© 2014, *Global Media Journal -- Canadian Edition* Volume 7, Issue 1, pp. 35-49
ISSN: 1918-5901 (English) -- ISSN: 1918-591X (Français)

Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research

Rocci Luppicini

University of Ottawa, Canada

Abstract:

Cybercrime is a relatively new area of research within criminology and media studies. The purpose of this paper is to pull together current research scholarship at the intersection of Actor-Network Theory (ANT) and cybercrime by addressing the following question: How does ANT apply to cybercrime research? A selective integrative review of cybercrime research utilizing ANT was conducted to examine recent developments and identify trends. The review draws on core research papers that span 2002 to 2013. Findings provided a strong indication of ANT's role in key areas of current cybercrime, namely, cyber bullying, cyber theft, and cyber terrorism and cyber espionage. More specifically, ANT was applied within cyber criminology research to address complex problems involving human-technological interactions, advance alternative models and theoretical perspectives, compare ANT with existing models and theoretical perspectives, and leverage understanding of network influences on actors. Recommendations are provided to help optimize the application of ANT to cybercrime research and practice. This paper helps advance knowledge at the intersection of ANT and the study of cyber criminology.

Keywords: Actor-Network Theory; Cyber Espionage; Cyber Terrorism; Cybercrime; Media Studies

Résumé:

La cyber criminalité est un domaine relativement nouveau de la recherche en criminologie et en études médiatiques. Le but de cet article est de regrouper et d'analyser les recherches actuellement financées s'intéressant à la frontière et à la relation entre la théorie de l'acteur-réseau (ANT) et de la cyber criminalité en répondant à la question suivante: Comment l'ANT s'applique à la recherche de la cyber criminalité? Une analyse des recherches faites sur la cyber criminalité utilisant l'ANT a été menée afin d'examiner les récents développements et d'identifier ses tendances. L'analyse s'appuie sur des documents de recherche important produits entre 2002-2013. Les résultats présentent une forte indication du rôle de l'ANT dans des domaines clés de la cyber criminalité actuelle, à savoir, la cyber intimidation, le cyber vol, le cyber terrorisme et le cyber espionnage. Plus précisément, nous observons que l'ANT a été utilisé dans les recherches concernant la cyber criminologie afin de résoudre des problèmes complexes impliquant des interactions humaines technologique. Cette théorie fut utilisée afin de promouvoir des modèles alternatifs et des perspectives théoriques, afin de comparer l'ANT aux modèles existants et à certaines perspectives théoriques, et enfin, afin de comprendre l'effet de levier de l'influence des réseaux sur les acteurs. Enfin, des recommandations sont formulées afin d'aider à optimiser l'application de l'ANT au sein de la recherche en cyber criminalité. Ce document permet donc de faire avancé les connaissances se situant à la frontière de l'ANT et de l'étude de la cyber criminologie.

Mots-clés: Cyber criminalité; Cyber espionnage; Cyber terrorisme; Études médiatiques; Théorie de l'acteur-réseau

---

Introduction

The Internet is, in most ways, a great development for our society. Unfortunately, it has other purposes and other uses, and young people are extremely vulnerable to things like cyber bullying, that I'd prefer to call things like cyber intimidation, cyber assault, and to some terrible crimes, and most shockingly of all, often crimes committed in virtually complete anonymity. We have consistently as a government made cracking down on crime one of our priorities in office, ever since we first came to power in 2006. But our Government will be doing more to ensure that our children are safe from online predators and from online exploitation. We are expediting a review of the criminal code with the provinces that was already underway on these very matters to identify potential gaps with regard to cyber bullying, cyber intimidation, and cyber assault, as well as the non-consensual distribution of images. And we are looking for other practical suggestions to combat such terrible acts.

— Canadian Prime Minister Stephen Harper

In a recent speech following the tragic events that led to the suicide of a young Canadian girl Amanda Todd, Prime Minister Stephen Harper delivered remarks concerning cyberbullying and the pressing need to revise the criminal code to better deal with cybercrimal activity (Harper, 2013, May 10). As eluded to in the above passage from the Prime Minister of Canada, one of the main challenges within the contemporary field of criminology is concerned with the increasing role of technology in crime and how to conceptualize areas of criminal activity where the nature of human-technical relationships are deeply intertwined (e.g., Brown, 2006; Grabosky & Smith, 1998; Wall, 2001; 2003). Part of the challenge lies in the paucity of theories of the techno-social to provide an adequate theoretical framework for the analysis of crime within criminal contexts where technology plays a strong role. Brown notes, "nowhere is captured the vision of the crucial nature of the world as a human/technical hybrid" (2006: 224). How can criminology deal with this new wave of crimes, like computer hacking, where many of the activities are carried out by non-human agents? Is cybercrime a new type of crime that requires a new approach? Brown (2006) looks to Latour's Actor-Network Theory (ANT) as a means of removing false dichotomies that separate crime from cybercrime and viewing technological crimes as network activities defined by humans and non-human agency. This raises the question as to what does ANT contribute to current scholarship on cybercrime?

