Penn State Journal of Law & International Affairs

Volume 1 | Issue 2

November 2012

The Growing Dark Side of Cyberspace (. . . and What To Do About It)

Ronald Deibert

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2012 VOLUME 1 NO. 2

THE GROWING DARK SIDE OF CYBERSPACE (. . . AND WHAT TO DO ABOUT IT)

*Ronald Deibert**

INTRODUCTION

Cyberspace—the global environment of digital communications—surrounds and embodies us entirely, 24 hours a day, 7 days a week. We are always on, always connected: emailing, texting, searching, networking, and sharing are all now as commonplace as eating, breathing, and sleeping. With the emerging "Internet of things," devices interact online independent of our direct control: our fridges, pacemakers, and automobiles, alive and networking with each other.

Governments around the world have seen these technologies as the recipe for social empowerment and development. Billions have been spent on wiring communities even in the most isolated areas, under the assumption that access to knowledge and networking are the keys to economic growth.[1] Numerous success stories provide

* Director of the Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto. Thanks to Masashi Crete-Nishihata, Adam Senft, and Marianne Lau for assistance, and to Rafal Rohozinski for helping to develop some concepts in the first half of the article. Support for research provided by the John D. and Catherine T. MacArthur Foundation.

[1] *See* PETER STENBERG ET AL., UNITED STATES DEPARTMENT OF AGRICULTURE, BROADBAND INTERNET'S VALUE FOR RURAL AMERICA, iii, iv, 21-22 (2009) (showing statistically how economically important broadband access is to rural communities in America). *See also* Jim Hopkins, *In Rural Areas, Fast Net Access Vital, but Elusive*, USA TODAY, Nov. 12, 2001, at 4E, http://usatoday30.usatoday.com/tech/bonus/1101/rural.htm (showing that

ample evidence for these assumptions, from crowd-sourcing disaster and humanitarian relief operations to farmers using mobile apps to access real-time data on markets.[2]

But there is a dark side to cyberspace—hidden contests and malicious threats—that is growing like a disease from the inside-out. This disease has many symptoms, and is being reinforced by a multiplicity of disparate but mutually reinforcing causes. Some of these driving forces are unintended byproducts of the new digital universe into which we have thrust ourselves with blind acceptance; others are more sinister and represent deliberate manipulations of the new opportunities for exploitation that have been created. I outline six of these driving forces below.[3]

As ominous as the dark side of cyberspace may be, our collective reactions to it are just as ominous—and can easily become the darkest driving force of them all should we over-react. Cyber security has vaulted itself to the top of the international policy agenda—now an urgent priority, ranked by some as high as nuclear weapons proliferation and terrorism.[4] Under extreme conditions,

---

federal and state subsidized loans are helping internet business development and tech education in previously inaccessible rural areas); Press Release, World Bank, *Remote Rural Communities in Papua New Guinea to Benefit from Improved Access to Telecommunications*, World Bank Press Release 2011/635/EAp (July 22, 2010), http://www.worldbank.org/en/news/2010/07/22/remote-rural-communities-papua-new-guinea-benefit-improved-access-telecommunications (using a $15 million dollar loan from the World Bank, an organization can provide public internet access to over 420,000 people in Papua New Guinea).

[2] *See, e.g., Hundreds of Thousands Back Iran Revolution*, BBC NEWS, Feb. 11, 2010, http://news.bbc.co.uk/2/hi/8509765.stm (focusing young Iranians, and bringing awareness to the rest of the world using social media and twitter during the Iranian "Green" Revolution); *#EgyPresElex - How election day in #Egypt was shared via social media*, GUARDIAN (STORIFY) (May 23, 2012), http://storify.com/guardian/egypreselex-top-tweets-from-election-day (pictures and social media involved the world in the Egyptian election).

[3] *See* Ronald Deibert, *Cybersecurity, in* FOREIGN POLICY ASS'N, GREAT DECISIONS 4 (2012). *See also* Ronald Deibert & Rafal Rohozinski, *Contesting Cyberspace and the Coming Crisis of Authority*, *in* ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 21 (Deibert et al. eds., 2012) (drawing from parts of these two works in the following sections).

