BLOG @CACM

The *Communications* Web site, <http://cacm.acm.org>, features more than a dozen bloggers in the BLOG@CACM community. In each issue of *Communications*, we'll publish selected posts or excerpts.

Follow us on Twitter at <http://twitter.com/blogCACM>

DOI:10.1145/2892708

<http://cacm.acm.org/blogs/blog-cacm>

Sampling Bias in CS Education, and Where's the Cyber Strategy?

Mark Guzdial examines a logical fallacy in consumer science education; John Arquilla sees an absence of discussion about the use of information technologies in future conflicts.

Mark Guzdial
"The Inverse Lake Wobegon Effect"

<http://bit.ly/1PpjWmn>
January 11, 2016

Every episode of the radio variety show "A Prairie Home Companion" includes a segment in which host Garrison Keillor tells stories from his mythical hometown, Lake Wobegon. Each segment ends with, "Well, that's the news from Lake Wobegon, where all the women are strong, all the men are good looking, and all the children are above average." That notion, that "all the children are above average," is an example of what is known as the Lake Wobegon Effect (<http://bit.ly/1JYKFKr>), also known as "illusory superiority" (<http://bit.ly/23JkX33>).

The Lake Wobegon Effect is where we consider the small sample in our experience superior to the population overall. A concrete example: 80% of drivers consider themselves above-average drivers. Obviously that cannot

be true, but it is common that we think what we experience is above average.

The Inverse Lake Wobegon Effect is a term I am coining for a fallacy that I see sometimes in computer science (CS) education: we sample from a clearly biased source and assume the sample describes the overall population. We know we are observing a superior sample, but act like we are getting a randomly distributed sample. This is a form of sampling bias (<http://bit.ly/1R358iK>).

I introduce the term in a book I just published with Morgan & Claypool, *Learner-Centered Design of Computing Education: Research on Computing for Everyone*. One example of the Inverse Lake Wobegon Effect in CS education is assuming a successful undergraduate introductory curriculum will be similarly successful in high school. Students in undergraduate education are elite. In the U.S., undergraduates are screened in an application process and are in the top half of most scales (such as intellectual achievement and wealth). Elite students can learn under conditions in which

average students might not succeed, which educators call *aptitude-treatment interactions* (<http://bit.ly/1PiaGB6>).

Consider Bennedsen and Caspersen's work on predictors for success in introductory computing (<http://bit.ly/1TEkY3W>). Students in undergraduate education have better math grades and more course work than average students in high school, and both factors predict success in introductory CS courses. Think about the role of algebra in programming. There are high schools in Atlanta, GA, where less than half the students pass algebra. The same CS curriculum that assumes success with algebra is unlikely to work well for undergraduate and high school audiences.

Imagine a highly successful undergraduate introductory computing curriculum in which 80% of the students succeed; that is, 80% of students from the top half of whatever scale we are talking about. The same curriculum might fail for 60% of the general population.

We see a similar sampling error when we talk about using MOOC data to inform our understanding of learning. The edX website says it offers a platform for "exploring how students learn." Students who take MOOCs are overwhelmingly well-educated, employed, and from developed countries—characteristics that describe only a small percentage of the overall population. We cannot assume what we learn from the biased sample of MOOC participants describes the general population.

Psychologists are concerned many of their findings are biased because they oversample from "WEIRD" students:

They found people from Western, educated, industrialized, rich and democratic (WEIRD) societies—representing up to 80% of study participants, but only 12% of the world’s population—are not only unrepresentative of humans as a species, but on many measures they are outliers. (<http://bit.ly/1S11gQo>).

It is easy to fall prey to the Inverse Lake Wobegon Effect. Those of us who work at colleges and universities only teach undergraduate and graduate students. It is easy for us to believe those students represent all students. If we are really aiming at computing for *everyone*, we have to realize we do not see *everyone* on our campuses. We have to design explicitly for those new audiences.

John Arquilla
**“Toward a Discourse
 on Cyber Strategy”**

<http://bit.ly/1J6TPE9>
 January 15, 2016

While cyber security is a topic of discussion all over the world today—a discourse shifting in emphasis from firewalls to strong encryption and cloud computing—little is heard about broader notions of cyber strategy. Efforts to understand how future conflicts will be affected by advanced information technologies seem to be missing—or are taking place far from the public eye.

