The Future of Geospatial Technologies in Securing Cyberspace

https://www.e-ir.info/2013/08/03/the-future-of-geospatial-technologies-in-securing-cyberspace/

CONNOR LATTIMER, AUG 3 2013

Critically Examine the Role of Geospatial Technologies in the Production of Geographical Knowledge, Making Reference to Specific Examples of Published Research

The paper is inspired by the work undertaken by BAE Systems Detica to deliver information intelligence solutions to government and commercial customers, collect and manage data to provide critical business services, and strengthen national security and resilience. The opinions expressed in this paper do not reflect those of BAE Systems Detica. The paper is dedicated to those who work tirelessly in the name of national security.

Firstly, I map a brief history of the role of geospatial technologies in crime mapping, to argue how this can be used as a tactic in cyber-space to produce knowledge that is inherently political which supports the claims of Lefebvre (1991[1905]). Secondly, I analyse the main challenges to crime-mapping to produce knowledge reflecting the work of Dodge and Kitchin (2001), and Replh (1976). Thirdly, I draw on normative examples from Detica's *NetReveal* technologies to argue how the binding of geospatial technologies and practices can be harnessed to monitor, identify and capture cyber-criminals. Finally, I will attempt to map the future contours of geospatial technologies to argue there is a shift in the threat of crime to cyberspace, and question whether such technologies can de-problematize the 'cyber'.

Crime & Technology

Cyberspace is inherently spatial. Cyberspace is an ongoing of the material and virtual relations of production (Crampton, 2003). Harvey (1989) and Amin (2002) argue that cyberspace is borderless and transcendent beyond space. Despite the fluidness of cyberspace and its activities through the Internet, this does not restrict geographers' capabilities to map it. "Cyberspace depends on real-world spatial fixity- the points of access, the physically and materiality of wires" (Kitchin, 1998:387). Activities of cyber-crime are spatially bound, as criminals operating within this space are tied to an identity of place. For example, the US cyber-security firm, Mandiant, used geospatial technologies, including social network analytics and real-time event scoring, to trace cyber-criminal activity to Unit 61398 in Shanghai, China (Mandiant, 2013). Turtle's (1995) argument that identity is difficult to map within cyberspace, as by nature, it is fluid and complex, separates geographers from spatial analytics. However, Crampton's (2003) problematization of cyberspace locates cyber-crime within a spatial context. As a result of this problematization, three assumptions are produced. Firstly, social space is struggled over. Secondly, cyberspace relies on meaning and knowledge to produce a particular discourse. Finally, spatial knowledge rests upon the map making and practices (*ibid*).

Reading Black (1997) advances Crampton's (2003) analysis further, by understanding that maps cannot be 'divorced' from the politics of representation. The practices of map making and spatial epistemologies rely on human logic, and thus, are wrapped within a particular politics. For example, BAE Systems Detica's mapping of cyber-criminal activity relies on a particular definition of what cyber-crime is. "In the use of the Internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government" (Detica, 2012:02). The definition is dependent on Detica's determination of 'illicit'; the interpretation of 'access' and 'attack';

and the understanding of 'information and services'; all of which are embedded into political agendas. Therefore, this paper frames the map and cyber as political entities for analysis to reflect the human dimensions of cyberspaces.

Geospatial technologies are transforming from identifying traditional crimes, to analysing cyber-spaces to protecting large volumes of information. The flow of information is regulated to determine access based on authenticity (identity). Foucault (1975) notes this as governmentality; where power operates to allow spaces of freedom and self-cultivation including the cyber-sphere. The notion of governmentality links to an understanding of 'technologies of the self'; the practices by which a person constitutes themselves within, through systems of power that appear natural or imposed (*ibid*). For example, social analytics uses Internet databases storing personnel information to detect fraud in cyber-space; including e-mail addresses, bank accounts and postal addresses located in clouds such as*Amazon* or *Google* (Howard *et al*, 2010). Geospatial technologies are part of a counter-mapping seeking to reveal hidden networks of criminal activity by analysing physical identities.

Crime Mapping

Traditionally, crime has been mapped using surveillance equipment, databases, and geographical information systems (GIS) to monitor, identify and capture criminal activity within particular spaces. Crime mapping is devoted to detecting areas of high-crime and the type of crime being committed to inform the best way to respond (Chainey and Ratcliffe, 2005; Eck *et al*, 2005).

