View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by OpenSIUC

Southern Illinois University Carbondale
OpenSIUC

Articles | Department of Criminology and Criminal Justice

Spring 4-15-2016

The use of specialized cybercrime policing units: An organizational analysis

Dale Willits
Washington State University, dale.willits@wsu.edu

Jeffrey Nowacki
Southern Illinois University Carbondale, jnowacki@siu.edu

Follow this and additional works at: http://opensiuc.lib.siu.edu/ccj_articles
This is an Author's Accepted Manuscript of an article published in *Criminal Justice Studies*, Vol. 29, No. 2 (2016) (copyright Taylor & Francis), available online via the link below.

This Article is brought to you for free and open access by the Department of Criminology and Criminal Justice at OpenSIUC. It has been accepted for inclusion in Articles by an authorized administrator of OpenSIUC. For more information, please contact opensiuc@lib.siu.edu.

Title:
The Use of Specialized Cybercrime Policing Units: An Organizational Analysis

Authors:
Dale Willits,
Assistant Professor
Department of Criminal Justice & Criminology
Washington State University
dale.willits@wsu.edu

Jeffrey Nowacki
Assistant Professor
Department of Criminology and Criminal Justice
Southern Illinois University Carbondale
jnowacki@siu.edu

Abstract
Given the increased focus and importance of cybercrime, some police agencies have turned to the use of specialized cybercrime policing units. Research has yet to examine the how frequently these units are used in policing, nor has research examined the types of agencies most likely to use these units. The current research, drawing on contingency theory, institutional theory, and Maguire's theory of police organizational structure, uses four waves of Law Enforcement Management and Administrative Survey data to provide a descriptive analysis of specialized cybercrime units with a focus on identifying organizational correlates, environmental pressures, and the role of time. Trend data show that cybercrime units have proliferated over time and are on the path to becoming a normative aspect of policing, with about one-half of all state-level agencies and around one-quarter of all county and municipal agencies making use of cybercrime units as of 2013. Regression results indicate that larger agencies, agencies facing more task routineness and larger task scope challenges, agencies which make use of broader material technologies, and agencies which have adopted specialization strategies are more likely to use cybercrime units than other agencies. The practical and theoretical implications of these results are discussed, as are promising future research directions.

As the reach of technology has grown in recent years, so have avenues for engaging in criminal behavior. As such, new forms of cybercrimes (e.g., crimes involving networked technologies) have surfaced. These cybercrimes, include, but are not limited to child pornography, cyber stalking, identity theft, cyber bullying, and computer piracy (Holt et al., 2015; Rege-Patwardhan, 2009; Wall, 2007). Some of these offenses are illegal only through the use of computer technology, while others are simply aided by the use of computers, but all of them are, in some way, facilitated through the use of technology.

As the prevalence and severity of cybercrime offenses has grown over time (Police Executive Research Forum, 2014), law enforcement agencies are faced with new demands. The skill set required to engage in some cybercrimes means that they are often difficult to detect. Thus, police departments adhering to traditional methods of crime fighting are unlikely to effectively track many of these offenses. Most crimes become known to police not through law enforcement's ability to uncover them, but because they are reported to police by a victim or observer (Mosher et al., 2010). In the case of cyber offenses, many times the victim does not realize that a crime has been committed. Even when the victim is aware, there are other obstacles to reporting (Goucher, 2010). Moreover, in the absence of specialized computer skills, these crimes are often more difficult to investigate even when they are reported to police. Indeed, popular press is awash with stories noting how the criminal justice system and the police in particular are ill-equipped to deal with cybercrime (Joshi, 2015; O'Neill, 2014; Peachey, 2014; Sullivan, 2013) and historically, research suggests that police have focused little of their attention on cybercrime (Goodman, 1997). Yet given the increased importance of cybercrime since 2000 (PERF, 2014), many police agencies have adopted new strategies to combat

cybercrime. In recent years, this has often meant the development of specialized cybercrime units (Hinduja, 2004; Marcum et al., 2010).

While a number of studies have begun to examine law enforcement responses to cybercrime (Broadhurst, 2006; Hinduja, 2004; Katos & Bednar, 2008; Marcum et al., 2010) this literature remains underdeveloped. As such, little research has examined how frequently specialized cybercrime units are used, nor has research examined the characteristics of police agencies likely to make use of specialized cybercrime units. Conceptualizing the development of cybercrime units as a form of police innovation, we examine the organizational predictors of using a specialized cybercrime unit. The current study, using four waves of Law Enforcement Management and Administrative Survey (LEMAS) data, provides a descriptive and organizational analysis of the use of cybercrime units by American police departments. Specifically, we explore trends in the adoption of specialized cybercrime units over time and use an organizational perspective to identify organizational characteristics associated with the use of cybercrime units.

Cybercrime and Policing

Though research suggests parallels in criminal motivation between cybercrime and traditional offending (Higgins & Makin, 2004; Moon, McCluskey, & McCluskey, 2010), the technological nature of cybercrime makes it fundamentally different from a policing perspective than other forms of criminal behavior. Wall (2007) argues that there are broadly, three types of cybercrimes. First, there are offenses where information for the crime is collected electronically, but in the absence of technology, the offense could still take place. Second, there are “true” cybercrimes which are only possible because they occur on the internet. These crimes may

include spamming, phishing, or hacking. Finally, there are hybrid offenses, where traditional crimes are enhanced and expanded through the internet (e.g., identity theft, distribution of child pornography).

Beyond the technical difficulty of investigating cybercrimes, these crimes also challenge law enforcement in that these crimes vary substantially in size and scope. Traditional crime scenes can be thought of as occurring at an address, a city block, or some other type of physical location. Conversely, cybercrime scenes are much broader, as they include all computers or persons that are affected. Some cybercrime scenes often appear temporarily and quickly disappear. Thus, evidence collection is more difficult in the investigation of cybercrimes.
In addition, there are large jurisdictional issues with investigating cybercrimes (Brenner, 2006) as the offenders and victims of cybercrimes may cross both local and national borders. Though issues of evidence integrity and jurisdiction occur in a variety of cases, we suspect that these issues are less common in dealing with traditional offenses than with cybercrimes.

Popular opinion suggests that police are not well prepared to address cybercrime. Dozens of articles are published in major newspapers and magazines each year with titles like "Police clueless on web crime, says chief" (O'Neill, 2014) and "Local level police ill-equipped for cybercrimes, cyber threats" (Sullivan, 2013). A ProQuest Newsstand search for news articles about the police and their inability to address cybercrime produces over 300 results as of November of 2015 with many of these articles citing sources from within police agencies. The notion that contemporary police are still struggling to address cybercrime goes beyond the popular press, however, as research suggests that police leadership and policing experts also acknowledge this problem. For example, a Police Executive Research Forum report titled "The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime" (PERF,

2014) presented numerous quotes from police chiefs, cyber-security specialists, and other experts about the challenges and difficulties in policing cybercrime at the PERF Cybercrime summit in 2014.

