had fewer employees were more likely to report higher levels of cooperation. There were no significant associations between the control variables and the other meta-clusters.

Sub-model Analysis – In order to ascertain which sets of variables (perceptions of cybercrime and effectiveness and importance scales) were most predictive in relation to each model we conducted sub-model analyses. The adjusted R^2 statistic was used to evaluate the sub-models[xiv]. Independently the set of perceptions of cybercrimes predictors accounted for 22 percent (R^2.22), 7 percent (R^2.07), and 7 percent (R^2.07) of the variance for front line, back stage government and back stage non-government meta-cluster cooperation respectively. Independently the set of perceptions of effectiveness and importance predictors accounted for 15 percent (R^2.15), 12 percent (R^2.12) and 17 percent (R^2.17) of the variance for front line, back stage government and back stage non-government meta-cluster cooperation respectively. These results indicate that perceptions of cybercrimes are most predictive of cooperation with the front line meta-cluster, while perceptions of effectiveness and importance are most predictive of cooperation with back stage government and non-government meta-clusters[xv].

Discussion

Results from the MDS and regression models provided the first quantitative evidence of cooperation in the UK cybersecurity space. Hypothesis 1 was largely supported by the MDS solution. We postulated that inter-sector cooperation would not be evident based on the nascence of new partnership initiatives and that previous research indicated tensions between private and public clusters inhibits cooperation (Dunn-Cavelty and Suter 2009; Huey et al. 2012; Sulek & Doscher 2011; Wall 2007). Contrary to our hypothesis, inter-sector cooperation was evident in an inner clique, with private finance firms emerging proximate to government, police and regulatory body clusters. However, in support of our hypothesis private IT, and to a greater extent private other clusters were markedly distant from all other sectors. Furthermore, the charity and local government clusters were also isolated, indicating a lack of cooperation with third-sector and non-central government nodes. In explaining these patterns we revisited the conceptual work outlined earlier in the paper. The degree of public – private cooperation evident in the inner circle indicates tensions, if they exist between private finance and government nodes, do not manifest in a way that stifles frequency of cooperation as suggested by Dunn-Cavelty and Suter (2009) and Sulek and Doscher (2011). While the issues of a lack of a clear business case and tensions between

	Model 1: front line meta-cluster			Model 2: back stage non-gov. meta-cluster			Model 3: back stage gov. meta-cluster		
	B	SE	β	B	SE	β	B	SE	β
Perceptions of cybercrime									
Problem of malware attacks	0.50	1.70	*0.38* ***	0.23	0.24	0.17	0.12	0.24	0.09
Problem of DoS attacks	−0.01	0.22	−0.01	−0.30	0.21	−0.24*	−0.23	0.19	−0.18
Problem of hacking	−0.08	0.21	−0.08	0.15	0.22	0.14	0.13	0.19	0.12
Problem of insider unauthorised access	−0.19	0.21	−0.19	0.01	0.14	0.01	0.02	0.14	0.02
Problem of personal ID theft	0.20	0.16	0.18	−0.13	0.21	−0.11	−0.26	0.20	−0.23*
Control of malware attacks	0.16	0.19	0.13	−0.29	0.20	−0.25*	−0.08	0.18	−0.06
Control of DoS attacks	−0.54	0.19	*−0.41* ***	0.11	0.21	0.09	−0.08	0.20	−0.06
Control of hacking	0.22	0.21	0.17	0.07	0.21	0.06	−0.02	0.21	−0.01
Control of insider unauthorised access	0.20	0.19	0.15	0.26	0.18	0.20*	−0.37	0.18	*−0.28* *
Control of personal ID theft	−0.29	0.18	−0.26	0.02	0.19	0.02	0.07	0.22	0.06
Perceptions of clusters									
Front line effectiveness scale	0.12	0.08	0.26*	−0.01	0.08	−0.01	−0.02	0.08	−0.04
Back stage gov. effectiveness scale	−0.14	0.11	−0.21	−0.02	0.10	−0.03	0.08	0.13	0.12
Back stage non-gov. effectiveness scale	0.02	0.05	0.07	0.01	0.05	0.03	−0.14	0.05	*−0.42* ***
Front line importance scale	0.10	0.09	0.18	−0.11	0.09	−0.18	0.01	0.08	0.02
Back stage gov. importance scale	−0.20	0.11	*−0.21* **	−0.26	0.11	*−0.27* **	−0.04	0.12	−0.04
Back stage non-gov. importance scale	0.03	0.05	0.07	0.17	0.06	*0.48* ***	0.05	0.06	0.14
Controls									
No. of employees	0.15	0.12	0.18	−0.19	0.13	−0.23*	0.15	0.13	0.18
Age of org.	−0.08	0.09	−0.13	0.16	0.08	*0.27* **	0.00	0.09	−0.01
Personal length of tenure	−0.01	0.06	−0.02	0.07	0.06	0.11	−0.06	0.06	−0.09
Constant	−2.05	1.70		−0.19	1.54		2.47	1.70	
Model fit									
Sig.	0.000			0.004			0.025		
R^2	0.28			0.20			0.14		
n	104			104			104		