The following results were established by the US Department of Justice's crime mapping report carried out in 2005 (Eck *et al*, 2005):

1. Multiple techniques must be deployed to identify crime hotspots.
2. The ability of technologies to map crime has significantly improved especially in areas of crime patterning and victimization.
3. Mapping crime hotspots produce geographical knowledge that is more effective than relying on theory to guide police action.

Plate 1 maps the relationship between the installation of CCTV cameras by Westminster City Council in 2001, and total crime in the area per ward in 2012 (Author, 2013). Although CCTV has been ineffective at preventing crime in the area, this pattern can only be exposed through producing counter-maps. This particular crime map does flag up issues about whether large amounts of crime in wards such as the West End, are the result of more crime being captured on camera compared to wards, including Maida Vale, which has far fewer CCTV cameras. Geospatial technologies produce knowledge that is enriching to crime or intelligence analysts, informing decision-making in the top tiers of government. However, both the map and its statistical foundations rely upon a political bias by excluding alternative ways of thinking (Crampton, 2010). For example, in Plate 1 the map only highlights CCTV owned by the Council and not privately-owned or other forms of surveillance. Therefore, the map and statistics are two great technologies in the production of particular truths and knowledge to project a political message (Monmonier, 2002).

Mapping crime is translated into cyber-space through geospatial technologies using social network analysis (SNA) and penetrating integrated databases to ensure the protection of information from cyber-criminals. Detica (2012:02) found in a recent report "there is a gradual convergence in offending digital and other crime", which has encouraged geospatial technologies of surveillance, databases, and GIS to adapt to tackling cyber-crime. The knowledge such technologies produce, which informs decision-making of law enforcement agencies and the government, is grounded in a particular way of thinking. The production of geospatial knowledge produces spaces in the cyber-sphere which are political; thus cyberspace becomes an extension of the geopolitical landscape (see Lefebvre, 1991[1905]). For example, neoconservatives from the Cold War to the War on Terror have reinvigorated the 'Precautionary Principle', by which the imagination of the worst-case scenario informs decisions. This marks a shift from evidence-based to speculative imaginations, as a way of thinking; including cyber-security (De Goede, 2008). Nonetheless, technologies such as *NetReveal* do not forgo evidence-based logic, but scare-mongering speculation through governmentality harnesses these geospatial technologies to narrate a particular political agenda through cyber-crime maps. Despite the inherent politics driving geospatial technologies in the production of knowledge in the cyber-

sphere, crime mapping is part of the future in understanding the threats within cyber-space.

Plate 1: Crime Mapping.

