A Doctrinal Thesis

Fred B. Schneider
Cornell University

Deirdre K. Mulligan
University of California, Berkeley

Cybersecurity is no longer being left to technologists. Governments, realizing that policy must be a crucial ingredient of any solution, are starting to flex their regulatory and legislative muscle. This is an important step in the right direction, since plenty of evidence indicates that technology alone can't lead us to a trustworthy cyberspace. New policy and new institutions are required.

Today's policy discussions, however, are profoundly disturbing. The problem is not only the specific policy proposals, but the bigger picture—a potpourri of narrowly focused initiatives. If there is an over-arching policy framework, it's that new proposals be consistent with increasingly irrelevant norms, incentives, and mechanisms from the past century. Entrenched special interest groups and single-issue advocates flourish in such a retrograde framework, but the policy landscape resulting from such "bottom-up" policy design won't be pretty, nor will it be effective. Rather, it will exhibit the well-known deficiencies of any bottom-up system design: components that won't interact easily, have overlapping instead of independent functionality, and with inconsistent semantics.

We must break out of the current dialogue and its focus on piecemeal solutions. New policy proposals need to be rationalized in terms of their support for a *cybersecurity doctrine*, which defines goals and means.

- The goals state which system properties will be preserved, as well as which policies will be enforced, for whom, at what costs (for example, monetary expenses, costs to convenience, and compromised societal values), and against what kinds of threats. Goals might be absolute, or they might specify a range of permissible trade-offs. Allowing trade-offs is crucial because that acknowledges cybersecurity's political nature and the need for conversations among those affected when goals are set.
- The means range broadly over technological, educational, and/or regulatory measures. Expect means to include policy that creates incentives—which might range from market based to coercive—to foster adoption and/or deployment of the measures being proposed.

This doctrinal high road not only offers a lens for evaluating current policy proposals, but it can also provide inspiration for new institutions, mechanisms, and regulation.

Some Current Policy Proposals Revisited

Much of the debate today about authentication and identity on the Internet is not, in fact, a debate about the mechanisms per se but is a proxy for the debate about a doctrine of deterrence through accountability. This doctrine equates attacks with crimes and focuses on policy and structures to support forensics, identify perpetrators, and prosecute them. However, this doctrine has no teeth and will fail absent an effective means for retribution. Moreover, the doctrine depends on attribution of a machine's actions to individuals, requires international agreements about illegality, and presumes cross-border enforcement that depends on unprecedented levels of cooperation among nations.

Other cybersecurity policy proposals currently under discussion derive from an analogy between computer malware and biological pathogens. The 2009 US National Leap Year Summit, for instance, discussed the creation of a Cyber-CDC, inspired by the existing Centers for Disease Control and Prevention (www.nitrd.gov/NCLYSummit.aspx).

The dialogue, however, is again proceeding piecemeal and bottom-up, although it is easy to imagine that a higher-level view—a cyberspace analogy to public health—could serve as the rationale for a Cyber-CDC proposal. But why should anyone accept this specific analogy as a basis for a doctrine? Public health concerns inform people's behaviors as does religion, yet "patch and pray" aside, few would argue that an analogy with religion is a good

1540-7993/11/$26.00 © 2011 IEEE COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES

starting point for a credible cybersecurity doctrine.

A New Doctrine

There is, in fact, a doctrinal high-road argument, based on ideas from economics, to rationalize a cybersecurity doctrine inspired by public health. Public health—the prevention of disease and promotion of good health in populations writ large—is what economists consider a *public good*, because public health is non-rivalrous and non-excludable. Cybersecurity is also non-rivalrous and non-excludable: one user benefiting from the security of a networked system does not diminish the ability of any other user to benefit from the security of that system, and users of a secure system cannot be easily excluded from the benefits that security brings.

We can further mine the analogy and observe that public health and cybersecurity both aim to achieve a positive state (health or security) in a loosely affiliated but highly interdependent network. With one, it's a network composed primarily of people existing in an environment over which they have some limited control; with the other, the network comprises people, software, and hardware (for communications, storage, and processing). And because this positive state is ultimately unachievable, both struggle with how to manage in its absence as well as with how to prompt its production. Success in the two settings ultimately depends not only on technical progress but on reaching a political agreement about the relative value of some public good in comparison to other societal values and the institutions granted authority to resolve conflicts (along with the methods they might use).

We are engaged in a discussion about a doctrine—a doctrine of public cybersecurity, whose goals are producing cybersecurity and managing insecurity that remains, where political agreement balances individual rights and public welfare. By extrapolating from public health, we then should advocate cybersecurity measures like prevention, containment, mitigation, and recovery, all of which are strategies that direct resources toward production and preservation of cybersecurity. Modern public health doctrines don't compensate victims of disease so, by analogy, public cybersecurity would not focus on restitution. Modern public health also doesn't punish victims of disease, so public cybersecurity shouldn't either. The parallel with public health also suggests that public cybersecurity favor prevention over recovery.

Looking to specific mechanisms, public health's quarantine in response to disease benefits the collective by depriving an individual of certain freedoms. By analogy, public cybersecurity could dictate responses that deprive individuals of actions (say, by severing a network connection) only if those responses benefit the collective. (But punishments solely for retribution could not be part of public cybersecurity.) Education and certification not only promote good health but also can help in the production of cybersecurity by creating better developers and less naïve users. Diversity leads to more resilient ecosystems, whether that ecosystem comprises individuals and species or comprises networks of computers. And there is the obvious correspondence between vaccinations and patches. The parallel continues: surveillance (intrusion detection), isolation (firewalls), the role of intermediaries (ISPs), and so on.

With regard to incentives, ensuring that actors contribute to public cybersecurity requires interventions to overcome positive and negative externalities that lead rational individuals to underinvest, just like for public health. And when incentives are insufficient to prompt private provisioning, the public interest requires making value-ridden choices to interfere with the rights and interests of individuals and organizations. Those choices would be embodied in goals that reflect political agreement about the good in question (its definition), the socially desirable level given competing priorities and values, and provisions for determining when the individual's desires yield to the collective's need. For example, an agreement might stipulate that state coercion is permitted only when certain incursions into the rights and interests of individuals are tightly circumscribed.

Cybersecurity doctrines are a powerful tool for organizing, inspiring, and analyzing new policy and new technology. They foster an approach that is top-down, thereby increasing the chances that the resulting landscape will be coherent and consistent. Deterrence through accountability and public cybersecurity are just two cybersecurity doctrines that we argue should be playing a central role in discussions; other doctrines are also possible, and these ought to be identified and explored. But, above all, we must resist being dragged into the details of policy proposals until after we have identified and analyzed the doctrines they are intended to support. □

Fred B. Schneider *is associate editor in chief of* IEEE S&P *and a faculty member at Cornell University's Department of Computer Science.*

Deirdre K. Mulligan *is on the faculty at the School of Information, University of California, Berkeley.*

This editorial is based on "Doctrine for Cybersecurity" (www.cs.cornell.edu/fbs/publications/publicCybersecDaed.pdf). —Ed.