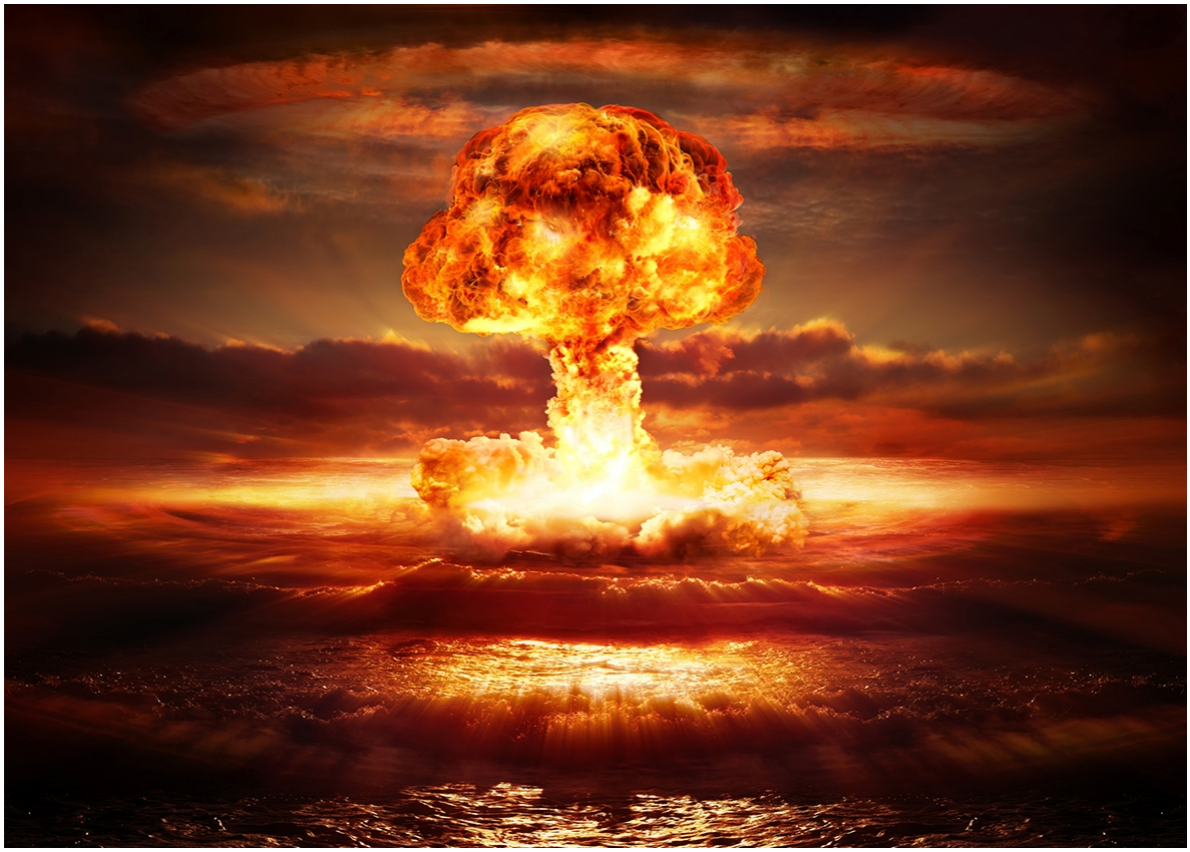
MARCH 15 2016 7:30 AM

FROM SLATE, NEW AMERICA, AND ASU

Cyberweapons Aren't Like Nuclear Weapons

Officials around the world like to compare the two—but the metaphor is incorrect, and dangerous.

By Patrick Cirenza



On the surface the analogy is compelling, but dive a little deeper and it becomes decidedly less convincing.

RomoloTavani/Thinkstock

FUTUROGRAPHY

"If Internet security cannot be controlled, it's not an exaggeration to say the effects could be no less than a nuclear bomb," **said** Gen. Fang Fenghui, chief of general staff of the People's Liberation Army of China, in April 2013. Fang is not alone in drawing comparisons between nuclear weapons and cyberweapons during the past few years. Secretary of State John Kerry responded to a cybersecurity question during his confirmation hearings in January 2013 by **saying**, "I guess I would call it the 21st century nuclear weapons equivalent." That same year, Russian Deputy Prime Minister Dmitry Rogozin **praised** cyberweapons for their "first-strike" capability. Since 2013, a number of leaders in the U.S.

