“The aims of the Internet economy and those of state security converge around the same functional needs: collecting, monitoring, and analyzing as much data as possible.”

The Geopolitics of Cyberspace After Snowden

RON DEIBERT

For several years now, it seems that not a day has gone by without a new revelation about the perils of cyberspace: the networks of Fortune 500 companies breached; cyberespionage campaigns uncovered; shadowy hacker groups infiltrating prominent websites and posting extremist propaganda. But the biggest shock came in June 2013 with the first of an apparently endless stream of riveting disclosures from former US National Security Agency (NSA) contractor Edward Snowden. These alarming revelations have served to refocus the world's attention, aiming the spotlight not at cunning cyber activists or sinister data thieves, but rather at the world's most powerful signals intelligence agencies: the NSA, Britain's Government Communications Headquarters (GCHQ), and their allies.

The public is captivated by these disclosures, partly because of the way in which they have been released, but mostly because cyberspace is so essential to all of us. We are in the midst of what might be the most profound communications evolution in all of human history. Within the span of a few decades, society has become completely dependent on the digital information and communication technologies (ICTs) that infuse our lives. Our homes, our jobs, our social networks—the fundamental pillars of our existence—now demand immediate access to these technologies.

With so much at stake, it should not be surprising that cyberspace has become heavily contested. What was originally designed as a small-scale but robust information-sharing network for advanced university research has exploded into the information infrastructure for the entire planet. Its emergence has unsettled institutions and upset the traditional order of things, while simultaneously contributing to a revolution in economics, a path to extraordinary wealth for Internet entrepreneurs, and new forms of social mobilization. These contrasting outcomes have set off a desperate scramble, as stakeholders with competing interests attempt to shape cyberspace to their advantage. There is a geopolitical battle taking place over the future of cyberspace, similar those previously fought over land, sea, air, and space.

Three major trends have been increasingly shaping cyberspace: the big data explosion, the growing power and influence of the state, and the demographic shift to the global South. While these trends preceded the Snowden disclosures, his leaks have served to alter them somewhat, by intensifying and in some cases redirecting the focus of the conflicts over the Internet. This essay will identify several focal points where the outcomes of these contests are likely to be most critical to the future of cyberspace.

BIG DATA

Before discussing the implications of cyberspace, we need to first understand its characteristics: What is unique about the ICT environment that surrounds us? There have been many extraordinary inventions that revolutionized communications throughout human history: the alphabet, the printing press, the telegraph, radio, and television all come to mind. But arguably the most far-reaching in its effects is the creation and development of social media, mobile connectivity, and cloud computing—referred to in shorthand as “big data.” Although these three technological systems are different in many ways, they share one very important characteristic: a vast and rapidly growing volume of personal information, shared (usually voluntarily) with entities separate from

RON DEIBERT *is a professor of political science and director of the Canada Center for Global Security Studies and the Citizen Lab at the University of Toronto. His latest book is* Black Code: Inside the Battle for Cyberspace *(Signal, 2013).*

the individuals to whom the information applies. Most of those entities are privately owned companies, often headquartered in political jurisdictions other than the one in which the individual providing the information lives (a critical point that will be further examined below).

We are, in essence, turning our lives inside out. Data that used to be stored in our filing cabinets, on our desktop computers, or even in our minds, are now routinely stored on equipment maintained by private companies spread across the globe. This data we entrust to them includes that which we are conscious of and deliberate about—websites visited, e-mails sent, texts received, images posted—but a lot of which we are unaware.

For example, a typical mobile phone, even when not in use, emits a pulse every few seconds as a beacon to the nearest WiFi router or cellphone tower. Within that beacon is an extraordinary amount of information about the phone and its owner (known as "metadata"), including make and model, the user's name, and geographic location. And that is just the mobile device itself. Most users have within their devices several dozen applications (more than 50 billion apps have been downloaded from Apple's iTunes store for social networking, fitness, health, games, music, shopping, banking, travel, even tracking sleep patterns), each of which typically gives itself permission to extract data about the user and the device. Some applications take the practice of data extraction several bold steps further, by requesting access to geolocation information, photo albums, contacts, or even the ability to turn on the device's camera and microphone.