[4] Director of National Intelligence James Clapper has called cyber security "a profound threat to this country, to its future, its economy, and its very

politicians can be tempted by simplistic and radical solutions. Fear is becoming the dominant driving force for a wide-ranging movement to shape, control, and possibly subvert cyberspace. As Samuel Coleridge once said, "In politics, what begins in fear usually ends in folly." In order to protect and preserve cyberspace as a secure and open communications environment—dealing simultaneously with the dark side while also benefiting from its positive effects—a return to some timeless principles may provide the best solution.

I. INTO THE CLOUDS

Cyberspace has always been characterized by change. But almost imperceptibly there has been a major shift in the constitution of cyberspace within the last several years with the rise of social networking, the shift to cloud computing, and the rapid emergence of mobile forms of connectivity. Although each of these developments are unique, together they have the combined effect of taking users out of an older communications paradigm and into new ones, governed by different rules, norms, and principles—not all of them necessarily benign.

For example, cloud computing has un-tethered PCs and operating systems into virtualized infrastructures. Data that used to be stored on our desktops and in our filing cabinets have evaporated into "the clouds." This shift has lowered the cost of access to high-powered computing facilities but raises significant issues with respect to jurisdiction, security and data privacy.

Very few citizens outside of the United States realize, for example, that their data stored on Google, even those physically residing on machines located in their own country, are subject to the

---

being." 158 CONG. REC. S618 (daily ed. Feb. 14, 2012) (statement of Senator Collins). Similarly, Robert Muller, Director of the Federal Bureau of Investigation (FBI), testified to Congress in January 2012 that "Counterterrorism—stopping terrorist attacks—with the FBI is the present number one priority. But down the road, the cyber threat, which cuts across all [FBI] programs, will be the number one threat to the country." Jason Ryan, *FBI Director Says Cyberthreats Will Surpass Threat from Terrorists*, ABCNEWS.COM (Jan. 31, 2012), http://abcnews.go.com/blogs/politics/2012/01/fbi-director-says-cyberthreat-will-surpass-threat-from-terrorists/.

U.S. Patriot Act because Google is headquartered in the United States and the Act compels Google to turn over its data when required no matter where it is stored.[5] For that reason, some European countries are now debating laws that will ban public officials from using Google or other cloud services that could put their citizen's personal data at risk.[6]

Likewise, mobile connectivity and social networking have given us an instant awareness of each other's thoughts, habits, and activities, while entrusting a massive and unprecedented amount of personally identifiable data to third parties. Our personal lives have been turned inside-out with the result that we can be tracked in time and space with a degree of precision that would make the greatest tyrants of days past envious—all by our own consent. Mobile devices and their accoutrement of "apps" are examples of what Jonathan Zittrain calls "tethered appliances" —they corral us into walled gardens controlled by private companies with potential repercussions for the positive networking effects of a borderless Internet.[7]

II. RISE OF THE SOUTH AND THE EAST

These technological changes are occurring alongside a major demographic shift in cyberspace, as a growing base of users come

---

[5] Andy Greenberg, *U.S. Government Requests for Google Users' Private Data Jump 37% In One Year*, FORBES.COM (June 17, 2012, 11:01 PM), http://www.forbes.com/sites/andygreenberg/2012/06/17/u-s-government-requests-for-google-users-private-data-spike-37-in-one-year/(showing that the U.S. Government made 6,321 information requests in 6 months during 2011, a significant increase from the number of requests made in 2009 and 2010, and that Google also has received information requests from foreign governments).

[6] *See, e.g.,* Malija Palmer, *Google Faces Norwegian Public Sector Ban*, FIN. TIMES TECH BLOG (Jan. 24, 2012, 6:01 PM), http://blogs.ft.com/tech-blog/2012/01/google-faces-norwegian-public-sector-ban/#axzz1kfe50lGX ("Norwegian public sector organizations will be banned from using Google Apps after the Norwegian data protection authorities ruled that the service could put citizen's personal data at risk. The data protection authority said that Google Apps did not comply with Norwegian privacy laws because there was insufficient information about where the data was being kept.").