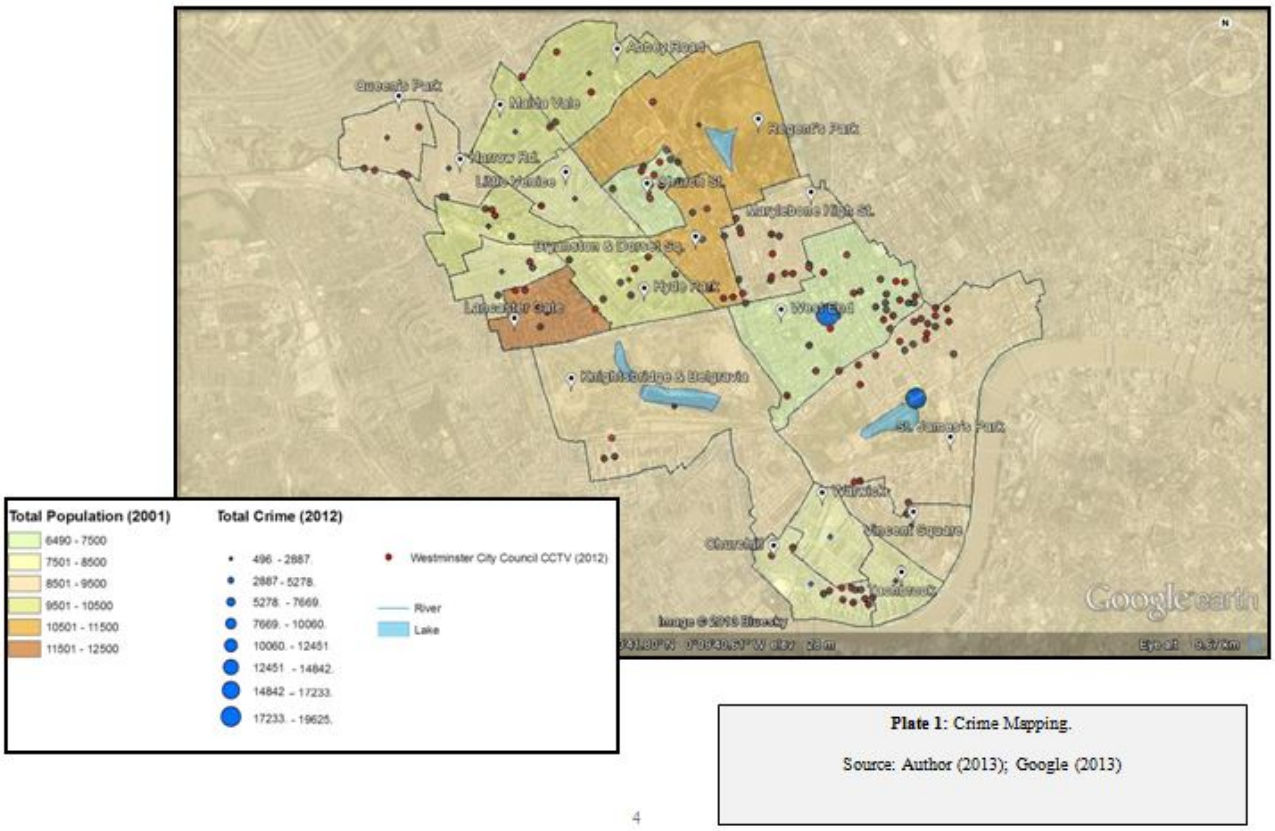

Plate 1: Crime Mapping.

Source: Author (2013); Google (2013)

Challenges from Cyberspace

In 2013, Mandiant released a report tracing a network of Advanced Persistent Threats (APT) to the Chinese military, Unit 61398 (Economist 2013; Mandiant, 2012). The attacks infected 141 companies across 20 industries, stealing hundreds of terabytes of information, costing the Western economy billions of dollars (BBC, 2013). Detica estimates in the UK alone cyber-crime costs the economy £27 billion per annum, with many businesses and government departments unaware that such attacks are being carried out (Detica, 2012). In 2011, there were over 900 million cyber-attacks with 26 million of those targeting the UK; this figure is based on those attacks reported (Spectator and Detica, 2012). Cyber-space produces both normative and theoretical challenges to the way in which traditional geospatial technologies prevent crime.

Monitor

Far more cyber-attacks are unreported and even more are going unnoticed. Thus, the scale of cyber-crime is far greater than first realised (Detica, 2013a). Cyberspace decentralises criminal activity around the world through globalised networked communications, whilst simultaneously creating new social spaces in where this kind of activity can hide (Morely and Robbins, 1995; Harvey, 1989). Traditional forms of surveillance, such as the CCTV camera or intelligence analysts, are unable to monitor and filter the vast amounts of data (big data), which could total up to 900 million events on one network per day (Detica, 2013a). Cyberspace has the appearance of being a 'spaceless' and 'placelessness' world. In contrast, criminals often are attached to physical locations from where the crime is committed to their hideouts (Dodge and Kitchin, 2001). However, cyber-criminals lack a sense of belonging and attachment to place; thus, monitoring a spaceless and placelessness is almost impossible using traditional geospatial

technologies that have relied so much on the territorial (Relph, 1976).

Identify

The database is situated within cyberspace to bring together all individuals' information in networks (Glenny, 2011). Traditionally, the database is able to identify individuals coming together with surveillance technologies and profiling practices based on ethnicity, sex, religion *etc*. Foucault (1975) suggests the power of technology can change the social construction of an individual's identity. Cyberspace is such a technology which hides identities through the formation of multiple identities and encryption (Poster, 1995). Lupton (1995) argues that at a Utopian level, the body is often 'data trash' or 'meat' that simply gets in the way of the online community. Therefore, cyber-criminals re-present themselves in cyberspace with new identities in order to target the vulnerable. For example, cyber-criminals, including *ShadowCrew* and *Darkmarket,* who participate in 'phishing' or 'spearphishing' to obtain information, such as usernames, passwords or credit cards, deceive the user through the intellectual fabrication of identity using e-mail, often with the identity of a user's bank (Howard *et al*, 2010). Knowledge of identities becomes blurred and skewed by the cyber-domain and presents a challenge to databases in identifying crime.

