It is unlikely that any such organisation will ever be able to completely resolve this predicament, as by their very nature political movements seek to create parallel governance structures and therefore exactly the sort of managerial bureaucracy that Shapiro sees as their Achilles' heel. By laying out in such detail how this weakness can be exploited, Shapiro is undertaking a task that will likely stand the test of time.

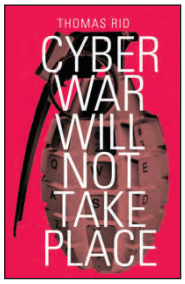
Raffaello Pantucci is a Senior Research Fellow at RUSI.

DOI:10.1080/03071847.2013.869731

Cyber War Will Not Take Place

Thomas Rid

Hurst, 2013



It is perhaps ironic that study of information-age conflict is beset by an information problem. The secrecy of cyber-capabilities and relative paucity of case studies present us with a plethora of known-unknowns, as do the pace of technological change and the increasing penetration of digital networks into economic and social life. In this environment of intellectual uncertainty, in many ways mirroring the early days of thought about air power and nuclear weapons, it may be no surprise that alarm is easier to generate than sober reflection.

This is the context in which Thomas Rid has written *Cyber War Will Not Take Place*, which offers a sceptic's take on the questions posed by computer-network operations. It is a bold effort, and one that largely succeeds because it fuses a solid technical grounding with a keen appreciation for strategy and politics.

At its heart is a consideration of the ontology of war and 'cyber-war'. Some basic Clausewitzean assumptions underlie the analysis: an act of war must be violent, instrumental and political. But most cyber-attacks – theoretical or empirical – are none of these. In other words, it is very difficult for computer-network operations or attacks to meet the necessary criteria to be defined as acts of war. Chief among these, Rid argues, is violence.

Violence, insofar as it may be achieved by computer code, is indirect. A cyber-attack intended to cause physical destruction must 'weaponise' the system it is attacking. This does not mean, however, that cyber-weapons are not capable of inflicting harm; plausible examples abound. The point Rid makes, is that truly destructive weapons that elicit a physical effect will require thorough intelligence, bespoke coding and testing – something beyond the means of most states. Further, some of these challenges – such as the human capability necessary for interpreting intelligence and physical penetration of a facility if necessary – may not be amenable to technological shortcuts.

Situating a technical capability in its strategic, social and political context is a running theme in *Cyber War Will Not Take Place*. It is a welcome approach, for much other analysis focuses on the micro-level without due consideration of the bigger picture or, indeed, the concept of friction.

For example, while espionage is the most frequent use of cyber-capabilities so far, and a most effective one at that, there are limits to it, as Rid notes. Making use of secrets is often harder than stealing them. Lifting gigabytes of intellectual property for innovative production processes may yield less of a boost without the attendant infrastructure or management culture that facilitated their generation in the first place. This is not to dismiss the corrosive impact such large-scale industrial espionage can have. But what we do not have yet is a 'through-life' perspective on cyber-espionage to truly gauge its strategic impact.

Likewise with subversion. Groups like the hacker collective Anonymous rose to prominence in the early years of the decade in seemingly posing a new, impenetrable and infinitely agile challenge to state authority. The Arab Awakening too seemed to lend credence to this new era of civic activism. But, again, Rid suggests the change may have been overstated. For all the technical advantages networks provide – instantaneous, unmediated communication, for example – the social constraints to collective action abide. Groups find it harder to exercise organisational control; after all, nicknames gathering in an Internet chatroom are a very different proposition to physical mobilisation (and comradery) in the face of real violence.

Yet it is anonymity, thanks to the architecture of the Internet, that forms one of the most troubling aspects of cyber-warfare. Like most, Rid agrees that it 'represents a fundamental, and in many ways disturbing, change'. Nevertheless, he persuasively suggests that this may not apply equally across all cases. The attribution problem may be inversely proportional to the severity of an attack. A basic nuisance attack – a denial-of-service attack on a website, for example – will not be worth committing extensive resources to identifying the perpetrator. But the more powerful and damaging the attack, 'the higher the political stakes, the more pressure the targeted country will be able to bring to bear on the country of the suspected origin to cooperate in a forensic operation' (p. 161).

Adding these together, Rid ultimately argues that cyber-security is ridden with too many poor metaphors and analogies. If war is diluted to just 'damaging, stealing or destroying', then it ceases to be a useful concept. More importantly, cyber-warfare will likely be marked by a *retreat of violence*; the old instincts of competition and conflict remain, but in a domain of indirect non-violence. In some sense, cyber-weapons sit happily with the liberal dream of 'bloodless war', achieving coercive effect without casualties.