We noticed you're using an ad blocker. Support Slate's journalism and help us reduce our dependence on advertising. Plus!

national security establishment—including former National Security Adviser **Brent Scowcroft** in January 2015, Adm. **Michael Rogers** of Cyber Command in March 2015, and Director of National Intelligence **James Clapper** in February of this year—have stated that the threat posed by cyberweapons is comparable to, or greater than, that of nuclear weapons. The list of high-ranking officials who have made an analogy between the fundamentally different nuclear and cyberweapons systems, and are using this flawed analogy as a basis for policy, is a long one.

On the surface, the analogy is compelling. Like nuclear weapons, the most powerful cyberweapons—malware capable of permanently damaging critical infrastructure and other key assets of society—are potentially catastrophically destructive, have short delivery times across vast distances, and are nearly impossible to defend against. Moreover, only the most technically competent of states appear capable of wielding cyberweapons to strategic effect right now, creating the temporary illusion of an exclusive cyber club. To some leaders who matured during the nuclear age, these tempting similarities and the pressing nature of the strategic cyberthreat provide firm justification to use nuclear deterrence strategies in cyberspace. Indeed, Cold War–style **cyberdeterrence** is one of the foundational cornerstones of the 2015 U.S. Department of Defense Cyber Strategy.

Advertisement

However, dive a little deeper and the analogy becomes decidedly less convincing. At the present time, strategic cyberweapons simply do not share the three main deterrent characteristics of nuclear weapons: the sheer destructiveness of a single weapon, the assuredness of that destruction, and a broad debate over the use of such weapons.

The development of fission and then fusion nuclear weapons made it possible to inflict truly unacceptable costs upon an adversary. The invention of delivery technologies—such as secure second-strike capabilities, intercontinental ballistic missiles, and nuclear payloads with multiple independently targetable re-entry vehicles—guaranteed the credibility of the threat. And finally, the vibrant and interconnected debates within government, academia, and think tanks about the use of nuclear weapons have guided policy and technology toward an outcome of stable deterrence. By contrast, strategic cyberweapons have not met these criteria.

Sheer destructiveness: Despite former Chairman of the Joint Chiefs of Staff Adm. Mike Mullen **claiming** in 2011 that cyberweapons are the "single biggest existential threat that's out there," they have actually inflicted very little physical destruction to date. Stuxnet, the

We noticed you're using an ad blocker. Support Slate's journalism and help us reduce our dependence on advertising — join Slate Plus!

largest known cyberweapon to cross the cyber-physical barrier, damaged only 1,000 uranium enrichment centrifuges. Further, it is **generally accepted** that not a single person has died as a direct result of a cyberattack.

The destructive power of even the smallest of nuclear devices still greatly eclipses that of the demonstrated destruction of cyberweapons. Even if the reverential statements of world leaders about the potential destructiveness of strategic cyberweapons are taken at face value, their power still does not compare to that of nuclear weapons. As Col. Jamie Wakefield, currently the chief of contingency operations for U.S. Northern Command, said in an interview for my thesis in April 2015, "Cyber may be able to threaten the way we live or the way we do business, but nuclear weapons threaten the fact that we live at all." Simply put, strategic cyberweapons are not currently capable of inflicting the unacceptable costs necessary for stable deterrence in cyberspace.

Advertisement

Assuredness of destruction: Questions about the assured delivery of cyber "payloads" also weaken strategic cyberweapons' credibility as a deterrent. While the delivery of a nuclear weapon relies on the vehicle that carries the weapon's warhead, the delivery of a strategic cyberweapon is much more dependent on weaknesses in the target's defenses. If a network administrator patches vulnerabilities in the target computer code, or an agent is unable to insert a USB drive to cross an air-gapped system (a system that is physically disconnected from unprotected networks), then a strategic cyberweapon that was deliverable yesterday might not be today.