When David Ronfeldt and I first published *Cyberwar Is Coming!* (<http://bit.ly/1PAL6uW>) nearly a quarter-century ago, we focused on overall military operational and organizational implications of “cyber,” not just specific cyberspace-based concerns. It was our hope a wide-angled perspective would help shape the strategic conversation.

Sadly, it was not to be. Forests have been felled to provide paper for the many books and articles about how to protect information systems and infrastructure, but little has emerged to inform and guide future development of broader strategies for the cyber era.

There have been at least a few voices raised in strong support of a fresh approach to strategic thought in our time—interestingly, with some of the best contributions coming from naval strategists. Among the most trenchant insights were those of two senior U.S. Navy officers. Vice Admiral Arthur Cebrowski, with his concept of “network-

centric warfare,” emphasized this period of technological change would favor the network form of organization. Admiral Bill Owens, in his *Lifting the Fog of War* (<http://bit.ly/1SYvEuL>), argued for extensive information gathering and sharing in what he called a “system of systems.” Both were writing over 15 years ago, and their respective visions proved to be a bit too cutting-edge to gain much traction.

Around the same time, some astute naval officers in China were doing much the same. Then-Captain Shen Zhongchang, the People’s Liberation Army Navy’s R&D director, along with a few staff officers, appreciated the importance of networks and systems thinking—keying on the former as principal targets in future conflicts and directing their energies on battle doctrines. They understood huge increases in the information content of weaponry virtually decoupled range from accuracy, making possible “remote warfare” and demanding dispersal rather than concentration of forces in future wars.

Zhongchang’s team played a measurable role in shaping Chinese strategic thought. Overall, though, there has been little open debate of ideas about the age of cyberwar in world strategic circles. How different this is from the international discourse that arose over the prospect of nuclear war. In the first decade of the atomic age, a range of strategic ideas shaped lively debates. In the U.S., enthusiasm for nuclear weapons among senior policymakers led to ideas about waging preventive wars against enemies before they could acquire such capabilities. Thankfully, scholars and others involved in security affairs rose up in protest and, in 1954, President Eisenhower publicly renounced the idea the U.S. would ever wage preventive nuclear war.

Other countries were ahead of the U.S. on this point, including the then-Soviet Union, and even France, where Charles de Gaulle put the notion of endless nuclear arms racing to rest with the formulation all that was needed was an “arm-tearing-off” capacity for deterrence to work well. Mao Zedong adopted this view, too; so have most others who have developed nuclear weapons. Eventually, in part because of public debate—and sometimes because of protests in both countries—Moscow and

Washington came around to this view, and arms racing turned into the nuclear arms reductions we see today.

This is not the case with cyber. There is a raging arms race in virtual weaponry, secretly, in many countries, with concomitant plans for preemptive, preventive, and other sorts of Pearl Harbor-like actions. The potential for “mass disruption” (as opposed to mass *destruction*) is generally the focus of these efforts. The results could be costly if these ideas were ever acted upon. As Scott Borg, director of the U.S. Cyber Consequences Unit, noted: “An all-out cyber assault can potentially do damage that can be exceeded only by nuclear warfare.”

Yet instead of an outcry about this looming threat and a thoughtful discourse about how to bring these capabilities under control, efforts to develop ever-more-sophisticated weaponry of this sort proceed unabated. In some places, the complacency in the face of the potential threats is staggering. Witness the comments of the current U.S. “cyber czar,” Michael Daniel: “If you know about it, [cyber is] very easy to defend against.” In an age where the world has repeatedly seen how vulnerable commercial enterprises are, and where even sensitive information guarded by governments is breached, the statement that cyber attack is “easy to defend against” rings all too hollow.

What is needed now is a lively discourse on cyber strategy. It should probably begin with consideration of whether offense or defense dominates, as parsing the peril in this way will affect the larger debate about continuing the cyber arms race or, instead, searching out various ways to craft sustainable, behavior-based international cyber arms control agreements. The wisdom or folly of using cyber weaponry in preemptive or preventive actions—à la Stuxnet—should also be openly debated.

In an earlier era, atomic scientists played central roles in guiding and informing the key nuclear debates—in the military, government, and among the mass public. In this era, it may be up to computer scientists and information technology experts to provide a similar service—and *now* is the time. ■

Mark Guzdial is a professor at the Georgia Institute of Technology. John Arquilla is a professor at the U.S. Naval Postgraduate School.

© 2016 ACM 0001-0782/16/04 \$15.00