The vast majority of Internet users now live in the global South.

We leave behind a trail of digital "exhaust" wherever we go. Data related to our personal lives are compounded by the numerous and growing Internet-connected sensors that permeate our technological environment. The term "Internet of Things" refers to the approximately 15 billion devices (phones, computers, cars, refrigerators, dishwashers, watches, even eyeglasses) that now connect to the Internet and to each other, producing trillions of ever-expanding data points. These data points create an ethereal layer of digital exhaust that circles the globe, forming, in essence, a digital stratosphere.

Given the virtual characteristics of the digital experience, it may be easy to overlook the material properties of communication technologies. But physical geography is an essential component of cyberspace: *Where* technology is located is as important as *what* it is. While our Internet activities may seem a kind of ephemeral and private adventure, they are in fact embedded in a complex infrastructure (material, logistical, and regulatory) that in many cases crosses several borders. We assume that the data we create, manipulate, and distribute are in our possession. But in actuality, they are transported to us via signals and waves, through cables and wires, from distant servers that may or may not be housed in our own political jurisdiction. It is actual matter we are dealing with when we go online, and that matters—a lot. The data that follow us around, that track our lives and habits, do not disappear; they live in the servers of the companies that own and operate the infrastructure. What is done with this information is a decision for those companies to make. The details are buried in their rarely read terms of service, or, increasingly, in special laws, requirements, or policies laid down by the governments in whose jurisdictions they operate.

BIG STATE

The Internet started out as an isolated experiment largely separate from government. In the early days, most governments had no Internet policy, and those that did took a deliberately laissez-faire approach. Early Internet enthusiasts mistakenly understood this lack of policy engagement as a property unique to the technology. Some even went so far as to predict that the Internet would bring about the end of organized government altogether. Over time, however, state involvement has expanded, resulting in an increasing number of Internet-related laws, regulations, standards, and practices. In hindsight, this was inevitable. Anything that permeates our lives so thoroughly naturally introduces externalities—side effects of industrial or commercial activity—that then require the establishment of government policy. But as history demonstrates, linear progress is always punctuated by specific events—and for cyberspace, that event was 9/11.

We continue to live in the wake of 9/11. The events of that day in 2001 profoundly shaped many aspects of society. But no greater impact can be found than the changes it brought to cyberspace governance and security, specifically with respect to the role and influence of governments. One immediate impact was the acceleration of a change in threat perception that had been building for years.

During the Cold War, and largely throughout the modern period (roughly the eighteenth century onward), the primary threat for most governments was "interstate" based. In this paradigm, the state's foremost concern is a cross-border invasion or attack—the idea that another country's military could use force and violence in order to gain control. After the Cold War, and especially since 9/11, the concern has shifted to a different threat paradigm: that a violent attack could be executed by a small extremist group, or even a single human being who could blow himself or herself up in a crowded mall, hijack an airliner, or hack into critical infrastructure. Threats are now dispersed across all of society, regardless of national borders. As a result, the focus of the state's security gaze has become omnidirectional.

Accompanying this altered threat perception are legal and cultural changes, particularly in reaction to what was widely perceived as the reason for the 9/11 catastrophe in the first place: a "failure to connect the dots." The imperative shifted from the micro to the macro. Now, it is not enough to simply look for a needle in the haystack. As General Keith Alexander (former head of the NSA and the US Cyber Command) said, it is now necessary to collect "the entire haystack." Rapidly, new laws have been introduced that substantially broaden the reach of law enforcement and intelligence agencies, the most notable of them being the Patriot Act in the United States—although many other countries have followed suit.