Note: Significant at: *$p < 0.10$, **$p < 0.05$ and ***$p \leq 0.01$

Table III.
BCa bootstrap OLS regression predicting UKIA network cooperation

hierarchical reporting and horizontal information sharing are likely to be evident, they are unlikely to create a significant barrier to cooperation between these specific clusters. This may be explained by the historic integration of parts of the finance industry in anti-fraud partnerships that predate the internet. These existing lines of cooperation may have been 'hi-jacked' in the cybersecurity effort, ensuring a close tie to government organisations such as the Home Office, the Serious Fraud Office, the police and regulatory bodies. Furthermore, as Dupont (2004) indicates, these nodes are most likely to display high amounts of social, cultural, economic, political and symbolic capital, ossifying their prominent position in the UK cybersecurity network. Furthermore, the history of centralisation in the UK was highlighted as an advantageous feature of the cybersecurity network in the qualitative data:

> "The most noteworthy distinction between UK and US law enforcement practice is the far greater coherence and centralization/consolidation of functions in the UK. On e-crime reporting, the UK has Action Fraud; the US has IC3, Consumer Sentinel, and independent channels into the US Secret Service and Postal Inspectorate, and the pooling of data among those disparate sources is highly incomplete and inconsistent. On e-crime investigation, the UK is more centralised also."
>
> Law Enforcement

This resonates with the observation that the privatisation of partnerships is more pronounced in the USA than in Britain, and that 'the centralized administrative powers of the British Home Office have allowed it to develop policies with greater speed and coherence than has been possible in the USA' (Garland 2001: 212).

Despite close cooperative relations, the MDS showed that remaining private clusters, especially 'other' (which included a large number of SMEs), cooperated much less frequently with other clusters, including government and police. While this pattern partly supports the first hypothesis, the issues raised by Dunn-Cavelty and Suter and Sulek and Doscher were not indicated as reasons for low levels of cooperation in the comments from respondents:

> "There are too many organisations looking at, and dealing with cybercrime - and this only provides confusion and uncertainty. SME outreach has been neglected for well over a decade, despite the rhetoric, and there is little follow-up on guidance. Frankly, I lose patience with decision-makers who take years to make decisions. The electronic economy requires us to make fast decisions as the law NEVER catches up with reality."
>
> Private Sector – Other

> "To be honest it is my view that the majority of UK bodies, in particular law enforcement know little of the cybercrime problem. Law enforcement is completely ineffective in this sector and there is a lack of any effective regulation. This has resulted in a massive gap between central Government policy and most industry sectors."
>
> Private Sector – Other

> "[There are] difficulties getting SME's to join and engage as well as our ability to deliver the right product to them."
>
> Charity

> "[Partnerships] should have a federated structure as particular industry sectors will have different needs. [A partnership] needs to link with the very senior level of engagement following the recent No. 10 event, otherwise it will become an isolated group of experts without the links to achieve outcomes at board level."
>
> Government – Non-Criminal Justice

> "Government agencies should aim to partner with private industry more. But, legislation inhibits this."
>
> Government – Criminal Justice

How might we account for the low inter-sector cooperation frequencies of these private non-finance nodes? This might result from a combination of an over-crowded cybersecurity space, the criminal justice system's poor record in apprehending and successfully prosecuting cybercrime perpetrators, inhibiting legislation and historically poor engagement with SMEs and a poor understanding of their security needs. However, it is also likely that SMEs–especially those that have poor cyberthreat awareness–find it difficult to justify a business case for cooperation in austere economic times. Private 'other' organisations are also likely to have less of the various forms of capital outlined by Dupont, inhibiting their desirability as partners in cooperation within the UK cybersecurity network. Maybe the expectation of involvement from SMEs is misplaced and so we should not expect an innate drive to want to cooperate. Perhaps then we can learn something from the cooperation initiatives espoused by the Virtual Global Taskforce that promotes more realistic views about what each public and private node in a network can contribute, and therefore make more efficient capability judgements.

