1-1-2016

# Controlling cyber arms, and creating new LEGOs

John Arquilla
*Naval Postgraduate School*

Joel C. Adams
*Calvin University*

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.

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

DOI:10.1145/2843530 http://cacm.acm.org/blogs/blog-cacm

# Controlling Cyber Arms, and Creating New LEGOs

*John Arquilla identifies flaws in a potential U.S.-China cyber arms control pact, while Joel C. Adams suggests an unusual way of preserving computer science history.*

**John Arquilla**
**"A Farewell to (Virtual) Arms?"**
http://bit.ly/1RkiAfA
October 2, 2015

Much attention has been focused recently on the budding possibility of a Sino-American cyber arms control agreement, whose foundation would be a mutual pledge of "no first use" of bits and bytes to cripple critical civilian infrastructure. It is an intriguing development, despite having three troubling flaws.

The first problem afflicts the agreement's logical basis, given that both sides pledge not to mount such attacks "in peacetime." But what if such an attack, a "digital Pearl Harbor," were to be the opening act of war—when "peacetime" would have been thereby ended? A bit of a conundrum, complicated further by the fact that most advanced militaries rely, to varying degrees, on civil infrastructures they do not own or control for much of their communications, logistics, and other functions. So, in a sense, civil infrastructure can actually be viewed as consisting of a range of strategic, military-related targets.

Next there is the major perceptual problem that lies at what might be called the "boundary layer" of this agreement that does not explicitly extend to cyber espionage. The difficulty here is that the sorts of actions, exploits, and intrusions that go with virtual spying are observationally equivalent to the preparatory access to the adversary's systems that would be sought prior to launching an actual attack. Thus the cyber peace would always be poised on a knife-edge of instability. A related perceptual complication is that the ultimate identity of the attacker is not always clearly or easily distinguished—and so the potential for a third party, C, to attack A anonymously, or to finger innocent B as the culprit, is a very real risk, one that might lead to escalation to war in the physical world—which was the scenario I unfolded in my short story in *Wired* back in 1998, "The Great Cyberwar of 2002" (http://bit.ly/1XMUSfy).

The third difficulty with the Sino-American cyber arms control initiative lies in its scope. The initially narrow focus on infrastructure protection does little or nothing to deal with the large-scale theft of intellectual property that constitutes what can be called the realm of "strategic crime." U.S. President Barack Obama has said much about this over the past few years, and has explicitly called out China as a culprit. In a public statement growing out of a meeting between him and Chinese President Xi Jinping, both leaders affirmed neither country would *knowingly* engage in intellectual property theft.

When asked during his recent testimony before the Senate Armed Services Committee whether there was any real chance of curtailing intellectual property theft, the director of National Intelligence, former general James Clapper, gave a one-word answer: "No." He went on to make critical comments about the possibility of cyber arms control, indicating instead his preference for a focus on improving defenses. His only nod to any sort of agreement was an allusion to Ronald Reagan's approach to engaging in arms-reduction talks with the Russians back in the 1980s: "Trust but verify." So it seems, even in American officialdom, the window of opportunity for cyber arms control has only been opened a crack.

Yet it may prove enough of an opening to move ahead, for the "no first use" doctrine has caught on in the nuclear realm—though it took many decades for the U.S. to decide to move in this direction (there are still some extreme conditions noted in the American nuclear posture statement that would allow first use, but for all practical purposes this is no longer a usable first option).

Issues of verification aside, nations—not just China and the U.S., but others, too—have incentives to behave

circumspectly about starting a strategic cyberwar that would incur huge economic costs and run the risk of a virtual conflict escalating into a shooting war in the physical world. Full disclosure: I introduced the idea of a cyber no-first-use doctrine in an article in the journal *Ethics and Information Technology* back in 1999 ("Can Information Warfare Ever Be Just?" http://bit.ly/1kpQRPq), so I am hardly impartial. It has been a long wait to hear leading heads of state talking about such a possibility, and we must allow the discourse to unfold, rather than simply to dismiss it as idealistic or quixotic.

The best way to envision cyber arms control may be to think of it as analogous to other controlled activities in areas in which diffusion of the enabling technology itself is unstoppable. In the varied realms of chemical and biological weapons, for example, countless nations have access to the materials required to craft such weapons. And yet there are behavior-based arms control agreements in force, to which nearly all countries subscribe, that forbid their use. In the main, there is strong compliance with few violations. Such compliance may well be possible in the cyber arena, too. It is an approach well worth exploring.