Though the media and police leadership suggest that police struggle to address cybercrime, it is worth noting that perceptions of the police's ability handle cybercrime do not prove that police are ill-equipped to address cybercrime. It is possible that public and police leadership perceptions are wrong and that the police are well situated to address cybercrime. In fact, Wall (2008) suggests that public perceptions of cybercrime and cyberpolicing are often erroneous, resulting in a reassurance gap between the public's risk for cybercrime victimization and actual cybercrime activity. Still, these public and leadership perceptions are potentially problematic for police agencies as public perceptions of ineffectiveness may harm the public's trust in the police and reduce perceptions of police legitimacy and professionalism. Indeed, research notes that reassurance gaps are closely linked to a lack of public confidence in police (Millie & Herrington, 2005; Skogan, 2009).

In addition to the increased concern about cybercrime and lack of confidence in the police's ability address cybercrime, the number of reported cybercrimes has increased since the early 2000's. For example, from 2007 to 2012, the FBI's Internet Crime Complaint Center (IC3) reported a 40% increase in cybercrime complaints. The increased concern about crime, increased reporting of cybercrime, and lack of confidence that the police can manage cybercrime create tremendous pressure for police agencies to adapt their enforcement strategies to these types of offenses. This may include developing the skills to efficiently investigate these types of crimes, leading to the apprehension of offenders. An early step in this process is for officers and agencies to identify cybercrime as a significant problem. As such, Senjo (2004) surveyed a number of

municipal police departments to examine officer perceptions of cyber offending. This study found that the majority of officers identified cybercrime as a serious problem, but that their perceptions of the most common types of offenses (pedophilia and credit card fraud) did not match empirical findings from criminological literature, where corporate "insider" offenses are most common.

One potential strategy for addressing cybercrime is through the formation of specialized cybercrime units (Hinduja, 2004; Marcum et al., 2010). A number of studies have examined agency-level responses to cybercrime (Broadhurst, 2006; Hinduja, 2004; Holt et al., 2012; Katos & Bednar, 2008; Marcum et al., 2010). These studies find that communication and networking are paramount in cybercrime investigations (Broadhurst, 2006; Katos & Bednar, 2008). Moreover, training and development of specialized units are among the most important needs of departments for investigating cyber offenses (Hinduja, 2004; Marcum et al., 2010). Broadly, these studies highlight the importance of establishing specialized units to assist with the investigation of cybercrimes. Thus far, however, only a single study has examined the use of specialized cybercrime units by police agencies (Yesilyurt, 2011). This study used contingency theory and institutional theory examine how police agencies used cybercrime units to implement digital forensics practice into the investigation of cybercrime. The current research builds on this prior study and further advances knowledge by further examining the role of time and technology in the use of specialized cybercrime units.

Police Organizations and Innovation

The formation and use of a specialized cybercrime units can be viewed as one type of organizational innovation that police agencies can adopt in response to an actual or perceived

problem with cybercrime. Prior literature on police agencies as complex organizations provide a number of perspectives and hypotheses regarding when and what type of agencies are likely to adopt an innovation. Here, as per Yesilyurt's (2011) prior study on specialized cybercrime units, we employ contingency theory (Donaldson, 2001) and institutional theory (Meyer & Rowan, 1977) to examine the use of specialized cybercrime units. We also examine specific hypotheses derived from Maguire's (2003) theory of police organizations. Though these theories vary in important ways, they all emphasize the concept of organizational structure – that is, the manner in which labor is labor is divided, managed, and accomplished within an organization. We briefly discuss each of the theories and link them to the issue of cybercrime below. For our purposes, we do not view these perspectives as competitive or mutually exclusive explanations and instead posit that these perspectives, used together, can provide a more complete explanation for the formation and use of specialized cybercrime units. Though some research describes contingency theory and institutional theory as rival explanations for organizational structure (Donaldson, 2006), other research suggests that the explanatory power of these perspectives is greatest when used in conjunction (Gupta, Dirsmith, & Fogarty, 1994; Scott, 1987). Indeed, Maguire's (2003: 110) theory of police organizations, though most closely derived from a contingency perspective, includes elements of institutional theory in its explanation for police organizational structure. Research suggests that both factors predict police innovation. For example, Giblin (2006) suggests that both contingency theory and institutional theory variables are important for understanding whether police agencies have a crime analysis unit.

Contingency Theory

Contingency theory suggests that organizations change their structure and behavior in response to the environment in which they work. In other words, the best organizational structure

for a particular organization is one that meets its environmental contingencies (Donaldson, 2001). In terms of policing, this suggests that police agencies respond to localized perceptions and demands to address concerns. Research links environmental pressures to a change in police organizational structure, suggesting that agencies become less vertically and horizontally differentiated when dealing with more environmental contingencies (Zhao, Ren, and Lovrich, 2010). Other research, though not always framed explicitly in a contingency perspective, suggests that the adoption of specific innovations by police agencies is linked to environmental contingencies. For example, structural complexity (Damanpour, 1991; 1996; Roberts et al., 2012), legislation (Drew, 2011), grant receipt (Helms & Gutierrez, 2007), pressure from the community (Katz, 2001), age of the organization (Katz et al., 2002), form of government (Morabito, 2010), technology (Darroch & Mazerolle, 2012), and department size (Morabito, 2010; Roberts et al., 2012) are all correlated with the adoption of police innovation.

For cybercrime and cyberpolicing more specifically, contingency theory suggests that as cybercrime becomes more prevalent and costly, local police departments are likely to devote greater resources to policing those types of crime, which may include the creation of specialized units. Indeed, one key hypothesis of the current research is that police agencies are more likely to use cybercrime units as complains about these types of offenses increase.

> Hypothesis 1: Cybercrime complaints are positively related to the use of cybercrime units by police agencies.

Institutional Theory

Institutional theory argues that organizations change and adapt to maintain their legitimacy (Meyer & Rowan, 1977). Institutional theory emphasizes that in order to survive, agencies must structure themselves in a manner that meets accepted norms. Over time, this results in institutional isomorphism: the tendency for organizations to become similar despite

operating in different environments and contexts (DiMaggio and Powell, 1983). In terms of policing, institutional theory has been applied to explain how and why police agencies change and fail to change (Crank, 2003). Institutional theorists have suggested that police agencies select approaches in order to maximize legitimacy. Research links institutional pressures to a number of policing-related outcomes, including the spread of community policing (Crank, 1994; Oliver, 2000) and the backlash to racial profiling (Engel, Calnon, & Bernard, 2002). Other research links institutional pressures to the adoption of innovations. For example, Katz (2001) suggested that gang units appeared to emerge in response to community pressure (a contingency explanation), the formation of the gang units can also be viewed as more of a ceremonial response that maintains police legitimacy rather than as a response that is designed to actually address the gang problem.