Beyond public-private partnerships, the MDS visualisation also evidenced low levels of cooperation with and between charities, professional bodies and local government clusters, further supporting the assumption made in the first hypothesis. Qualitative comments from respondents resonated with the distance evident in the visualisation:

> "[A partnership should not be] another old boys network. The e-Crime community already suffers from cliques. Membership should be free and include government, business, consumers groups and civil society groups. There needs to be funding for groups such as not-for-profits and academics to attend so that it isn't biased towards large organisations that can afford to fund public policy people."
>
> Charity

The exclusion of these clusters from the inner circles of partnership working in cybersecurity, especially the charity and not-for-profit cluster, are evident in other areas of criminal justice. Mills et al. (2011) in their study of the role of the third sector in work with offenders found that the erosion of the funding 'security net' in the form of grants from Government had resulted in the exclusion of some charities in partnerships. Moreover, they concluded that a substantial gap existed between the Government rhetoric surrounding the third sector and the actual partnership opportunities. Parallels between this research and ours are evident, most notably in relation to a lack of funding, or as Dupont puts it economic capital, and the impactions this has for participation in partnership endeavours. Attending national meetings, developing and maintaining information sharing protocols, and compliance with international cybersecurity standards all require resource that many charities and smaller organisations find it difficult to justify. Furthermore, the exclusion (whether active or not) of local government, private – other and professional body clusters from partnerships may signal that they are perceived to have little to provide cybersecurity networks, whether it is technical expertise, or any other form of network capital. Again, the point made above in relation to taking a realistic view on possible contributions based on capabilities is also important, if not more so in relation to these more isolated nodes.

Crawford (2002) argues that patterns of inclusion and exclusion are characteristic of crime reduction partnership spaces, and are often borne out of contradiction, ambiguity and ambivalence. Comments from respondents showed that while the rhetoric of cyber

security was evident from government departments, incongruity and uncertainty around the issues were apparent:

> "…In my experience government departments are out of touch, and insufficiently dynamic to take a lead in this area…In addition, it is also my experience that there is a lack of co-ordination between government departments 'rushing' to the 'cyber' threat. For example; during a recent conversation with the National Fraud Authority, it was apparent that there was insufficient knowledge of what the private sector was doing or even what other (government) departments were doing. The idea that central government could lead and co-ordinate responses ignores the cultural and other limitations of central government."
>
> Private Sector - Finance

> "The Home Office has ownership of cyber in formal terms. However no-one has any real oversight or overview of e-issues as a whole, nor any desire for it, as they are trapped in their own silos and ambitions."
>
> Law Enforcement

These comments resonate with Edwards and Hughes' (2009) conclusion that divisions exist between security talk, decisions and actions that result in gaps in cooperation and security outcomes. These gaps are both enlarged and contracted by the time-variable power-play between the various public, private, law enforcement and voluntary nodes in the networks who draw on their various mixtures of network capital. Furthermore, outcomes are sectorially and geographically uneven, furthering political (with a small 'p') tensions in networks that both open up new opportunities for further cooperation, and narrow and close off others. Ultimately the pluralized cyber security space is shaped by contradictory and unstable forces that are endemic to crime reduction partnership endeavours (Edwards and Hughes 2009).

In our second hypothesis we postulated that perceptions of the seriousness of cybercrime problems and the difficulty of their control would be significantly associated with levels of cooperation, based on the partnership literature that suggests networks of security arrange around significant and complex crime problems (Crawford 1997; Garland 2001; Hughes 2007). The regression model results provided limited support for this hypothesis, showing that these sets of variables were most significantly associated with cooperation with the front-line meta-cluster (private organisations and the police), while being weakly associated (only approaching conventional levels of significance) with both back stage non-government and government cooperation. It is likely that the strong statistical association between the perception that malware attacks were a serious problem and cooperation with the front line can be explained by the link between malware attacks and forms of corporate and personal identity theft/duplication. We suggest that those who consider that these particular crimes are more/most serious compared to other cybercrimes are more likely to seek cooperation with clusters with experience and expertise in the area. Of course, conversely we can argue that it is an artefact of intensification of views resulting from like-minded cooperation itself: those who cooperate with these clusters are more likely to think these types of cybercrime are more serious (see Williams & Levi 2013). Unpacking the association between the perception that DoS attacks are easy to control and front line cooperation is more complex. As above we could argue that cooperation promotes this perception, while still acknowledging that the reverse is also possible (but also counter-intuitive). Identifying causality is problematic in cross-sectional quantitative designs and further qualitative work is necessary to begin to flesh out these various associations. What we can be confident of is that the sub-model analysis shows that perceptions of cybercrime are by far the strongest association in relation to front line cooperation, when compared to back stage government and non-government cooperation. This