What is an actor-network and how do humans and non-humans come together and demonstrate agency? Latour's ANT provides an alternative theoretical lens for conceptualizing and analyzing the human-technical relationship (Law & Hassard, 1999), which is becoming entrenched within the field of criminology (Brown, 2006). Bruno Latour, Michel Callon, and John Law pioneered ANT during the mid-1980s as an alternative conceptual framework for exploring collective socio-technical processes (Callon, 1986). Actor-Network Theory helps to explain how socio-technical "humanchine" networks (comprised of humans and technologies as actors) intersect through translation and create agency (Law & Hassard, 1999). It is a sophisticated theoretical framework for exploring how ideas, values, and intentions of social actors become inscribed in technology (Akrich & Latour, 1992).

In terms of defining features, Actor-Network Theory is intended to allow researchers to trace the complex interplay of humans and digital technologies because it provides a focus on the relationships between non-humans and humans that captures the mediated nature of contemporary life within an evolving technological society (Luppicini, 2010). One particularly interesting area where ANT is being applied revolves around the misuse of technology and growing proliferation of cybercrime around the world (e.g., Jaishankar, 2011; McQuade, 2006; 2009).

What is cybercrime? Cybercrime is a fairly new type of crime that has only become possible with the advent of the Internet and advanced digital technologies. Cybercrime refers to any crime that involves a computer and a network. According to the Britannica Online Encyclopedia:

> Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.
>
> (Britannica Online Encyclopedia, 2013)

What challenges does cybercrime create for society? Given the widespread growth of the Internet and networking technologies within the global economy and social life, efforts to locate and eliminate cybercrime represents a serious challenge for law enforcement agencies around the world. One of the challenges in dealing with cybercrime is that we live at a time when computing is at the heart of the knowledge economy and social life itself (Luppicini, 2009). In other words, we need technology to function in society but the same technology can harm society and its members. Another challenge concerns the lack of knowledge about the myriad of cybercrime varieties that exist and continue to arise, including: cyber espionage (Lin & Luppicini, 2011), cyber terrorism (e.g., Eid, 2010; Minei & Matusitz, 2011; Rid, 2012), cyber stalking and online harassment (Madge, 2007), and cyberbullying (e.g., Thompson & Cupples, 2008; Valentine & Holloway, 2002). The third challenge concerns the lack of adequate theory to deal with the complexity of human and machine actions involved in cybercrime. Based on extensive research literature review, this researcher has found that much of the existing research scholarship on cybercrime is descriptive in focus and dedicates little space to theoretical considerations that address the complex nature and large scope common to cybercriminal activities. Therefore, there appears to be a gap in the research literature and need for adequate theoretical lenses to help explain the complex interplay of human-technological relationships involved in cybercriminal activity.

ANT offers a promising theoretical approach to the study of cybercrime that is beginning to receive attention within various cybercriminology circles (e.g., Lin & Luppicini, 2011; Mahring et al., 2004; Murray, 2011; Prins, Broeders & Griffioen, 2012; Soderberg, 2010; Taylor, 2005; Thompson & Cupples, 2008). This can be attributed to a number of factors. First, ANT is intended to be versatile and well suited for dealing with the complex interplay of human-technological digital relationships. To this end, ANT has been used to study in a variety of human-technological contexts of interaction including, the assessment of digital inclusion (Teles & Joia, 2011), information security awareness (Tsohou et al., 2012), complexity and information systems (Merali, 2006), crime media effects (Mopas, 2007), online newsroom practices (Weiss & Domingo, 2010), science journalism and communication (e.g., Besel, 2011; Fioravanti & Velho, 2010), information privacy (Bonner, Chiasson & Gopal, 2009), e-government initiatives (Gunawong & Gao, 2010), and networks of practice (Takhteyev, 2009). Second, ANT can be applied to networks at micro or macro levels to describe network relations within a small organizational unit or large scale global network relations that span the world. Regardless of the scope, ANT is designed to open the "black box" of network relations to dig below the surface at the deeper complexities that cause networks to form the way they do and spread knowledge. Third, in line with the complex nature of cybercriminal activity, ANT is an approach that acknowledges the complex interplay of humans and non-humans as actors with agency in their networks that simultaneously act upon each other. It views non-human actors and human actors as constantly acting upon each to create new meaning. This mirrors well the practical context of cybercrime, which involves human and machine interactions.

