Security and Surveillance in Virtual Worlds:

Who's Watching the Warlocks and Why?

Stevens, Tim (2015), Security and surveillance in virtual worlds: Who's watching the warlocks and why? *International Political Sociology* 9(3): 230-47.

Accepted 10 December2014.

Abstract

Virtual worlds, persistent online spaces of social interaction and emergent game-play, have hitherto been neglected in international studies. Documents disclosed by Edward Snowden in December 2013 suggest that intelligence agencies, including the National Security Agency and GCHQ, have been less reticent in exploring and exploiting these environments for signals and human intelligence. This article introduces virtual worlds as sociological sites in the matrix of international politics and explores how the intelligence community (IC) has conducted operations in these environments, principally for counter-terrorism purposes. Reconstructing the activities of the IC shows how virtual worlds have been drawn into the ambit of state surveillance practices, particularly as a means to generate intelligence from virtual world behaviours that correlate with and predict 'real-world' behaviours indicative of terrorism and other subversive activities. These intelligence activities portend a general colonisation by the state of previously unregulated interstices of the sociotechnical Internet and their analysis contributes to our understanding of the relationship between government and the Internet in the early 21st century.

Keywords

Counterterrorism. Virtual Worlds. Internet. Surveillance. Security.

Introduction

> *The bomb hit the ABC's headquarters, destroying everything except one digital transmission tower. The force of the blast left [the] site a cratered mess. Just weeks before, a group of terrorists flew a helicopter into the Nissan building, creating an inferno that left two dead. Then a group of armed militants forced their way into an American Apparel clothing store and shot several customers before planting a bomb outside a Reebok store. This terror campaign …. has left a trail of dead and injured, and caused hundreds of thousands of dollar's damage. The terrorists belong to a militant group bent on overthrowing the government.* (O'Brien, 2007)

So reported *The Australian* newspaper in July 2007, describing attacks against the Australian Broadcasting Corporation and commercial interests by an insurgent group employing spectacular urban violence to cause economic damage and the death of innocent civilians, a year before Lashkar-e-Taiba would do the same in Mumbai. Yet, these incidents occurred not in a major Pacific or south Asian city but in the 'virtual world' of Second Life, in which 'people create their own characters, known as avatars, and live an alternative life …. in a community of more than eight million people from across the world' (O'Brien, 2007). According to *The Australian*, all was not well in this digital utopia: Second Life was taking a 'sinister turn', with 'weapons armouries …. where people can get access to guns, including automatic weapons and AK47s', and amongst its users were 'three jihadi terrorists' and 'two elite jihadist terrorist groups' (O'Brien, 2007). Once these groups take root in Second Life, argued the article, they could 'start spreading propaganda, recruiting and instructing like minds on how to start terrorist cells and carry out jihad …. Just as September 11 terrorists practised flying planes on simulators in preparation for their deadly assault on US buildings, law enforcement agencies believe some of those behind the Second Life attacks are home-grown

Australian jihadists who are rehearsing for strikes against real targets' (O'Brien, 2007; also, The Economist, 2007; Gourlay & Taher, 2007).

This shift from the description of activities that *look* like terrorism to the identification of behaviours that *are* terrorism—or acts preparatory to terrorism—attracted hostility and derision from the online commentariat (e.g. Au, 2007; Burke, 2007; also Cole, 2008). This scepticism was well founded: establishing direct connections between acts of 'virtual' vandalism and actual terrorism was as absurd as it was unsubstantiated. Why would a jihadist group form a recognisable entity in a quasi-public space to wage an insurgency against the 'government' of Second Life, let alone to pursue more nefarious ends? What was the basis for 'expert' claims that terrorists were using virtual worlds for training and recruitment? Why would *The Australian* even persist with this reasoning when it eventually admitted the ABC 'attack' was actually 'a computer server error' fixed 'within a couple of hours' (O'Brien, 2007)?

Second Life experienced substantial media hype during 2006-2008 and we might dismiss contemporary news reports of Second Life terrorism as minor historical chaff were it not for subsequent disclosures by Edward Snowden, a former contractor for the US National Security Agency (NSA). Documents released in December 2013 show that the NSA and its British signals intelligence (SIGINT) counterpart GCHQ infiltrated virtual worlds like Second Life and World of Warcraft on national security grounds. This demonstrates that intelligence agencies, like elements of the mainstream media, saw these environments as potential loci of terrorist planning and training and as sources of actionable intelligence, including through the cultivation of human agents. Together with other indicators, including the US Reynard project (2009-2012), which aimed to detect suspicious (i.e. terrorist) behaviours from in-world surveillance, there emerges a picture of serious interest from the intelligence community in monitoring and exploiting virtual worlds, even after media interest waned.

This article establishes virtual worlds as 'meaningful sites for social action' (Boellstorff, 2009: 62-63) that have been largely ignored in international studies. It describes various modes of state interaction with MMOs before focusing on the construction of MMOs as security threats and the focus of counterterrorism activity, in particular. Through an examination of classified documents released by Edward Snowden, this article develops a picture of specific measures implemented by NSA and GCHQ to counter the perceived terrorist threat of MMOs. It then discusses how intelligence agencies attribute meaning to MMOs, allowing them to be constructed as sites of (in)security, and explores how the consequent surveillance practices blur the virtual and the 'actual'. The article proposes that MMOs mark another stage in the process of surveillance and intelligence agencies' colonisation of previously unregulated interstices of the sociotechnical Internet.

Conceptualising Virtual Worlds

A virtual world or massively multiplayer online (MMO) world is a computer-simulated environment, defined as 'an expansive, world-like, large-group environment made by humans, for humans, and which is maintained, recorded, and rendered by a computer' (Castronova, 2005: 11). They are synchronous and persistent, which additionally speaks to their real-time interactivity and the manner in which they continue to function once participants, visually represented by personalised 'avatars', are no longer 'in-world'. Virtual worlds have their roots in the computer-networking experiments of the 1970s (Damer et al, 2004) and the two best-known MMOs today are probably Second Life and World of Warcraft, launched in 2003 and 2004, respectively. Each is emblematic of the main categories of MMO accessible on personal computers and games consoles via the Internet. World of Warcraft is an example of the most popular form of MMO, the sub-category of massively multiplayer online role-playing games (MMORPG). Participants are players in a game whose behavioural parameters are set principally by the world designers, Activision Blizzard. World of Warcraft gameplay, in common with other MMORPGs, usually requires the use of violence, generally

combat allied to ‘questing’, which has a long history in on- and offline role-playing games. Like the video-gaming and live action roleplaying heritage to which MMORPGs owe much (Barton, 2008), there is a strong narrative structure to these games, in which the ‘test’ of the hero(ine) is beating adversaries in battle, a modern iteration of traditional folk tales (Jantzen & Jenzen, 1993). Popular MMORPGs include EVE Online, Everquest I and II, Guild Wars, Ultima Online and Lineage I and II.

Second Life is a ‘social’ MMO, developed by Linden Lab, in which socialisation rather than status progression in a game-space is the core activity of participants. Rules in social worlds relate more to what forms of social behaviour are allowed and which are not, rather than what is permitted in order to play and potentially win a game. Whereas players of MMORPGs enter an environment in which objects and roles are largely predetermined and constrained by game architecture, the architecture of social worlds encourages participants to modify their environment. The emphasis on autogenerative process and user creativity allows participants to ‘inhabit’ *their* world rather than someone else’s; hence Second Life participants are known as ‘residents’ rather than players. Social worlds are often framed as the authentic realisation of the Metaverse, the virtual world at the heart of Neal Stephenson’s highly influential science-fiction novel, *Snow Crash* (1992). Other non-combat MMOs include There, Club Penguin, Habbo, Active Worlds and dozens of others, many of which are aimed at the ‘teen’ market.