Capture

GIS relies upon sufficient monitoring and identification to produce a visualisation of the criminal terrain. Therefore, GIS can only be used to capture criminals with the aid of such crime maps, which are reliant on surveillance and databases. The collapse of spatial and temporal boundaries causing the 'death of distance' means criminals are no longer constrained to geography; they can now relocate anywhere within the cyberspace, as well as create new hidden spaces and disguise physical identities (Dodge and Kitchin, 2001). Mapping spacelessness and emerging new spaces is impossible for GIS as it requires spatial coordinates to make decisions on phenomena distributed across landscapes (Wright *et al*, 1997). GIS, as a science, is unable to engage with the abstract, the metaphysical and the non-existence which characterises cyberspace. Thus, the advancement of geographical knowledge using GIS is severely hindered within the cyber-sphere. Nonetheless, geospatial technologies are being adapted to monitor, identify and capture the cyber-world to bring cyber-criminals to justice. The responses to the challenges of cyberspace posed are addressed in the next section of this paper in an attempt to spatialise the cyber.

Responding to the Challenge of Cyberspace

Responding to the spatial challenges of cyberspace de-problematises this discourse by adapting existing geospatial technologies, including surveillance, databases, and GIS, to monitor, identify and capture cyber-crime. The use of normative examples provides hope for the future of geospatial technologies in mapping cyberspace. Nonetheless, drawing on geographical and political research, I shall argue geospatial technologies are driven by political doctrines which subsequently makes mapping these spaces political (Crampton, 2003; 2010).

Mapping Cyberspace

In 2012, Detica combined manual search tools with *NetReveal Analyzer*, which specialises in turning large amounts of structured and unstructured data into intelligence (Detica, 2013b). The *Analyzer* relies of SNA to monitor individual activities within networks and event-scoring up to 600 million events per day on a network, whilst also filtering information that could serve as important to analysts (*ibid*). *NetReveal* combines surveillance and database geospatial technologies to produce topological maps of cyber-activity. These maps rely on elements of GIS but instead are more abstract in nature, using a system of relative location (Dodge and Kitchin, 2001). Spatial coordinates are drawn from the data collected in stored clouds within networks; including stolen bank details, names of the deceased, postal addresses of other cyber-criminals, family, or friends, use of multiple 'fake' e-mail addresses, to name but a few. Harnessing multiple geospatial technologies was able to produce a map of organised crime groups' tactics and methods for conducting cyber-crime. *Analyzer's* crime maps produce counter-geographies by exposing what traditional forms of geospatial technologies see as hidden. Therefore, Lupton's (1995) claim that the identity is separated from cyberspace is challenged by the holistic approach to spatialising the cyber-sphere. Although identities can be multiplied, the liquidity of surveillance and mapping bolsters identity to place within cyber-

spaces by merging physical and virtual spaces to expose hidden networks (Bauman, 2007).

NetReveal Scenario Manager (*SM*) and *Live* move one step further than *Analyzer* by mapping cyberspace in real-time. Thus, maps can be produced within seconds to detail real-time patterns and behaviours of cyber-criminals, including fraud, phishing and malware (Detica, 2013c). The maps produced by these two technologies are more conceptual, using GIS as toolmaking rather than a science (Wright *et al*, 1997). Cyberspace becomes described (albeit not calculated) "as the sum of countless interactions among countless users of global ICT infrastructure." Thus, cyber-space becomes a matter of risk management rather than scientific calculation (Cornish *et al*, 2009:17). Nonetheless, real-time risk management still relies on evidence-base logic to determine levels of threat, rather than the Precautionary Principle, which is often criticised for imagining threats from cyber-crime and cyber-terrorism. In 2011, Detica worked with several banks (unnamed for security reasons) to uphold their reputation after a chain of cyber-attacks. The attacks were from a decentralised group working inside the banks, as well as across London, operating in a 'hub' (Detica, 2013c). The group directed purposeful online criminal activity in core groups of members linked to wider periphery of criminal associates. The patterns in activity were analysed in real-time by *Live* and *SM* to detect a malware system that was intrusively spying on information sharing across the entirety of the banks (*ibid*). Detica was able to identify a clear command structure and generate map-based evidence that illustrated the illicit activity on the network. Geospatial technologies are able to spatialise cyberspace through representations of information activity into geographical knowledge, that can locate cyber-criminal groups (Dodge and Kitchin, 2001).