[7] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT 63, 105, 101-27, 129, 149-50, 181, 193 (2008).

from the global South—those countries that constitute the least developed in the world. The Internet may have been born in the West but its future will almost certainly be decided elsewhere. Today, North America and Europe combined make up less than 35 percent of all Internet users.[8] The Asian region comprises 45 percent of the world's Internet population (the most by region),[9] but it ranks only sixth in terms of penetration as a percentage of population, meaning that there is an enormous group yet to be connected, most of them young.

Some of the fastest growth is happening among the world's weakest states and zones of conflict, where semi-authoritarianism or organized crime are prevailing characteristics: Africa, the Middle East, and Latin America. How burgeoning populations in these zones will use and shape the technology is an open question. For example, the young netizens who launched the Arab Spring were born into a world of satellite broadcasts, mobile phones, and Internet cafes. They were plugged in to the digital world, and able to rapidly exploit viral networks in ways that were difficult for authorities to anticipate and control. On the other hand, among the most innovative users of social networking and mobile technologies in Latin America today are the drug cartels, which use these very same tools to instill fear in citizens and lawmakers, intimidate journalists, and ultimately suppress free speech.[10] Technology's many uses are unpredictable and often contrary to the designer's original intent.

To understand how and in what ways cyberspace will be characterized in years to come we need to closely analyze innovation that is coming from the global South, and from the users of cities like Tegucigalpa, Nairobi, and Shanghai. If the Californian culture of libertarianism and individual entrepreneurship defined the early history of cyberspace, we should be asking ourselves what the future

---

[8] MINIWATTS MARKETING GROUP, INTERNET WORLD STATS: USAGE AND POPULATION STATISTICS, http://www.internetworldstats.com/stats.htm (last updated Nov. 6, 2012).

[9] *Id.*

[10] *See, e.g.,* Ashley Fantz, *The Mexico Drug War: Bodies for Billions*, CNN.COM (Jan. 20, 2011, 9:03 AM), http://www.cnn.com/2012/01/15/world/mexico-drug-war-essay/index.html (describing how Mexican drug cartels are beheading journalists, and using the internet and blogs to disseminate propaganda).

of cyberspace holds as the centre of gravity for usage and innovation shifts to the global South.

III. THE GROWING MENACE OF CYBER CRIME

Cyber crime has been a part of cyberspace since the origins of the Internet itself. However, its growth and complexity has become explosive in recent years. The economy of cyber crime has morphed from small and isolated acts undertaken by lone "basement" criminals to a diversified, segmented and highly professionalized transnational enterprise worth billions annually.[11] Security companies now routinely receive new samples of malicious software on the order of tens of thousands each day. Botnets that can be used to engage in denial of service attacks against any target can be rented from public forums and websites for as little as one hundred dollars. Some offer 24/7 technical help. Security operations centers that maintain network security for banks and enterprises face millions of cyber crime incidents each week.[12]

---

[11] *See generally* MISHA GLENNY, DARK MARKET: CYBERTHIEVES, COPS, AND YOU (2011) (studying and describing the important players and the complexities of modern cybercrime).

[12] *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 201-02 (2009) (The U.S. Department of Defense says more than 3 million attacks have occurred every year since 2008). *See also* David E. Sanger & Eric Schmitt, *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure*, N.Y. TIMES, July 27, 2012, at A8, http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html ("The top American military official responsible for defending the United States against cyberattacks said Thursday that there had been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations."); Robert Koenig, *With Cyber Attack Threat Rising: Senate Bill Falters*, ST. LOUIS BEACON, July 31, 2012, https://www.stlbeacon.org/#!/content/26295/senate_debates_cyber_security ("This month, the Bipartisan Policy Center's Cybersecurity Task Force reported that more than 50,000 cyberattacks on private or government networks were reported to the DHS [Department of Homeland Security] between last fall and February – 86 of those aimed at critical infrastructure networks."); *Too Many Cyber Attacks Hushed Up*, AFP, July 19, 2012, http://www.google.com/hostednews/afp/article/ALeqM5jyKNZaQg5lvAoeciyPgXmh0ScuSA (showing

