ISN
ETH Zurich

3 July 2014

Who Leads? Avoiding the Balkanization of Cyberspace

With the control of electronic information becoming part of the geopolitical high ground, is the 'Balkanization' of cyberspace possible? Chris Bronk thinks so. Its primary stakeholders, after all, have failed to provide the broader, beyond-infrastructure leadership that's needed on this issue.

By Christopher Bronk for ISN

Although unfolding crises in Iraq and Ukraine might persuade us otherwise, the world remains a reasonably safe and secure place for many, if not most of its inhabitants. A century ago, Europe was about to embark on a horrific conflict, one difficult to imagine for the globalization advocates of the time. Things were just too interconnected and interdependent, they thought, to make war fathomable. Nonetheless, war happened. This historical example must be borne in mind in contemporary discussions about the security of cyberspace.

As the United States winds down its wars in Afghanistan and Iraq, its military is attempting to reorient itself to a world in which the primary national security concerns are terrorism; the efforts of large rivals such as China and Russia; those of smaller ones such as North Korea and Iran; and finally a set of conflicts and contingencies throughout the developing world – in places like Somalia, Colombia, Syria, Mali, the Sudans, Mexico, and a few others. On top of these conflicts and crises is a concern with the security of cyberspace. While the technical underpinnings of cyberspace may be resilient, the larger construct of ideas and information transfer that it represents – and without which it would not exist – could be quite fragile. Today, declarations of sovereign control and the risk of 'Balkanization' are major threats to the maintenance of what has become a vital, engaging, and lucrative global commons.

The development and proliferation of technical standards for digital communication and interchange have been remarkable. But as political interest rises in cyberspace, boundaries on the Internet are increasingly apparent. According to Mark Raymond, Boundary Gateway Protocol (BGP) controls are evidence of the assertion of sovereign control and of the deflation of the concept of cyberspace as a commons. Research with my colleagues on censorship and blocking of content shows how access to information in cyberspace depends on the degree to which countries or corporations assert themselves in determining what may be read, seen, or heard.

Only a few years ago, the United States constructed a strategy of 'Internet Freedom,' although largely as an asymmetric wedge in response to Chinese cyber-espionage. In Silicon Valley, high-minded

rhetoric about digital freedoms is abundant but, in reality, money talks. Early in 2012, Twitter implemented a "country withheld content"epolicy, in which it announced that it would submit to requests for certain types of content to be blocked at national boundaries. This was just a few months after Saudi Prince Alwaleed bin Talal had invested $300 million in the company. This shows that many of the world's political leaders remain hostile to the idea of ubiquitous and universal access to information. Moreover, governments appear increasingly willing to consider military action in cyberspace, including not only information operations or extensive intelligence gathering campaigns, but real kinetic attacks via computer upon military platforms and critical infrastructure.

Inconsistency, naivety and worse

Although the United States Department of Defense has declared cyberspace a domain for conflict -- on an equal footing with land, sea, air, and space – there is good reason to ask what exactly this means. What, for instance, is the nature of the battles to be fought in cyberspace? Are they analogous, in some way, to traditional military engagements? Or are they antiseptic clashes in which the score is kept with tallies of compromised computers and phones, crashed out systems, or disabled networks? What of stolen information? How about backdoors and Trojans on critical infrastructure? What occupies the dashboard of metrics for cyber conflict? On the whole, despite rising interest in and downright excitement about cyber conflict, there is little consensus about answers to these questions.

There is also enormous inconsistency in the official positions of the world's major powers on the issue of cybersecurity. For years, the United States castigated China for its state-sanctioned cyber espionage activities, before the Snowden affair recast the debate between th e two parties . The United States also raised the alarm about cyber critical infrastructure attacks, often using the Maroochy Shire sewage hack as an example. Nevertheless, it was Stuxnet that made these hypothetical discussions a reality. Despite all of the official pronouncements about assuring the security of information, national policies on cyberspace are frequently contradictory.

The voices of the national security establishment, with its cyber threat politics and securitization agenda, largely embody a perspective of distrust, paranoia, and suspicion. It should not be forgotten that despite all of the official pronouncements from Washington, Moscow, London, Berlin, Brasilia, Delhi, and Beijing, no country among them appears truly serious about trading away the latitude for offensive cyber action or espionage, especially those likely to possess capabilities that significantly outmatch those of their adversaries. There is also a reluctance among governments to advocate for an international treaty or agreement on cyber issues, which would be difficult to enforce.

This reluctance, however, is not common to *all* in government. Europe's young parliamentarians, for instance, many hailing from Green or Pirate parties, have placed Internet issues prominently on their agenda. While this is to be welcomed – as these issues deserve attention from more than just self-interested lobbyists or cybersecurity businesses that stand to profit – the idealism of these groups at times resembles naiveté. The Pirates reject copyright as outdated, desire the most direct democracy possible, and seek to strengthen privacy protections while at the same time calling for greater transparency. Their ideals are admirable, but, in a pragmatic world, they are unprepared to lead.