Given the recent interest in ANT within criminology and cybercriminology research, it is important to understand how it is used. Is ANT employed in many areas of cybercrime or is it restricted to particular areas? Such considerations are paramount in understanding the influence of ANT on current cybercrime research. Therefore, the purpose of this paper is to provide an integrative research review to pull together current research scholarship at the intersection of ANT and cybercriminology. This is accomplished by addressing how ANT is being used in cybercriminology research. The following two main research questions are used to help gauge

the state of ANT in cybercrime research: 1) What are the main areas of current cybercrime research where ANT is applied, and 2) How is ANT applied within current cybercrime research? This paper explores how ANT has been applied in current cybercrime research to leverage understanding of cybercrime and the network of actors linked to these crimes.

Method

This integrative review draws on guidelines by Creswell (2009) following Cooper (1984), which views the aim of an integrative review as a means of summarizing the state of knowledge concerning a research topic of interest and capturing important issues that research has left unresolved. An integrative review of cybercrime research utilizing ANT was conducted to examine recent developments and identify trends of ANT use. The initial search uncovered 62 articles, which was reduced to 15 research articles using inclusion and exclusion criteria to select core peer reviewed articles that span 2002 to 2013. This paper pulls together the best available work on the topic in an effort to better understand trends in this emerging body of scholarship and suggest areas for future research.

In terms of specific procedures, several steps were involved in the collection and analysis of articles in this integrative review. First, the inclusion criteria specified peer-reviewed journal articles published between 2002 and 2013. This excluded unpublished research and research published before 2002. Next, procedures employed to select relevant studies included both library databases and on-line searches. In all, 15 articles were retained on the basis of their research quality (peer reviewed research articles only) and inclusion of ANT within the cybercriminology context. Predominant themes from the final were compared across studies, utilizing the constant comparative method (Glaser, 1992) and key themes were synthesized according to the area or type of cybercrime described. The next section provides a breakdown of the general findings concerning areas of cybercrime where ANT is currently applied. This strategic focus has the advantage of providing a detailed sketch of ANT within the current research landscape of cybercrime.

Findings

The main research findings are organized in Table 1 (below) to provide a general illustration of cybercrime and ANT research published between 2002 and 2013. As discussed above, cybercrime is a type of crime that involves the use of the Internet and digital technologies to commit a wide variety of crimes. The table below provides a basic breakdown of current areas of cybercrime research where ANT is found (cybercrime area).

***Table 1*: ANT Influenced Cybercrime Research Published Between 2002 and 2013**

Source	Cybercrime Research Area
Aradau (2010)	Cyber terrorism and cyber espionage
Beekhuyzen, Hellens & Nielsen (2011)	Cyber theft (music piracy)
Brown (2006)	Cybercrime theory
Castells (2011).	Cyber terrorism and cyber espionage
Hand & Sandywell (2002)	Cyber terrorism and cyber espionage
Hayward (2012)	Cyber theft and cyber fraud
Lin & Luppicini (2011)	Cyber terrorism and cyber espionage
Mahring et al. (2004)	Cyber terrorism and cyber espionage
Murray (2011)	Cyber terrorism and cyber espionage
Prins, Broeders, & Griffioen (2012)	Cyber theft and cyber fraud
Soderberg (2010)	Cyber theft and cyber fraud
Taylor (2005)	Cyber theft and cyber fraud
Thompson & Cupples (2008)	Cyber bullying and cyber harassment
Valentine & Holloway (2002)	Cyber bullying and cyber harassment
Wang & Zhu (2003)	Cyber theft and cyber fraud

The findings discussed below focus on the areas of cybercrime research where ANT is currently applied. The outcome of the research review provides a sketch of key areas of current cybercrime to which ANT has been most commonly applied, namely, cyber theft and cyber fraud, cyber terrorism and cyber espionage, and cyber bullying.

