Arms, Arms Control and Technology

Bruno Tertrais

Cyber War Will Not Take Place

Thomas Rid. London: C. Hurst and Co., 2013. £14.99. 218 pp.

Two decades after the pioneering RAND studies heralding the 'coming cyber war', such a threat increasingly makes headlines, to the point that it was presented as the dominant issue in the first meeting between US President Barack Obama and Chinese President Xi Jinping in June 2013. It is therefore tempting to see the topic as the twenty-first century equivalent of the nuclear threat, which dominated the US–Soviet relationship during the Cold War.

Not so, claim a few contrarian Western analysts – a small group among whom Thomas Rid, reader at King's College London, is a new and influential voice. His book grew out of a widely-read article that appeared in the January 2012 issue of the *Journal of Strategic Studies*. Its title comes from Jean Giraudoux's play *La Guerre de Troie N'aura Pas Lieu* ('*The Trojan War Will Not Take Place*'). The pun may have been intended, given the importance of so-called Trojan viruses, a type of computer malware.

Cyber War Will Not Take Place is a methodical attempt to demonstrate that there is not – and will probably never be – such thing as cyber-war: 'a highly problematic, even a dangerous, concept' (p. 37). Rid describes classic Clausewitzian war as being violent, instrumental (that is, as a means to an end) and political. In fact, according to the author, few cyber attacks have even one of these features, and all nefarious cyber activities are mere variations on either sabotage, espionage or subversion. Although he notes that Stuxnet, which attacked Iranian nuclear installations, took computer sabotage to an entirely new level, he also believes that – so far, at least – a cyber attack that produces a level of pain comparable to that caused by a strategic air campaign is 'plainly unimaginable', even if it involves an attack on infrastructure (p. 17). Another reason that the term cyber-war is misleading, of course, is the attribution problem. Publicly known cases of a successful attribution (such as the 2011 episode involving the Georgian government and a Russian attacker) are rare, and cases in which a government can be identified as the perpetrator are even rarer.

Rid usefully distinguishes between aggressive cyber attacks, which are not necessarily intentional and instrumental, and cyber weapons, which are computer codes aimed at 'threatening or causing physical, functional, or mental harm to structures, systems, or living beings' (p. 37). As the author puts it, 'code ... does not come with its own explosive charge' (p. 13). He notes that cyber capabilities have also proven unable to take effective control of weapons such as drones.

The book re-examines the poster children of the cyber threat, a small number of well-known events that took place in the past three decades. He shows that interpreting the gigantic explosion of a Soviet pipeline in 1982 as the work of a CIA-planted virus is highly problematic. He correctly points out that the origin of the cyber attacks on the Estonian government in 2007 and the Georgian government in 2008 was never ascertained, and that their effects were relatively minor – hardly the stuff of Hollywood thrillers. Rid acknowledges that the supervisory control and data acquisition systems that operate industrial infrastructure are becoming more vulnerable in some ways, but argues that oversight, vender security and the complexity of the systems are making them less vulnerable overall. Both Stuxnet and Shamoon, the virus that attacked oil company Saudi Aramco, required insider access to be effective.

For these reasons, Rid convincingly argues that if cyber-war has any meaning, it is as a metaphor, not as the description of a form of genuine warfare. Logically, he also refuses to consider cyberspace as the fifth domain of conflict because it permeates the other four (land, sea, air and space). This short but dense, wellconstructed book concludes with rapid, intriguing demonstrations of the ways in which cyber attacks favour the defensive over the offensive, comparisons with nuclear weapons are misplaced and the militarisation of cyber security is unwarranted.