The conceptual boundaries between these two categories are fluid. Game worlds can also be social, for example. A player of EverQuest, one of the longest-running MMORPGs, related how some long-term players have not progressed beyond the lowest levels of the game because ‘the only reason they log on is to hang out with their friends’ (Ludlow & Wallace, 2007: 30). Additionally, those who pursue the core purpose of MMORPGs—to elevate one’s status—often do so through collaborative means, like World of Warcraft ‘guilds’ (Williams et al, 2006) and ‘corporations’ in space-themed MMORPG EVE Online (Mildenberger, 2013). There is a substantial academic literature on social

interaction in MMORPGs and it would be misleading to imply any social deficit in MMORPGs relative to social worlds. Anthropologist Bonnie Nardi asserts, for example, that World of Warcraft is 'an exemplar of a new means of forming and sustaining human relationships and collaborations through digital technology' (Nardi, 2010: 5). Indeed, empirical studies show that social factors are integral to making the MMORPG experience so enjoyable (Cole and Griffiths, 2007).

Conversely, even if social MMOs have 'no established and universal game objectives' (Malaby, 2009: 2), they do have significant ludic components. Malaby emphasises that game-playing was deeply embedded in the culture of Second Life creators Linden Lab and its employees were often serious gamers (Malaby, 2009: 80). In its prototypical private incarnation as LindenWorld, Second Life was generally constructed as a 'first-person shooter', gaming jargon for game-play seen from a first-person perspective and involving guns and other projectile weapons. From its earliest days, too, Second Life saw violent clashes between groups of 'residents' which might be characterised as warfare, like the infamous 'War of the Jessie Wall' (2003), in which a dispute over behavioural norms escalated into a proxy conflict over the US invasion of Iraq (MacCallum-Stewart, 2007; Au, 2008: 103-117). Organised combat between Second Life 'armies' has also been an historical commonplace and is deserving of study in its own right. In both types of MMO, violence is closely tied to the construction and maintenance of group identities. Conflicts occur between relatively well-defined groups, all of which have histories and might be identified as 'imagined communities': most never meet face-to-face, 'yet in the minds of each lives the image of their communion' (Anderson, 2006: 6).

Neither 'play' nor 'game' is sufficient alone to identify what makes MMOs distinctive (Boellstorff, 2008: 21-24). Often referred to as a 'game', even by participants, it is probably more proper, borrowing from sociologist Henri Lefebvre, to refer to an MMO as a 'lived space', a 'space of play' coexisting with 'spaces of exchange and circulation, political space and cultural space' (Lefebvre,

1996: 172). Violence is a problematic concept in the context of 'virtuality', as the long-running debate over 'media violence' attests, but is only one expression of political exchange and circulation in MMOs. Since their inception, MMOs have been seen by developers and participants as expressions of community sovereignty outside the Westphalian system of international sovereignty (Kücklich, 2009). This may seem an exaggerated claim but cyber-libertarian narratives in particular continue to influence how MMOs are experienced and perceived.

Castronova terms the corporate owners and managers of MMOs 'coding authorities', which have the power to constrain behaviours through game architecture and rule sets and to intervene in disputes between participants if necessary or desirable (Castronova, 2003). As the *de facto* and *de jure* in-world authority, they may also come into direct conflict with participants, as when a coding authority's decision proves unpopular and elicits collective player actions against it (e.g. Kline et al, 2003: 161-163). Coding authorities have the ability 'to create and destroy any amount of good, at virtually zero cost' (Castronova, 2003), clearly a powerful sanction, and many protests have been terminated by suspending players' accounts and other drastic actions (Taylor, 2006). Some have been resolved more productively. The owners of EVE Online diffused tensions by encouraging players to form a 'Council of Stellar Management' which, despite having little real power, permitted players to govern aspects of gameplay and provided a forum for interaction with the coding authority (Óskarsson, 2008). It is notable that even as junior partners in highly asymmetric socio-economic relationships, MMO participants have consistently cared enough about their online lives to confront authorities with absolute control over their existence.

MMOs are sociological sites that exhibit political dynamics of many kinds yet they have received little attention in international studies. Despite ongoing debates on the significance of the Internet in international relations and global politics MMOs are barely mentioned except as tools for the teaching of international politics (Carvalho, 2013; Weir and Baranowski, 2011). This work recognises

the general educational utility of MMOs like Second Life (Warburton, 2009) and the role of 'new media' in the practice and pedagogy of disciplinary International Relations (Carpenter and Drezner, 2010: Sjoberg, 2013) but does not treat MMOs as specific objects of study. This is perhaps because they are not felt to be important enough, despite the millions of people that regularly interact in them and renewed attention to 'the mundane' in international politics (Enloe, 2011). If MMOs command the attention of the state and its intelligence agencies, as I argue they do, we should explore why. The following section outlines the ways in which governments have perceived MMOs as opportunities; subsequent sections examine why they have also been seen as threats and how intelligence agencies have responded.

Virtual Worlds and Government

Intelligence agencies' interests in MMOs are set against a background of state actors reasserting sovereign power over the Internet after a long period in which commercial interests led the way in developing the Internet's 'strategic resources' (Franklin, 2013: 183).A key narrative has been the erosion of state sovereignty by non-state actors empowered by the tools and techniques of the 'information age'. This has been shown to be overly reductive and simplistic (Dunn Cavelty et al, 2007; Eriksson and Giacomello, 2009; Betz and Stevens, 2011) but there have undoubtedly been substantial increments in non-state access to information and communications technologies (ICTs) and a proliferation of political uses to which these may be put. This does not, however, necessarily portend decreased state authority and control. Even if state sovereignty is somehow in decline, states, 'despite their multi-dimensional crises, do not disappear; they transform themselves to adapt to the new context' (Castells, 2009: 39). Importantly, governments—or, more properly, their many parts with responsibility in this field—detect shifts in state and non-state uses of ICTs and seek new organisational modalities through which to extend governance over the Internet, not least through forms of networked governance that may themselves eventually alter the nature of the state (Mueller, 2010: 49).

These forms of state adaptation have two key dynamics: states have 'partially deterritorialised themselves' by adopting network topologies to cope with 'information age' risks and threats but they have also 'partially territorialised cyberspace' (Herrera, 2009: 88). Saco (1999) identifies a similar dynamic in which 'cyberspace' colonises social and political life whilst simultaneously being colonised by security discourses and practices. These authors take issue with the libertarianism of so-called cyberspace 'pioneers', who promoted cyberspace as 'a place apart', beyond the reach of sovereign governments. As they observe, ICTs are neither exclusively physical infrastructures nor cognitive collectivities but sociotechnical entities not divorced from 'the rest' of human life. How ICTs are framed has had significant implications for the politics of the Internet, with differing teleologies facilitating different forms of political (re)action (Deibert, 2002; Dunn Cavelty, 2008). What actors think the Internet is *for* catalyses what actions they take with respect to it.

One early example of government engagement with MMOs was their supposed potential as sites of diplomatic practice. In May 2007, the Republic of Maldives opened the first 'virtual embassy' on Second Life's Diplomacy Island, an innovation heralded as particularly important for small countries in that it might help them 'participate meaningfully in international relations' (Republic of Maldives, 2007). A clutch of other countries followed suit, including a Swedish project run by the independent Swedish Institute but backed by the Swedish foreign minister as a sign of national ambitions to be on the 'front line' of Internet innovation (Bengtsson, 2011: 12). The Swedish 'embassy' was widely reported in the media during the period of Second Life hype (2006-2008) and considered a net contributor to 'nation branding' while media attention remained high and positive but was quietly retired once media attention turned elsewhere (Bengtsson, 2011).