Even if a strategic cyberweapon makes it past a system's defenses, there is no guarantee that it will have its intended effect—it could do nothing at all or cause significant unintended collateral damage. There simply is no analogue in the nuclear world, where a weapon's destruction is a predetermined, known quantity. As President Barack Obama observed when I spoke with him at the White House Summit on Cybersecurity and Consumer Protection in February 2015, "With nuclear weapons there is a binary. Either there are no nuclear explosions or there are big ones and it is a real problem. In cyberspace, there are all sorts of gradations." While a state may promise to massively retaliate against a cyberattack, neither the attacker nor the defender can be entirely sure that this will happen because the state may not have the capability to fulfill its threat. This problem significantly undermines the feasibility of applying deterrence principles in cyberspace.

We noticed you're using an ad blocker. Support Slate's journalism and help us reduce our dependence on advertising — join Slate Plus!

A common understanding: Finally, the open-source debate surrounding the use of strategic cyberweapons is still very much in its infancy. In the absence of major public demonstrations of strategic cyberweapons, the debate largely centers on speculation about cybercapabilities. Without a common understanding of strategic cyberweapons, participants take uncoordinated stabs in the dark over what the policy implications of the weapons are. In combination with the limited interaction between the public debate and its classified counterpart, the result is a rather weak conversation. As former CIA Director Michael Hayden commented when I interviewed him in March 2015, "No one has yet begun to write the ***On Thermonuclear War*** [Herman Kahn's classic 1959 text on nuclear strategic concepts] for cyberconflict." Adm. Jim Ellis, former commander of U.S. Strategic Command, put it far less charitably in my interview with him, also in March 2015, saying that the debate was "like the Rio Grande, a mile wide and an inch deep."

The flawed analogy of nuclear weapons and cyberweapons is dangerous because it creates the illusion of security when potentially there is none. At present, a number of factors—including other forms of deterrence and economic interdependence—are discouraging use of the strategic cyberweapons that states around the world are quickly amassing. However, if the global security situation unexpectedly changes, and the United States bases its cyberpolicy on the shaky assumption that it can deter strategic cyberweapons, then it could be vulnerable to attack by those who do not share its views. Chinese experts, for example, have espoused **skepticism** about the feasibility of cyberdeterrence. A misjudgment now about strategic cyberweapons could have catastrophic consequences later.

Advertisement

Why does such a flawed analogy have so much traction at the moment? It could be because it is a ploy to inflate budgets for what **some call** the "cybersecurity industrial complex." Such methods have a proven track record; by **one estimate** the United States spent upward of $5.5 trillion on nuclear weapons between 1940 and 1996. Indeed, there is talk of an ongoing U.S. "**cyber Manhattan Project**" (again, note the pervasive nuclear analogizing). However, the analogy is much more likely a way for a generation of leaders who were not "born digital" to come to terms with the intricacies of cyberspace through concepts with which they are familiar. Just as military commanders confounded by nuclear weapons in the 1950s reached for works on air power by Gens. Giulio Douhet and Billy Mitchell, so too are the national security leaders of today looking to the treatises of American nuclear strategists Bernard Brodie and Thomas Schelling for guidance on cyberwarfare.

We noticed you're using an ad blocker. Support Slate's journalism and help us reduce our dependence on advertising — join Slate Plus!

Under certain conditions, it is possible that the cyber-nuclear analogy could apply in the future. As societies adopt more cyber-reliant technologies in **transportation infrastructure**, **the electrical grid**, and **nuclear power plants**, a massive cyberattack could result in prohibitively high costs and deaths. In combination with the more pernicious second-order effects of cyberattacks on **emergency responder communications networks**, **municipal water and wastewater systems**, and **agricultural** and **pharmaceutical supply and distribution chains**, the effects may even become comparable to those of nuclear weapons. Provided that the most powerful cyberweapons do not proliferate beyond a small subset of states, destruction could be assured, and cyberactors could reach a consensus about how they should use the weapons, it might be possible to have stable, nuclear-style deterrence in cyberspace.

It is far more likely, however, that the nuclear template will not fit neatly onto the situation in cyberspace. As the barriers to entry lower, it may be that thousands or even millions of untraceable actors will become capable of inflicting enormous damage through cyberspace. It could also be that the world overestimated the prowess of these weapons and that they are not nearly as dangerous as first thought.