suggests that, if we are to assume perception precedes cooperation, that the complexity of cybercrime problems is only significant in motivating cooperation with the front line, and as indicated below, not with government or non-government meta-clusters.

In our final hypothesis we made the assumption that respondents who perceived a cluster as effective or important would cooperate frequently with that cluster, based on research that shows nodes will seek to cooperate with other nodes who demonstrate they can assemble certain forms of network capital to achieve effective outcomes, which increases their importance in cybersecurity networks (Nhan and Huey 2008; Huey et al. 2012; Dupont 2004). Regression analyses provided evidence to partially support this hypothesis, especially in relation to cooperation with back stage non-government. However, conversely, in most cases, perceptions that certain clusters of nodes were ineffective or not important were associated with cooperation with alternative clusters. For example, those that felt that government was unimportant in the fight against cybercrime were more likely to cooperate with front line and non-government meta-clusters. Furthermore, those perceiving that non-government was ineffective were more likely to cooperate with government. Given that our sub-model analysis revealed that perceptions of clusters were most important in predicting cooperation with government and non-government meta-clusters (as opposed to perceptions of cybercrimes – see previous paragraph), these symmetrical negative perceptions of both these clusters are important, as they may indicate that some nodes only exclusively cooperate with one or the other type of node in the cybersecurity network.

Conclusions

In this paper we have provided evidence showing how multi-agency partnership working operates in the cyber security space. Our mapping of the cyber security cooperation space utilising MDS revealed that gaps exists in the network. Qualitative comments from the survey of UKIA community respondents allowed us to interpret gaps in public-private partnerships in terms of a combination of an over-crowded cybersecurity space, the criminal justice system's poor record in apprehending and successfully prosecuting cybercrime perpetrators, inhibiting legislation and historically poor engagement with SMEs and a poor understanding of their security needs. We also highlighted the possibility that SMEs with poor cyberthreat awareness may find it difficult to justify a business case for spending time and its opportunity cost – money – on cooperation in austere economic times. Furthermore, SMEs are likely to exhibit fewer of the various forms of network capital outlined by Dupont, inhibiting their desirability as partners in cooperation within the UK cybersecurity network. Similarly, we explained that low levels of network capital, especially a poor partnership funding structure, were partly responsible for infrequent communications between non-private-non-central government organisations, such as charities and local government, and central government and private clusters. Our regression models indicated that various characteristics emerged as significantly associated with cooperation. Perceptions of cybercrimes were strongly correlated with cooperation with the front line cluster, while perceptions of organisations, in terms of effectiveness and importance, were correlated with cooperation with back stage government and non-government clusters. These various associations indicate that there are different motivators and inhibitors for cooperation with the various clusters in the cybercrime cooperation network. Understanding the origin of these motivations requires further qualitative study. Our data suggest that the neo-liberal rationality that has been evoked in other areas of crime control (Edwards and Hughes 2009) is also evident in the control of cybercrimes, where state intervention is rolled back (and/or never is rolled out) as private actors adopt individualized, responsibilised and practical roles in a networked fashion. These cyber security networks mobilise the diverse specialist resources, beyond those marshalled by criminal justice agencies, that are required to mitigate the cybercrime threat. However,

divisions exist between the High Policing rhetoric of the Cyber Security Strategy (Cabinet Office 2011) and the Lower Policing cooperation outputs and outcomes in this networked space. The influence of network capital, especially economic capital, creates a power-play between the various public, private, law enforcement and voluntary nodes resulting in sectorially and geographically uneven cooperation patterns. We conclude, like Edwards and Hughes (2009), that the pluralized cyber security space is shaped by contradictory and unstable forces that are endemic to crime reduction partnership endeavours. A way forward may be to formally acknowledge the limited capabilities and interests of some nodes in the cyber security network, therefore reducing expectations and opening a space for discussion on compensation for low levels of appropriate network capital.