For cyberpolicing, the institutional perspective suggests that agencies are more likely to use specialized cybercrime units over time. This is because, as noted in the introduction to this paper, it is likely that police agencies feel increased pressure over time to adopt anti-cybercrime strategies, even if historically the institution of policing has resisted tackling computer-related crimes (Goodman, 1997). Over time, this could result in police agencies forming specialized cybercrime units even if they have little need to do so, similar to the arguments that have been levied against the proliferation of SWAT (Kappeler & Kraska, 2015) and gang units (Katz & Webb, 2006). Moreover, as more agencies use specialized cybercrime units, institutional theory suggests this practice becomes an accepted or legitimated response to cybercrime.

> Hypothesis 2: Agencies are more likely to use specialized cybercrime units in more recent years.

Maguire's Theory of Police Organizational Structure

Maguire's (2003) theory of police organizational structure suggests that organizational context, complexity, and control are central to understanding the manner in which police agencies manage and divide labor. Specifically, Maguire (2003) states that organizational context predicts organizational complexity, and that organizational context and complexity predict organizational control. Maguire's theory builds off of both prior theorizing on police organizations and a variety of organizational perspectives, including contingency theory and institutional theory. The concept of organizational complexity, in particular, builds off of Langworthy's (1986) work on the organizational structure of police agencies, suggesting that this structure can be understood in terms of vertical, horizontal, and functional differentiation. The use of specialized divisions, like cybercrime units, reflects an increased level of functional differentiation. Organizational control, conversely, is expected to be caused by organizational context and complexity, hence it is not discussed it in more detail here.

Given that the adoption of new organizational units, like specialized cybercrime divisions, reflects an increase in organization complexity, organizational context is hypothesized to predict the use of specialized units. On the surface, this argument is very similar to a contingency theory explanation, though Maguire's theory allows for organizations to adapt either in hopes of addressing a problem (the contingency explanation) or for reasons of legitimacy and institutional pressure (the institutional explanation).

Maguire's (2003) theory links a variety of dimensions of organizational context to organizational complexity. These include organizational size and organizational technology, which further consists of material technology, task scope, and task routineness. Specifically, Maguire's (2003) theory suggests that each of these aspects of organizational context is positively related to functional differentiation. That is, organizations which are larger, face a

great task scope, and experience more task routineness are all more likely to be more functionally differentiated and therefore are more likely to use specialized units.

In terms of size, we expect that larger agencies are more likely to form cybercrime units. This is partially because larger agencies may process a larger volume of crimes with internet or computer aspects, but also because larger agencies have more resources and greater access to technical personal to address the special challenges associated with cybercrime and because "larger police organizations, with more personnel to juggle, must implement some degree of structural complexity in order to improve coordination, reduce conflict, and/or achieve tighter organizational control" (Maguire, 2003, p. 74).

Hypothesis 3: Larger agencies are more likely to use specialized cybercrime units.

Organizational technology encompasses the ideas of both material and social technology. Though Maguire (2003) focuses more on social technology than material technology, there is reason to believe that material technology is also quite important. Research on police organizations suggests that prior use of advanced technologies predicts future use of other technologies. For example, research suggests that police agencies with preexisting interests in mapping and with expertise in related technologies were most likely to be early adopters of crime mapping technologies and strategies (Charmard, 2006; Weisburd & Lum, 2005). Similarly, Skogan and Hartnett (2005) find that prior experience with police database management systems predicted the adoption of new database systems in Chicago. Given the clustering of innovations, some police organizations can be thought of as early adopters. These early adopters are police agencies which are more willing to experiment and implement technological innovations. Applied to cyberpolicing, it is possible that police departments which

already make use of a broad range of technological advances may be more likely to form specialized cybercrime units.

> Hypothesis 4: Agencies using a broader set of material technologies are more likely to use specialized cyberpolicing units.

Social technology consists of both task scope and task routineness (Maguire, 2003). Task routineness reflects the degree to which an organization addresses tasks or problems that are routine in nature. Maguire's suggests that agencies with a greater proportion of officers assigned to patrol duties are more likely to specialize. As front-line law enforcement officers engage in the routine task of patrol-oriented policing, specialized units are needed to address non-routine problems and tasks. Though Maguire's supported his argument about patrol and specialization with LEMAS data, it is worth noting that in cases where the vast majority of officers are assigned to patrol that there will be few officers left for specialized units. Therefore, we examine hypothesis 5A (that the proportion of officers patrol is positively associated with the use of specialized cybercrime units) and hypothesis 5B (that there is a curvilinear relationship between the proportion of officers assigned to patrol and the use of a specialized cybercrime unit).

> Hypothesis 5A: Agencies with larger proportions of officers assigned to patrol duties are more likely to have specialized cybercrime units.

> Hypothesis 5B: The relationship between the proportion of officers assigned to patrol duties and the use of a specialized cybercrime is curvilinear such that agencies with nearly all officers assigned to patrol are less likely to utilize specialized cybercrime units.

Task scope, the other aspect of social technology, refers to the breadth of an organization's mission. Maguire (2003) argues that agencies addressing a greater variety of tasks are more likely to functionally differentiate, as the use of specialized units may be a rational response to working in an environment with varied demands. Research suggests that there are important policing differences by agency type (Falcone & Wells, 1995; Reisig & Correia, 1997)

and, given the jurisdictional issues associated with cybercrime, it may be the case that specific agencies may be more likely to engage in cyberpolicing. As such, we expect county and state level agencies to be more likely to have cybercrime units. This is both because the vast majority of municipal police agencies in the United States are quite small and may be less likely to have cybercrime problems, but also because the cross-jurisdictional nature of cybercrime may create pressure for agencies with broader geographic reaches to address the problem. Moreover, researchers note that county-level police agencies are typically "characterized by a broader and more diverse assortment of legal responsibilities than those associated with local policing" (Falcone & Wells, 1995, p. 130). It is likely that state-level agencies deal with an even broader set of responsibilities and that this broader set of responsibilities is perhaps more likely to include cybercrime investigations.

> Hypothesis 6: State and county agencies are more likely to have specialized cybercrime units than municipal agencies.

Methods

In order to analyze the use of specialized cybercrime units and to test the above hypotheses, we provide a descriptive and exploratory analysis. We begin by describing the data available to examine cybercrime units in policing and describe general trends and patterns in the use of specialized cybercrime units since 2000. Then, building off of the theoretical perspectives described above (contingency theory, institutional theory, and Maguire's (2003) theory of police organizations), we examine the degree to which organizational and environmental factors are associated with the use of specialized cybercrime units.

Data for this study were primarily drawn from the 2000, 2003, 2007, and 2013 Law Enforcement Management and Administrative Statistics (LEMAS) surveys. The LEMAS is a survey of police agencies which include items regarding organizational characteristics of

departments, including the presence of innovations such as cyberpolicing units. We include data from four different waves of LEMAS data, as each of these waves contained questions regarding the use of specialized cyberpolicing units and, as previously discussed, we expect time to be an important predictor of the adoption of cybercrime units. In total, we examine data from 5,324 observations over the course of 4 years. As LEMAS data captures most large agencies and a random sample of a smaller agencies, some of these observations are repeated measures. In total, the analyses represent a total of 3,097 different agencies with each agency appearing in the dataset 1.7 times on average. Though much research on police agencies focuses on large municipal departments, we consider all police agencies for which there LEMAS data available.