The reasons for this sudden surge in cyber crime can be connected back to the previous two drivers.[13] First, our expanding and constantly evolving communications systems have emerged so quickly that organizations and individuals have yet to adapt proper security practices and policies. We have created a hypermedia environment characterized by constant innovation from the edges, extensive social sharing of data, and mobile networking from multiple platforms and locations. We have immersed ourselves and entrusted our information to "clouds" and social networking services operated by thousands of companies of all shapes, sizes, and geographic locations. In doing so, we have unintentionally opened up endlessly multiplying opportunities for criminal exploitation.

Cyber crime thrives as well in part because of a lack of controls. Cyber criminals are able to reap a digital harvest from across the globe, while hiding locally in jurisdictions safe from law enforcement agencies protecting victims' interests. Cyber crime moves at the speed of electrons; international law enforcement cooperation moves at the speed of bureaucratic institutions. It is almost routine now to hear about cyber criminals living openly in places like St. Petersburg, Russia, practically exalted as tech entrepreneurs in an underworld of illicit innovation that shows no sign of abatement.

IV. FROM CRIME TO ESPIONAGE AND BEYOND

Cyber crime is a major nuisance and growing economic cost. But what is most concerning is the way the worlds of cyber crime are blurring into acts of espionage, sabotage and even warfare. Nearly every day we hear of high-level cyber breaches against government departments, private companies, and other infrastructure.[14] The

---

the government is aware that the United States combats many more cyber attacks than reported because private firms keep cyber attack information secret).

[13] *See generally* Ron Deibert and R. Rohozinski, *Meet Koobface, Facebook's Evil Doppelganger*, GLOBE & MAIL, Nov. 12, 2010, http://www.theglobeandmail.com/news/national/time-to-lead/internet/meet-koobface-facebooks-evil-doppelgnger/article1795650/page2/.

[14] *See, e.g.,* Jill R. Aitoro, *EPA Security Breach Exposes Personal Information of 8,000 People*, WASH. BUS. J., Aug. 2, 2012, http://www.bizjournals.com/washington

Citizen Lab, at the University of Toronto's Munk School of Global Affairs, has been involved in investigating several of these cases, two of which were published as major reports: *Tracking Ghostnet*[15] and its follow on, *Shadows in the Cloud*.[16] The victims uncovered in the reports, all compromised by Chinese-based perpetrators, ranged from major defense contractors and global media, to government agencies, ministries of foreign affairs, embassies and international organizations, like the United Nations.

Most of these types of incidents can be categorized as "espionage": they seek to gather information, either of a proprietary or national security sort, through clandestine means. Of even greater concern are those that aim to cause damage. Recently a *New York Times* report revealed that the United States and Israel were responsible for the Stuxnet virus, which sabotaged air-gapped Iranian nuclear enrichment facilities.[17] If true, the attack would represent the first time governments have taken responsibility for a cyber attack on a critical infrastructure: a de facto act of war through cyberspace.[18]

/news/2012/08/02/epa-security-breach-exposes-personal.html (explaining how an EPA data breach, compromising very personal information, was likely caused by a virus in an e-mail attachment).

[15] INFORMATION WARFARE MONITOR, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK (2009), http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[16] INFORMATION WARFARE MONITOR & SHADOWSERVER FOUNDATION, SHADOWS IN THE CLOUD: INVESTIGATING CYBER ESPIONAGE 2.0 (2010), http://www.nartv.org/mirror/shadows-in-the-cloud.pdf.

[17] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran,* N.Y. TIMES, June 1, 2012, at A1, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?page_wanted=all.

[18] *See id. See also* Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 850 (2001) (arguing that cyber attacks that directly and purposefully cause innocent deaths and destruction of property violate contemporary prohibitions on the use of force); Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, at A1 ("The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force."). *But cf.* Shackelford, *supra* note 12, at 195-99, 201, 217-19 (examining difficulty in defining cyber attacks as "acts of war" under traditional international law).

