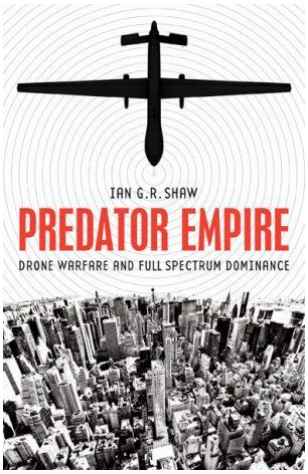
Science

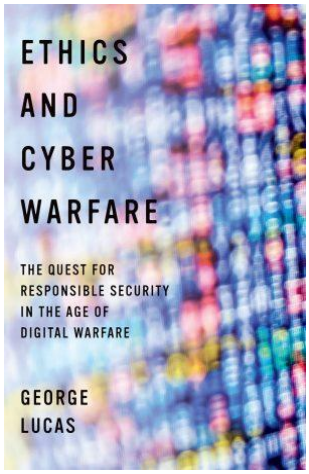
Tomorrow's arsenal: Two authors probe the technologies transforming warfare

By Nayef Al-Rodhan
December 19, 2016



Predator Empire: Drone Warfare and Full Spectrum Dominance

Ian G. R. Shaw
University of Minnesota Press
2016
334 pp



Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare

George Lucas
Oxford University Press,
2016
201 pp

From everyday life to the expansion of empires, technology has accompanied individuals and served to anchor geopolitical power. New technologies, however, are changing standard operating procedures due to their subtler and boundless capacity for surveillance. In warfare, they are generating the unprecedented potential for remote engagement, distancing attackers from the attacked.

Ian Shaw's Predator Empire is a provocative analysis of the outreach of technology, specifically drones, as new tools to entrench U.S. power globally. The "Predator Empire" (so named by Shaw after Predator drones), aims at "full spectrum dominance": the control of all physical domains—terrestrial, maritime, and atmospheric. We are, in Shaw's opinion, "sleepwalking into totalitarianism," because the Predator Empire is, in essence, a "rule by nobody": tyrannical but without one discernible tyrant. It is a rule by "technics."

The technological power of the Predator Empire can be suffocating. For those living under drone-dotted skies, it can be traumatizing. So common is the trend toward unmanned surveillance that the drone is bound to become a brand of state power, "as recognizable as Coca Cola," Shaw maintains.

Shaw forebodingly reflects on this predicament but overstates the hopelessness of the situation, disregarding potential resistance. Calls for accountability show that we are not passively waiting for technology to crush our liberties. Amnesty International, for instance, has taken a public stance on encryption, calling it a matter of human rights (**1**).

Shaw argues that drones must be seen as geopolitical actors. There is merit to this argument because it provokes scholars to rethink the practical and theoretical role of technology. However, it must be challenged on technical grounds, because the technology on which drones are based allows for limited autonomy. Although they can infringe on people's space and affect their public lives, ultimately, they cannot—technically—take over. Shaw's book also launches a larger critique of the all-encompassing electromagnetic spectrum, which mediates our surveillance. He believes that government surveillance has started to be legitimized too easily: Instead of being seen as a risk to democracy, it is increasingly seen as its savior. But many would argue that this is not an either/or question. Like drones, cyberattacks are challenging traditional notions of warfare. George Lucas's Ethics and Cyber Warfare offers an eloquent, substantive, and original discussion of the main controversies and dilemmas related to the cyberdomain, including privacy and the legality of cyberwarfare.

ICHOLAKOV/ISTOCK

Drones are changing the rules of modern warfare and dramatically enhancing the capacity for state- sponsored surveillance.

As is the case with drones, the perpetrators of cyberattacks are removed from the targeted physical location. This has often raised fears about the attribution of responsibility, the applicability of international law, and the threshold at which cyberattacks amount to acts of war.

Lucas cautions against the need to prepare for extreme scenarios. More plausible, he maintains, is the rise of state-sponsored hacktivism, operating with "weapons of mass disruption" that cause nuisances more than large-scale physical damage. He demonstrates that both ethics and existing laws can be effectively applied in cyberconflicts, despite significant gaps. The book also offers a meticulous exposé of ethical theories and examples that debunk some of the assumptions about cyberspace as a largely ungoverned space, where anything can happen.

In both tone and message, Lucas's book differs from Shaw's critique of the intrusive and repressive nature of late-20th- and early-21st-century technologies. For example, Lucas makes a compelling case that NSA surveillance, although morally problematic, will never replicate the atrocious Stasi-like surveillance programs of the 20th century. On the contrary, he contends, the intent of the U.S. government will always differ from that of an authoritarian regime.

This is a sensible takeaway: Technology does not exist above states or political agendas, but rather it is instrumental to their goals. The same thing could not be said about lone attackers, who are not bound by considerations outside their own moral compasses. Lucas suggests that a "code of ethics for cyber warriors" could be effective in limiting their attacks. However, power can be highly addictive if unchecked. Given an environment where one can enjoy anonymity and no constraints, the thrill derived from such acts would likely outweigh a code of conduct (**2**).

Both of these books are valuable contributions to the literature, furthering relevant questions and raising still more. We should never be complacent about the trajectory of technology and especially technologies that can be immensely powerful tools of control.

References

1. Amnesty International, "Encryption: A Matter of Human Rights," March 2016, http://www.amnestyusa.org/ sites/default/files/encryption_-_a_matter_of_human_ rights_-_pol_40-3682-2016.pdf

2. N.Al-Rodhan,"The Neurochemistry of Power: Implications for Political Change," 27 February 2014, http://blog.politics.ox.ac.uk/ neurochemistry-power-implications-political-change/.

About the author

The reviewer is at the Geneva Centre for Security Policy, Genève, Switzerland, and Oxford University, St. Antony's College, Oxford, UK.