In this case, the Internet was *for* the promotion of national interests through political communication and MMOs were then the latest incarnation of this emerging practice (Tumber and

Bromley 1998). In the re-energised debate about 'strategic communication' and 'public diplomacy', information communication technologies (ICTs) have been central to reconfiguring advocacy and cultural diplomacy for the 21st century. We should not be surprised that MMOs have been identified as sites of diplomatic practice and as venues for more sustained government communications initiatives (Cull, 2008: 51; Ondrejka, 2007), in which multi-user collaboration substitutes for the authoritative monologue (Cowan and Arsenault, 2008). In the contemporary informational environment, in which 'strategic narratives' compete to 'order the chaos' of international politics (Roselle et al, 2014), one can imagine the utility of various platforms to national communications projects, MMOs included, not least because of their multinational and multi-ethnic character.

Manjikian (2010) identifies three perspectives on the nature of the Internet that are extensible to the issue of government and MMOs: the utopian, the regulatory and the realist. The utopian view is separatist, in that it treats cyberspace as an entity normatively and practically beyond government control. The regulatory perspective proposes cyberspace as a global commons deserving of legal and normative regimes preserving it as a public good. The realist view frames the Internet's basic characteristics—'its amorphous, networked nature; the anonymity which it offers; and the speed and cheapness of transactions which it offers' (Manjikian, 2010: 386)—as dangerously inimical to state interests. From this viewpoint, the utopian 'global village' becomes 'the virtual battlespace', replete with 'dark places offering sanctuary to one's enemies' (Manjikian, 2010: 387). Crucially, the realist perspective suggests that the 'real world' is now vulnerable to 'invasion' by entities and initiatives from the 'virtual world' (Manjikian, 2010: 391), often expressed in the language of biological contagion and through metaphors of public health (Betz and Stevens, 2013). Thus emerges a realpolitik of cyberspace engagement as governments conceive of 'cyberspace as both a territory which shelters and hides insurgents [and terrorists] as well as a crucible which breeds them' (Manjikian, 2010: 394). Doctrine and political discourses therefore stress the need to eradicate the sociotechnical interstices in which threats might find footholds.

In the mid-2000s, these concerns began to be expressed with reference to MMOs as possible platforms for acts preparatory to terrorism. These fears surfaced publicly in 2005-2007, roughly contemporaneous with the synthesis of moral panics over terrorism and the Internet into mainstream political concerns over the communicative and instrumental uses of the Internet by terrorists (e.g. Weimann, 2006). That this should coincide with a period of substantial MMO hype is no doubt also a major contributory factor. The following section narrates the construction of MMOs as terrorist threats during this period, described as a fast-approaching 'Meta-Terror'.

'Meta-Terror'

After 9/11, the Internet was often referred to as a 'safe haven', 'virtual sanctuary' or 'training camp' for terrorists and insurgents (Brachman and Forest, 2007; Ranstorp, 2007). This demonstrated the adaptability of organisations like al-Qaeda to circumvent challenges to their operations on account of not being bound by 'spatial limitations of territoriality, transportation, and communications' (Innes, 2005: 300). The apparent liberation of terrorism from the constraints of neoliberal modernism is at the core of the conceptualization of al-Qaeda as a rhizomatic expression of global postmodernity (e.g. Devji, 2005). So too, defence academics' reinterpretation of al-Qaeda strategy from 'international terrorism' to 'global insurgency', which requires understanding them as 'an insurgent archipelago which flourishes in a space that is not territorially defined' (Mackinlay, 2009: 222; Kilcullen, 2009). This space is both the 'virtual territories of the mind' (Mackinlay and al-Baddawy, 2007: 5) and the informational networks of global telecommunications and the Internet. In this narrative, terrorists *qua* global insurgents utilise every available technology that enables them to capitalise upon the global flows of capital, personnel and information for the purposes of radicalisation, recruitment, fundraising, propaganda, training and the prosecution of large-scale attacks against (principally) Western governments and citizens.

Although not on the radar of global insurgency theorists, the possibility that al-Qaeda in particular might also infiltrate MMOs, closely followed by 'a sudden influx of Feds and international legal authorities', was suggested as a plausible trajectory of virtual world evolution as far back as 2005 (Au, 2005). Edward Castronova dedicated a whole chapter of his benchmark volume, *Synthetic Worlds* (2005), to the possible use of MMOs as 'topographies of terror'. By linking known terrorist uses of the Internet with speculative scenarios involving MMO technologies, Castronova described how any competent individual could assemble the components necessary to construct a training environment sufficient to turn 'a bumbling thug' into 'a successful terrorist' (Castronova, 2005: 232). More intriguingly still, Castronova proposed that through a series of live uplinks from operatives on the ground into a virtual simulacrum of an operational environment, a 'mastermind can not only talk to his followers; now he can effectively see a site through their eyes' (Castronova, 2005: 234). Given what we have learnt about the remote command-and-control aspects of the Mumbai attacks of 2008 (Kilcullen, 2013: 52-66), that a commander might be able to direct his operatives in this fashion is perhaps not as far-fetched as it sounds.

In mid-2007, the security blogosphere published articles dismissing mainstream media reports of Second Life terrorism but still warning of the possibilities that MMOs might 'enhance the terrorist threat' (Tanji, 2007; also, Cochran, 2007; Jones, 2007a). One imaginative scenario involved the creation of botnets to be 'rented, exploited and utilized to host a virtual world where terrorists would rehearse their real world performances' (Jones and Schrage, 2007). These 'jihadinet' scenarios directly referenced the sorts of off-the-shelf 'middleware' to which Castronova (2005) had previously drawn attention. One suggested that if 'the physical past can serve as a digital prologue to the future [policymakers] must invest in both the capacity and capability to deny aspiring terrorists this medium for mayhem' (Jones, 2007b). Several of these authors were involved in a panel event, 'Meta-Terror: Terrorism and the Virtual World', held on Capitol Hill in February 2008, and were interviewed on this topic by the BBC (Vallance, 2008). The message from the panel was that these

eventualities remained speculative but plausible and that government agencies should be empowered to deal with potential terrorist uses of MMOs (Cochran, 2008).

In April 2008, the specific issue of terrorists using MMOs for recruitment, radicalisation, training and operational planning was addressed before a Congressional subcommittee intended to develop a 'clear-eyed understanding' of potential terrorist use of virtual worlds (US House of Representatives, 2008: 5). Quizzed in public on news reports of the use of Second Life as a terrorist platform, Linden Lab CEO Philip Rosedale stated that his company had no evidence of such activity. Furthermore, given the historical ability of Linden to monitor irregular activity in Second Life, 'virtual world activities are somewhat more policeable and the law somewhat more maintainable within virtual worlds than it is today on Web sites' (US House of Representatives, 2008: 61). The implication was that MMOs might be entirely unsuitable terrorist environments on account of the omniscience of coding authorities.

A month after the Congressional hearing, the US Office of the Director of National Intelligence (ODNI) released a 'Data Mining Report', which defined data mining as 'a program involving pattern-based queries, searches or other analyses of 1 [sic] or more electronic databases [in order to] discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity' (US ODNI, 2008: 1). Much of the short report detailed what programs were being, or might be, developed by the ODNI's Office of Science and Technology's Intelligence Advanced Research Projects Activity (IARPA), which invests in research that has 'the potential to result in revolutionary, game-changing capabilities for the IC' (US ODNI, 2008: 2). One project was called Reynard, 'a seedling effort to study the emerging phenomenon of social (particularly terrorist) dynamics in virtual worlds and large-scale online games and their implications for the Intelligence Community'. In particular, stated ODNI, Reynard 'will seek to identify the emerging social, behavioural and cultural norms in virtual worlds and gaming environments', the findings from which would be applied 'to determine

the feasibility of automatically detecting suspicious behavior and actions in the virtual world' (US ODNI, 2008: 5).