This imperative to "collect it all" has focused government attention squarely on the private sector, which owns and operates most of cyberspace. States began to apply pressure on companies to act as a proxy for government controls—policing their own networks for content deemed illegal, suspicious, or a threat to national security. Thanks to the Snowden disclosures, we now have a much clearer picture of how this pressure manifests itself. Some companies have been paid fees to collude, such as Cable and Wireless (now owned by Vodafone), which was paid tens of millions of pounds by the GCHQ to install surveillance equipment on its networks. Other companies have been subjected to formal or informal pressures, such as court orders, national security letters, the withholding of operating licenses, or even appeals to patriotism. Still others became the targets of computer exploitation, such as US-based Google, whose back-end data infrastructure was secretly hacked into by the NSA.

This manner of government pressure on the private sector illustrates the importance of the physical geography of cyberspace. Of course, many of the corporations that own and operate the infrastructure—companies like Facebook, Microsoft, Twitter, Apple, and Google—are headquartered in the United States. They are subject to US national security law and, as a consequence, allow the government to benefit from a distinct home-field advantage in its attempt to "collect it all." And that it does—a staggering volume, as it turns out. One top-secret NSA slide from the Snowden disclosures reveals that by 2011, the United States (with the cooperation of the private sector) was collecting and archiving about 15 billion Internet metadata records *every single day*. Contrary to the expectations of early Internet enthusiasts, the US government's approach to cyberspace—and by extension that of many other governments as well—has been anything but laissez-faire in the post-9/11 era. While cyberspace may have been born largely in the absence of states, as it has matured states have become an inescapable and dominant presence.

DOMAIN DOMINATION

After 9/11, there was also a shift in US military thinking that profoundly affected cyberspace. The definition of cyberspace as a single "domain"—equal to land, sea, air, and space—was formalized in the early 2000s, leading to the imperative to dominate and rule this domain; to develop offensive capabilities to fight and win wars within cyberspace. A Rubicon was crossed with the Stuxnet virus, which sabotaged Iranian nuclear enrichment facilities. Reportedly engineered jointly by the United States and Israel, the Stuxnet attack was the first de facto act of war carried out entirely through cyberspace. As is often the case in international security dynamics, as one country reframes its objectives and builds up its capabilities, other countries follow suit. Dozens of governments now have within their armed forces dedicated "cyber commands" or their equivalents.

The race to build capabilities also has a ripple effect on industry, as the private sector positions itself to reap the rewards of major cyber-related defense contracts. The imperatives of mass surveillance and preparations for cyberwarfare across the globe have reoriented the defense industrial base.

It is noteworthy in this regard how the big data explosion and the growing power and influence of the state are together generating a political-economic dynamic. The aims of the Internet economy and those of state security converge around the same functional needs: collecting, monitoring, and analyzing as much data as possible. Not surprisingly, many of the same firms service both segments. For example, companies that market facial recognition systems find their products being employed by Facebook on the one hand and the Central Intelligence Agency on the other.

As private individuals who live, work, and play in the cyber realm, we provide the seeds that are then cultivated, harvested, and delivered to market by a massive machine, fueled by the twin engines of corporate and national security needs. The confluence of these two major trends is creating extraordinary tensions in state-society relations, particularly around privacy. But perhaps the most important implications relate to the fact that the market for the cybersecurity industrial complex knows no boundaries—an ominous reality in light of the shifting demographics of cyberspace.

SOUTHERN SHIFT

While the "what" of cyberspace is critical, the "who" is equally important. There is a major demographic shift happening today that is easily overlooked, especially by users in the West, where the technology originates. The vast majority of Internet users now live in the global South. Of the 6 billion mobile devices in circulation, over 4 billion are located in the developing world. In 2001, 8 of every 100 citizens in developing nations owned a mobile subscription. That number has now jumped to 80. In Indonesia, the number of Internet users increases each month by a stunning 800,000. Nigeria had 200,000 Internet users in 2000; today, it has 68 million.

