ROUNDTABLE: COMPETING VISIONS FOR CYBERSPACE

Introduction

Duncan B. Hollis and Tim Maurer

The phrase "cyberspace is man-made" has been stated so often that it may now sound trite. Yet it has profound implications, particularly for a discussion of ethical questions relating to the Internet. Unlike land, sea, air, or space, the Internet would not exist without humans. And while at least the land and sea have been the subject of significant human interventions, neither one can be modified or shaped on the same scale as the Internet. It is entirely human behavior that continues to drive the technology's global expansion, connecting ever more people and devices. And that behavior is ultimately the result of ethical choices—choices that are often implied but seldom explicitly discussed.[1]

Governing cyberspace is notoriously difficult, raising at least three sets of challenges. First, there are questions about *what* is to be shaped with respect to both governance *of* the Internet and governance *on* the Internet. What should the rules of behavior be for how we construct cyberspace and for those who use it? Second, there are challenges in terms of *who* gets governed. What are the rules for states, for companies, or for all the remaining users of information communication technologies (ICTs)? Third, there is the challenge of *how* we should govern cyberspace. Is it best regulated through law, and, if so, should it be via domestic or international laws? Or is cyberspace better regulated by using nonlegal means for interested stakeholders? All three areas have generated sustained and substantial inquiry by states and scholars alike.

In this roundtable we seek to add and explore a fourth focal point for questions of cyberspace governance: *Why* do we try to shape cyberspace? To this end, we have invited experts from a variety of disciplines to explore the implications of some of the more popular justifications for regulating cyberspace. We believe that responses in each of the first three baskets of questions—what to govern, whom to govern, and how to govern—often depend on answering *why* the

Ethics & International Affairs, 32, no. 4 (2018), pp. 407–410.

doi:10.1017/S089267941800062X

regulation is sought in the first place. Moreover, there are substantially different answers to the "why" question. Are we governing cyberspace to protect privacy or are we doing so to further economic interests? Are we governing cyberspace to advance the free flow of information or to ensure that states can pursue security? Of course, different stakeholders may answer these questions differently. And some may be inclined to a pluralist "all of the above" response, which then raises the question of how to prioritize among such competing purposes.

In the popular television series *Star Trek: The Next Generation*, the captain of the starship states that "the prime directive is not just a set of rules, it is a philosophy."[2] The "prime directive" in that case was to refrain from interfering with the natural development of alien civilizations, making it essentially the space equivalent of the absolutist nonintervention doctrine that has been a foundational principle of international relations dating back to the seventeenth century. In this series of essays, we have asked the contributors to adopt the *concept* of a prime directive for cyberspace—an overarching guiding principle based on an underlying notion of the good. The term "prime directive" is thus employed here in a more abstract sense, as a guiding principle, rather than a concept of nonintervention. We use it to ask a fundamental question: As the Internet evolves, what ought to be the prime directive for how we interact with it?

Specifically, the roundtable considers three prime directives for cyberspace: to promote human expression and privacy above all else (Ronald J. Deibert); to promote economic prosperity above all else (Daniel J. Weitzner); and to engage in warfare above all else (Duncan B. Hollis and Jens David Ohlin). We chose these three because they reflect three of the most prominent orientations around which regulatory discourse occurs: human rights, economics, and security. Still, we are cognizant that these are not the only possible prime directives. Others might prioritize a particular social or cultural value. Putting oneself in the shoes of an authoritarian regime, the surveillance and suppression of content that could undermine social stability might appear as an appealing prime directive.[3] Or, instead of importing prime directives from outside of cyberspace, we could examine a more endogenous directive, such as treating cyberspace's prime directive as the acquisition and transmission of information itself. If the good lies in the communication of information, for example, we might expect a different hierarchy of regulatory priorities, whether in terms of promoting the spread of ICTs that allow the collection of data by governments or companies, or resisting state efforts to engage in data localization.

https://doi.org/10.1017/S089267941800062X Published online by Cambridge University Press

Having assigned various prime directives as to what constitutes the good, we invited each contributor to explore what answers would follow in terms of what to regulate, who to regulate, and how to regulate. For example, if the given good were protecting human privacy, it might follow that cyberspace governance should preserve user capacity to employ encryption, favor regulating states to limit their capacity to surveil, or require companies to protect data. Or, if the good were warfighting, we might favor regulations that require ICTs to operate in ways that allow increased attribution and more transparent distinctions among civilian and military sources while encouraging states to hack first rather than attack via kinetic means.

Ultimately, the prime directive is an abstraction and ideal. Human behavior is usually the opposite: contradictory not only over time but often also in real time. Consider, for example, the U.S. Department of State actively funding the development of surveillance circumvention technology while the U.S. National Security Agency was actively working on trying to break it.[4] With this in mind, the final essay, written by Martha Finnemore, offers a more realistic and pluralistic picture, and considers some of the underlying questions and trade-offs that follow from adopting any one prime directive alone.

A major theme that cuts across the contributions is the distinction of looking at the world and humankind holistically or as divided into nation-states. Whereas Deibert and Weitzner take on a more humanitarian perspective focusing on individuals and people independent of their nationality, Hollis and Ohlin concentrate on nation-states as their primary focus. This is not surprising given that the first two authors advance the notion of a universal good, namely human rights and the economic benefits to all consumers from a free trade regime, respectively. Nevertheless, this common theme reveals how questions that have been challenging moral philosophy more broadly (namely, whether the nation-state is to be taken as a given, bounding ethical discussion, or as one of many possible worlds to be contested)[5] are also influencing current debates with respect to the future of cyberspace. When it comes to the Internet, the answer to this question partly depends on how globally interdependent the network will be in the future—a choice that users, companies, and states are confronting today.

Of course, this roundtable is unlikely to definitively resolve what those choices should be. But in unearthing the ethical underpinnings of different policy prescriptions and regulations, these essays offer a more rational and reasoned path forward. There may never be a single prime directive for cyberspace, but the effort to examine the most likely candidates may help us navigate this complex and pluralist sociotechnical institution on which human existence increasingly depends.

https://doi.org/10.1017/S089267941800062X Published online by Cambridge University Press

NOTES

[1] Some scholars, such as Harvard Law School professor Jonathan Zittrain, have dedicated monographs to these questions, peeling away the various layers of ethical choices embedded in the creation of hardware and software, while also making an ethical argument in furtherance of the Internet's openness and "generativity." See Jonathan Zittrain, *The Future of the Internet and How to Stop It* (New Haven, Conn.: Yale University Press, 2008). Others, like Evgeny Morozov, offer a more skeptical view of the technology's promises. See Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011). Such in-depth analytical and ethical treatments of the Internet remain exceptional, however.

[2] Jean-Luc Picard, in "Symbiosis," *Star Trek: The Next Generation*, season 1, episode 21, directed by Win Phelps, aired April 18, 1988.

[3] See Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," Citizen Lab, available at openeffect.ca/code-conduct/.

[4] Andrea Peterson, "The NSA is Trying to Crack Tor. The State Department Is Helping Pay for It," *Washington Post*, October 5, 2013, www.washingtonpost.com/news/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/?utm_term=.029a46b2157c.

[5] See for example John Rawls, *A Theory of Justice* (Cambridge, Mass.: Harvard University Press, 2009); and Thomas W. Pogge, *World Poverty and Human Rights: Cosmopolitan Responsibilities and Reforms* (Cambridge, U.K.: Polity Press, 2002).