Dependent Variable

The outcome variable in this study is a measure of whether polices agencies operate a specialized unit for cybercrime. This is a dichotomous variables where departments with a specialized full-time personnel or part time personnel are coded as "1", while agencies where cybercrime is not addressed are coded as "0." Figure 1 shows a general upward trend in the proportion of agencies using cybercrime units over time, with an interesting dip in 2013. It is unclear if the 2013 decline is reflective of a genuine decrease (perhaps reflecting the budget crunch experienced by many police agencies in the wake of the great recession) or this is reflective of changes in the LEMAS instrument. The number of missing cases for the 2013 LEMAS item measuring the presence of a cybercrime unit decreased sharply from prior LEMAS estimates, so it is possible that changes in the administration of the 2013 LEMAS somehow shifted agencies from being recorded as missing to recorded as a 0 (no cybercrime unit). Regardless, the overall trend demonstrates that the use of specialized cybercrime units has

increased since 2000, though the overall trend is somewhat undetermined given the issues with the 2013 LEMAS data.

FIGURE 1 ABOUT HERE

The formation of specialized units is not the only response that police agencies can marshal in response to cybercrime concerns. For example, police can also dedicate certain personnel or formulate specific policies and procedures to address cybercrime. LEMAS data also records information on which agencies did not address cybercrime with any specialized personnel or procedures. Analyzing this data supports the claim that more and more police agencies are dedicating resources to address cybercrime over time, as 51% of agencies did not address cybercrime at all in 2000, while only 15.5% of agencies failed to address cybercrime in 2013.

Independent Variables

Having established that there has been a dramatic increase in the use of specialized cybercrime units over time, our next focus is on explaining which types of police agencies have adopted the use of these units. Specifically, we examine the degree to which contingency theory, institutional theory, and Maguire's (2003) theory of police organizations can explain the pattern of cybercrime units across police departments. Here, we operationalize key measures as applied to the six hypotheses described above.

Contingency theory suggests that organizations change and adapt to meet environmental pressures. In order to address this possibility, we include a measure of cybercrime complaints as a proxy for cybercrime and as our basic measure of environmental pressure. We utilize data drawn from the FBI's Internet Crime Complaint Center (IC3), which collects information about cybercrime complaints and produces annual reports which summarize the number of cybercrime

incidents reported per state. For the current research, we include cybercrime complaints per 100,000 people recorded in 2000, 2003, 2007, and 2013. These state-level estimates are merged with each agency for the appropriate years.

Relatedly, institutional theory suggests that organizations change and adapt to maintain their organizational legitimacy (Meyer & Rowan, 1977). Given the increase in cybercrime complaints over time and the increased media and public focus on cybercrime, we argue that this is largely a time-driven process. In other words, agencies likely feel pressure to form cybercrime units over time in order to show that they are seriously addressing cybercrime and demonstrate their organizational legitimacy. In order to account for this, we include dummy variables for each year of LEMAS data.

A number of potential measures of organizational size exist in the LEMAS data, including the number of full-time sworn officers, the size of the population served, and the operating budget of the agency. The log of the budget, sworn officer, and population variables are highly correlated with each other (each correlation is .91 or greater), indicating that these variables all tap into the same underlying concept. We utilize the natural log of the population served as our measure of agency size, as this provides information not only on the size of an agency, but also provides descriptive information about the types of cities, counties and states covered by our data. It should be noted that the choice of size measure had no impact on the pattern or direction of statistically significant results.

In order to measure organizational technology, we include measures of both material technology and social technology. Our measure of material technology reflects officer access to MVD, driving, and criminal history records on computers while in the field. We combined these three binary indicator variables into a simple additive index (α = 0.88). It is not that we

necessarily believe that use of these specific technologies lead in a causal fashion to the formation of cybercrime units. Instead, we view this index as a general, but limited, measure of organizational technological adoption and hypothesize, as supported by the early adoption literature (Skogan & Harnett, 2005; Tolbert & Zucker, 1983; Weisburd & Lum, 2005), that agencies which already use and have expertise in advanced material technologies are more likely to form polices to address other advanced technological outcomes. In other words, agencies which have already invested in and experimented with technology are more likely to invest in and engage in the social and material technologies needed to address other policing issues (including cybercrime).

Social technology consists of both task routineness and task scope (Maguire, 2003). We measure task routineness as the percentage of full-time sworn officers assigned to patrol duties and, as discussed in hypothesis 5B, include a quadratic term as an additional independent variable. Task scope is measured with a dummy variable indicating whether a law enforcement agency is municipal, county, or state-level.

In addition to addressing the type of agency, we include the number of specialized units used within a given agency as a control variable. Though this measure is typically seen as an outcome of task scope and routineness, we include it as a predictor variable as it seems plausible that departments characterized by greater levels of specialization are also more likely to approach cyberpolicing with specialization as well. That is, the same factors which result in organizational specialization in general may also be related to the use of specialized cybercrime units specifically. While various waves of LEMAS data have included a number of specialized unit questions, only 8 specific problems or issues have been asked in all four waves of the LEMAS data used in this project. In addition to our dependent variable (cybercrime), all four

waves of LEMAS data have asked whether an agency has a specialized unit dedicated to the following problems or areas: bias crimes, child abuse, intimate partner violence, driving while intoxicated, gang crime, juvenile crime, and victims' issues. Using these 7 indicators, we constructed an additive scale ranging from 0 (they did not address any of these issues or problems with special units) to 7 (they addressed all of the above issues with special units) (α = 0.79).

Descriptive statistics for dependent and independent variables are presented in Table 1. Aggregated over the four years of LEMAS data, about one-quarter of all law enforcement agencies utilize specialized cybercrime units. The data are disproportionately drawn from the 2013 LEMAS, which contained far fewer missing cases than prior LEMAS waves. As expected, the majority of agencies within sample are municipal departments, with progressively smaller proportions representing county and state agencies.

TABLE 1 ABOUT HERE

Findings

We present both bivariate and regression-based results. The bivariate results provide a simple preliminary test for each of the hypotheses, while the regression results allow for a comparison of factors while invoking the concept of statistical control.

Bivariate Results

Table 2 presents a summary of all bivariate results. For the numeric variables, we present correlation coefficients between each variable and the presence of a specialized cybercrime unit. For the categorical variables, we estimate both Chi-Squared tests of independence and

correlations between the dummy variables and the presence of a cybercrime unit (though only the correlation values are presented in the table).

The results of the bivariate analyses broadly support both the contingency (hypothesis 1) and institutional (hypothesis 2) theory derived hypotheses. The cybercrime complaint rate is positively and statistically significantly associated with the presence of a cybercrime unit. Similarly (and given Figure 1), there is unsurprisingly a statistically significant relationship between year and the presence of a cybercrime unit (χ^2= 225.57), though the correlations between the year dummy variables and the cybercrime unit variable suggest that the difference was most marked in 2007 and 2013.