Cyber Theft and Cyber Fraud

A core area of cybercrime where ANT was commonly applied focused on cyber theft (piracy) and cyber fraud. Common examples of cyber theft include, identity theft, information theft, illegal sharing and downloading (music, movies, games, information, etc.), along with any other copyright violations facilitated by digital technology. Under an Actor-Network Theory approach, the websites and programs that allow easy access, downloading, and distribution of files are considered actors in this network along with the human actors (copyright owners, hackers, and individuals downloading). In this research review, it appeared that ANT was used mainly to help explain the broad implications and risks connected to digital technology use and to raise questions about values and priorities to help avoid falling prey to cybercriminal activity. For instance, in the context of government networking of information services to its citizens, major concerns address the following questions: Who is responsible for specific information about citizens that circulates within government networks? Who owns and is responsible for safeguarding the integrity of this networked information from sabotage or theft?

In describing the government networking of information services and information theft safeguards, ANT has been used to illustrate the very real connections between network activities and actors (citizens) affected by it. Prins, Broeders, and Griffioen (2012) address current ICT

developments within governments shaping the emergence of eGovernment. The paper explores the challenges of information exchange within policy domains and between public/private sector stakeholders. The authors state, "[i]nformation is exchanged or managed collectively without it being passed along a fixed sequence of actors . . . Sometimes a network is also a web in which citizens can become entangled or become the victim of identity fraud" (Prins, Broeders & Griffioen, 2012: 276) In this case, the power of ANT to provide a detailed analysis of action relations without a priori knowledge of all human and non-human actors within the network. In doing so, a provisionary understanding of network activity can be derived independent of expert knowledge or experience within the network under study.

Moreover, the significance of using ANT to view this type of cybercrime lies in ANT's capacity to examine the relationships between different types of actors within file sharing communities. Beekhuyzen, Hellens, and Nielsen (2011) explore the motivations, rules, and rituals of members involved in underground music file sharing communities from an ethnographic stance. The authors use ANT to focus on the unauthorized sharing of music (cyber theft), "Actor-Network Theory (ANT) provides the tools to investigate the sensitive balance between the technical and social aspects of an underground community" (Beekhuyzen, Hellens & Nielsen, 2011: 703). Because peer-to-peer file sharing systems can blur the distinction between technologies within the network, the authors use ANT to overcome the black box effect on not being able to see the key processes at work to explore how individuals interact in a the highly technical network of music cyber theft. As stated by the authors:

> When mapping the music actor-network it is necessary to consider the relationships between the actors. The mapping process revealed a number of issues that contribute to the controversies of file sharing, many of which were based on power relations, for instance the marginalisation of file sharers through language and criminalization.
>
> (Beekhuyzen, Hellens & Nielsen, 2011: 703)

This above passage highlights the perceived benefit of using ANT in cyber theft research to help map out key actors and issues (illegal and legal file use, power relations, etc.) within networks where controversies over file use arise.

In a slightly different vein, Wang and Zhu (2003) attempt to map out the key dimensions of film piracy in Mainland China. To accomplish this task, they use ANT to leverage understanding by identifying actor links within cyber theft networks.

> By examining actors or "actants" both human and non-human, and how they are hooked up with some of these circulating entities (e.g. piracy networks), one might understand how they achieve, and what might have been provided them with, their subjectivities, reflexivity, actions and intentionalities.
>
> (Wang & Zhu, 2003: 101)

Overall, ANT has been applied to current cyber theft and cyber fraud research to overcome the black box effect on not being able to see the key processes at work within music networks, to map out music actor-networks, and to identify actor links within cyber theft networks.

Cyber Terrorism and Cyber Espionage

A second area of cybercrime where ANT is currently applied relates to cyber terrorism and cyber espionage. Cyber terrorism commonly entails attacks on virtual infrastructures of institutions within society and cyber espionage (or cyber spying) deals with the unlawful acquisition of confidential information without the permission of the holder of the information. Cyber terrorism and cyber espionage are challenging areas of research partly due to the large scale of actions and events taking place. ANT was applied in this area to accommodate cyber terrorism and cyber espionage networks, which are often large with complex agency and difficult to describe. For instance, in exploring cyber terrorism from an ANT perspective Aradau eludes to the complexity of agency involved:

> Agency is not only human and institutional, but the agency of grids, nodes, tubes, soil, foundations and construction materials. All these interact with forms of knowledge, humans and institutional practices to create particular materializations of "(critical) infrastructure" to be protected.
>
> (Aradau, 2010: 504)