And beyond the Pirates willing to stand for election are the voices of cyber anarchists. For a few months in 2011, Anonymous was an awfully frightening organization. It turned Zero Day vendor and cyber intelligence firm HBGary on its head and generally pursued its vision of justice through hacking. In addition to being idealistic, the Anonymous organization was also extremely powerful. When it promised to visit chaos on the Mexican drug cartels after the kidnap of a confederate of the organization, the kidnapped individual was released – a rare outcome in such cases.

The future of cyberspace

None of these groups, however, has exercised genuine leadership on the core issue at hand: securing cyberspace. For now, we are lucky enough to live at a time when a set of technologies and protocols permits connectivity across global distances at incredibly low cost. As geopolitics has begun to catch up with this remarkable innovation, democratically elected leaders and dictators alike have grown to fear its power. Even President Obama, who so skillfully employed information technologies in his primary and general election campaigns, has demonstrated a penchant for controlling information, indicting NSA whistle-blower Thomas Drake in 2010. Increasingly unpopular Turkish PM Recep Tayyip Erdogan also became the first Western democratic leader to block a major social media service after his meltdown over Twitter. Control of information may be emerging as the new geopolitical high ground, but so far it appears to be a hill that cannot be taken.

Much as when Gutenberg's invention of the printing press found widespread application, cyberspace is threatening established orders. Before that innovation, it was acceptable in some places to countenance political systems whose legitimacy was grounded in a putative relationship between God and the sovereign. Today, elected leaders employ specialists to troll through Twitter and Facebook, looking for opportunities and weaknesses, while at the same time seeking to shape discussion and sell policy through cyberspace, at times at an incredibly granular level. Want to serve up advertisements to 22-35 year olds with elite degrees employed by Fortune 500 companies in Los Angeles? Facebook can do that.

The greatest threat to cyberspace, beyond censorship and the breakdown of intellectual property regimes, is that the security of networked computer systems and devices remains abysmally bad. Even worse, the underlying technical assumptions for distributed, networked computing are driven by forces that undermine privacy and security. As my Rice Security Lab colleagues have asserted, "The dominant monetization model for applications on the Android platform consists of free applications where the developers receive compensation through the sale of ads." As adware reaches across device functions, user capacity to manage security and privacy dwindles. Millions of potentially compromised PCs are being superseded by billions of inherently compromised mobile devices.

This is the technical topography upon which the struggle to secure cyberspace will likely take place. Again and again, organizations have been breached, hacked, or knocked offline by denial of service campaigns and no end appears to be in sight. For years, corporations have generally accepted that cyber events are a small, requisite cost of doing business in the digital economy, one that is well offset by productivity gains, reduced costs, and new areas of revenue generation. That period is now coming to an end. The data breach against U.S. retailer Target will likely cost the company several hundred million dollars, with possible additional costs from the 33 lawsuits it faces.

The geopolitically-motivated *Shamoon* cyber attack, the Syrian Electronic Army's compromise of the AP's Twitter feed and denial of service attack against the NY Times, and the spate of attacks against South Korea all clearly indicate that cyber attacks against commercial and political targets are likely to become more common. Whether for financial gain or to assert political will, conflict within cyberspace continue and the credible leadership necessary to prevent it is absent. Most policymakers simply fail to understand that cyberspace is an ideational construct, not just a set of technologies.

While there is no shortage of metaphorical applications for cyber, I would argue that what exists today across the globe is an emergent Pinkerton model of cybersecurity. Those who can afford the security services will pay, and, for those who cannot, the world will become a more dangerous place. In the United States, the Internet Service Providers and the major IT firms have successfully avoided regulation, as the recent remarks of FCC Chairman Tom Wheeler make clear. Regulating cybersecurity is not even on the table in the United States.

What is needed is a cybersecurity agenda that protects the intangible, ideational but very real elements that make cyberspace such a vital (and lucrative) global commons. The language of “cyber dominance” undermines any such agenda, and the world’s militaries and intelligence services should take notice. Cyberspace cannot be reduced to its technical infrastructure – its information content simply cannot be taken for granted.

For more information on issues and events that shape our world, please visit the ISN Blog or browse our resources.

Christopher Bronk is the Baker Institute fellow in technology, society and public policy (TSPP) at Rice University. He previously served as a career diplomat with the United States Department of State on assignments both overseas and in Washington, D.C. He holds a Ph.D. from The Maxwell School of Syracuse University and studied international relations at Oxford University.

Publisher

International Relations and Security Network (ISN)

---

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=181188&lng=en

---

ISN, Center for Security Studies (CSS), ETH Zurich, Switzerland