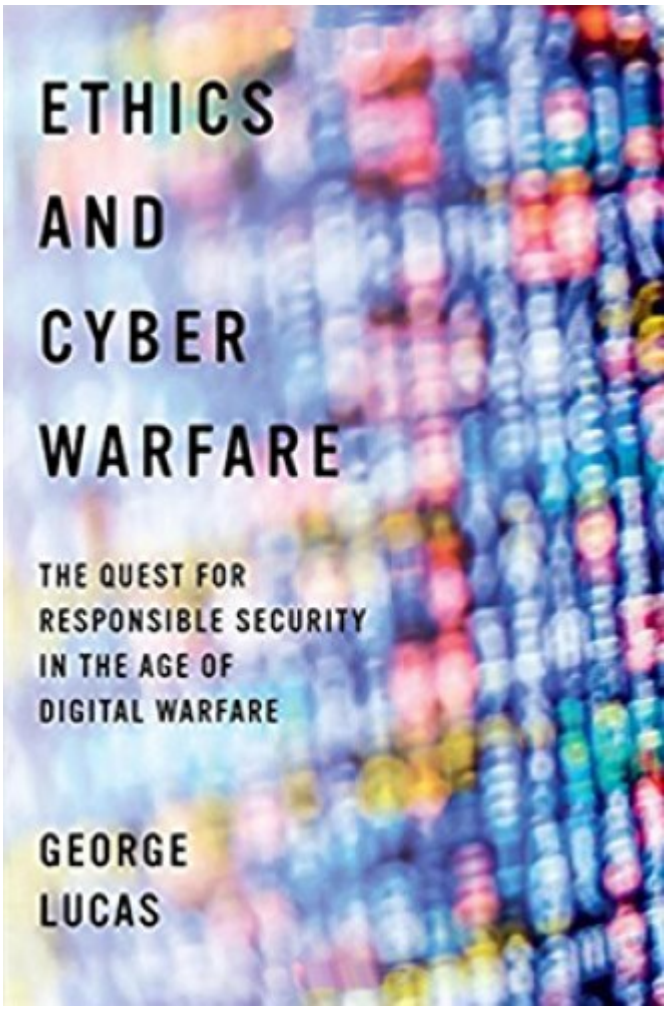
The values and moral quandaries of cyber war

Ethicist George Lucas argues that new forms of warfare are "mired in epistemological crisis."

by Keagan Holt Potts in the August 30, 2017 issue

In Review



Ethics and Cyber Warfare

The Quest for Responsible Security in the Age of Digital Warfare

By George Lucas
Oxford University Press

In 2010, a German computer security expert detected a cyber weapon called “Stuxnet” in systems of large industries in nations across the world. This malware was a cyber weapon that originally targeted nuclear centrifuges inside Iran’s Natanz nuclear power facility. The worm was loaded onto a thumb drive, but eventually it made its way onto computers across the world. Given the precision with which this weapon can discriminate between military targets and noncombatants and its ability to minimize collateral damage, it could be one of the most ethical weapons to date.

Should we be afraid of the implications of such technology, or should we find hope in the prospect that hyper-specific weapons technology will reduce the harm caused by warfare? George Lucas outlines the problems and potential of cyber technology, providing a useful framework for identifying stakeholders, moral tensions, and the values that arise in the context of cyber war.

Solutions to ethical issues in cyber war have immediate ramifications. For instance, cyber technology helps the government predict and neutralize internal threats to national security, but it also threatens Internet privacy. Lucas discusses the NSA Management Directive #424—a response to Edward Snowden’s security leaks—which concerns programs (e.g., XKeyscore and PRISM) that aim to prevent crime by tracking online “record events” and analyzing the resulting metadata in hopes of highlighting suspicious activity. He investigates the permissibility of such programs and the implications of this kind of monitoring for citizens’ right to privacy.

Cyber technology plays a significant role in repelling attacks by foreign countries on critical industries and infrastructure. A security breach in these sectors could be fatal. For instance, Lucas discusses North Korea’s hacktivism that targeted Sony Pictures before it released *The Interview*. Although this attack was limited in scope, and far from an act of war, Lucas suggests that similar cyber technology could be used to hack public transit systems or obtain classified government documents. Our nation currently uses cyber technology to detect and defend against such threats.

Yet both professionals in the field and nonexperts lack a common framework for determining the moral principles that govern the new technology. Cyber warfare, he explains, “is mired in epistemological crisis, and in need of a comprehensive framework through which thinkers can engage with each other to resolve disputes

regarding what constitutes good evidence, what are the appropriate methods and ends of cyber war, and so on.”

Though primarily concerned with ethics, Lucas’s comprehensive approach helps to address more theoretical quandaries as well. What is the difference between cyber crime and acts of cyber warfare? Do theorists have the tools necessary to track the norms that emerge as cyber technology develops? How much should an interest in privacy constrain the government’s use of cyber technology in the pursuit of cyber security? Lucas addresses these pressing and complex concerns with concision, and his forays into theory appear sparingly. He analyzes best practices among experts in the field to draw out a set of general rules.

Lucas suggests that just war theory provides guidance when it comes to justifying the use of cyber weapons technology and limiting the kinds of cyber weapons it is permissible to develop. Yet there are new issues, Lucas says, that are beyond the reach of just war theory—issues related to national security, privacy, and the justification for cyber surveillance. These topics warrant more discussion than Lucas affords them. Lucas also fails to address fully the complexities of state-sponsored hacktivism—an issue that is particularly pertinent since the 2016 United States presidential election.

Nevertheless, this book is a must-read for those who want to understand cyber technology and its implications for national security and international relations. Cutting through the inflated versions of the threats posed by emerging technology, Lucas clears the way for congenial and productive discussion.