During 2008, Reynard's focus changed from pattern-based data mining to 'leveraging expertise in the social science research community' to understand MMO behaviours (US ODNI, 2009: 7). In April 2009, solicitations for this reoriented Reynard Program were published and more details given as to the intended outcomes of the project. In particular, it would seek 'to identify behavioral indicators in VWs [virtual worlds] …. that are related to the RW [real-world] characteristics of the users' (IARPA, 2009: 6), whether these be individuals or groups. Research areas might include, 'Avatars and Representation, Communication, Things That Avatars Do, Group Formation and Dynamics, Money and Economics, and Cultural Differences' (IARPA, 2009: 7-8). At a meeting of possible Reynard partners, researchers and defence contractors were told that it was 'highly likely that persons of interest were using virtual spaces to communicate or coordinate' (Mazzetti and Elliott, 2013). These claims were not further substantiated but one successful grant applicant recalled that, '[we] were specifically asked not to speculate on the government's motivations and goals' (Mazzetti and Elliott, 2013). Teams from Lockheed Martin, Palo Alto Research Center, SAIC, SRI International and the University of Southern California were awarded contracts under the program, which ended in 2012. A summary of program outputs reports that researchers studied 15 thousand players from nine countries in 12 MMOs and found that real world characteristics could be predicted from MMO behaviours with an accuracy of over 75 percent (IARPA, 2013). None of the eight scholarly papers subsequently published mentioned terrorists or other agents of political or criminal violence.[1]

During the period of Reynard research, little was heard from the intelligence and security communities about MMOs. In September 2008, a Pentagon researcher showed how *World of Warcraft* could be used to plan an attack on the White House (Schachtman, 2008). Steven Aftergood

[1] A list of these papers is provided in IARPA (2013: 2).

of the Federation of American Scientists dismissed this exercise: 'Could terrorists use Second Life? Sure, they can use anything. But is it a significant augmentation? That's not obvious. It's a scenario that an intelligence officer is duty-bound to consider. That's all' (Schachtman, 2008). The speculative nature of these horizon-scanning exercises is encountered elsewhere, like Cole's walk-through of Second Life with an avatar named 'Farid' to demonstrate 'how easy it is for extremists to make use of the immersive nature of virtual worlds to draw individuals towards radical views' (Cole, 2012). The experiment did nothing of the sort but played to existing fears of Islamist radicalisation of 'empty vessel' Muslims via the Internet. A somewhat paranoid book on the topic (ar-Raqib and Roche, 2010) also tapped into concerns about Internet-enabled jihadism, and a novel, *MMORPG*, painted 'a chilling picture of the potential use terrorists could make of online computer games' (van Veen, 2011). The academic community expanded and intensified its research efforts but it seemed Reynard might have been the last evidence of IC interest in MMOs. That is, until late 2013, when disclosures by Edward Snowden suggested that the IC had been operationally engaged with MMOs even *before* Reynard and might still view these environments as potential sources of secret intelligence.

The Intelligence Community and Virtual Worlds

In December 2013, *The New York Times*, *The Guardian* and ProPublica, an online journalism non-profit, jointly released documents relating to the US/UK IC and virtual worlds (Mazzetti and Elliott, 2013; Ball, 2013; Elliott and Mazzetti, 2013). The documents consisted of two NSA documents classified 'Top Secret' (NSA, 2007, 2008) and a client report by the government contractor SAIC on the use of MMOs in government 'influence activities' (SAIC, 2007), written before their involvement with Reynard.[2] The earlier NSA document—possibly informed by the SAIC report—recommended increased IC investment in exploring and exploiting MMOs, what it called Games and Virtual Environments (GVE) (NSA, 2007). Extrapolating from known terrorist use of other Internet platforms

[2] As of September 2014, these were the only documents on this topic. See, https://www.aclu.org/nsa-documents-search, accessed September 1, 2014.

and applications it deduced that by 2010 terrorists would make 'wide use' of MMO functionality. These include the collaborative 'planning, comms [communications] and training' tools provided by these 'essentially private meeting places' which, crucially, are beyond the reach of conventional IC network surveillance. It bolstered this assertion by recognising existing technologies like Hezbollah's Special Forces 2 game for recruitment and training—'a radicalizing medium'—which is itself based on US government platforms like America's Army (see, Brady, 2012: 86-90)—and the use of Microsoft's Flight Simulator software in terrorist planning for 9/11. The NSA noted that when 'the [terrorist] mission is expensive, risky, or dangerous, it is often a wiser idea to exercise virtually, rather than really blow an operative up assembling a bomb or exposing a sleeper agent to law enforcement scrutiny', an approach also adopted by military forces worldwide, including the US (Smith, 2014).

The document drew attention to existing IC operations, which had identified 'Al Qaida terrorist target selectors and GVE executables […] associated with XboxLive, Second Life, World of Warcraft, and other GVEs'. These were identified via the NSA's PINWALE 'digital network intelligence' surveillance system and through the activities of the Office of Tailored Access Operations (TAO), a key intelligence-gathering unit headquartered at the NSA's Remote Operations Center at Fort Meade, MD. It also listed other targets, including 'Chinese hackers, an Iranian nuclear scientist, Hizballah, and Hamas members', whose online profiles and activities had presumably been linked with their 'real-world' identities and categorised as risky on that basis. GCHQ was already engaged in a 'vigorous effort to exploit GVEs' and the FBI, CIA and the Defense Human Intelligence (HUMINT) Service (now part of the Defense Clandestine Service of the Defense Intelligence Agency), 'all have HUMINT operations in Second Life and other GVEs'. Predicated on both possible and recorded terrorist use of these environments, MMOs 'offer a SIGINT/HUMINT opportunity space' ripe for exploitation by the IC if further resources were allocated to do so. It also recommended that IC-wide operations in GVEs should be 'deconflicted' to improve coordination, an indication of the

disorganised state of IC involvement in MMOs at that point, which included operations by the major US defense intelligence agencies (NSA, DIA), FBI, CIA and UK GCHQ.

If the 2007 document aimed to establish the general parameters of a programme for IC operations in MMOs, the later note focused on NSA collaboration with GCHQ in World of Warcraft (NSA, 2008). It outlined GCHQ's efforts via its Applied Research Special Topics (B18) branch to work with NSA's Global Network Exploitation (OPD-GNE) unit at Fort Meade and its Mission Development Center at Menwith Hill Station (MHS) in northern England. This project, based on two continents, aimed to 'filter the FORNSAT [foreign satellite] survey environment' to extract World of Warcraft 'metadata for SIGINT development and network knowledge enrichment'. GCHQ provided the technical means to extract and collate specific metadata from the raw satellite traffic provided by NSA, which was then returned to GCHQ for additional processing. From this process, GCHQ were able to correlate 'target entities to WoW [World of Warcraft] logon events and continues to uncover potential SIGINT value by identifying accounts, characters, and guilds related to Islamic Extremist Groups, Nuclear Proliferation and Arms Dealing'.

Metadata in this context referred to 'country and time zone information, local IP [Internet Protocol] addresses and realm server addresses [specific to MMO servers]', and was insufficient alone to provide real world identities, although GCHQ analysts had already 'correlated known SIGINT targets to online gaming events'. The note implies that 'traditional SIGINT' could 'follow emails, chat and buddy lists, whereas WoW target development [GCHQ's task] may follow character IDs and logons, gaming communication channels and guilds'.[3] The implication is that GCHQ's metadata project should be accompanied by content-focused SIGINT capable of generating more detailed knowledge about SIGINT targets, which *The New York Times* indicated GCHQ were capable of doing later that year (Mazzetti and Elliott, 2013). We do not know if GCHQ's project was the 'vigorous effort'

[3] On the distinction between 'content' and 'metadata' in the context of government surveillance, see Brown (2012).

referred to previously but the NSA reported that MHS and GCHQ would continue to collaborate on 'this potentially lucrative venue' (NSA, 2008).