The Politics of Maps

The geospatial technologies of NetReveal produce counter-maps that are problematic, as they rely on particular political narratives, despite such maps being founded on evidence-based logics. The statistical basis which informs Detica's technologies to monitor, identify and capture, is determined by laws and regulations around cyber-space that are central to discussions in political arenas, including Parliament or Congress. The House of Lords Science and Technology Committee criticised the Government in 2007 for placing the main responsibility of Internet lawlessness on individuals involved, leaving those who fail to implement adequate cyber-security measures un-prosecuted and un-scrutinised (Emm, 2009). NetReveal geospatial technologies are driven by the current Computer Misuse Act (1990), which does not regulate the individuals involved in establishing the cyber-security barriers. Consequently, the maps created only show cyber-criminal individuals or groups who breach the security firewalls, missing those who are responsible for often poor cyber defences (Murray, 2007). Wood (1992) argues that this opportunity cost of forgoing representations, in this case of those responsible for cyber-security on the map, is a deliberate (and thus, political) choice. Therefore, geospatial technologies and maps are political. Crampton (2010) argues further that this kind of map production is part of a 'political economy' of government, reflecting a Foucauldian rationality of governmentality whereby the state sets political goals that are achieved through the deployment of geospatial technologies in cyberspace. In this respect, the counter-maps produced by NetReveal achieve political goals established by central government. The Government's digital architecture outlined in The UK Cyber Security Strategy (2011) fails to recognise the relationship between criminals in the offline world and their illegal activities in cyber-security. Although Detica has called for this relationship to be recognised, its current geospatial technologies fail to produce maps that display behaviour patterns of criminals operating online and offline. The UK achieves its political economy of cyberspace by ignoring difficulties and challenges to geospatial technologies. Therefore, the representations on maps are ordered by this logic, and thus, the role of geospatial technologies in producing geographical information is political.

The Future of Geospatial Technologies

The future of criminality will be orientated around the cyber-sphere. To what extent is unknown, but one assertion that is certain, is that there is an increasing shift towards cyber-crime in the 21st Century. The growing number of adversaries using cyberspace to steal and compromise critical data has caused the UK government to raise cyber attacks to a 'Tier 1' threat in the *National Security Strategy* (2010). There are also growing concerns by the intelligence communities, including GCHQ, that terrorist networks, including al Qaeda, will harness cyber-criminal tactics and use them for purposes known as 'cyber-terrorism'. Cyber-terrorism is generally understood to mean unlawful attacks and threats of attack against computers, networks and the information stored, to intimidate or

coerce government or its people in furtherance of political or social objectives (Denning in Arquilla and Ronfeldt, 2001). Cyberspace is a real threat and in the future, will be at least as dangerous as the physical battlefield.

Neither worst-case scenario analysis, nor its opposite, complacency, offers a good basis for policy-making and understanding the future of geospatial technologies (Cornish *et al*, 2009). Cyberspace has been de-problematised by understanding the normative examples of technologies used by BAE Systems Detica to protect business and government information. Geospatial technologies are being adapted by combining technologies of surveillance, data and GIS, as well as the practices of monitoring, identification and capturing. Nonetheless, the geographical knowledge produced by such geospatial technologies is inherently political through a 'Political Economy of Government', as well as the production of new political spaces within the cyber-sphere (Crampton, 2003, 2010; De Goede, 2008).

Bibliography

Amin, A. (2002) Spatialities of Globalisation, *Environment and Planning A*, 34(*3*), 385-400.

Bauman, Z. (2007) Liquid Times: Living in an Age of Uncertainty, Polity Press, Massachusetts.

BBC, British Broadcasting Company. (2013) China Military Unit 'Behind Prolific Hacking', *BBC News Online*, http://www.bbc.co.uk/news/world-asia-china-21502088 [Accessed 06/03/2013].

Black, J. (1997) Maps and Politics, University of Chicago Press, Chicago.

Chainey, S. And Ratcliffe, J. (2005) GIS and Crime Mapping: Mastering GIS: Technologies, Applications and Management, John Wiley and Sons Ltd, West Sussex.

Cornish, P. Hughes, R. And Livingstone, D. (2009) Cyberspace and the National Security of the United Kingdom: Threats and Responsibilities, *Chatham House* and *BAE Systems Detica*, London.

