Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

Saving Cyberspace

One year after the Snowden revelations of NSA spying, it is worth looking at what is really at stake.

Imagine that twenty years after Johannes Gutenberg invented mechanical movable type, the petty princes of Europe or the Pope – or anyone who truly tried -- had the ability to exactly determine who was printing, and what they were printing, as the new technology spread around Europe. Worrying about intellectual property theft, privacy or civil rights violations, had those concepts existed, would be missing the bigger picture.

The future of Europe, and probably the entire world, would have been profoundly changed not just for five years, but five hundred. If people lost trust in the underlying communication technology, could there even have been a Renaissance or Enlightenment?

In 2014, and still relatively at the dawn of the Information Age, we face this same dilemma, and the stakes could not be higher: What future Enlightenments will we miss because we can't fully trust the Internet? Our immediate task must be ensuring the Internet and cyberspace remain at least as free, and as awesome, for future generations as they have been for ours.

ABOUT THE CYBER STATECRAFT INITIATIVE

Through global engagement and thought leadership, the Atlantic Council's Cyber Statecraft Initiative focuses on international cooperation, competition, and conflict in cyberspace. Our goal is to demystify cyberspace by focusing on the overlap between it and traditional national security and international relations.

Cyberspace is similar to many things but different to everything. Accordingly, while some of the levers of statecraft that deal with cyberspace may be the same as in the real world; some may seem the same yet operate differently, and others may be completely novel. Cyber statecraft will be a key tool to guide policymakers through the maze of cyberspace.

The Internet is perhaps the most transformative invention since Gutenberg, and yet, it is not being used in a sustainable manner. It is under grave threat from data breaches, theft of commercial secrets, the opportunity for widespread disruptive attacks and systemic failures, the erection of sovereign borders and mass surveillance. As Snowden's revelations and the Heartbleed bug show, we are all becoming absolutely dependent on an unknowably complex system where threats are growing far faster than the Internet's own defenses and resilience.

Today, the Internet is a lawless Wild West. Because the Internet was built on trust, not security, it has been easier to attack others online than to defend against those attacks. This is a decades-old trend. But clearly, if the attackers retain the advantage year after year, the Internet must pass a tipping point.

Perhaps someday soon, there will be too many predators and not enough prey. Unfortunately, the ability of governments to protect those of us that are prey is clearly outweighed by their ability—and willingness—to compete to be the most voracious and efficient predators.

The only way to ensure the Internet remains as free, resilient, secure and awesome for future generations is to flip the historic relationship, giving the defenders the advantage over attackers.

Giving cyber defenders the advantage of the high ground is just barely imaginable with a push for new technology, policy, and practice, which is applied patiently, internationally, at scale and with the private sector at the fore. It is not imaginable if nations continue to escalate large-scale espionage or mass surveillance, subvert Internet companies, engage in shadowy wars against real adversaries or coerce former satellite states.

America's national-security community gives lip service to these dangers, but is in fact enamored of the benefits of cyberspying and cyberattacking. Of course, the president should have these tools at his disposal, but then again, every other national leader wants the same privilege, and the U.S. digital economy is perhaps more open to disruption than any other. America's cyberexperts in the military understand this, but feel if the United States has gone too far, it will be okay because "the pendulum always swings back."

But the earth doesn't care who claws at its back; the sea doesn't know who pollutes its waves. The Internet does know, or rather those who create, maintain, and use it do. Unlike the air, land or sea, it was built by us and it can be changed by us. In short—the pendulum can get stuck.

Perhaps the Internet will no longer a Wild West, but rather become a war-torn, failed Somalia. Every time we try to rebuild the Internet—to be as safe and secure as it used to be—there is (and will be) some new threat to drag it down into chaos, with devastating consequences to America's IT-dependent economy and those of us who have come to love our online lives.

Technologies that seem so promising today, such as online voting or Smart Grid for more environmental and economic electricity, will never materialize due to the security challenges. Our children and theirs may look back and wonder why anyone would feel safe buying something online, or how online videos survived without being quickly hacked.

How many future Renaissances or Enlightenments will never occur simply because we treated the Internet as a place for crime, spying and warfare ("everyone does it" after all), rather than the most innovative and transformative product of human minds in five hundred years?

Sadly, without true commitment by all of us to exercise more sustainable practices in cyberspace, our generation will likely be the last one to truly enjoy the Internet.

Ideas which might work toward Saving Cyberspace include:

D>O, Getting Defense Superior to Offense: For decades on the Internet, it has been easier to attack than to defend, but this does not have to be an iron rule. The only truly strategic goal for cybersecurity is to flip this historic relationship. After all, in almost every other field of human conflict, since man first lifted a stick against one another, the balance between offense and defense has shifted all the time. Through technology, policy, and practice it is possible for defense to gain the advantage over the offense (D>O as shorthand).

If current trends persist, attackers may not have just a local advantage but true supremacy (O>>D). The Internet would no longer be like the Wild West, but a war-torn and failed Somalia.

Building a Sustainable Cyberspace: Cyberspace is not being used in a sustainable manner. A Sustainable Cyberspace would not just be stable, secure, and resilient, but also tie cybersecurity goals directly to ICT capacity building. Large-scale surveillance, huge botnets or erecting Internet borders are just as likely to be unsustainable practices as clear-cutting tropical forests or emitting endless CO2.

By snappng today's debate out of the unproductive deadlock of security versus privacy, this framework offers novel pathways for global governance.

Private-Sector Centric Cyber Approach: The United States and other OECD nations should re-focus their national cyber approaches to harness the potential of non-state actors which are most nations' true cyber power. Very few significant cyber conflicts have ever been decisively resolved by governments but by the private sector with its agility, subject-matter expertise, and ability to bend cyberspace.

Governments lack these strengths but do have deep pockets, staying power, and access to other levers of power. The most successful nations will be those with strategies which build on these strengths, not as a mere partnership, but which puts the private sector at the center of the defense, the “supported” not the “supporting” command