Under ANT, things and artifacts are seen as social entities that play an active role in the "generation, stabilization and reproduction of social order and sociality" (Aradau, 2010: 495). Similarly, in a study of cyber-espionage, Lin and Luppicini (2011) conduct a case study exploring the influences of GhostNet on affected organizations by critically reviewing GhostNet documentation and relevant literature on cyber espionage. The authors use ANT to examine the largest cyber-espionage incident to date (Ghostnet), "[a]s applied to this study, ANT suggests that several aspects should be studied: the actors of cyber espionage (behaviours), hackers (people), and technology (objects), as well as the network associated with these actors" (Lin & Luppicini, 2011: 66). These researchers appeared to use ANT as a means to unearth the deeper understanding and complexity of agency within cybercrime networks under investigation. As stated by Lin and Luppicini in the analysis of a cyber espionage network, "[b]ecause GhostNet involves the interaction of technology, human actors, and communications, ANT can be used to leverage understanding of GhostNet influences within affected organizations when conceptualized as a human communications system (Ibid: 72).

Lin and Luppicini (2011) discuss the conscious raising consequence of ANT in addressing questions about competing values and to highlight the need to establish priorities in approaching ICT use to avoid falling prey to cybercriminal activity:

> The case of Ghostnet provided a good example of a technoethical inquiry into controversial cyber behaviours drawing on the theoretical perspective of ANT. It highlights the fact that almost all technology use for information exchange and communications is intermediated by human agency, along with the social and ethical (and unethical) values of participating agents that need to be taken to be a top priority within developing and deploying ICT's within society.
>
> (Lin & Luppicini, 2011: 75)

Taken together, ANT has been used within current research on cyber terrorism and cyber espionage to explain social order and sociality within actor-networks, unearth the deeper

understanding and complexity of agency within cybercrime networks, address questions about competing values among network actors, and highlight the need to establish priorities in approaching ICT to protect against cyber espionage.

Cyberbullying and Cyber Harassment

Cyberbullying generally describes the use of the Internet, cell phones, or other ICT's to hurt or embarrass another person. Cyberbullying includes a variety of inappropriate online behaviour that may include online flaming, stalking, and harassment of individuals. In applying ANT to cyberbullying, the cyberbullies (those doing the bullying), victims, and other stakeholders are considered actors with agency engaged in practice within networks of cyberbullying. Valentine and Holloway (2002) examine children's identities and social networks in online and offline worlds in an effort to reveal how the real and the virtual mutually shape each other in the context of cyberbullying. As noted by Valentine and Holloway in a study of cyberbullying:

> For advocates of what has become known as Actor-Network Theory (ANT), society is produced in and through patterned networks of heterogeneous materials in which properties of humans and nonhumans are not self evident but rather emerge in practice. . . . Our study of children's internet use is informed by these ideas.
>
> (Valentine & Holloway, 2002: 306)

Other actors with agency include technologies used for bullying (e.g., mobile phones, computers, Internet, social networking sites) within the network that contributes to cyberbullying. An example of this is provided by Thompson and Cupples (2008) in the study of youths' use of cell phone texting to cyberbully:

> The human cell-phone entanglement produces in the words of Law, "machinic pleasures" and ANT enables us to explore these pleasures without reverting to technologically or socially determinist arguments or acting as Law says as if certain phenomena, in this case bullying or bad spelling, are "given in the order of things" and without denying that at times and at particular nodes in the network the machines might interpolate painfully, as in the case of the suicide of a 12-year-old North Island girl who had been the victim of text bullying.
>
> (Thompson & Cupples, 2008: 103)

When examining cyber bullying through the ANT lens, cyberbullying is a complex network too large and diffuse to attribute to a single cause because there are multiple actors (along with other factors) that contribute to it (Thompson & Cupples, 2008). In the article analysis, ANT appeared to be a useful theory to deal with the complexity of the human-technological network that can give rise of cyberbullying. This was particularly useful in accommodating the multiple ways in which cyberbullying activity occurs when using digital technologies.

ANT and Cybercrime Theory

Findings revealed that ANT is beginning to be used within cybercrime research to provide a theoretical framework to help frame the research study. For instance, in an effort to address the status of cybercrime in the discourse on crime, Brown (2006) provides a critical perspective on crime and law within techno-social networks using ANT to propose an alternative conceptualization. The author argues that the complexities of our technological culture require that criminology steps away from traditional binary logic and human/technical separation in the examination of crime, and move towards a criminology of hybrids where theories like ANT are used to help map techno-social networks, along with their actants and assemblages.

