Western Security and Virtual Space: Some Examples From 2013

https://www.e-ir.info/2013/03/06/western-security-and-virtual-space-some-examples-from-2013/

PHILIP KIRBY, MAR 6 2013

The US Department of Homeland Security launched a new website last Thursday (February 21): the National Initiative for Cybersecurity Careers and Studies (NICCS). A "One Stop Shop for Cybersecurity Careers and Studies", "NICCS provides a comprehensive online resource for cyber education and training", in the words of DHS Chief, Janet Napolitano. The Initiative's purpose, she continues, "[is] to develop the next generation of cyber professionals to protect against evolving cyber threats". It reflects part of a broader shift at the DHS; an organisation that, since their inception in 2003, have devoted greater and greater attention to the threat of cyberterrorism. This latest website follows the institution of a specialist Cyber Security Division in 2011, "in response to the increasing importance of the cybersecurity mission [to homeland security efforts]."

The website comes just days after a report by Mandiant, a US cyber security firm, which claimed to have discovered the Chinese source of a series of international cyber-attacks. In recent weeks, US newspapers including *The New York Times* and *The Wall Street Journal*, as well as the technology firms, Apple and Microsoft, have been the targets of cyber terrorism, linked to China. The Chinese authorities vociferously denied the accusations, noting that they, too, were often victims of such attacks. The US State Department, however, appeared to endorse Mandiant's findings. "We've… regularly and repeatedly raised our concerns at the highest level with the Chinese Government about cyber theft," the spokesperson said, "including with senior Chinese officials and the military. We'll continue to do that." The State Department's specific comments followed the more general statements of President Obama, in his State of the Union address in January this year. "America must… face the rapidly growing threat from cyber-attacks," the President said. "Now, we know hackers steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems."

These examples are interesting for their construction of space. The importance of safeguarding virtual space, they imply, is so that the imagined space of the nation might be similarly protected. NICCS will train a new generation of cyber warriors, for example, to defend the American homeland (an equally intangible concept) from the threat of 'cyber terrorists' (another vague, ill-defined group). The State Department and Obama want to protect the 'imagined community' of the nation through control of the digital environment, too. Only later, once the battle for virtual space has been won (or lost) will effects actually be seen and felt; through the destruction of physical infrastructure, such as power networks or transportation systems. In this way, the new battleground of the War on Terror is painted as an updated, cyber version of Thomas Barnett's influential formulation, 'The Pentagon's New Map'. In Barnett's opinion, the world was split, at the dawn of the War on Terror, between a safe, 'integrating' section, and an unsafe, 'non-integrating gap'; full of dangers. The solution, as such, was for Western warriors to intervene in the latter; to defeat Eastern foes, amongst others, by controlling this volatile region. Today the 'non-integrating gap' has shifted from the physical to the virtual, and requires a similar change in military skill sets. Now 'troops' need to be computer literate, not just armed and ready.

Indeed, the increasing overlap of virtual and physical skills in the Western military was also demonstrated recently, by an actor on the other side of the Atlantic. Prince Harry, second in line to the British throne, returned (with great media fanfare) from a three month deployment in Afghanistan in late January. The second of his deployments, the

first was curtailed after news of his location was leaked by the press, thus putting Harry and his fellow soldiers at greater risk from Taliban attacks. To better safeguard Harry this time the army transferred him from the dangerous space of ground level, to the relatively safer region of air space; retraining him as a gunner on a British Apache helicopter (the Taliban have never brought down such an aircraft). But it is not the martial differences between air space and ground level that I want to focus on here (for this, see Pete Adey, Mark Whitehead, and Alison William's forthcoming book, *From Above*). Rather, it is the importance of virtual space in the Prince's stated approach to fighting.

In a series of interviews, Prince Harry spoke of his satisfaction at being on active duty. In particular, he cited his ability to play computer games as an advantage in the fighting that he had undertaken; fighting that included, he implied, killing the enemy. "I'm one of those people who loves playing PlayStation and Xbox, so with my thumbs [on the trigger] I like to think that I'm probably quite useful." He then continued to say that, if the Taliban were a threat to him or his comrades, he'd have no hesitation in taking them, "out of the game". Whilst the initial media response to the interview focussed on the Prince's admission that he had killed people, later questions concerned his method, and the fact that he had likened the experience to a computer game. The Prince's reference, though, was hardly novel; the British Army themselves have endorsed the kind of connection that Harry made. In 2009, they introduced a recruiting campaign called, "Start Thinking Soldier", which involved playing through a set of virtual missions to see whether one had the 'right stuff'. This followed a similar approach in the US, where the military introduced a recruitment tool, 'America's Army', which required comparable actions from its users.

What is notable about all of these examples is how they create immersive worlds. Modern combat computer games, such as those for the PlayStation, as well as Start Thinking Soldier and America's Army, attempt to make the experience of playing as realistic as possible. Through the screen, a close-up perspective of the action is given, in which the viewer is invisible. As the geographer, Derek Gregory, says, "video games do *not* stage violence as passive spectacle; they are profoundly immersive, drawing players in to their virtual worlds". And Apaches helicopters, such as Prince Harry's, recreate just such an experience, with a zoomed video display of the target and controls akin to a games console. Prince Harry's comparison of war with computer games, then, might be read less as a suggestion that Western soldiers are becoming increasingly divorced from war (although this may be true, too), and more as evidence that the experience of computer games is being replicated by militaries to facilitate easier and simpler killing.

Already, the interface between computer games and the military is an important research agenda in geopolitics (see, for example, Marcus Power, Mark Salter, and Ian Shaw). And the signs are that virtual space, on a variety of different terrains and at a variety of different scales, promises to be a rich research field in the future. Were Prince Harry's comments a slip of the tongue, a poor metaphor, or a reflection of the fact that, for many Western militaries (especially in the age of the drone), the remote, the virtual, and the playful are an accurate way to describe the experience of war? And, if Western nations are increasingly seeing virtual space as a volatile and potentially dangerous space that requires control, might this experience only become more common in the future?

—

Philip Kirby *is a final year PhD student at Royal Holloway, University of London, funded by the ESRC. Read more of GPS: Geopolitics and Security – Critical Perspectives From Royal Holloway.*