MICHIGAN WAR STUDIES REVIEW
MiWSR.COM

2022-018 16 Feb. 2022

Bitskrieg: The New Challenge of Cyberwarfare by John Arquilla.

Medford, MA: Polity Press, 2021. Pp. xxi 212. ISBN 978–1–5095–4363–2.

Review by Matthew Ford, University of Sussex (m.c.ford@sussex.ac.uk).

Donald Rumsfeld was right. Small, highly networked, light-footprint Special Operations Forces backed by airpower working in support of local proxy forces is an effective combination for defeating an enemy. The technique worked in Afghanistan in 2001; defense analyst John Arquilla (US Naval Postgraduate School) now argues in his latest book, *Bitskrieg*, that it still has application today. He cautions, however, that without securing connectivity, embracing networked tactical formations, and rethinking cyber arms control, international security will be subject to "mass disruption" in the future (166–67).

Arquilla and co-author David Ronfeldt first explored Rumsfeld's thinking in their seminal 1993 RAND report *Cyberwar is Coming!* In chapter 1 of *Bitskrieg*, "'Cool War' Rising," Arquilla explains how they sought to revolutionize how the Pentagon thought about war. They maintained that information technology would deliver "less bloody, yet more decisive" (15) victories, leaving behind modes of warfare that went back to the 1940 Fall of France. In the new world, information advantage would supersede mass and mobility and "cyberwar [would] be to the 21st century what blitzkrieg was to the 20th."[1]

Lamenting that their ambitions for cyber were diluted as web technology came into its own in the late 1990s, Arquilla spends much of chap. 1 explaining how the original ideas behind cyberwar concerned physical warfighting as much as managing the virtual domain (18). Unlike others in the Pentagon, then US Secretary of Defense Rumsfeld used success in Afghanistan to lobby for a program of force transformation. This so alarmed senior generals that Rumsfeld found himself eased out by those who preferred a more traditional invasion of Iraq in 2003. The result was an invasion too small to manage the chaos produced by the US occupation.

Arquilla argues that Gen. David Petraeus realized that superior information was essential for quashing insurgents. He quotes classicist Victor Davis Hanson's summary of the surge strategy, noting that the goal was to get "men outside the compounds, embed them within Iraqi communities and develop human intelligence" (23). The claim that this was a cyberwar strategy is, however, a stretch. After all, the surge of US forces was meant in part to flood troops onto Iraqi streets in order to quell rising tensions. That the US forces in Iraqi neighborhoods became targets for insurgents who then generated an intelligence signature means the surge was not the kind of cyber campaign Arquilla stipulates .

At the same time, however, the techniques that Petraeus's colleague Gen. Stanley McChrystal oversaw at Joint Special Operations Command constituted a cyberwar campaign in Iraq. Information gathered from local forces in Baghdad neighborhoods could be combined with data points from other agencies and intelligence assets. This fusing of intelligence—if analysed and assessed quickly—could enable Special Operations Forces and drone operators to pinpoint insurgent networks. Unfortunately, the emergence of these techniques is not properly explored in *Bitskrieg*. This

1. See, further, Arquilla and Ronfeldt, "Cyberwar is Coming!" (RAND Corporation, 1993). Available online.

in turn obscures the impact of *Bitskrieg* and makes it harder to see how Arquilla and Ronfeldt's original conception of cyberwar applied during the occupation of Iraq.

Of course, insurgents managed to mobilize their campaign against coalition forces in Iraq through the internet. Improvised Explosive Devices and ambushes were sited to achieve maximum media spectacles. As social media and smartphones entered the market the armed forces lost control of the new media environment, to the benefit of keyboard warriors or citizens recording the chaos around them: "networks, even small ones—and even individuals—can now wage one or another form of cyberwar" (30).

Unfortunately, as Arquilla notes (chap. 2), neither the American government nor the marketplace has done enough to bolster cybersecurity. Instead, "the need to protect the people while at the same time retaining a right to intrude upon their privacy for national-security purposes" (40) has caused an ambivalence over maintaining cyber defences. As a result, America's potential adversaries have developed their own cyber capabilities, while the federal government has chosen to undermine the private sector's capacity to protect the IT infrastructure. When these factors are combined with the deregulation of critical national infrastructure, Arquilla notes, the United States becomes open to cyberterrorism, political warfare, and enemies pursuing attacks in the virtual domain.

Chapter 3 concerns the application of Artificial Intelligence (AI) both on the battlefield and at the level of strategic decision-making. Networked units, precision munitions, and AI enabled robots hold out the prospect of even greater dispersion on the battlefield. The use of AI to concentrate capabilities in swarms could free armed force from being fixed in position. Large scale troop deployments and big platforms become unnecessary. This in turn frees *Bitskrieg* from quagmires, heavy casualties, and political paralysis. Whether a technical fix might overcome the political impossibility of counterinsurgency[2] remains to be seen, but Arquilla hopes to make it possible to use force without the same liabilities of the Blitzkrieg era. This would require reforms in the structure of the armed forces and defense more broadly (89). The application of AI to strategic decision-making might well highlight opportunities to test various approaches to a campaign. The danger is that such changes will make war more thinkable, thus creating greater insecurity (91).

Chapter 4 concerns the possibility of an arms control agreement to forestall a "cyber Pearl Harbor" (97). Citing in particular agreements about the use of chemical and biological weapons, Arquilla hopes that nations can act responsibly to secure cyberspace as well (108-119). Up to now, US efforts to develop cyberweapons have exacerbated current fears in the international community (102-108), whether "unwittingly" or not. As Arquilla notes, the shame of it is that the failure to grasp these chances now exposes the world to even greater threats.

In his fifth and final chapter, Arquilla laments failures to create greater security but holds out the hope that it is not too late to avoid serious threats to international security. This will require a new willingness to capitalize on the strengths of open societies while avoiding the pitfalls of authoritarianism and populism. To start, societies must make greater use of data encryption and cloud-based data storage and processing, rather than firewalls and anti-virus software.

John Arquilla offers us a route through the fears caused by a conception of warfare he first outlined in 1993. At the same time, however, he recognizes that the moment to act has likely already passed and the same bureaucratic debates will persist, subject to various industry, government, and Service interests. This will make it hard to secure the future from an information infrastructure grown far beyond the control of any one sovereign power.

---

2. M.L.R. Smith and D. Martin Jones, *The Political Impossibility of Modern Counterinsurgency-Strategic Problems, Puzzles and Paradoxes* (NY: Columbia U Pr, 2015).