TABLE 2 ABOUT HERE

The hypotheses linking organizational characteristics derived from Maguire's (2003) theory to the presence of a cybercrime unit are also largely supported. There is a positive statistically significant correlation between size (r =.32) and technology (r =.21) and the use of a specialized cybercrime unit, lending support to hypotheses 3 and 4 respectively. Similarly, there is a relationship between agency type and the presence of a cybercrime unit (χ^2= 44.09). The correlational analysis and descriptive statistics suggest that this relationship is driven by state-level agencies, as a far greater proportion of state agencies (48%) make use of cybercrime units than county (26%) or municipal agencies (23%), supporting for hypothesis 6. It is worth noting that the specialization index is also significantly related to the use of a cybercrime unit, indicating that this control variable is important to include in our models.

Interestingly, hypothesis 5 is not supported here. In fact, the relationship between the percentage of officers assigned to patrol duties and the presence of a cybercrime unit is negative and statistically significant (r =-.07). This suggests that as an agency faces an environment

characterized by more and more of a routine task, they are less likely to form specialized cybercrime units, though the magnitude of this coefficient is quite small.

Regression Results

As the cybercrime variable is dichotomous, we utilize a logistic regression approach. In order to account for the non-independence of our data due to the fact that some agencies are measured repeatedly from wave to wave of the LEMAS data and because our cybercrime complaint data is at the state-level, we present the results from a random effects logistic regression model in which a random intercept is predicted for each agency. Effectively, this is an unbalanced repeated measures logit model, in which each agency is measured up to four times, where random effects are used to measure cluster effects and year dummy variables used to capture time effects. Substantively, these results are similar to a standard logistic regression approach in terms of the sign and statistical significance of the model coefficients, though the AIC for the random effects model indicates a modest improvement in model fit ($AIC_{random\text{-}effects}$ = 3943.40 vs AIC_{logit} = 4071.98). The random-effects model also reveals that there is considerable within-class (police agency) correlation (ICC = 0.39), and so we report the random effects models instead of the standard logit models. Given that the cybercrime complaints variable is measured at the state-level, it was also possible to view our data a three-level mixed-effects logistic regression (in which years were nested within agencies which were nested within states). Supplementary analysis suggests that a three-level model did not substantively change the model results or improve fit, so the more parsimonious random effects logistic regression model is presented in Table 3 instead.

TABLE 3 ABOUT HERE

Overall, the model provides general, but not universal, support for the hypotheses. The basic contingency theory expectation, that agencies experiencing more cybercrime complaints are more likely form specialized cybercrime units, is unsupported. This suggests that while cybercrime complaints appeared important from a bivariate perspective, cybercrimes do not remain a significant predictor of the use of a cybercrime unit controlling for other factors in the logistic regression model. Other contingency factors, like size and task scope, remain important predictors in the regression model.

The year dummy variables remain significant predictors of the use of a cybercrime unit, indicating statistically significant differences between each year and the reference year (2000). Moreover, the size of the coefficients increases progressively with time units. Specifically, the odds that a police agency has a cybercrime unit are 175% greater in 2003 than in 2000 (*OR* = 2.75), 362% greater in 2007 than in 2000 (*OR* = 4.62) and 830% greater in 2013 than in 2000 (*OR* = 9.30), controlling for other variables in the model. This indicates that specialized cybercrime units are more likely to be used in recent years, lending support to the idea that having a dedicated cybercrime unit is becoming normative police agencies. Further, these year-effects are not simply reflective of underlying organizational characteristics or increases in cybercrime complaints.

In terms of size, the results suggest that larger agencies are significantly more likely to use specialized cybercrime units than smaller agencies. Specifically, a 1-unit increase in the natural log of population served is associated with an expected increase of 65% in the odds that an agency has a cybercrime unit (*OR* = 1.65). Technology remains a significant predictor of having a specialized cybercrime unit, controlling for other factors, providing support for hypothesis 4. Specifically, the odds that an agency has a cybercrime unit are 16% (*OR* = 1.16)

greater in agencies that that score 1 point higher on the technology index. Similarly, the percentage of the department assigned to patrol duties is positively related to the use of a cybercrime division, while the quadratic term for patrol officers is negatively associated with the use of a cybercrime division. This provides support for hypothesis 5b, which suggests that task routineness increases the likelihood of using a specialized division to a certain point, but that when a very large proportion of officers are assigned to patrol the effect becomes negative. Here, the percentage of officers assigned to patrol is positively related to the use of a cybercrime unit until it reaches about 83% ($.03/-3.6x10^{-4}$).

The regression results for agency type conform to the bivariate results and mixed provide support for hypothesis 6. State-level police agencies are significantly more likely to have cybercrime units, controlling for other factors. Specifically, the expected odds that a state-level agency has a cybercrime unit are 278% (*OR* = 3.78) greater than a municipal agency, while there are no significant differences between municipal and sheriff agencies.

Lastly, the specialization index remains a statistically significant and positive predictor of the presence of a specialized cybercrime unit. The odds that an agency has a cybercrime unit are 112% (*OR* = 2.12) greater in agencies that that score 1 point higher on the specialization index, controlling for other factors in the model.

Conclusions and Discussion

The findings of this study highlight the spread of specialized cybercrime units over time. From 2000 to 2013, the use of cybercrime units has tripled (from 9% to around 27.5%). Clearly, many police agencies view the formation and maintenance of a cybercrime unit as a viable or at least acceptable strategy to use against cybercrime. As more and more agencies form these units, institutional theory suggests there is likely to be increased isomorphic pressure for other units to

form these units as well. Given current trends in cybercrime and internet use, we expect cybercrime units to become more common in the future.

All organizational variables, including agency size, type, percentage of officers assigned to patrol, material technology use, and specialization are statistically significant predictors of the use of a cybercrime unit. Specifically, larger agencies are more likely to have a cybercrime unit than smaller agencies, state-level agencies are more likely to have a cybercrime unit than municipal and county agencies, and agencies with increased advanced material technology use and specialization are more likely to have cybercrime units than other agencies. The patrol results are more nuanced, as they are indicative of a curvilinear relationship between the percentage of officers assigned to patrol and the use of a cybercrime unit.

These results largely support the theoretically informed hypotheses. Larger agencies may have more resources to start and support a cybercrime unit and may have a greater need for cybercrime units as they may experience more cybercrime. Similarly, state-level agencies may have a greater need for cybercrime units given the geographically diverse nature of cybercrime. Further, there is research suggesting that state and, indeed, federal law enforcement agencies play an important role in providing resources for cybercrime investigations for smaller agencies (PERF, 2014). The results also highlight the role of specialization in policing: Specialization begets specialization. More specialized policing agencies, that is, those who use specialized units to address a wide variety of other problems, are also more likely to use specialization as the basis for their strategy for addressing cybercrime.

