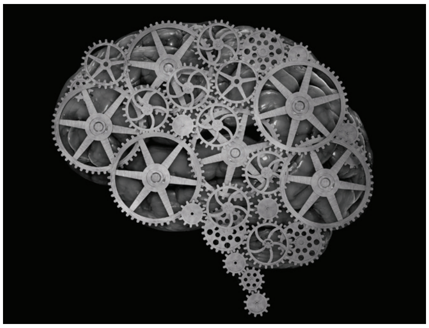

Assets to the Table

David Alan Grier, *George Washington University*

As engineers have built and shaped Internet technology for the past 50 years, they can claim that they have some right to participate in the discussion over the governance of that technology.

You have to follow the logic because that logic makes sense once you understand the context. In the policy world, a fading pop star can play a more prominent role in discussing the issues of our time than a highly experienced engineer. Before you get angry over the shallowness, you need to understand the underlying reasoning because it might offer an unusual opportunity for those with technical expertise

Pop stars, by the reasoning in the policy world, are important because they have the job of engaging the masses. To do that job, they capture the mindset of ordinary people. They can either speak for the people or influence public opinion. Therefore, they're valuable in the public debate.

In contrast, engineers understand things better than ordinary people, but they talk almost exclusively among themselves and so can neither represent public opinion nor do anything to change it. So, in the logic of the policy world, engineers can be part of the policy debate only if their role is to ensure that the Wi-Fi never goes down

I recently discovered that policy logic has taken an unusual twist in the form of a report from the Council on Foreign Relations on Cybersecurity. The Council is one of the think tanks founded in the aftermath of the first World War as part of a grand effort to make the world safe for democracy. Historically, it has had little interest in technology, except for perhaps weapons of mass distribution.

The report, entitled "Defending an Open, Global, Secure, and Resilient Internet," was left for me by a colleague who probably thought that it was a technical document, although it contains not even a single equation. Most of the points in the document would be familiar to most computer scientists. "Cyberspace is now an arena for strategic competition among states," the report explains in urgent tones. "Multiple sources of power and influence, divergent values, and clashing interests all complicate policymaking within countries and across borders."

I didn't expect to find much in the report. None of the authors were technical leaders in the field of cybersecurity. As I flipped the pages, I caught several small technical misstatements. None invalided the thesis of the report but taken as a whole, they suggested that the authors understood the implications of failed Internet security better than how they might secure the global information infrastructure. However, one phrase caught my attention because it was repeated in paragraph after paragraph: "governments, industry and civil society."

Repetition is common in think-tank reports. These documents are written by interns who rarely talk with each other. In this case, the repetition revealed a surprising concession by an organization that has devoted its history to the nation-state. They suggested that the council believes that cyber security can't be addressed by national governments alone: it requires an alliance of interests.

As long as we have had nation-states, they have been the dominant player in global politics. With the Internet age, they may have lost some of that monopoly over technical talent. In a small way, the Council might be acknowledging that world peace is now maintained by a wide variety of global actors and that the logic of diplomacy now has room for those with technical expertise to bring their assets to the table. ◼

David Alan Grier is a professor at George Washington University. His podcasts from #erranthashtag and other sources can be found at http://video.dagrier.net.

Published by the IEEE Computer Society