Crampton, J. (2003) The Political Mapping of Cyberspace, University of Chicago Press, Chicago.

(2010) Mapping: A Critical Introduction to Cartography and GIS, Wiley-Blackwell, Oxford.

De Goede, M. (2008) The Politics of Preemption and the War on Terror in Europe,*European Journal of International Relations*, 14(*1*), 161-185.

Denning, D. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in Aquilla, J. And Ronfeldt, D. (eds.) Networks of Netwars: The Future of Terror, Crime and Militancy, RAND, Arlington.

Detica, BAE Systems. (2008) Customer Intelligence: It's all in the Network, *BAE Systems Detica*, London.

(2012) The Cost of Cyber Crime, *BAE Systems Detica* and *Cabinet Office*, London.

(2013a) Cyber Security, https://www.baesystemsdetica.com/services/cyber-security/ [Accessed, 07/03/2013].

(2013b) Detica NetReveal, https://www.baesystemsdetica.com/technologies/detica-netreveal/ [08/03/2013].

(2013c) Detica NetReveal Detection, http://www.deticanetreveal.com/en/technology/detection.html [Accessed 08/03/2013].

Dodge, M. and Kitchin,R. (2001) Mapping Cyberspace, Routledge, London.

Eck, J. Chainey, S. Cameron, J. Leitner, M. And Wilson, R. (2005) Mapping Crime: Understanding Hotspots,*US Department of Justice* and *National Institute of Justice*, Washington.

Economist, The. (2013) Smoking Gun, *The Economist*, February 23rd Issue, London.

Emm, D. (2009) Cybercrime and the Law: A Review of UK Computer Crime Legislation, *SecureList*, www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation [Accessed, 08/03/2013].

Foucault, M. (1975) Discipline and Punish: The Birth of the Prison, Penguin Publications, London.

Glenny, M. (2011) Dark Market: How Hackers Became the New Mafia, The Bodely Head, London.

Harvey, D. (1989) The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change, Blackwell Publishers Inc, Massachusetts.

Howard, D. Prince, K. and Schneier, B. (2010) Security 2020: Reduce Security Risks This Decade, Wiley Publishing Inc, Indianapolis.

HM Government. (2010) A Strong Britain in an Age of Uncertainty: The National Security Strategy, HM Government, Whitehall.

HM Government. (2011) The UK Cyber Security Strategy, HM Government, Whitehall

Kitchin, R. (1998) Towards Geographies of Cyberspace, *Progress in Human Geography*, 22(*1*), 385-406.

Lefebvre, H. (1991[1905]) The Production of Space, Translated by Nicholson-Smith, D. Blackwell Publishing, Oxford.

Lupton, D. (1995) The Embodied Computer User, in Featherstone, M. And Burrows, R. (eds.) Cyberspace, Cyberbodies and Cyberpunk: Cultures of Technological Embodiment, Sage, London.

Moreley, D. and Robbins, K. (1995) Spaces of Identity: Global Media, Electronic Landscapes and Cultural Boundaries, Routledge, London.

Mandiant. (2013) APT1: Exposing One of China's Cyber Espionage Units, *Mandiant*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [Accessed 06/03/2013].

Monmonier, M. (2002) Maps, Politics and History, An Interview with Mark Monmonier Conducted by Jeremy Crampton, *Environment and Planning D: Society and Space*, 20(*6*), 637-646.

Murray, A. (2007) The Regulation of Cyberspace: Control in the Online Environment, Routledge-Cavndeish, Oxon.

Poster, M. (1998) Jean Baudrillard: Selected Writings, Polity Press, Cambridge.

Relph, E. (1976) Place and Placelessness, London, Pion.

Spectator, The. And Detica, BAE Systems. (2012) The Cyber Threat: How Thieves and Spies are Attacking Our Computers-and How we can Protest Against them, *The Spectator* and *BAE Systems Detica*, London.

Wood, D. (1992) The Power of Maps, The Guildford Press, New York.

Wright, D. Goodchild, M. And Proctor, J. (1997) GIS: Tool or Science? Demystifying the Persistent Ambiguity of GIS

as “Tool” Versus “Science”, *Annals of the Association of American Geographers*, 87(*2*), 346-362.

—

Written by: Connor Lattimer
Written at: Royal Holloway, University of London
Written for: Dr. Gwilym Eades
Date written: April 2013