References

Andersson, J.J. and Malm. A. (2007), 'Public-private Partnerships and the Challenge of Critical Infrastructure Protection', in Isabelle Abele-Wigert and Myriam Dunn (eds.), *International CIIP Handbook*. ETH: Zurich.

Butler, J. B., and Lachow, I. (2012), *Multilateral Approaches for Improving Global Security in Cyberspace*, Washington, VA: The MITRE Corporation.

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

Cabinet Office (2012), *The UK Cyber Security Strategy: Report on Progress – December 2012*. Cabinet Office: London.

Coxon, A. P. M. (1982), *The User's Guide to Multidimensional Scaling*. Heinemann Educational Books Ltd.: London.

Crawford, A. (1997), *The Local Governance of Crime: Appeals to Community and Partnerships*. Oxford: Clarendon Press.

Crawford, A. (2002) 'The Governance of Crime and Insecurity in an Anxious Age: The Trans-European and the Local', in A. Crawford (ed.) *Crime and Insecurity*, 27--51. Cullompton: Willian Publishing.

Doig, A. and Levi, M. (2009) 'Inter-agency work and the UK public sector investigation of fraud, 1996-2006: joined up rhetoric and disjointed reality', *Policing and Society*, 19/3: 199--215.

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

Dunn-Cavelty, M., and Suter, M. (2009), 'Public-Private Partnerships Are No Silver Bullet: an Expanded Governance Model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*. 2/4: 179--187.

Dupont B (2004), 'Security in the age of networks', *Policing & Society,* 14/1: 76--91.

Edwards, A., and Hughes, G. (2009) 'The Preventive Turn and the Promotion of Safer Communities in England and Wales', in A. Crawford (ed.) *Crime Prevention Policies in Comparative Perspective*, 62--85. Cullompton: Willan.

Efron, B., & R. Tibshirani (1993), *An Introduction to the Bootstrap*. London: Chapman and Hall.

Fick, J. (2009), 'Cybercrime in South Africa: Investigating and prosecuting cybercrime and the benefits of public-private partnerships', *Council of Europe octopus interface conference cooperation against cybercrime 10-11 March 2009*, Strasbourg: France.

Garland, D. (2001), *The Culture of Control*. Oxford: Oxford University Press.

Gilling, D. (2007) *Crime Reduction and Community Safety: Labour and the Politics o Local Crime Control*. Cullompton: Willan Publishing.

Home Office (2010) *Policing in the 21st Century: Reconnecting police and the people*. Cm 7925, Home Office: London.

Huey, L., Nhan, J. and Broll, R. (2012), 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime', *Criminology and Criminal Justice* (advance online access).

Hughes, G. (2007), *The Politics of Crime and Community*. London: Palgrave.

Irion, K. (2012) 'The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R)', *27th European Communication Policy Research Conference: Policies For The Future Internet* , 25--27 March 2012, Ghent: Belgium.

Johnston, L. and Shearing, C. (2003), *The Governance of Security*. London: Routledge.

Jones, T. and Newburn, T. (2002), 'The Transformation of Policing? Understanding Current Trends in Policing Systems', *British Journal of Criminology*, 42/1: 129--46.

Kline, P. (1999), *The handbook of psychological testing (2nd ed.)*. London: Routledge

Kruskal, J.B. and Wish, M. (1978), *Multidimensional Scaling, Sage University Paper series on Quantitative Applications in the Social Sciences*, London: Sage.