The NSA documents give few clues as to the overall efficacy of this counterterrorism venture but there are hints from other unpublished papers as to its potential utility. GCHQ, for example—in a multi-agency enquiry called Operation Galician—assisted London's Metropolitan Police in arresting a criminal group selling stolen credit card data in an unnamed MMO (Mazzetti and Elliott, 2013). This case was successfully prosecuted in a British court in 2012 (The Telegraph, 2012). In what may be the first instance of an intelligence agency running a civilian agent in an MMO, GCHQ was helped by a Second Life informer who 'helpfully volunteered information on the target group's latest activities' (Mazzetti and Elliott, 2013). That GCHQ was interested in cultivating more HUMINT sources in MMOs is implied by the minutes of a January 2009 meeting, in which it was reported that GCHQ's 'network gaming exploitation team' had identified individuals as possible recruitment targets, including 'engineers, embassy drivers, scientists and other foreign intelligence operatives' with avatars in World of Warcraft (Mazzetti and Elliott, 2013).

In the absence of evidence describing the further development of IC attitudes to and activities in MMOs it is difficult to assert that they have been discounted as intelligence sources. This is particularly so when we consider that political discourses of the links between the Internet and terrorism—and other forms of political violence and criminality—have continued to intensify since 2009. This is allied to the emergence of cyber security as a central component of national and international security strategies. Under these conditions, in which cyber security has emerged to regulate all forms of Internet use and in which the scale and scope of Internet and communications surveillance have become increasingly apparent (Bauman et al, 2014), it would be unwise to contend that MMOs are no longer of interest to the IC. Notwithstanding uncertainty about the status of IC engagement with MMOs, what can we learn from the relationship between intelligence agencies

and virtual worlds about surveillance and security? In particular, how do intelligence agencies ascribe meaning to MMOs and MMO behaviours such that they are constructed as sites of security? How do intelligence practices blur the line between the virtual and the 'actual'?

Security and Surveillance

Post-9/11 security has often identified 'bad neighbourhoods' of cyberspace which 'deserved to be destroyed' (Manjikian, 2010: 392) but this does not seem to apply to MMOs, which intelligence agencies have preferred thus far to infiltrate rather than eliminate. Intelligence agencies have yet to articulate publicly legitimate reasons for legal or coercive interventions in MMOs and there is little current sign of an appetite to do so. They have preferred to maintain MMOs as research environments and as sources of potentially actionable intelligence instead. On a superficial level, why might this be so? If we argue that coding authorities are analogous to governments in their authority to act within their territories—whatever or wherever the integuments of MMOs actually *are*—they are not necessarily in control of people's actions within those spaces. There were early worries that the 'unbounded authority' of coding authorities might lead to 'virtual dictatorships' but by 2005 it had become clear that Second Life, for instance, had become an 'unknowable entity, even to its creators (Boellstorff, 2008: 222-223). Contrary to its CEO's statement before Congress, Linden Lab repeatedly showed an 'inability to control its own people and form a stable community' (MacCallum-Stewart, 2007: 205). MMOs had already become so big and so complex that coding authorities were no longer able to see or record all that went on in the environments they created.

This is to be expected. MMOs are worlds coded by their originators and their residents but they are not static. Code catalyses emergent forms of social action and social relations, non-linear interactions utilising low-level rules to generate outcomes not predictable by coders or architects (Boellstorff, 2008: 223; Malaby, 2008: 83-90). Malaby argues that the deliberate cultivation of emergent social phenomena is a novel innovation of MMOs, one that 'confounds the well-

entrenched modernist aspirations of total control' (Malaby, 2009: 131). Intelligence agencies are likely therefore to wonder whether MMOs facilitate conditions favourable to the emergence of potentially subversive activities, particularly if these are not identified or interdicted by coding authorities. MMOs are therefore constructed as sites of (in)security requiring some form of intervention to prevent the transmission of insecure behaviours from the virtual to the real world, or, as Boellstorff more correctly notes, the 'actual' world; virtual worlds are just as phenomenologically 'real' as anywhere else (Boellstorff 2008: 19).

In keeping with the intelligence community's general preference for cultivating sources rather than eliminating them, the favoured mode of generating knowledge about MMO behaviours is surveillance, although future use of more coercive forms of intervention cannot be discounted (Castronova, 2005: 236-246). Bauman et al (2014: 125) note how intelligence agencies network transnationally in order to circumvent legal constraints on gathering intelligence on domestic targets via surveillance, thereby rendering the boundaries between foreign and domestic jurisdictions indistinct and practically irrelevant to the IC. Given the heterogeneous national make-up of MMO populations (Nardi, 2010: 8), it is almost inevitable that bulk collection of data and metadata from virtual worlds will be unable to discriminate between foreign and national, at least during the acquisition phase. It is more likely that the IC will seek an accommodation with coding authorities than with MMO players and inhabitants, none of whom have consented for their personal data in such fashion. That NSA and GCHQ targeted MMOs operated by US companies only is perhaps a function of the 'ambiguous complicity' of Internet companies with the IC (Lyon, 2014). All the MMO operators mentioned in NSA documents denied being asked for or granting consent for IC activities but it is a matter of record, post-Snowden, that western intelligence agencies obtained personal data from private companies like Google and Skype and telecommunications providers like BT, Vodafone and Verizon, sometimes in coercive fashion but often through voluntary data-sharing arrangements (Bauman et al, 2014: 123).

We do not know the precise relationship between the surveillant IC and coding authorities but it may be that the latter's denial of complicity is an attempt to maintain the proprietary boundary between MMOs over which they exert control and the actual world over which they do not. This digital carapace is both an engineering construct maintained by coding authorities to exclude non-paying or non-registered users out but it is also congruent with a fundamental notion at the core of the MMO experience. Castronova formulates the demarcation between the 'virtual' and the 'real' as a membrane, 'a shield of sorts, protecting the fantasy world from the outside world' (Castronova, 2005: 147). This is a porous boundary across which people transmit beliefs and behaviours but it is still an identifiable interface that serves to reinforce the distinctive identities of the actual and the virtual (Boellstorff, 2008: 23). This concept is foundational to game studies and is derived from the idea of the 'magic circle' within which games are played and sacralised and which marks off the space of play from the wider world (Salen and Zimmerman, 2004: 95).

The membrane is also useful as a means of understanding the threshold between the 'illicit' practices of state surveillance and 'licit' commercial dataveillance. Nakamura reports that prior to Reynard MMOs were relatively free of state surveillance and users could conduct themselves with little fear of state censure or interdiction (Nakamura, 2009). They were not, however, exempt from dataveillance, the collection of personally identifiable information by coding authorities which, as outlined previously, are able to restrict users' activities in ways analogous to the state. Nakamura distinguishes dataveillance from surveillance in that the former 'refrains from watching actual users, only their avatars' (Nakamura, 2009: 155). Given Reynard's claim to correlate in-world (avatar) and actual behaviours to statistically significant levels, Nakamura's prediction that the line between dataveillance and surveillance may become 'radically blurred' (Nakamura, 2009: 155) is a prescient one. If intelligence projects like Reynard and those discussed in classified NSA documents were to become normalised, this 'would fail to exempt any type of "social interaction" [in MMOs] from

scrutiny' (Nakamura, 2009: 157), on the basis that any social activity *might be* terrorist activity. Under these conditions, presumptions of anonymity of identity and personal privacy in virtual worlds would be meaningless and by this reasoning, 'all virtual worlds are potentially "jihad worlds" and must be monitored as such' (Nakamura, 2009: 156).