Remarkably, some of the fastest growing online populations are emerging in countries with weak governmental structures or corrupt, autocratic, or authoritarian regimes. Others are developing in zones of conflict, or in countries that have only recently gone through difficult transitions to democracy. Some of the fastest growth rates are in "failed" states, or in countries riven by ethnic rivalries or challenged by religious differences and sensitivities, such as Nigeria, India, Pakistan, Indonesia, and Thailand. Many of these countries do not have long-standing democratic traditions, and therefore lack proper systems of accountability to guard against abuses of power. In some, corruption is rampant, or the military has disproportionate influence.

Consider the relationship between cyberspace and authoritarian rule. We used to mock authoritarian regimes as slow-footed, technologically challenged dinosaurs that would be inevitably weeded out by the information age. The reality has proved more nuanced and complex. These regimes are proving much more adaptable than expected. National-level Internet controls on content and access to information in these countries are now a growing norm. Indeed, some are beginning to affect the very technology itself, rather than vice versa.

In China (the country with the world's most Internet users), "foreign" social media like Facebook, Google, and Twitter are banned in favor of nationally based, more easily controlled alternatives. For example, WeChat—owned by China-based parent company Tencent—is presently the fifth-largest Internet company in the world after Google, Amazon, Alibaba, and eBay, and as of August 2014 it had 438 million active users (70 million outside China) and a public valuation of over $400 billion. China's popular chat applications and social media are required to police the country's networks with regard to politically sensitive content, and some even have hidden censorship and surveillance functionality "baked" into their software. Interestingly, some of WeChat's users outside China began experiencing the same type of content filtering as users inside China, an issue that Tencent claimed was due to a software bug (which it promptly fixed). But the implication of such extraterritorial applications of national-level controls is certainly worth further scrutiny, particularly as China-based companies begin to expand their service offerings in other countries and regions.

It is important to understand the historical context in which this rapid growth is occurring. Unlike the early adopters of the Internet in the West, citizens in the developing world are plugging in and connecting after the Snowden disclosures, and with the model of the NSA in the public domain. They are coming online with cybersecurity at the top of the international agenda, and fierce international competition emerging throughout cyberspace, from the submarine cables to social media. Political leaders in these countries have at their disposal a vast arsenal of products, services, and tools that provide their regimes with highly sophisticated forms of information control. At the same time, their populations are becoming more savvy about using digital media for political mobilization and protest.

While the digital innovations that we take advantage of daily have their origins in high-tech libertarian and free-market hubs like Silicon Valley, the future of cyberspace innovation will be in the global South. Inevitably, the assumptions, preferences, cultures, and controls that characterize that part of the world will come to define cyberspace as much as those of the early entrepreneurs of the information age did in its first two decades.

WHO RULES?

Cyberspace is a complex technological environment that spans numerous industries, governments and regions. As a consequence, there is no one single forum or international organization for cyberspace. Instead, governance is spread throughout numerous small regimes, standard-setting forums, and technical organizations from the regional to the global. In the early days, Internet governance was largely informal and led by non-state actors, especially engineers. But over time, governments have become heavily involved, leading to more politicized struggles at international meetings.

The original promise of the Internet as a forum for free exchange of information is at risk.

Although there is no simple division of camps, observers tend to group countries into those that prefer a more open Internet and a tightly restricted role for governments versus those that prefer a more centralized and state-led form of governance, preferably through the auspices of the United Nations. The United States, the United Kingdom, other European nations, and Asian democracies are typically grouped in the former, with China, Russia, Iran, Saudi Arabia, and other nondemocratic countries grouped in the latter. A large number of emerging market economies, led by Brazil, India, and Indonesia, are seen as "swing states" that could go either way.

Prior to the Snowden disclosures, the battle lines between these opposing views were becoming quite acute—especially around the December 2012 World Congress on Information Technology (WCIT), where many feared Internet governance would fall into UN (and thus more state-controlled) hands. But the WCIT process stalled, and those fears never materialized, in part because of successful lobbying by the United States and its allies, and by Internet companies like Google. After the Snowden disclosures, however, the legitimacy and credibility of the "Internet freedom" camp have been considerably weakened, and there are renewed concerns about the future of cyberspace governance.