Levi, M (2010), 'Public and Private Policing of Financial Crimes: the Struggle for Co-ordination', *Journal of Criminal Justice and Security*, 12/4: 343--357.
Levi, M. and Williams, M. (2012), Cybercrime Reduction Partnership Mapping Study, Cardiff: Nominet Trust. Available at: http://www.cardiff.ac.uk/socsi/resources/Levi%20Williams%20cybercrime%20Reduction%20Partnership%20Mapping%20Study.pdf.
Mills A., Meek R., and Gojkovic D. (2011), 'Exploring the relationship between the voluntary sector and the state in criminal justice', *Voluntary Sector Review* 2/2: 193--211.
Naurin, D., and Lindahl, R. (2007) 'Network Capital and Cooperation Patterns in the Working Groups of the Council of the EU', *European University Institute Working Paper*, Florence: RSCAS.
Nhan, J. and Huey, L. (2008), 'Policing through nodes, clusters and bandwidth: The role of network relations in the prevention of and response to cyber-crimes', in: S. Leman-Langlois (ed.) *Technocrime: Technology, Crime and Social Control*, 66--87. Portland, OR: Willan.
PwC (2013) *Information Security Breaches Survey 2013: Technical Report*, London: Price Waterhouse Coopers.
Salfati, C. G. (2000), 'The Nature of Expressiveness and Instrumentality in Homicide', Homicide Studies, 4/3: 265--293.
Santtila, P., Hakkanen, H., Alison, L., and Whyte, C. (2003), 'Juvenile firesetters: Crime Scene actions and offender characteristics', *Legal and Criminological Psychology*, 8: 1--20.
Sulek, D. and Doscher, M. (2011), 'Beyond Public-Private Partnerships', in K. Andreasson (Ed.) *Cybersecurity: Public Sector Threats and Responses*, 127--145. Boca Raton, FL: CRC Press.
Symantec (2013), *Internet Security Threat Report 2013*, Volume 18, Mountain View, CA: Symantec.
Tabachnick, B. G., and Fidell, L. S. (2013), *Using Multivariate Statistics*, 6th ed. Boston: Allyn and Bacon.
Wall, D. (2007), 'Policing cybercrimes: Situating the public police in networks of security within cyberspace', *Police Practice and Research* 8/2: 183--205.
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.
White, A. and Gill, M. (2013) 'The Transformation of Policing: From Ratios to Rationalities', *British Journal of Criminology*, 53/1: 74--93.
Williams, J. (2005) 'Reflections on the Private Versus Public Policing of Economic Crime', *British Journal of Criminology*, 45/3: 316--39.
Williams, M. and Levi, M. (2012) 'Perceptions of the cybercrime Controllers: Modelling the Influence of Cooperation and Data Source Factors', *Security Journal* [online advance access].

[i] Third or voluntary sector organisations are missing from this list. Such organisations play a vital role in cybercrime reduction partnerships in the UK and have been included in our analysis reported later.

[ii] IACG is an initiative within the Government Communications Headquarters (GCHQ) Communications–Electronics Security Group (CESG).
[iii] European Network & Information Security Agency
[iv] Information Security Forum
[v] The Information Security Alliance
[vi] The Chartered Institute for IT

[vii] 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

[viii] We used the Bristol Online Survey tool: http://www.survey.bris.ac.uk/. Given this online element the fieldwork was conducted in line with the ethical guidelines established by the Association of Internet Researchers and the British Society of Criminology. We 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.
[ix] These interviewees were identified from the survey. We ensured that informed consent was gained at that the respondents understood that their data would remain confidential and their identities and organisations anonymous.

[xi] Not presented here due to space restrictions. Available upon request.
[xii] Other standard diagnostics also indicated the factorability of the correaltion matrix. The Kaiser-Meyer-Oklin value was .887, exceeding the recommended value of .6 (Kaiser 1974), and Bartlett's Test of Sphericity reached statistical significance.
[xiii] Cronbach's alpha is commonly used to indirectly indicate the degree to which a set of items measures a single underlying latent construct based on an assesssment on the degree of intercorrelations of the set of items. Kline (1999) details an anlpha of .70 and above is acceptable for evidencing internal consistency of a set of items (i.e. the items are all measuring the same underlying construct). The Cronbach's alpha reulsts for our item scales were: Front line effectiveness scale: Cronbach's α .70; back stage gov. effectiveness scale: Cronbach's α .84; back stage non-government effectiveness scale: Cronbach's α .81; Front line importance scale: Cronbach's α .77; back stage gov. effectiveness scale: Cronbach's α .72; back stage non-government effectiveness scale: Cronbach's α .78.

[xiv] This is a measure of *model fit* and is the coefficient of determination that indicates how well the model predicts the observed data: *r .10* is small, *r .30* is medium and *r .50* is large. The social science standard for a 'good' fit is R^2 .30 (Cohen 1988).
[xv] Of course the inverse is also possible; that cooperation levels predict perceptions of cybercrimes, effectiveness and importance of organisations. Concluding causality is problematic in cross-sectional designs and we can only establish associations with a degree of statistical certainty (Tabachnick and Fidell 2013).