However, there is a hint of lingering modernity about the inside/outside dichotomy suggested by the magic circle and its derivatives. Under conditions of networked globalisation and its reconfiguration of established modalities of identity and sovereignty, boundaries have become 'elusive phenomena' (Bauman et al, 2014: 136). It is not sufficient to note that intelligence agencies disrupt a sacred boundary between in-world and out-world when MMOs themselves challenge this comfortable demarcation. Lehdonvirta proposes that MMOs are part of a social reality in which numerous social worlds overlap and intersect, whether these are 'international or local, emergent or established, public or hidden, hierarchical or anarchic' (Lehdonvirta, 2010). Every MMO is situated at and constructed by the intersection of many social worlds rather than 'a cradle of a single monolithic social world' (Lehdonvirta, 2010). Its technical perimeter is not identical to its social one, which includes the relations of many different actors and assemblages, amongst which we must number the interactions of the IC with a range of other individuals and communities. Those who frequent MMOs have been characterised as 'geopolitically unconstrained global citizens' (Hinrichs, 2011), at ease in the globalised flows and spaces of contemporary ICTs. Presumably, intelligence agencies are concerned that terrorists might be just such people, as theories of global insurgency predict, for example.

The surveillance of MMOs attempts to stabilise these global flows long enough that they become subject to manipulation in the name of security. This 'surveillant assemblage' (Haggerty and Ericson, 2000) requires that avatars and the real-life individuals whom they represent are transformed into 'data subjects', information about whose identities and behaviours are seen as having potential

future value or utility (Bauman et al, 2014: 138). Moreover, data subjects can be tracked as they move between social worlds, between the spaces of online play (Lefebvre 1996: 172) and other spaces of both the virtual and the actual. Data mining and algorithmic means of generating meaning from large data sets are calibrated towards identifying problematic behaviours and associations between data subjects (Gandy, 2003). From the perspective of the IC, if there is a membrane between actual and virtual, it is a thin, technical one, its social construction and social meaning unimportant relative to the concerns of the security state. Sociological understandings of 'inside' and 'outside' a virtual world are reformulated as 'inside' and 'outside' the state, a transformation contingent not on locality but on the politics of intent, as revealed through infallible data and algorithmic analysis.Intelligence agencies have shown themselves adept at riding roughshod over distinctions between public/private and virtual/actual and, instead, the inference of 'association rules' between people, places, events and things transforms ludic spaces into 'violent geographies' (Amoore 2009) of counterterrorism and security, contiguous with both the physical and behavioural landscapes of the actual world. The subtleties of actual-virtual and virtual-virtual border construction are subordinated to the construction of a world in which borders themselves are considered inimical to the exigencies of surveillance.

Conclusion

Wagner James Au, Second Life's first 'embedded journalist', opened his account of the history of Second Life with the statement: 'This is the epic story of an empire that exists inside a metal box' (Au, 2008: ix). If this allusion to a computer server was ever accurate, it is not any more. Virtual worlds are not entities somehow insulated from society but they exist at the intersection of multiple social worlds, including those concerned with national security and its constituent practices of surveillance and interdiction. The intelligence community employs a range of algorithmic techniques for the processing of 'big data' and the generation of knowledge about the potentially risky behaviours of those who frequent these virtualised environments. The mass collection of data and

metadata across jurisdictional boundaries allows intelligence agencies to map the relations between data subjects and construct probabilistic models of undesirable behaviour. Reynard, in particular, has been praised by a former director of GCHQ as a worthy example of social media intelligence (SOCMINT) and a necessary development of data analytics in virtual worlds research (Omand et al, 2012: 822). These projects emphasise the identification of behaviours and norms consistent with and predictive of terrorist and insurgent actions that might be transferred to the 'real world'.

We cannot know if potent forces of political violence will eventually emerge from the ludic and we are limited in what we can say about intelligence agencies' actual or possible modes of engagement or their specific institutional attitudes to MMOs. MMOs continue to attract large numbers of regular participants and are important sites of social interaction but they have had rather less impact on the 'real world' than either their initial public hype promised or elements of the security and intelligence communities have imagined. It is hoped that more details of intelligence activities will emerge to enable researchers to develop further the empirical and conceptual themes of this article. We can be certain that all virtual environments, of which MMOs are a small subset, will be subject to increased surveillance and monitoring in the name of security, particularly for the purposes of counterterrorism and domestic counter-subversion. However MMOs evolve they are unlikely to be ignored by an intelligence community armed with research funds and powerful 'big data' analytics. Historically, the events and processes outlined in this article will be regarded as another stage in the development of the hyper-surveillant state, when 'the minacious twinkle in the electronic eye' (Lyon, 2001: 147) turned to virtual worlds and their experimental populations and practices.

Acknowledgements

I thank the editors and two anonymous reviewers for their constructive comments on draft versions of this article.

References

AMOORE, LOUISE. (2009) Algorithmic War: Everyday Geographies of the War on Terror. *Antipode* 41(1): 49-69.

ANDERSON, BENEDICT. (2006 [1983]) *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London: Verso.

AR-RAQIB, AKIL AND EDWARD M. ROCHE. (2010) *Virtual Worlds, Real Terrorism*. Den Haag: Aardwolf Publications.

AU, WAGNER JAMES. (2005) Taking New World Notes: An Embedded Journalist's Rough Guide to Reporting from Inside the Internet's Next Evolution. *First Monday* special issue no. 5: Virtual Architecture at State of Play III, 6-8 October 2005. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/1562/1477. (Accessed April 7, 2014.)

AU, WAGNER JAMES. (2007) "Jihad and Second Life (Updated)." *New World Notes*, 7 August. Available at http://nwn.blogs.com/nwn/2007/08/second-life-and.html. (Accessed April 9, 2014.)

AU, WAGNER JAMES. (2008) *The Making of Second Life: Notes from the New World*. New York: Harper Collins.

BALL, JAMES. (2013) "Xbox Live Among Services Targeted by US and UK Spy Agencies." *The Guardian*, 9 December. Available at http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life. (Accessed September 2, 2014.)

BARTON, MATT. (2008) *Dungeons and Desktops: The History of Computer Role-Playing Games*. Wellesley: A.K. Peters.

BAUMAN, ZYGMUNT, DIDIER BIGO, PAOLO ESTEVES, ELSPETH GUILD, VIVIENNE JABRI, DAVID LYON AND R.B.J. WALKER. (2014) After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8(2): 121-144.

BENGTSSON, STINA. (2011) Virtual Nation Branding: The Swedish Embassy in Second Life. *Journal of Virtual Worlds Research* 4(1). Available at http://journals.tdl.org/jvwr/index.php/jvwr/article/viewFile/2111/5547. (Accessed April 7, 2014.)

BETZ, DAVID J. AND TIM STEVENS. (2011) *Cyberspace and the State*. London: Routledge.

BETZ, DAVID J. AND TIM STEVENS. (2013) Analogical Reasoning and Cyber Security. *Security Dialogue* 44(2): 147-164.

BOELLSTORFF, TOM. (2008) *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*. Princeton: Princeton University Press.

BRACHMAN, JARRET AND JAMES F. FOREST. (2007) Exploring the Role of Virtual Camps. In *Denial of Sanctuary: Understanding Terrorist Safe Havens*, edited by Michael A. Innes. Westport: Praeger Security International.

BRADY, SARA. (2012) *Performance, Politics and the War on Terror: 'Whatever It Takes'.* Basingstoke: Palgrave Macmillan.

BROWN, IAN. (2012) Government Access to Private-Sector Data in the United Kingdom. *International Data Privacy Law* 2(4): 230-238.

BURKE, TIMOTHY. (2007) "More Dots! Cried the Terrorist." *Terra Nova*, 1 August. Available at http://terranova.blogs.com/terra_nova/2007/08/more-dots-cried.html. (Accessed April 9, 2014.)

CARPENTER, CHARLI AND DANIEL W. DREZNER. (2010) International Relations 2.0: The Implications of New Media for an Old Profession. *International Studies Perspectives* 11(3): 255-272.

CARVALHO, GUSTAVO. (2013) Virtual Worlds Can Be Dangerous: Using Ready-Made Computer Simulations for Teaching International Relations. *International Studies Perspectives*. Available at http://onlinelibrary.wiley.com/doi/10.1111/insp.12053/abstract. (Accessed April 7, 2014.)