Meanwhile, less noticed but arguably more effective have been lower-level forms of Internet governance, particularly in regional security forums and standards-setting organizations. For example, Russia, China, and numerous Central Asian states, as well as observer countries like Iran, have been coordinating their Internet security policies through the Shanghai Cooperation Organization (SCO). Recently, the SCO held military exercises designed to counter Internet-enabled opposition of the sort that participated in the "color revolutions" in former Soviet states. Governments that prefer a tightly controlled Internet are engaging in partnerships, sharing best practices, and jointly developing information control platforms through forums like the SCO. While many casual Internet observers ruminate over the prospect of a UN takeover of the Internet that may never materialize, the most important norms around cyberspace controls could be taking hold beneath the spotlight and at the regional level.

TECHNOLOGICAL SOVEREIGNTY

Closely related to the questions surrounding cyberspace governance at the international level are issues of domestic-level Internet controls, and concerns over "technological sovereignty." This area is one where the reactions to the Snowden disclosures have been most palpably felt in the short term, as countries react to what they see as the US "home-field advantage" (though not always in ways that are straightforward). Included among the leaked details of US- and GCHQ-led operations to exploit the global communications infrastructure are numerous accounts of specific actions to compromise state networks, or even the handheld devices of government officials—most notoriously, the hacking of German Chancellor Angela Merkel's personal cellphone and the targeting of Brazilian government officials' classified communications. But the vast scope of US-led exploitation of global cyberspace, from the code to the undersea cables and everything in between, has set off shockwaves of indignation and loud calls to take immediate responses to restore “technological sovereignty.”

For example, Brazil has spearheaded a project to lay a new submarine cable linking South America directly to Europe, thus bypassing the United States. Meanwhile, many European politicians have argued that contracts with US-based companies that may be secretly colluding with the NSA should be cancelled and replaced with contracts for domestic industry to implement regional and/or nationally autonomous data-routing policies—arguments that European industry has excitedly supported. It is sometimes difficult to unravel whether such measures are genuinely designed to protect citizens, or are really just another form of national industrial protectionism, or both. Largely obscured beneath the heated rhetoric and underlying self-interest, however, are serious questions about whether any of the measures proposed would have any more than a negligible impact when it comes to actually protecting the confidentiality and integrity of communications. As the Snowden disclosures reveal, the NSA and GCHQ have proved to be remarkably adept at exploiting traffic, no matter where it is based, by a variety of means.

We leave behind a trail of digital “exhaust” wherever we go.

A more troubling concern is that such measures may end up unintentionally legitimizing national cyberspace controls, particularly for developing countries, “swing states,” and emerging markets. Pointing to the Snowden disclosures and the fear of NSA-led surveillance can be useful for regimes looking to subject companies and citizens to a variety of information controls, from censorship to surveillance. Whereas policy makers previously might have had concerns about being cast as pariahs or infringers on human rights, they now have a convenient excuse supported by European and other governments’ reactions.

SPYWARE BAZAAR

One byproduct of the huge growth in military and intelligence spending on cybersecurity has been the fueling of a global market for sophisticated surveillance and other security tools. States that do not have an in-house operation on the level of the NSA can now buy advanced capabilities directly from private contractors. These tools are proving particularly attractive to many regimes that face ongoing insurgencies and other security challenges, as well as persistent popular protests. Since the advertised end uses of these products and services include many legitimate needs, such as network traffic management or the lawful interception of data, it is difficult to prevent abuses, and hard even for the companies themselves to know to what ends their products and services might ultimately be directed. Many therefore employ the term “dual-use” to describe such tools.