The percentage of officers assigned to patrol and the technology results are perhaps the most interesting of the organizational findings in the study. In terms of the patrol results, the basic result is supportive of Maguire's (2003) theorized hypothesis that increases in task

routineness are associated with organizational complexity, though the curvilinear result suggests that there is a practical limit to that relationship. That is, when the vast majority of officers are assigned to patrol, specialized units may become unviable. This suggests that the relationship between task routineness and innovation may be curvilinear, though research in other domains is needed to further evaluate this possibility.

Regarding technology, results suggest that police agencies with more expertise and experience in technological issues are likely to be at the forefront of responding to cybercrime. Indeed, prior research suggests that much the same is true for police agencies and crime mapping and database technologies (Charmard, 2006; Skogan & Hartnett, 2005; Weisburd & Lum, 2005). Yet the technology index used in this study contained technology variables that are loosely, at best, related to the concept of cybercrime. Each part of this index reflected access to data from a patrol car, an idea that is not easily connected to cyberpolicing. Despite the imprecision of this tool, this index was significantly associated with the presence of a specialized cybercrime unit in both the bivariate and regression results. To the degree that the formation of a cybercrime unit is a form of engaging in both social and material technologies for police agencies, this suggests that there is a subset of experimental and technologically sophisticated police agencies which are likely to be at the forefront of many police innovations. Future research on police innovation would benefit from examining the link between technological engagement and other contemporary advances in policing strategy and technology. It very well could be the case that the same technologically sophisticated agencies likely to start cybercrime units are also likely to be early adopters of other innovations, like body-worn cameras.

Though the current research shows correlates of cybercrime units, there is more research to be done in this area. Organizational theorists suggest that the factors which predict early

adoption and late adoption are different. For example, research links the early adoption to organizational characteristics, including size and resources (Skogan & Harnett, 2005; Tolbert & Zucker, 1983; Weisburd & Lum, 2005), a result which is also found in other studies of police innovation (Morabito, 2010; Roberts et al., 2012). Conversely, organizational scholars link late adoption to broader forces, like the widespread acceptance or legitimation of a particular innovation (Tolbert & Zucker, 1983). Though the LEMAS data do not provide specific dates for which cybercrime units are formed, it may be possible to use this data to development proxy models which examine the organizational and environmental predictors of early and late adoption of specialized cybercrime units. Further, while organizational practices likely matter, there are reasons to expect police leadership and the availability of funding and especially federal grants to matter here as well. LEMAS data do not include these measures, though future research should explore other avenues of investigating these factors.

A key question moving forward is the efficacy of specialized cybercrime units for addressing cybercrime and the broader consequences of the proliferation of cybercrime units. The specialist versus generalist tension is one of the more pressing topics in all of policing and is embedded in issues related to community policing, police strategies, and police efficiency more broadly (Falcone & Wells, 2002). The recent PERF (2014) summit on cybercrime revealed this tension, as police leaders were split on whether to address cybercrime with a special unit, to train patrol officers to deal with cybercrime, or to engage in a mixture of these strategies. There is evidence from research on gang units that specialized units do little to quell the problems they were formed to face (Katz & Webb, 2006), though some argue that this may be largely an implementation issue (Decker, 2007). Moreover, there is evidence that specialized units become focused more on maintaining their legitimacy than on addressing the underlying problem (Katz,

2001) and that the formation of these units can have large, unintended consequences (Kraska, 2007). Yet, it seems premature to transfer these findings to the topic of cybercrime. While the use of cybercrime units could potentially have deleterious effects on privacy and how police gather intelligence, it is also quite possible that some cybercrimes require a level of technological expertise that goes beyond the reasonable training and background expectations for most police officers. In that regard, cybercrime units may be an important feature for police moving forward, given the increased use and reliance on the internet.

Unfortunately, current data are ill-suited for examining the degree to which cybercrime units are effective at combating cybercrime. The cybercrime complaints measure used in this study reflects state-level trends in complaints. Even if complaint data could be disaggregated to the agency level, the potential for endogeneity is clear: police might form cybercrime units in response to complaints and the presence of these units might encourage to the public to make complaints about cybercrimes that they otherwise might have ignored. It seems that clearance rates for cybercrimes before and after the formation of a cybercrime unit would be a much better measure of the success of cybercrime units, though this will involve new data collection efforts. Jurisdictional issues are likely to prove a challenge here, as the geographic distance between offenders and victims can result in questions about which agency should lead a particular investigation and about the police's ability to investigate specific crimes. Still, this could prove a fruitful avenue for future case study research and will be important for assessing the value of cybercrime units more broadly. Related to this, future research exploring cybercrime statutes, the link between these statutes and cybercrime investigation strategies, and how police agencies and prosecutors navigate these jurisdictional challenges is likely to be quite valuable.

There are some key limitations which should be noted for the current study. First, our results are largely descriptive and exploratory. Given the data available and our inability to specify exactly when a cybercrime unit was started, we do not make any causal statements. Second, there are important limitations of the LEMAS data. First, LEMAS data do not include measures of all of the organizational factors that might be related to the use of a specialized cybercrime unit. For instance, Maguire (2003) also suggests that organizational age is related functional differentiation, but this was not in all LEMAS waves.

Second, even for questions asked in each wave, there are important wave to wave differences in LEMAS data that limited our analysis. These differences greatly limited the number and type of variables we could utilize in the analysis and, in particular, limited our ability to more thoroughly examine the role of technology and specialization. Though we feel it was important to utilize the most recent LEMAS data available for the current project given that cybercrime is increasing in importance, the 2013 LEMAS was particularly problematic, as the questions included in this measure were substantially different than prior LEMAS years.

Matusiak et al. (2014), in their systematic review of research utilizing LEMAS data, noted that LEMAS data through 2007 suffered from "inconsistency in survey question format and variables" which "impedes the ability of researchers to conduct time series investigations related to police organizational structure." (p. 640). The 2013 LEMAS appears to continue this trend and we hope that Matsuiak et al.'s (2014) call to standardize the core component of LEMAS data in the future is heeded. Beyond this, prior waves of LEMAS data contained much larger counts of missing data. In the 2013 LEMAS, missing data is fairly rare. Where there was a data processing decision which impacted how the 2013 LEMAS data were coded or improved response rate procedures, these differences are notable. To guard against this, we estimated our

models with only the 2000, 2003, and 2007 data. The results were substantively quite similar, though the effects of agency type fell from significance in these models.

Lastly, the measurement of cybercrime complaints used in this study is limited. This state-level measure likely masks important within state variation in complaints and thus introduces measurement error in the model. It is also not clear from IC3 documentation whether complaint data are always forwarded to local agencies and, that when forwarded, that agencies are required to investigate these crimes. Though the bivariate analyses indicate that cybercrime units were more likely to be used in agencies where there were more cybercrime complaints, it is possible that this was an artifact of time (there are positive and statistically significant correlations between complaints and the year dummy variables). Moreover, the complaints variable did not remain statistically significant in the regression model. If cybercrime complaints are a useful proxy for cybercrime itself, then taken at face value, these suggests that proliferation of cybercrime units is happening even when agencies are not facing a high volume of cybercrime. This further suggests that the adoption and formation of a cybercrime unit may have more to do with the institutional pressure to engage in normative policing practices and less to do with responding to a specific environmental demand to investigate more cybercrimes. Given the limitations of the cybercrime complaint data and that many other contingency theory related variables were significant in this analysis, we caution against this devaluation of the contingency theory perspective. Better, agency-specific data on cybercrimes and/or cybercrime complaint data are needed to examine the degree to which the formation of cybercrime units are the result environmental need for these units or, if as we have argued here, that cybercrime units are proliferating over time as a normative practice in policing.

