Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

Saving Cyberspace

A project of the Cyber Statecraft Initiative

Imagine that twenty years after Johannes Gutenberg invented mechanical movable type, petty princes had the secret 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 point.

The future of Europe, and probably the entire world, would have been profoundly changed for 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?

Entering 2014, and still relatively at the dawn of the Information Age, we face this same dilemma and the stakes could not be higher: ensuring the Internet and cyberspace remain at least as free, and as awesome, for future generations as they have been for ours.

The Internet and cyberspace are the most transformative inventions since Gutenberg and yet today, these technologies are under grave threat from widespread disruptive attacks, crime, systemic failures, nation state attempts to erect sovereign borders, espionage, and privacy intrusions by widespread surveillance.

For decades, it has been easier to attack others through the Internet than to defend. Clearly no system can stay in balance forever with one side forever gaining the advantage. At some point, the system must tip: too many predators and not enough prey. Unforunately, 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 focus of the Cyber Statecraft Initiative is to examine the overlap of national security, international relations, and economic security issues and provide practical and relevant solutions to challenges in cyberspace. Accordingly, as a traditional national security think tank we look to the past, present, and future of the Internet and convince governments and companies to not become obsessed with short-term gains which put our shared digital future at risk.

The Cyber Statecraft Initiative has accordingly made "Saving Cyberspace" the mission to guide its work with many novel concepts and projects (see reverse side) to help bring this vision to a practical reality in Washington DC and other national capitals and technology centers.

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.

Key Concepts and Projects for Saving Cyberspace

Building a Sustainable Cyberspace: The Internet may not be as free, reliable or simply as awesome for future generations as it has been for ours. Like any other resource, 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 CO_2. By snappng today's debate out of the unproductive deadlock of security versus privacy, this new framework offers new ideas for global governance.

D>O, Getting Defense Superior to Offense: The only truly strategic goal for cybersecurity is to flip the historic relationship between attackers and defenders. For decades on the Internet, it has been easier to attack than to defend, but this does not have to be an iron rule. 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 shifts all the time. Through technology, policy, and practice it is possible for defense to have the advantage over the offense (or D>O as shorthand). However, if we continue with the current trends, attackers may not have just a local advantage but true supremacy (O>>D). As a result the Internet will no longer be compared to the Wild West, but to war-torn and failed Somalia.

Private-Sector Centric Cyber Strategy: Hardly any 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 United States and other OECD nations should re-write their national cyber strategies to harness the potential of non-states actors which are most nations' *true* cyber power.

Focus on Systemic Cyber Risks: Companies and governments focus their risk management attention on their own internal systems, ignoring external *systemic* cyber risks. This is strikingly similar to how the financial sector addressed risks prior to the 2008 financial crisis when risks were assessed one financial institution at a time with little understanding of the complex *interconnections* between financial risks. The chance for a cascading catastrophe was not just widely ignored, but most experts insisted that the system was so well diversified that linkages between risks made catastrophe *impossible*.

Just as good internal risk management didn't save companies exposed to the cascading collapse of the financial system, strong but isolated computer security controls will not shield even the best-protected companies from future increasing upstream cyber shocks. This project by the Atlantic Council and Zurich Insurance is working on a report (due April 2014) on systemic cyber risk with recommendations.

Smart Governance for Cybersecurity and Resilience: The project explores the intersection of strong cybersecurity and maintaining an open, interoperable, secure, and reliable Internet through a series of discussions and workshops. The path to comprehensive cybersecurity leads through responsible Internet governance and a balance of liberty and security. Through events and representation at key global governance discussions, the Cyber Statecraft Initiative has been an important player in the debate.

The History of Cyber Conflict: Though it has only a short history, cyber conflict holds important lessons. Yet, these are largely ignored, forcing policymakers to repeat the same mistakes. This project has resulted in the first-ever cyber conflict history book, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, which explores the twenty-six-year history of cyber conflict and analyzes the most significant incidents and lessons-learned.