Book Reviews

Cyber War Will Not Take Place

By Thomas Rid

Reviewed by Squadron Leader Paul Withers

Introduction

The 2010 Strategic Defence and Security Review classified cyber security as one of the United Kingdom's four 'Tier-One' risks to National Security. The reality of this threat had been acknowledged in the 2009 Cyber Security Strategy, which highlighted the malicious use of cyberspace by '…criminals, terrorists and states, whether for reasons of espionage, influence or even warfare.' The interest in cyber security across government, industry and the media has intensified, not least because under the auspices of the National Cyber Security Programme, it has attracted new money in times of severe austerity. Thomas Rid uses a deliberately provocative title in a volume that aims to bring a little political science rigour to the debate. His argument is supported by the available evidence, which to date suggests that 'Cyber War' is a largely meaningless concept based upon the norms of understanding around the nature of war.

For a cyber act to be classified as war it must at least have the potential to be violent, it must be instrumental in the sense that it is a means to an end, and it must be a part of a wider political purpose. As Rid points out, to date 'not a single human being has been killed or hurt as a result of a code-triggered cyber attack' (p 13). This key point on the potential of computer code to cause death or injury is the basis of the argument against cyber war. Rid's analysis of the publicly available examples that might constitute war finds most of them wanting on the presence of violence. He argues that even those attacks that have the potential to be violent, *'are bound to be violent only indirectly'* (p12).

He sets out his argument, based on a wealth of empirical evidence that all the acts witnessed in cyberspace, rather than being acts of war, belong to one of three categories: *sabotage, espionage or subversion*. After a discussion on the nature of 'cyber weapons', Rid analyses the historical record of cyber attacks across each of his three categories, focussing on *what has happened*, rather than the speculative approach taken by some other authors. In the chapters on sabotage, espionage and subversion, Rid offers the reader a detailed and more nuanced view of numerous historical cyber attacks. He also offers a window on the complex problem of attribution of acts in cyberspace, which he argues is as much a political problem as it is a technical one. He concludes by looking *Beyond Cyber War*, where he identifies the possibilities of cyber operations being more ethical than, for example, an airstrike as 'a cyber attack may be less violent, less traumatizing, and more limited' (p171).

Despite its title, Rid's argument is not dismissive of the role of action in cyberspace as a military instrument or as an instrument of power more generally. If one were to translate his categories of espionage, sabotage and subversion into military parlance, the threats and opportunities of operations in cyberspace become apparent. *Espionage* obviously becomes intelligence; *sabotage* becomes non-kinetic (or potentially even kinetic) effects; and *subversion* could be countered (or enabled) by a complex mix of Information Activities including Media Operations and Information Operations.

This book can be viewed as a useful foil to Richard Clarke and Robert Knake's 'Cyber War: *The Next Threat to National Security and What To Do About It'* (see CAS Reading List 2011). Clarke's bleak outlook stimulated the discussion, but Rid manages to bring clarity to a debate that suffers from excessive hype; indeed in writing the book it is one of the author's stated aims to 'attenuate the hype' (p ix).

Some may be left feeling that perhaps it is the definition of war *per se* that needs readdressing in the modern context. However, whatever your definition of war, it is clear that a Cyber War in its own right still seems extremely unlikely, but that cyberspace, inextricably linked with the physical domains of warfare, is and will remain a part of warfare. If we accept Rid's thesis that *Cyber War Will Not Take Place*, his argument and the underpinning evidence should lead us to the conclusion that operations in cyberspace are very much here to stay.

Much of the extant literature on cyberspace rests around highly technical 'Information Security' topics, but whilst Rid occasionally dips into essential technical explanation, his well-reasoned and extremely readable volume lifts the debate to a level appropriate to the general military audience. As air power's reliance on cyberspace continues to grow, airmen need to understand its threats and opportunities across military operations, including the implications for air power. This excellent book is highly recommended for both the cyber specialist and the general air power audience as a means to help educate and stimulate the debate.