Despite these limitations, the findings from this study are important in that they demonstrate that the use of specialized cybercrime units has increased over time and that this increase is at least partially explained by organizational factors like size, agency type, technology, and specialization. Broadly speaking, the current results provide general support for the hypotheses derived from Maguire's (2003) theory of police organizations and to institutional theory, as well as to prior research on early adoption of organizational innovations within police agencies (Morabito, 2010; Roberts et al., 2010; Skogan & Harnett, 2005; Tolbert & Zucker, 1983; Weisburd & Lum, 2005). These results also suggest that some aspects of these theories may need to be further refined. For instance, these results suggest that the hypothesized relationship between task routineness and innovation is curvilinear and not simply positive linear. Further, the results of the current research add to prior research on police organizations which suggests that policing cannot be understood without a focus on organizational theory and structure. We hope that the current research provides the foundation for future research on adoption of police organizational and technological innovations, as well as more directed research on the effectiveness of cybercrime strategies.

References

Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, law and social change*, *46*(4-5), 189-206.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*, 408-433. doi: 10.1108/13639510610684674

Chamard, S. (2006). The history of crime mapping and its use by American police departments. *Alaska Justice Forum*, *43*.

Crank, J. P. (1994). Watchman and community: Myth and institutionalization in policing. *Law & Society Review*, *28*, 325.

Crank, J. P. (2003). Institutional theory of police: a review of the state of the art. *Policing: An International Journal of Police Strategies & Management*, *26*(2), 186-207.

Damanpour, F. (1996). Organizational complexity and innovation: Developing and testing multiple contingency models. *Management Science*, *42*, 693-716. doi: 10.1287/mnsc.42.5.693

Damanpour, F. (1991). Organizational innovation: A meta-analysis of effects of determinants and moderators. *Academy of Management Journal*, *34*, 555-590. doi: 10.2307/256406

Darroch, S. & Mazerolle, L. (2012). Intelligence-Led policing: A comparative analysis of organizational factors influencing innovation uptake. *Police Quarterly*, *16*, 3-37. doi: 10.1177/1098611112467411

Decker, S. H. (2007). Expand the use of police gang units. *Criminology & Public Policy*, *6*, 729-733.

DiMaggio, P., & Powell, W. W. (1983). The iron cage revisited: Collective rationality and

institutional isomorphism in organizational fields. *American Sociological Review*, *48*(2), 147-160.

Donaldson, L. (2001). *The Contingency Theory of Organizations*. Sage.

Donaldson, L. (2006). The contingency theory of organizational design: challenges and opportunities. In Organization Design (pp. 19-40). Springer US.

Drew, J. M. (2011). Police responses to the methamphetamine problem: An analysis of the organizational and regulatory context. *Police Quarterly, 14*, 99-123. doi:10.1177/1098611111404017

Engel, R. S., Calnon, J. M., & Bernard, T. J. (2002). Theory and racial profiling: Shortcomings and future directions in research. *Justice Quarterly*, *19*(2), 249-273.

Falcone, D. N., & Wells, L. E. (1995). The county sheriff as a distinctive policing modality. *American Journal of Police*, *14*, 123-149. doi: 10.1108/07358549510111983

Falcone, D. N., Wells, L. E., & Weisheit, R. A. (2002). The small-town police department. *Policing: An International Journal of Police Strategies & Management*, *25*, 371-384. doi: 10.1108/13639510210429419

Giblin, M. J. (2006). Structural elaboration and institutional isomorphism: The case of crime analysis units. *Policing: an international journal of police strategies & management*, *29*(4), 643-664.

Goodman, M. D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law & Technology*, *10*, 465-694.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, *2010*, 16-18.

Gupta, P. P., Dirsmith, M. W., & Fogarty, T. J. (1994). Coordination and control in a

government agency: Contingency and institutional theory perspectives on GAO audits. *Administrative Science Quarterly*, 264-284.

Helms, R. & Gutierrez, R. S. (2007). Federal subsidies and evidence of progressive change: A quantitative assessment of the effects of targeted grants on manpower and innovation in large U.S. police agencies. *Police Quarterly, 10*, 87-107. doi: 10.1177/1098611106296480

Higgins, G. E., & Makin, D. A. (2004). Self-Control, Deviant Peers, and Software Piracy. *Psychological Reports*, *95*(3), 921-931. doi: 10.2466/pr0.95.3.921-931

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management, 27*, 341-357. doi: 10.1108/13639510410553103

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2015). *Policing cybercrime and cyberterror.* Durham, NC: Carolina Academic Press.

Joshi, P. (2015, October 16). Cyber-crime on the increase in the UK. *International Business Times*. Retrieved from http://www.ibtimes.co.uk/uk-cyber-crime-increase-1524219

Kappeler, V. E., & Kraska, P. B. (2015). Normalising police militarisation, living in denial. *Policing and Society*, *25*, 268-275. doi: 10.1080/10439463.2013.864655

Katos, V. & Bednar, P. M. (2008). A cyber-crime investigation framework. *Computer Standards & Interfaces, 30*, 223-228. doi:10.1016/j.csi.2007.10.003

Katz, C. M. (2001). The establishment of a police gang unit: An examination of organizational and environmental factors. *Criminology, 39*, 37-74. doi: 10.1111/j.1745-9125.2001.tb00916.x

Katz, C. M., Maguire, E. R., & Roncek, D. W. (2002). The creation of specialized gang units: A

macro-level analysis of contingency, social threat and resource dependency explanations. *Policing: An International Journal of Police Strategies & Management, 25*, 472-506. doi: 10.1108/13639510210437005

Katz, C. M., & Webb, V. J. (2006). *Policing gangs in America*. Cambridge University Press.

Kraska, P. B. (2007). Militarization and policing—Its relevance to 21st century police. *Policing, 1*, 501-513. doi: 10.1093/police/pam065

Maguire, E. R. (2003). *Organizational structure in American police agencies: Context, complexity, and control*. SUNY Press.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cyber crime. *International Journal of Police Science and Management, 12*, 516-515. doi: 10.1350/ijps.2010.12.4.201

Matusiak, M., Campbell, B., & King, W. (2014). The legacy of LEMAS: Effects on police scholarship of a federally administered, multi-wave establishment survey. *Policing: An International Journal of Police Strategies & Management, 37*, 630-648. doi: 10.1108/PIJPSM-12-2013-0117

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*, 340-363. doi: 10.1086/226550

Millie, A., & Herrington, V. (2005). Bridging the gap: understanding reassurance policing. The *Howard Journal of Criminal Justice*, 44(1), 41-56.

