Bitskrieg

The New Challenge of Cyberwarfare
Door John Arquilla
Cambridge (Polity Press) 2021
240 blz.
ISBN 9781509543632
€ 20,-

So you think you know a great deal about cyber? Clearly, it presents many challenges for the military, society, and contemporary international relations. State and non-state actors are increasingly affecting and disrupting Western societies and military institutions through cyberspace. Professor John Arquilla argues that free societies have shown an inability to address cybersecurity adequately. In his new book *Bitskrieg* he shares his views on the future of competition, crisis, and conflict, enabled by information technology. Arquilla should know, being a Naval Postgraduate School Distinguished Professor in international relations, defense analysis, and cyber strategy. He has advised several US administrations on national security matters, mainly concerning information strategies.

Wake-up call

Arquilla presents *Bitskrieg* as a wake-up call for the military, politicians, and security professionals. Although most have realized that threats from the cyber realm pose several challenges, the greatest challenge may be to recognize that the current Western approaches to dealing with the growing threat of mass disruption do not suffice. There is a critical need for comprehension of information technology utilization from senior leaders to the smallest tactical unit. Although the book title might suggest a military perspective focused on cyber operations, Arquilla presents a much broader array of challenges with possible solutions. For instance, he describes our societal problem as follows: 'Our existing framework of cybersecurity, primarily based on the twin pillars of firewalls and antiviral software, has proved insufficient to protect citizens, businesses, and other key institutions of society and governance' (p. 132). In other words, the way cybersecurity is measured is too narrow and needs expansion.

Arquilla sees three categories of solutions that would improve the current situation. First, (Western) nations should better connectivity and information sharing by retooling cybersecurity with improved cryptologic solutions combined with cloud-based data storage. Effective use of cryptology raises the bar for nefarious activity. As for data, data at rest is data at risk. The second category embraces a major change in military and security affairs to cope with the emergence of a range of new information technologies. A change in physical warfighting, to include deep integration of information technology, is most important (p. 158). Third, an arms control concept applicable to cyber operations is needed. The intended cyber arms control mechanism should be pursued with some urgency. It is to be behavior-based and must minimally prohibit the use of cyber to wage political warfare and restrict strategic attacks on civilian infrastructure.

Revolutionary changes

The reasoning Arquilla displays is built on historical examples, research, and previous case studies. For the subject matter expert, his book does not present news. However, for most readers who think they know something about cyber, Arquilla manages to present valuable insights. Understanding cyber and information technology is one of the main challenges, and it ought to improve drastically. Having worked at the tactical and policy levels at the Netherlands Ministry of Defense, I could not agree more. On many occasions, I have found the current knowledge and comprehension lacking from top to bottom. Arguably, cyber and information operations are not easy concepts to fully grasp in any regard. Regrettably, Arquilla does not go into depth on improving understanding, which could be the critical success factor for each of his three main challenges.
The inability to adopt new tools or practices might sound all too familiar from a military and government point of view. Bureaucratic inertia must be overcome to introduce revolutionary changes. As Arquilla mentions, this will be most challenging given

military tradition, the pull of political influence, and commercial interest. While working at the Defense Planning department, these challenges were very familiar. On the positive side, the potential to improve and the likely return on investment are considerable in the foreseeable future operating environment.

A point of critique is Arquilla's writing style. Historical examples and personal experiences enlighten his arguments. However, his tone is often pedantic. Mentioning his seminal and visionary article 'Cyberwar Is Coming' (1993), co-authored by David Ronfeldt, again and again, is wearing. The 'I-told-you-so' way of presenting arguments distracts from its valuable content. In general, the storyline often wanders and makes it difficult to grasp the essence of his arguments. Arquilla tries to make that up by repeating solutions in a different context, but the repetition is often unnecessary. A better structure combined with the 'art of leaving out' would have resulted in a more robust book that should be on the desk of every politician, military, business, or security professional dealing with the unpredictable future. However, *Bitskrieg* offers an insightful overview of the current and flawed state of cyber and information technology in their brief history. Now is the time to move forward. We, military and civilians, are all involved and part of information technology and cyber. Whether we like it or not, that is a wake-up call. ■

Major Mark Haasdijk MSc, Netherlands Marine Corps/HDV, Naval Postgraduate School Monterey