CASTELLS, MANUEL. (2009) *Communication Power.* Oxford: Oxford University Press.

CASTRONOVA, EDWARD. (2003) On Virtual Economies. *Game Studies* 3(2). Available at http://www.gamestudies.org/0302/castronova/. (Accessed April 9, 2014.)

CASTRONOVA, EDWARD. (2005) *Synthetic Worlds: The Business and Culture of Online Games*. Chicago: University of Chicago Press.

COCHRAN, ANDREW, (2007) "Part II of "MetaTerror: The Potential Use of MMORPGs by Terrorists." *Counterterrorism Blog*, 12 March. Available at

http://counterterrorismblog.org/2007/03/part_ii_of_metaterror_the_pote.php. (Accessed April 7, 2014.)

COCHRAN, ANDREW. (2008) "Event Transcript and Related Links: "Meta-Terror: Terrorism and the Virtual World." *Counterterrorism Blog*, 7 March. Available at http://counterterrorismblog.org/2008/03/event_transcript_and_related_l.php. (Accessed April 7, 2014.)

COLE, JAMES. (2012) Radicalisation in Virtual Worlds: Second Life Through the Eyes of an Avatar. *Journal of Policing, Intelligence & Counter Terrorism* 7(1): 66-79.

COLE, HELENA AND MARK D. GRIFFITHS. (2007) Social Interactions in Massively Multiplayer Online Role-Playing Games. *CyberPsychology & Behavior* 10(4): 575-583.

COLE, JUAN. (2008) Osama Bin Laden's 'Second Life'. *Salon*, 25 February. Available at http://www.salon.com/2008/02/25/avatars_2/. (Accessed 9 April, 2014.)

COWAN, GEOFFREY AND AMELIA ARSENAULT. (2008) Moving from Monologue to Dialogue to Collaboration: The Three Layers of Public Diplomacy. *The ANNALS of the American Academy of Political & Social Science* 616(1): 10-30.

CULL, NICHOLAS J. (2008) Public Diplomacy: Taxonomies and Histories. *The ANNALS of the American Academy of Political & Social Science* 616(1): 31-54.

DAMER, BRUCE, STUART GOLD, KAREN MARCELO AND FRANK REVI. (2004) Inhabited Virtual Worlds in Cyberspace. In *Virtual Worlds: Synthetic Universes, Digital Life, and Complexity*, edited by Jean-Claude Heudin. Boulder: Westview Press.

DEIBERT, RONALD J. (2002) Circuits of Power: Security in the Internet Environment. In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany: State University of New York Press.

DEVJI, FAISAL. (2005) *Landscapes of the Jihad: Militancy, Morality, Modernity*. London: Hurst & Company.

DUNN CAVELTY, MYRIAM. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

DUNN CAVELTY, MYRIAM, VICTOR MAUER AND SAI FELICIA KRISHNA-HENSEL, eds. (2007) *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate.

THE ECONOMIST. (2007) "A World Wide Web of Terror." 12 July. Available at http://www.economist.com/node/9472498. (Accessed April 7, 2014.)

ELLIOTT, JUSTIN AND MARK MAZZETTI. (2013) "World of Spycraft: NSA and CIA Spied in Online Games". *ProPublica*, 9 December. Available at http://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games. (Accessed April 22, 2014.)

ENLOE, CYNTHIA. (2011) The Mundane Matters. *International Political Sociology* 5(4): 447-450.

ERIKSSON, JOHAN AND GIAMPIERO GIACOMELLO, eds. (2009) The Forum: Who controls the Internet? Beyond the Obstinacy or Obsolescence of the State. *International Studies Review* 11(1): 205-230.

FRANKLIN, M.I. (2013) *Digital Dilemmas: Power, Resistance, and the Internet*. New York: Oxford University Press.

GANDY, OSCAR H. (2003) Data Mining and Surveillance in the Post-9/11 Environment. In *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, edited by Kirstie Ball and Frank Webster. London: Pluto Press.

GOURLAY, CHRIS AND ABUL TAHER (2007) 'Virtual Jihad Hits Second Life Website', *Sunday Times*, 5 August. Available at http://www.thesundaytimes.co.uk/sto/news/world_news/article69229.ece. (Accessed April 7, 2014.)

HAGGERTY, KEVIN D. AND RICHARD V. ERICSON. (2000) The Surveillant Assemblage. *British Journal of Sociology* 51(4): 605-622.

HERRERA, GEOFFREY. (2009) Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In *Power and Security in the Information Age: Investigating the Role of the State in*

Cyberspace, edited by Myriam Dunn Cavelty, Victor Mauer and Sai Felicia Krishna-Hensel. Aldershot: Ashgate.

HINRICHS, RANDY J. (2011) Avatars as the First Manifestation of Geo-Politically Unconstrained Global Citizens. *Journal of Virtual Worlds Research* 4(2). Available at http://journals.tdl.org/jvwr/index.php/jvwr/article/view/3533. (Accessed April 7, 2014.)

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY. (2009) Broad Agency Announcement—Reynard Program, IARPA-BAA-09-05, 21 April. Available at http://ai.arizona.edu/mis510/other/6_Reynard_IARPA-BAA-09-05a.pdf. (Accessed April 9, 2014.)

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY. (2013) Reynard Program Summary. November. Available at http://s3.documentcloud.org/documents/837419/iarpa-reynard-summary-nov2013.pdf. (Accessed April 23, 2014.)

INNES, MICHAEL A. (2005) Terrorist Sanctuaries and Bosnia-Herzegovina: Challenging Conventional Assumptions. *Studies in Conflict & Terrorism* 28(4): 295-305.

JANTZEN, GITTE AND JANS F. JENZEN. (1993) Powerplay—Power, Violence and Gender in Video Games. *Artificial Intelligence & Society* 7(4): 368-385.

JONES, RODERICK. (2007a) "MetaTerror: The Potential Use of MMORPGs by Terrorists." *Counterterrorism Blog*, 1 March. Available at http://counterterrorismblog.org/2007/03/metaterror_the_potential_use_o.php. (Accessed April 7, 2014.)

JONES, RODERICK. (2007b) "Jihadinets." *Counterterrorism Blog*, 17 December. Available at http://counterterrorismblog.org/2007/12/jihadinets.php. (Accessed September 2, 2014.)

JONES, RODERICK, AND MICHAEL SCHRAGE. (2007), 'Jihadinets', *Counterterrorism Blog*, 17 December. Available at http://counterterrorismblog.org/2007/12/jihadinets.php. (Accessed April 9, 2014.)

KILCULLEN, DAVID. (2009) *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. London: Hurst.

KILCULLEN, DAVID. (2013) *Out of the Mountains: The Coming Age of the Urban Guerrilla*. London: Hurst.

KLINE, STEPHEN, NICK DYER-WITHEFORD AND GREIG DE PEUTER. (2003) *Digital Play: The Interaction of Technology, Culture, and Marketing*. Kingston: McGill-Queen's University Press.

KÜCKLICH, JULIAN RAUL. (2009) Virtual Worlds and Their Discontents: Precarious Sovereignty, Governmentality, and the Ideology of Play. *Games & Culture* 4(4): 340-352.

LEFEBVRE, HENRI. (1996) *Writings on Cities*, translated and edited by Eleonore Kofman and Elizabeth Lebas. Oxford: Blackwell.

LEHDONVIRTA, VILI. (2010) Virtual Worlds Don't Exist: Questioning the Dichotomous Approach in MMO Studies. *Game Studies* 10(1), n.p. Available at http://gamestudies.org/1001/articles/lehdonvirta. (Accessed April 25, 2014.)

LUDLOW, PETER AND MARK WALLACE. (2007) *The Second Life Herald: The Virtual Tabloid that Witnessed the Damn of the Metaverse*. Cambridge: MIT Press.