Morabito, M. S. (2010). Understanding community policing as an innovation: Patterns of adoption. *Crime & Delinquency, 56*, 564-587. doi: 10.1177/0011128707311643

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and

computer crime: An empirical test. *Journal of Criminal Justice*, *38*(4), 767-772. doi:10.1016/j.jcrimjus.2010.05.003

Mosher, C. J., Miethe, T. D., & Hart, T. C. (2010). *The mismeasure of crime*. Sage Publications.

Oliver, W. M. (2000). The third generation of community policing: Moving through innovation, diffusion, and institutionalization. *Police Quarterly*, *3*(4), 367-388.

O'Neill, S. (2014, April 26). Police clueless on web crime, says chief. *The Times*. Retrieved from http://www.thetimes.co.uk/tto/news/uk/crime/article4073529.ece

Peachy, P. (2014, December 7). Police 'failing to train key staff to fight growing threat of cyber crime.' *Independent*. Retrieved from http://www.independent.co.uk/news/uk/crime/police-failing-to-train-key-staff-to-fight-growing-threat-of-cyber-crime-9909334.html

Police Executive Research Forum. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime*.

Reisig, M. D., & Correia, M. E. (1997). Public evaluations of police performance: An analysis across three levels of policing. *Policing: An International Journal of Police Strategies & Management*, *20*, 311-325. doi: 10.1108/13639519710169153

Rege-Patwardhan, A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies*, *22*, 261-271. doi: 10.1080/14786010903166965

Roberts, A., Roberts J. M., & Liedka, R. V. (2012). Elements of terrorism preparedness in local police agencies, 2003-2007: Impact of vulnerability, organizational characteristics, and contagion in the post-9/11 era. *Crime & Delinquency*, *58*, 720-747. doi: 10.1177/0011128712452960

Scott, W. R. (1987). The adolescence of institutional theory. *Administrative Science Quarterly*, 493-511.

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal, 17*, 55-71. doi:10.1057/palgrave.sj.8340168

Skogan, W. G., & Hartnett, S. M. (2005). The diffusion of information technology in policing. *Police Practice and Research, 6*, 401-417. doi: 10.1080/15614260500432949

Skogan, W. G. (2009). Concern About Crime and Confidence in the Police Reassurance or Accountability? *Police Quarterly*, 12(3), 301-318. doi: 10.1177/1098611109339893

Sullivan, E. (2013, April 14). Local level police ill-equipped for cybercrimes, cyber threats. *The Spokesman-Review.* Retrieved from http://www.spokesman.com/stories/2013/apr/14/local-level-police-ill-equipped-for-cybercrimes/

Tolbert, P. S., & Zucker, L. G. (1983). Institutional sources of change in the formal structure of organizations: The diffusion of civil service reform, 1880-1935. *Administrative Science Quarterly, 28*, 22-39. doi: 10.2307/2392383

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Polity.

Weisburd, D., & Lum, C. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police Practice and Research, 6*, 419-434. doi: 10.1080/15614260500433004

Yesilyurt, H. (2011). *The Response of American Police Agencies to Digital Evidence* (Doctoral dissertation, University of Central Florida Orlando, Florida).

Zhao, J., Ren, L., & Lovrich, N. (2010). Police organizational structures during the 1990s:

An application of contingency theory. *Police Quarterly*, 13, 209-232.

Zucker, L. G. (1987). Institutional theories of organization. *Annual review of sociology*, *13*, 443-464.

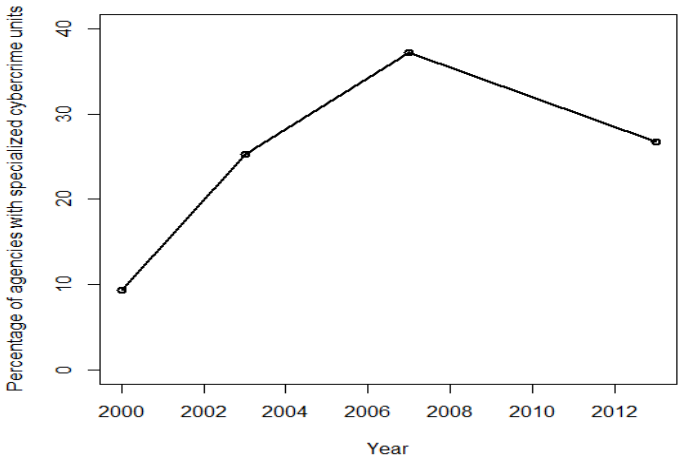

Figure 1. Proportion of agencies with specialized cybercrime units from 2000 to 2013.

Table 1. Overall sample characteristics (n = 5324)

Variable	Mean	Std. Dev.	Min	Max
Cybercrime Unit	0.25	0.43	0	1
Complaints (per 100,000)	44.99	29.08	2.7	362.11
Year 2000	0.23	0.42	0	1
Year 2003	0.16	0.36	0	1
Year 2007	0.15	0.35	0	1
Year 2013	0.47	0.50	0	1
ln(Population Served)	10.99	1.83	5.02	17.45
Technology	1.98	1.21	0	3
% Patrol Duties	61.31	21.01	0	100
Municipal Agency	0.68	0.47	0	1
Sheriff Agency	0.30	0.46	0	1
State Agency	0.02	0.15	0	1
Specialized Units	2.09	2.06	0	7

Table 2. Bivariate correlations between independent variables and use of a cybercrime unit.

Variable	r
Complaints (per 100,000)	.19**
Year 2000	-.19**
Year 2003	.01
Year 2007	.12**
Year 2013	.07**
ln(Population Served)	.32**
Technology	.20**
% Patrol Duties	-.07**
Municipal Agency	-.05**
Sheriff Agency	.02
State Agency	.08**
Specialized Units	.50**

* $p < .05$, ** $p < .01$. N = 5324.

Table 3. Random effects logistic regression models examining specialized cybercrime units

Variable	b / (se)	Odds-ratio
Complaints (per 10,000)	.03	1.04
	(.04)	
Year 2003	1.01**	2.75
	(.19)	
Year 2007	1.53**	4.62
	(.27)	
Year 2013	2.23**	9.30
	(.30)	
ln(Population Served)	.50**	1.65
	(.05)	
Technology	.15**	1.16
	(.05)	
% Patrol Duties	.03**	.99
	(.01)	
% Patrol Duties Squared	-3.6×10^{-4}	
	(1.1×10^{-4})	
Sheriff Agency	0.19	1.21
	(.15)	
State Agency	1.33**	.35
	(.42)	
Specialized Units	.75**	2.12
	(.04)	
Constant	-12.11**	.00
	(.77)	(.00)
Random intercept	1.44**	-
	(.11)	

* $p < .05$, ** $p < .01$. N = 5324. *LL* = -1958.70. Year 2000 and State agencies are the reference categories for the year and agency type variables.