> We need to dissolve the "scientific" theories and the "social" theories in order to grasp where we are now, and that is immutably in the techno-social. Above all, this is a world where the "objects" and the "subjects", the "social" and "scientific", of criminology's purview are co-extensive and symmetrically active.
>
> (Brown, 2006: 225)

In a slightly different vein, Mahring and colleagues (2004) used ANT as an alternative theory to compare with existing theories and explain the complexities of information technology project escalation and unintended development of Trojan actor-networks, which can lead to IT project disasters. The study used ANT to examine the Trojan actor-networks and the problem with the computerized baggage handling system at Denver International. A Trojan actor network is an embedded network that develops and creates problems for the host actor network. "Over time the host actor-network grew weaker, as a result of its inability to control developments in the embedded CBHS actor-network" (Mahring et al., 2004: 230). From this, it can be observed that ANT is useful in providing theoretical framing for complex problems involving human-technological interactions, in this case, the complex problem with the computerized baggage handling system at Denver International:

> In analyzing the case from the point of view of ANT, the emphasis was placed on the efforts to create a sufficiently powerful consortium of actors to support and push forward the underlying ideas behind the project. Thus, understanding the escalation of the CBHS project from an ANT perspective is based to a large extent on the particular way in which a durable actor-network and its inscriptions were created.
>
> (Mahring et al., 2004: 226)

In a different ANT application, Murray (2011) examines power relations in how the cybercommunity functions as both a community and a group of nodes, which communicates with each other. The author uses ANT to provide an alternative analysis of the regulation of cyberspace while comparing ANT with existing models and theoretical perspectives. This helps leverage knowledge by connecting individuals (dots) within an existing matrix model of cyberspace regulation. Murray indicated, "[t]here I re-examine the Berkman School's 'code is law' model and find that in applying the principles of Actor-Network Theory (ANT) and social science theory (SST) we can consider the dot rather differently" (2011: 205). The use of ANT to leverage theoretical explanations of cybercrime is echoed in Taylor (2005) where ANT is used in

the analysis to address hacking and the free sharing of copyrighted information. Taylor states "[h]acktivists exemplify Latour's theory in action because they purposively favour the associations that blend the social and the technical, unlike hackers with their tendency to privilege the technical for its own seductive sake" (2005: 636).

Taken together, ANT is gradually becoming entrenched in cybercrime research as a theoretical tool to provide a critical perspective on crime and law within techno-social networks, offer alternative theory to compare with existing theories, explain the complexities of information technology project escalation, and guard against unintended development of Trojan actor-networks that may allow cybercrime to occur.

Conclusion

What are the main areas of current cybercrime research where ANT is applied and how is ANT applied within current cybercrime? Taken together, the findings appear to indicate that ANT does play a key role in selected areas of current cybercrime, namely, cyber bullying, cyber theft, cyber terrorism and cyber espionage, and theory. In current research on cyberbullying ANT has been applied to deal with the complexity of the human-technological network that allows cyberbullying to occur. ANT has been applied to current cyber theft and cyber fraud research to examine key processes at work within music networks, to map out music actor-networks, and to identify actor links within cyber theft networks. In current research on cyber terrorism and cyber espionage, ANT has been used to explain social order and sociality within actor-networks, unearth the deeper understanding and complexity of agency within cybercrime networks, address questions about competing values among network actors, and highlight the need to establish priorities in approaching ICT to protect against cyber espionage. Finally, in terms of theoretical contribution to cybercrime research, ANT was used to address complex problems involving human-technological interactions, advance alternative models and theoretical perspectives, compare with existing models and theoretical perspectives, and leverage understanding of network influences on actors.

This paper provides a strong indication of ANT's key role in selected areas of current cybercrime, namely, cyber bullying, cyber theft, and cyber terrorism and cyber espionage. As echoed by Hayworth, "Actor-Network Theory is an anti-essentialist social theoretical framework emerging form Science and Technology studies that seeks to understand the networked relations between human and non-human phenomena" (2012: 451). This provides a powerful analysis tool to help break down complex problems involving human-technological interactions and leverage understanding of network influences on actors.

In terms of the specific study limitations, only the explicit articulation of ANT was documented which leaves out the implicit use of ANT logic within current cybercrime research. Not all scholarship that drew on ANT made explicit reference to it but instead, followed the logic of ANT in articulating the role of human and technological agency in cybercrime. For instance, in a recent work, Castells (2011) employs ANT logic to illustrate how the security networks deal with threats of cyber terrorism. Castells states, "[t]here is indeed a symbiotic relationship between the disruption of strategic switches by resistance actions and the reconfiguration of power networks towards a new set switches organized around security networks" (2011: 779). This limitation may be overcome in future cybercrime research given more time for ANT to become popularized within the growing body of cybercrime research literature.