LYON, DAVID. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

LYON, DAVID. (2014) Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society* 1(2).

MACCALLUM-STEWART, ESTHER. (2007) The Warfare of the Imagined—Building Identities in *Second Life*. *International Journal of Performance Arts & Digital Media* 3(2-3): 197-208.

MACKINLAY, JOHN. (2009) *The Insurgent Archipelago: From Mao to Bin Laden*. London: Hurst.

MACKINLAY, JOHN AND ALISON AL-BADDAWY. (2005) *Rethinking Counterinsurgency.* RAND Counterinsurgency Study, Vol. 5. Santa Monica, CA: RAND Corporation.

MALABY, THOMAS M. (2009) *Making Virtual Worlds: Linden Lab and Second Life*. Ithaca: Cornell University Press.

MANJIKIAN, MARY MCEVOY. (2010) From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* 54(2): 381-401.

MAZZETTI, MARK AND JUSTIN ELLIOTT. (2013) “Spies Infiltrate a Fantasy Realm of Online Games”. *The New York Times*, 9 December. Available at http://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html. (Accessed April 22, 2014.)

MILDENBERGER, CARL. (2013) The Constitutional Political Economy of Virtual Worlds. *Constitutional Political Economy* 24(3): 239-264.

MUELLER, MILTON L. (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge: MIT Press.

NAKAMURA, LISA. (2009) The Socioalgorithmics of Race: Sorting It Out in Jihad Worlds. In *The New Media of Surveillance*, edited by Shoshana Magnet and Kelly Gates. Abingdon: Routledge.

NARDI, BONNIE. (2010) *My Life as a Night Elf Priest: An Anthropological Account of World of Warcraft*. Ann Arbor: University of Michigan Press.

NATIONAL SECURITY AGENCY. (2007) Topic: Exploiting Terrorist Use of Games and Virtual Environments. Available at: https://freesnowden.is/wp-content/uploads/2013/12/nsa-games-paper.pdf. (Accessed April 22, 2014.)

NATIONAL SECURITY AGENCY. (2008) MHS and GCHQ ‘Get in the Game’ with Target Development for World of Warcraft Online Gaming. Available at: http://www.freesnowden.is/wp-content/uploads/2013/12/First.pdf. (Accessed April 8, 2014.)

O’BRIEN, NATALIE. (2007) “Virtual terrorists.” *The Australian*, 31 July. Available at http://www.theaustralian.com.au/news/features/virtual-terrorists/story-e6frg6z6-1111114072291. (Accessed April 9, 2014.)

OMAND, DAVID, JAMIE BARTLETT AND CARL MILLER. (2012) Introducing Social Media Intelligence (SOCMINT). *Intelligence & National Security* 27(6): 801-823.

ONDREJKA, CORY. (2007) Collapsing Geography: *Second Life*, Innovation, and the Future of National Power. *Innovations* 2(3): 27-54.

ÓSKARSSON, PÉTUR JÓHANNES. (2008) The Council of Stellar Management: Implementation of Deliberative, Democratically Elected, Council in EVE. Available at http://www.nytimes.com/packages/pdf/arts/PlayerCouncil.pdf. (Accessed April 9, 2014.)

RANSTORP, MAGNUS. (2007) The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalization. In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello. London: Routledge.

REPUBLIC OF MALDIVES. (2007) "Maldives Unveils World's First Virtual Embassy". 22 May. Available at http://www.maldiveshighcommission.org/archive/?s=10&grupa=1&id=57&new=ok. (Accessed April 10, 2014.)

ROSELLE, LAURA, ALISTER MISKIMMON AND BEN O'LOUGHLIN. (2014) Strategic Narrative: A New Means to Understand Soft Power. *Media, War & Conflict* 7(1): 70-84.

SACO, DIANA. (1999) Colonizing Cyberspace: 'National Security' and the Internet. In *Cultures of Insecurity: States, Communities, and the Production of Danger*, edited by Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall. Minneapolis: University of Minnesota Press.

SAIC. (2007) Games: A Look at Emerging Trends, Uses, Threats and Opportunities in Influence Activities. Available at https://freesnowden.is/wp-content/uploads/2013/12/Third.pdf. (Accessed April 22, 2014.)

SALEN, KATIE AND ERIC ZIMMERMAN. (2004) *Rules of Play: Game Design Fundamentals*. Cambridge: MIT Press.

SCHACHTMAN, NOAH. (2008) Pentagon Researcher Conjures *Warcraft* Terror Plot. *Wired*, 15 September. Available at http://www.wired.com/2008/09/world-of-warcra/. (Accessed April 9, 2014.)

SJOBERG, LAURA. (2013) Feminist IR 101: Teaching Through Blogs. *International Studies Perspectives* 14(4): 383-393.

SMITH, ROGER. (2014) Military Simulations Using Virtual Worlds. In *The Oxford Handbook of Virtuality*, edited by Mark Grimshaw. Oxford: Oxford University Press.

STEPHENSON, NEAL. (1992) *Snow Crash*. New York: Random House.

TANJI, MICHAEL. (2007) "Second Life: Elevating Terrorist Training." *ThreatsWatch*, 14 May. Available at http://threatswatch.org/rapidrecon/2007/05/second-life-elevating-terroris/. (Accessed April 9, 2014.)

TAYLOR, T.L. (2006) Beyond Management: Considering Participatory Design and Governance in Player Culture. *First Monday* special issue no. 7: Command Lines: The Emergence of Governance in Global Cyberspace. Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/1611/1526. (Accessed April 23, 2014.)

THE TELEGRAPH. (2012) "Police Search for 11,000 in Identity Scam." Available at http://www.telegraph.co.uk/news/uknews/crime/9321081/Police-search-for-11000-in-identity-scam.html. (Accessed April 22, 2014.)

TUMBER, HOWARD AND MICHAEL BROMLEY. (1998) Virtual Soundbites: Political Communication in Cyberspace. *Media, Culture & Society* 20(1): 159-167.

US HOUSE OF REPRESENTATIVES. (2008) *Online Virtual Worlds: Applications and Avatars in a User-Generated Medium*. Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, hearing, 1 April. Washington, DC: Government Printing Office. Available at http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg50918/pdf/CHRG-110hhrg50918.pdf. (Accessed April 9, 2014.)

US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. (2008) Data Mining Report. 15 February. Available at http://www.fas.org/irp/dni/datamining.pdf. (Accessed April 9, 2014.)

US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. (2009) Data Mining Report. March. Available at http://info.publicintelligence.net/ODNI_Data_Mining_Report_09.pdf. (Accessed April 23, 2014.)

VALLANCE, CHRIS. (2008) "US Seeks Terrorists in Web Worlds." *BBC News*, 3 March. Available at http://news.bbc.co.uk/1/hi/technology/7274377.stm. (Accessed April 9, 2014.)

VAN VEEN, EMILE. (2011) *MMORPG: How a Computer Game Becomes Deadly Serious*. Self-published.

WARBURTON, STEVEN. (2009) Second Life in Higher Education: Assessing the Potential for and the Barriers to Deploying Virtual Worlds in Learning and Teaching. *British Journal of Educational Technology* 40(3): 414-426.

WEIMANN, GABRIEL. (2006) *Terror on the Internet: The New Arena, the New Challenges*. Washington, DC: US Institute of Peace Press.

WEIR, KIMBERLY and MICHAEL BARANOWSKI. (2011) Simulating History to Understand International Politics. *Simulation & Gaming* 42(4): 441-461.

WILLIAMS, DMITRI, NICHOLAS DUCHENEAUT, LI XIONG, YUANYUAN ZHANG, NICK YEE AND ERIC NICKELL. (2006) From Tree House to Barracks: The Social Life of Guilds in World of Warcraft. *Games & Culture* 1(4): 338-361.