So how should leaders think about the wide-open future of cyberwarfare? Comparing cyberweapons almost exclusively to nuclear weapons straitjackets thinking into the narrow confines of a single weapons system. A better approach would be to go back to the principle that makes the analogy compelling and expand from there. The core element of the nuclear-cyber analogy is that strategic cyberweapons appear set to revolutionize military affairs in a comparable way to nuclear weapons. However, strategic cyberweapons could develop into a revolution that more closely resembles another military technology, or a mixture of several, or none at all. To cover the full range of possible outcomes, it would therefore be prudent to broaden the analogy to include the lessons of other revolutions in military affairs.

Advertisement

A prime example would be the “offset strategy” technologies that enabled the United States and its allies to achieve overwhelming victory over Saddam Hussein’s then-vaunted military in the **First Gulf War**, but then became **bogged down** against lightly armed insurgents during the occupation of Iraq. Drawing insight from how revolutions such as the offset strategy reached critical mass, how actors exploited them, and how other actors countered and eventually conventionalized them could provide the conceptual flexibility and hybrid strategy necessary to confront the presently unforeseeable challenges that lie ahead in cyberspace.

We noticed you’re using an ad blocker. Support Slate’s journalism and help us reduce our dependence on advertising — join Slate Plus!

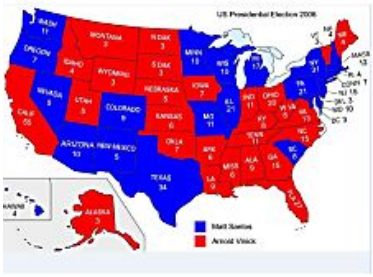
This article was originally published as part of the **Bulletin of the Atomic Scientists**' *Voices of Tomorrow program, which focuses on young authors. It is appearing on* **Slate** *as part of the cyberwar installment of* ***Futurography****, a series in which Future Tense introduces readers to the technologies that will define tomorrow. Each month from January through June 2016, we'll choose a new technology and break it down. Read more from Futurography on cyberwar:*

- "What's the Deal With Cyberwar?"
- "Your Cyberwar Cheat Sheet"
- "Inside 'Eligible Receiver,' the NSA's Disturbingly Successful Hack of the American Military"
- "A Brief Guide to the Weapons of Cyberconflict"
- "The Fuzzy International Rules and Norms for War in Cyberspace"

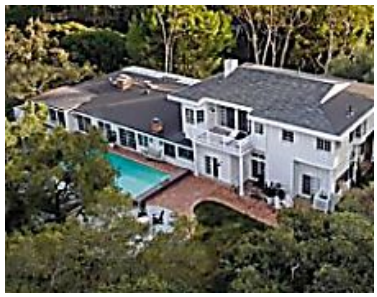
Future Tense is a collaboration among ***Arizona State University****,* ***New America****, and* ***Slate****. To get the latest from Futurography in your inbox, sign up for the weekly Future Tense newsletter.*

ENTER EMAIL HERE SUBSCRIBE TO FUTURE TENSE!

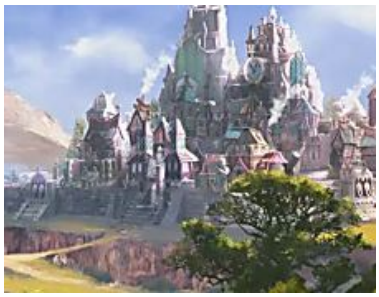
PROMOTED STORIES



Baltimore Firm Has Scary Record of Predicting World Events
MoneyWise 411



What A Million Dollars Can Buy You Around the World
Mansion Global by Dow Jones



Gamers around the world have been waiting for this game!
Elvenar

Lenny Kravitz's Form Beach Home Is Unrea [Photos]
Mansion Global

BROW BEAT SLATE'S CULTURE BLOG

JULY 29 2016 10:23 AM

Broad City's Abbi and Ilana Played Women From 1776 Learning About Hillary's Historic Nomination From Colbert

By Aisha Harris

We noticed you're using an ad blocker. Support Slate's journalism and help us reduce our dependence on advertising — join Slate Plus!