Based on the outcome of this cybercrime research review, a number of recommendations can be offered for advancing future work. First, more emphasis should be placed on proper citation and critical research writing strategies among researchers and journal reviewers within the research field of cybercrime. This would allow a more accurate gauge of the true influence of ANT, rather than having to interpret implicit use of ANT or reject any non-explicit references to ANT (as this study does). This would allow ANT to have a greater impact as a useful theoretical framework for guiding cybercrime studies. Second, more attention to ANT in other areas of cyber criminology may increase the impact of ANT beyond selected areas of cybercrime (cyber bullying, cyber theft, and cyber terrorism and cyber espionage). It is recommended that future cybercrime studies focus on specific areas of cybercrime to help expand research.

Overall there is reason for modest optimism about the future of ANT within cybercrime research since cybercrime is a relatively new research field, it is expected that new areas of cybercrime research will arise to which ANT may be applied.

References

Akrich, Madeleine & Latour, Bruno. (1992), A summary of a convenient vocabulary for the semiotics of human and non-human assemblies. In Wiebe E. Bijker and John Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 259-264). Cambridge, MA: MIT Press.

Aradau, Claudia. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *41*(5), 491-514.

Beekhuyzen, Jenine, von Hellens, Lisa & Nielsen, Sue. (2011). Underground online music communities: Exploring rules for membership. *Online Information Review*, *35*(5), 699-715.

Besel, Richard D. (2011). Opening the "black box" of climate change science: Actor-Network Theory and rhetorical practice in scientific controversies. *Southern Communication Journal*, *76*(2), 120-136.

Bonner, Bill, Chiasson, Mike & Gopal, Abhijit. (2009). Restoring balance: How history tilts the scales against privacy. An Actor-Network Theory investigation. *Information and Organization*, *19*(2), 84-102.

Britannica Online Encyclopedia (2012). *Cybercrime*. Retrieved October 15, 2012, from www.britannica.com/EBchecked/topic/130595/cybercrime.

Brown, Sheila. (2006). Virtual criminology. In Eugene McLaughlin and John Muncie (Eds.), *The Sage dictionary of criminology* (pp. 224-258). London: Sage.

Callon, Michel. (1986). The sociology of an actor-network: The case of the electric vehicle. In Michel Callon, John Law, and Arie Rip (Eds.), *Mapping the dynamics of science and technology* (pp. 19-34). Basingstoke, UK: Macmillan Press.

Cooper, Harris M. (1984). *The integrative research review: A systematic approach*. Beverly Hills, CA: Sage.

Creswell, John W. (2009). *Research design: Qualitative and quantitative approaches*. Thousand Oaks, CA: Sage Publications.

Eid, Mahmoud. (2010). Cyber-terrorism and ethical journalism: A need for rationalism. *International Journal of Technoethics*, *1*(4), 1-19.

Fioravanti, Carlos, & Velho, Lea. (2010). Let's follow the actors! Does Actor-Network Theory have anything to contribute to science journalism? *Journal of Science Communication*, *9*(4), 1-8.

Glaser, Barney G. (1992). *Basics of grounded theory analysis: Emergence vs. forcing*. Mill Valley, CA: Sociology Press.

Grabosky, Peter N. & Smith, Russell G. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities.* New Brunswick, NJ: Transaction Publishers.

Grabosky, Peter N. (2006). *Electronic crime*. Upper Saddle River, NJ: Prentice Hall.

Gunawong, Panom & Gao, Ping. (2010). Understanding eGovernment failure: An actor-network analysis of Thailand's smart ID card project. Retrieved September 1, 2013, from http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN042473.pdf.

Halder, Debarati & Jaishankar, Karuppannan. (2011). Cyber crime and the victimization of women: Laws, rights, and regulations. Hershey, PA: IGI Global.

Harper, Stephen (2013, May 10). PM delivers remarks at a roundtable on cyberbullying. Retrieved September 1, 2013, from http://pm.gc.ca/eng/news/2013/05/10/pm-delivers-remarks-roundtable-cyberbullying.

Hayward, Keith. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*, 441-462.

Jaishankar, Karuppannan. (Ed.). (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton, FL: CRC Press.

