blogs.lse.ac.uk http://blogs.lse.ac.uk/lsereviewofbooks/2013/06/17/book-review-cyber-war-will-not-take-place/

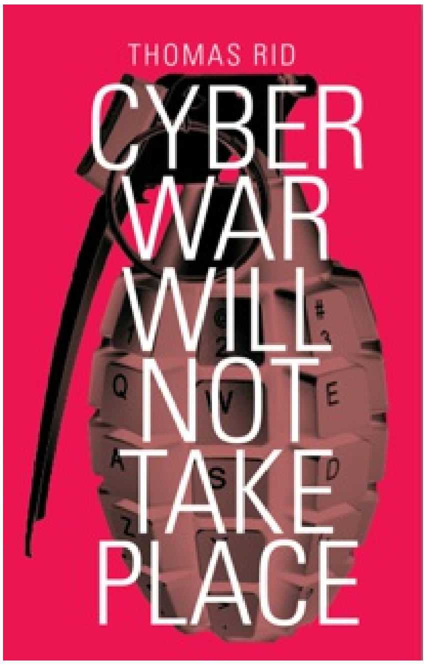
Book Review: Cyber War Will Not Take Place

by Blog Admin June 17, 2013

In 2005, the U.S. Air Force boasted it would now fly, fight, and win in cyberspace, the 'fifth domain' of warfare. This book takes stock to consider whether or not cyber war is a real threat. ***Thomas Rid*** *argues that the focus on war and winning distracts from the real challenge of cyberspace: non-violent confrontation that may rival or even replace violence in surprising ways. Tracing the most significant hacks and attacks, and exploring case studies from the world of computer espionage and weaponised code, this is an undoubtedly impressive work, writes* ***Julia Muravska****.*

Cyber War Will Not Take Place. Thomas Rid. Hurst. April 2013.

Find this book:



That warfare and crime are "indistinguishable in the shadowy online world" was the central claim of a recent *Financial Times* report on cybersecurity, and it is a reflection of the issue's rise to the "dominant feature of the global political agenda" that several major media outlets and policymaking outfits have dispensed with the space between "cyber" and "security", all the better to convey its unprecedented nature. Thomas Rid, the author of *Cyber War Will Not Take Place,* would have wholeheartedly agreed with this assessment, arguing, as he does in the book, that "all known political cyber offenses are neither common crime nor common war" (p. 10). However, Rid would have been highly critical of the implicit message that we are witnessing the advent of the "much-vaunted war in the ostensible fifth domain" of cyberspace. And he has written *Cyber War Will Not Take Place* to explain exactly why (p. 164).

Rid sets out his chief claim right at the beginning, namely that "cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future" (p. xiv). What we are rather seeing, he contends, are political cyber attacks that are "sophisticated versions of three activities…as old as human conflict itself: sabotage, espionage, and subversion" (p. xiv). All three types of activity use the opportunities and are subject to the limitations of digitised computer networks. But none can be credibly classified as war. And to be truly successful, as Rid insists throughout the book, all three continue to rely on the proverbial "human factor" – that critical knowledge or cooperation of somebody "on the inside", the key tip-off from an informant, the indispensable context that only human intelligence can provide.

In a divergence from the book's title, Rid's core message may best be both paraphrased and summarised as "there is no such thing as cyber war". Rather, there is cyber war*fare*, one amongst many methods and instruments of waging war whose nature has remained unchanged throughout human history. Rid builds this argument gradually, in an empirically detailed, conceptually sophisticated, and technically precise, but yet concise and not overly complex manner – no small feat when discussing a phenomenon of which most of us have at best an inadequate understanding. In the process, he brings much-needed clarity and perspective to the current cyber security debate and is to be commended for doing so in an area where secrecy, anonymity, and deniability are the norm.

Rid's foundation is the revered founding father of modern theory of war, the Prussian general and brilliant strategic thinker Carl von Clausewitz, who defined war as "an act of force to compel the enemy to do our will" (p. 1). As such, war is inherently violent, always instrumental, and thoroughly political. Physical violence "is the pivotal point of all war" (p.2). Cyber attacks, however, could ever only be "indirectly violent", and most "cannot [even] sensibly be understood as a form of violent action" (p. 12). This is because, first, the "act of force" at the heart of conventional war, from a drone strike to a suicide bomber attack means "pushing a button or pulling a trigger will immediately and directly result in casualties" (p. 3). This is fundamentally different from an act of cyber war. Taking out a major urban electricity grid through pre-installed logic bombs, for instance, would mean that the link between "somebody pushing a button and somebody else being hurt" is complex, indirect, and contingent on numerous circumstances (p. 3).

Second, as Rid argues, cyber weapons, which he defines as "computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional or mental harm to structures, systems or living beings," do not "come with their own explosive charge" (p. 13). They can only do such damage by "parasitically…unleashing the violent potential" of the target, be it a power plant manipulated to explode or a traffic control system forced to fail (p. 13). Finally, Rid really wants us to appreciate that "publicly known cyber weapons have far less firepower than is commonly assumed" (p. 41). Thus, attacking industrial control systems, "the most probable way for a computer… to create physical damage and indirectly injure or kill people" is extremely difficult in practice due to the complex structure and continuously improving defences of such networks (p. 67). Similarly, Grade-A "online sleuthing," a highly customised, resource-hungry, intelligence-intensive affair, is also difficult to pull off, doable for "only very few sophisticated [state] actors" (p. 169).

Rid's work is undoubtedly impressive, relying on a wealth of diverse sources to provide little-known, tantalising details of known "cyber security incidents" such as the infamous Stuxnet, annoying ILOVEYOU, impressive Flame, and obscure Duqu, to name but a few. Yet, throughout the book, the reader cannot shake off a sense of confusion as to what Rid is actually attacking. In building his case for "why cyber war will not take place," he never sets out how such a war might actually look. As a result, one may be convinced that it will not happen, but is not entirely sure of what the myth of cyber war is and why it is in need of thorough debunking. A similar critique may be levelled against his violence argument – a conceptualisation of physical violence in war would have been helpful; as it is, Rid has not really discredited the argument that war need not be inherently violent and violence need not be fundamentally directed against the human body as he alleges, a point that seems to be borne out by recent developments such as the emergence of nonlethal weapons, proliferation of robotics and increased efforts to avoid collateral damage in war.

In addition, Rid's otherwise robust case for pervasive exaggeration plaguing analyses of cyber attacks' impact is somewhat undermined by his drawing conclusions from an incomplete empirical record – for instance, just because some attacks cannot be unequivocally attributed to Russia or China, does not mean that these states were not in fact behind them, as Rid seems to suggest. Similarly, just because the level of damage wrought by a particular piece of malware or breach is not known, does not mean it was not alarmingly significant. Finally, Rid's argument would have been considerably bolstered by a greater focus on future trends – after all, war continuously evolves and reinvents itself. More specifically, by Rid's own admission, the implications of an intelligent, *learning* coded weapon able to evaluate the environment, analyse courses of action, and "then take action" –in fact, it would be surprising if such an agent has not yet been developed— would be fundamental for the nature of cyber security and Rid's argument. It would have been very interesting to learn what Rid thinks these implications may be.

Julia Muravska is a PhD student at the LSE's International Relations Department. Her doctoral research examines the emergence of the defence equipment market in the EU. Previously, Julia worked for the Defence and Security Programme of Transparency International UK, with a focus on counter-corruption in defence procurement and defence corporate initiatives. She holds an MSc in International Relations from the LSE and an Honours BA from the University of Toronto, also in International Relations. Read more reviews by Julia.