Research by the University of Toronto’s Citizen Lab from 2012 to 2014 has uncovered numerous cases of human rights activists targeted by advanced digital spyware manufactured by Western companies. Once implanted on a target’s device, this spyware can extract files and contacts, send e-mails and text messages, turn on the microphone and camera, and track the location of the user. If these were isolated incidences, perhaps we could write them off as anomalies. But the Citizen Lab’s international scan of the command and control servers of these products—the computers used to send instructions to infected devices—has produced disturbing evidence of a global market that knows no boundaries. Citizen Lab researchers found one product, Finspy, marketed by a UK company, Gamma Group, in a total of 25 countries—some with dubious human rights records, such as Bahrain, Bangladesh, Ethiopia, Qatar, and Turkmenistan. A subsequent Citizen Lab report found that 21 governments are current or former users of a spyware product sold by an Italian company called Hacking Team, including 9 that received the lowest ranking, “authoritarian,” in the *Economist*’s 2012 Democracy Index.

Meanwhile, a 2014 Privacy International report on surveillance in Central Asia says many of the countries in the region have implemented far-reaching surveillance systems at the base of their telecommunications networks, using advanced US and Israeli equipment, and supported by Russian intelligence training. Products that provide advanced deep packet inspection (the capability to inspect data packets in detail as they flow through networks), content filtering, social network mining, cellphone tracking, and even computer attack targeting are being developed by Western firms and marketed worldwide to regimes seeking to limit democratic participation, isolate and identify opposition, and infiltrate meddlesome adversaries abroad.

Pushing back

The picture of the cyberspace landscape painted above is admittedly quite bleak, and therefore one-sided. The contests over cyberspace are multidimensional and include many groups and individuals pushing for technologies, laws, and norms that support free speech, privacy, and access to information. Here, too, the Snowden disclosures have had an animating effect, raising awareness of risks and spurring on change. Whereas vague concerns about widespread digital spying were voiced by a minority and sometimes trivialized before Snowden's disclosures, now those fears have been given real substance and credibility, and surveillance is increasingly seen as a practical risk that requires some kind of remediation.

The Snowden disclosures have had a particularly salient impact on the private sector, the Internet engineering community, and civil society. The revelations have left many US companies in a public relations nightmare, with their trust weakened and lucrative contracts in jeopardy. In response, companies are pushing back. It is now standard for many telecommunications and social media companies to issue transparency reports about government requests to remove information from websites or share user data with authorities. US-based Internet companies even sued the government over gag orders that bar them from disclosing information on the nature and number of requests for user information. Others, including Google, Microsoft, Apple, Facebook, and WhatsApp, have implemented end-to-end encryption.

Internet engineers have reacted strongly to revelations showing that the NSA and its allies have subverted their security standards-setting processes. They are redoubling efforts to secure communications networks wholesale as a way to shield all users from mass surveillance, regardless of who is doing the spying. Among civil society groups that depend on an open cyberspace, the Snowden disclosures have helped trigger a burgeoning social movement around digital-security tool development and training, as well as more advanced research on the nature and impacts of information controls.

Wild card

The cyberspace environment in which we live and on which we depend has never been more in flux. Tensions are mounting in several key areas, including Internet governance, mass and targeted surveillance, and military rivalry. The original promise of the Internet as a forum for free exchange of information is at risk. We are at a historical fork in the road: Decisions could take us down one path where cyberspace continues to evolve into a global commons, empowering individuals through access to information and freedom of speech and association, or down another path where this ideal meets its eventual demise. Securing cyberspace in ways that encourage freedom, while limiting controls and surveillance, is going to be a serious challenge.

Trends toward militarization and greater state control were already accelerating before the Snowden disclosures, and seem unlikely to abate in the near future. However, the leaks have thrown a wild card into the mix, creating opportunities for alternative approaches emphasizing human rights, corporate social responsibility, norms of mutual restraint, cyberspace arms control, and the rule of law. Whether such measures will be enough to stem the tide of territorialized controls remains to be seen. What is certain, however, is that a debate over the future of cyberspace will be a prominent feature of world politics for many years to come. ■