With regard to the logical possibility that a "peacetime" pledge is not violated if a strategic cyber attack *starts* a war, the response to this concern is that such an attack could still be limited to military-related targets. To return to the nuclear analogy, this would be very much like the "counterforce" strategic doctrine of the Cold War era that sought to target missiles and other military targets, not population centers. In this way, it was thought, a nuclear war could be waged without massive civilian deaths.

Only a small portion of critical infrastructure is essential for military operations, so cyber combatants would have good chances of operating against armed forces without imposing too much civilian suffering. To be sure, a conflict of this sort would inflict much costly, disruptive collateral damage, but far less than would be the case in a city-busting, apocalyptic general nuclear war. Thank God counterforce nuclear doctrine was never put to use. But cyberwar is much more thinkable than an atomic Armageddon, so the counterforce doctrine that never had to be used for its original purpose may well be dusted off when thinking about how to conduct conflict in the virtual domain.

The most nettlesome problem, of course, is the veil of anonymity in which cyber aggressors—nations or networks—may be inclined to enshroud themselves. Clearly, forensics must continue to improve so as to identify attackers accurately. And just as clearly, a great deal of work is needed to bring forensics up to the needed level of accuracy. Also, strategic deception about the identity of the perpetrator, as mentioned earlier, must be guarded against. But these challenges are no reason to give up on the promise of cyber arms control.

On balance, the emerging, maturing discourse about applying notions of arms control to the cyber realm is a "net positive" (no pun). There are indeed obstacles to overcome, but the potential gains for peace and cybersecurity make the efforts to master these challenges more than worth the while.

**Joel C. Adams**
**"A Lovelace, Babbage, and Analytical Engine LEGO Set?"**
**http://bit.ly/1JvpkC6**
**August 29, 2015**

LEGO has a crowdsourcing ideas site, at https://ideas.lego.com/, where LEGO fans can pitch ideas for new LEGO sets. What a great way to let your audience help you conduct market research!

Hugh McGuire was kind enough to send me a note about a Lovelace and Babbage set (https://ideas.lego.com/projects/102740) that Stewart Lamb Cromar has proposed. The set would include LEGO figurines for Ada Lovelace and Charles Babbage, LEGO pieces to build a representation of the Analytical Engine, punch cards, and related pieces. The various pieces would be styled with "a steampunk aesthetic" to capture the imaginations of young builders. The set would thus let young LEGO builders realize Babbage's vision by completing his Analytical Engine, and learn about the historical roles played by Babbage and Lovelace.

(For those who have forgotten their early computing history: back in 1837, Charles Babbage designed a general-purpose (that is, programmable with punch cards) mechanical computer he called the Analytical Engine. Although a working Analytical Engine was never built, Ada [the Countess of] Lovelace understood the design's potential and corresponded with Babbage about it. She developed a detailed algorithm for using the Analytical Engine to compute Bernoulli numbers, for which she has been dubbed the first computer programmer. In honor of her contributions, the Ada programming language was named after her. Those interested in more details should read "Lovelace and Babbage and the Creation of the 1843 'Notes'" (http://inroads.acm.org/article.cfm?aid=2810201) by Fuegi and Francis.)

Many stories from the "steampunk" genre take place in alternative universes where Babbage actually built an Analytical Engine powered by steam and Ada wrote programs for it. Such stories generally explore the question, "What if ... the power of computing was unleashed in the Victorian era?"

Back in our universe, the dimensions of the LEGO Analytical Engine would be sufficient to accommodate a Raspberry Pi 2 (https://www.raspberrypi.org/products/raspberry-pi-2-model-b/), if one wishes to put a computer inside. That would be fun to see: a LEGO Analytical Engine driving an LCD display, mouse, and keyboard!

One of the motivations for the set is to commemorate the 200th anniversary of Ada's birth (Dec. 10, 1815). The set would thus teach young LEGO builders some early computing history, and that women have been involved in computing since its origins. It would thus help to counter the popular misperception that only men belong in computer science.

If an idea on the LEGO site receives 10,000 supporting votes, they will consider building the set. To support a project, you must register on their site, but registration only takes a minute, so if you want to raise awareness of computer science in our society, and help young boys and girls realize computer science is not limited to males, I encourage you to support this proposal by clicking the blue button on the proposal page (https://ideas.lego.com/projects/102740).

**John Arquilla** is a professor at the U.S. Naval Postgraduate School. **Joel C. Adams** is a professor at Calvin College.