Latour, Bruno. (1993). *We have never been modern*. Cambridge, MA: Harvard University Press.

Latour, Bruno. (1996). *Aramis or the love of technology* (Catherine Porter, Trans.). London: Harvard University Press.

Law, John. (1999). After ANT: Complexity, naming and topology. In John Law and John Hassard (Eds.), *Actor-Network Theory and after* (pp. 1-14.) Oxford: Blackwell Publishers.

Lin, Xue & Lupiccini, Rocci. (2011). Socio-technical influences of cyber espionage: A case study of the GhostNet system. *International Journal of Technoethics*, *2*(2), 1-18.

Luppicini, Rocci. (2009). Technoethical inquiry: From technological systems to society. *Global Media Journal -- Canadian Edition*, *2*(1), 5-21.

Madge, Clare. (2007). Developing a geographers' agenda for online research ethics. *Progress in Human Geography*, *31*(5), 654-674.

McQuade, Samuel. (2006). *Understanding and managing cybercrime*, Boston, MA: Allyn & Bacon.

McQuade, Samuel. (Ed.). (2009). *The encyclopedia of cybercrime*. Westport, CT: Greenwood Press.

Merali, Yasmin. (2006). Complexity and information systems: The emergent domain. *Journal of Information Technology*, *21*(4), 216-228.

Minei, Elizabeth & Matusitz, Jonathan. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment*, *21*, 995-1019.

Mopas, Michael. (2007). Examining the CSI effect through an ANT lens. *Crime, Media, Culture: An International Journal*, *3*(1), 110-117.

Murray, Andrew. (2011). Nodes and gravity in virtual space. *Legisprudence*, *5*(2), 195-221.

Prins, J. E. J., Broeders, Dennis & Griffioen, H. M. (2012). iGovernment: A new perspective on the future of government digitisation. *Computer Law & Security Review*, *28*(3), 273-282.

Rid, Thomas. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, 35, 5-32.

Takhteyev, Yuri. (2009). Networks of practice as heterogeneous actor-networks. *Information, Communication & Society*, *12*(4), 566-583.

Taylor, Paul A. (1999). *Hackers: Crime in the digital sublime*. London: Routledge.

Teles, Adonai & Joia, Luiz Antionio. (2011). Assessment of digital inclusion via the Actor-Network Theory: The case of the Brazilian municipality of Piraí. *Telematics & Informatics*, *28*(3), 191-203.

The Economist. (2006, September 23). Secrets of the digital detectives. Retrieved September 1, 2013, from http://www.economist.com/node/7904281.

Thompson, Lee & Cupples, Julie. (2008). Seen and not heard? Text messaging and digital sociality. *Social & Cultural Geography*, *9*(1), 95-108.

Tsohou, Aggeliki, Karyda, Maria, Kokolakis, Spyros & Kiountouzis, Evangelos. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, *25*(3), 327-352.

Wall, David S. (2003). Cybercrimes: New wine, no bottles? In David S. Wall (Ed.), *Cyberspace crime* (pp. 3-38). London, UK: Ashgate.

Wall, David S. (Ed.). (2001). *Crime and the Internet*. London: Routledge.

Weiss, Amy & Domingo, David. (2010). Innovation processes in online newsrooms as actor-networks and communities of practice. *New Media & Society*, *12*(7), 1156-1171.

About the Author

Rocci Luppicini is an Associate Professor in the Department of Communication and affiliate of the Institute for Science, Society, and Policy at the University of Ottawa, Canada. Dr. Luppicini is the Editor-in-Chief of the *International Journal of Technoethics*. He is a social scientist and philosopher of technology who pursues work at the intersection of communication, technology (media), ethics, decision-making, and policy. He has authored and edited over a dozen books including, *The Handbook of Conversation Design for Instructional Applications* (2008), *The Handbook of Research on Technoethics: Volume I & II* (2009, with R. Adell), *Technoethics and the Evolving Knowledge Society: Ethical Issues in Technological Design, Research, Development, and Innovation* (2010), *Ethical Impact of Technological Advancements and Applications in Society* (2012), and *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (2013). His most recent edited work, *The Handbook of Research on Technoself: Identity in a Technological Society: Volume I & II* (2013) provides the first comprehensive reference work in the English language on human enhancement and identity within an evolving technological society.

Citing this paper:

Luppicini, Rocci. (2014). Illuminating the dark side of the Internet with actor-network theory: An integrative review of current cybercrime research. *Global Media Journal -- Canadian Edition, 7*(1), 35-49.