In one respect, the analysis could have gone further. While the book does outline the benefits large states enjoy – implying that cyber-capabilities might not be the great equaliser often supposed – this reviewer was left wanting more on what a more sober assessment of cyber-capabilities might mean for the frequency and direction of their use. Will cyber-conflict invite escalation, or become a useful 'vent' for great-power competition

between the US and China, rather than hot war? What would – or will – happen when more medium-sized powers begin large-scale computer-network operations? In which strategic context might judicious use of cyber-capabilities be most useful? Some more consideration of the potential effect of computer-network capabilities on the stability of the international system and the balance of power would have been welcome.

There are, of course, those who will disagree with the central thrust of *Cyber War Will Not Take Place*. Rid is a sceptic, but he is not dismissive of the real risks of cyber-conflict. He is, however, against unwarranted militarisation of the domain and the lumping together of crime and subversion under the rubric of security.

But the value of the book is not in being definitive: given the lack of data, and the immaturity of the topic, all work on it is necessarily speculative to some degree. Its worth is derived from the critical interrogation to which it submits a host of assumptions and helps us sharpen our own thinking. For this and other books are fundamentally beset by an epistemological problem. Cyber-capabilities are, perhaps by necessity, veiled in secrecy. We also have very little information on the political outcomes of cyber-attacks, simply because, again, there have been so few. Cyber was a sideshow in the 2008 Russo–Georgian war; the disruption to Estonia in 2007 is often overplayed; and Stuxnet did not seem to fundamentally alter the Iranian nuclear trajectory.

While hypothetical attacks can also be plausible ones, perhaps here is a strong sceptic's point: while it is easy to generate plausible attack vectors and mechanisms in hypothetical scenarios, it is more difficult to discern plausible strategic and operational outcomes, for they affect very complex processes. It is therefore difficult to link tactical considerations (our understanding of how code will affect a given system) to strategic considerations (how a government or society may react and how a desired *political* outcome may be achieved).

The information problem about cyber-war means that in some sense we must grope in the dark. Yet Rid's book is valuable precisely because it offers a careful assessment of what we do know. It will be an essential work for some years to come.

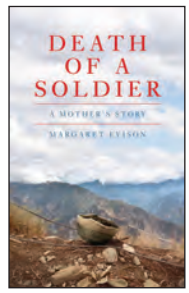
Adrian Johnson is Director of Publications and a research fellow at RUSI.

DOI: 10.1080/03071847.2013.869732

Death of a Soldier: A Mother's Story

Margaret Evison

Biteback, 2012



Lieutenant Mark Evison of the Welsh Guards was shot and gravely wounded on 9 May 2009 while leading a patrol in the Nad-e Ali district of Helmand Province in Afghanistan. He was flown back to Britain, but died from his injuries three days later in Selly Oak Hospital in Birmingham. He was twenty-six and had been in Afghanistan for less than a month, on his first tour.

Death of a Soldier, written by Mark's mother Margaret, is a moving account of his life and death, and the aftermath of his death, from her perspective. In a sense, it is a tale as old as history, and there have been many such deaths – 'old war cemeteries speak of these'. But the fact of this book, the sequence of events it relates, and the fact that we know of this particular young man's death are testimony to there now being something different about how we view such loss.

Margaret Evison writes affectingly and elegantly about the swirl of emotions and memories she felt as she saw her son go off to war and first received the news that he had been shot, as well as the limbo of uncertainty and anxiety that followed, and the human drama in Selly Oak Hospital as the family had to let go and Mark's life-support machines were switched off. But this book is also about how the author's mix of sadness and grief turned to anger and frustration as she felt the authorities refused to answer her questions about the circumstances of her son's death – including why it took as long as it did for a rescue helicopter to arrive and whether his platoon's radios were working properly – fuelled by her dissatisfaction at the way in which the inquest into her son's death was handled.

It also explains why the circumstances of Lieutenant Evison's death became a prominent element in the debate and controversy in Britain at the time over how the Afghanistan campaign was being fought and particularly how it was being resourced – of which the political sandstorm over the alleged lack of helicopters was just one part. The young officer kept a detailed journal, key parts of which attracted attention when they first appeared in public. And it is quoted extensively here.

The key passage, written on 21 April 2009 less than three weeks before he was shot, seemed to offer evidence from the front line, as it were, of what many critics felt was going wrong: 'As it stands I have a lack of radios, water, food and medical equipment. This with manpower is what these missions lack. It is disgraceful to send a platoon into a very dangerous area with two weeks' food and water and one team medics pack'.

Margaret Evison writes affectingly and elegantly

Of course, families of the past may also have questioned, in many instances, whether their loved ones had died needlessly, because of poor planning or a lack of resources. What is different now is the fact that the whole political, social and legal context in which conflict is conducted has transformed dramatically. And the degree of public tolerance of casualties – whether friendly, enemy or innocent – is dramatically less in these distant 'wars of choice' like Afghanistan.

That has been reflected in the controversy over Afghanistan, in whatever the 'Wootton Bassett effect' represents, and the legal proceedings over the army's duty of care that