What all of these breaches and attacks share in common is that their basic techniques are largely indistinguishable from those used by cyber criminals. Even in spite of its sophisticated effects, Stuxnet has been described as a "Frankenstein" of existing cyber crime methods and tradecraft.[19] Many actors now see the growing underbelly of cyber crime as a strategic vector for the exercise of state-based and corporate espionage. Hidden in the shadows of low-level thuggery and economic crime, in other words, are more serious and potentially devastating operations: undertaking malicious acts of sabotage against critical infrastructure, like nuclear enrichment facilities and power plants.

The growth of cybercrime is thus much more than a persistent nuisance; it has become a highly ranked risk factor for governments and businesses. The consequences of this exploding threat vector are going to be numerous and wide-ranging, leading (among other things) to pressures for greater state regulation, intervention, and even exploitation—a fifth driver to which I now turn.

V. THE "STATE" COMES KNOCKING

These four drivers are happening simultaneously with a sea change in the way that governments approach cyberspace. Whereas once the dominant metaphor of Internet regulation was "hands off," today the dominant metaphor is one of intervention, control, assertion of state power, and increasingly geopolitical contestation over the domain of cyberspace itself. States are knocking on the doors of cyberspace governance.

For example, the OpenNet Initiative (ONI), which documents Internet content filtering worldwide, has tracked a growth of Internet censorship from a handful of countries in the early 2000s when it started to more than 40 today. ONI estimates as many as 960

[19] James P. Farwell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 SURVIVAL: GLOBAL POL. & STRATEGY 23, 25 (2011).

million people are living in jurisdictions that censor the Internet – almost half (47%) the entire Internet population worldwide.[20]

The ONI's research has also shown states becoming much more adept at using what have been dubbed second and third generation techniques of cyberspace control.[21] These include implementing tighter content control regulations, or subjecting the Internet to more traditional media and publication laws. More nefarious are examples of governments engaging in offensive information operations, including disabling opposition sites through denial of service or other attacks, or using pro-government bloggers as a way of directly competing in the information space.

While conventional wisdom has long assumed authoritarian regimes would wither in the face of the Internet (and some in the Middle East and North Africa appear to have done just that) many show a resilience that belies the conventional wisdom. Tunisia and Egypt may have succumbed to Facebook-enabled protestors, but China, Vietnam, Syria, Iran, Belarus and others have successfully employed second and third generation control techniques to penetrate and immobilize opposition, cultivating a climate of fear and self-censorship.

It would be a mistake to see the growing assertion of state power in cyberspace as solely an authoritarian phenomenon. The reality is much more complex. The norms of cyberspace controls, in fact, are being driven and legitimized just as much by liberal democratic countries as others. Many liberal democratic governments have enacted or are proposing Internet content filtering, mostly for copyright, pornography, or content deemed to be hateful or inciting of violence.[22] Most liberal democratic governments have also pushed

---

[20] ONI Team, *Global Internet Filtering in 2012 at a Glance*, THE OPENNET INITIATIVE (Apr. 3, 2012), http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance.

[21] *See* ACCESS CONTROLLED: THE SHAPING OF POWER, RIGHTS, AND RULE IN CYBERSPACE (Ronald Deibert et al., eds., 2010).

[22] *See, e.g.,* Michael J. Brown, *The Children's Internet Protection Act: A Denial of A Student's Opportunity to Learn in A Technology-Rich Environment*, 19 GA. ST. U. L. REV. 789, 791 (2003) (state legislation requiring schools to use computer software to prevent children from viewing pornography as part of the Children's Internet

for new surveillance powers, downloading responsibilities for collection of data to private sector actors while relaxing judicial oversight of sharing with law enforcement and intelligence agencies.[23] They are also developing offensive information operations of their own. For example, the United States and many other western countries have stood up within their armed forces cyber commands and talk openly about fighting and winning wars in this domain (as the Stuxnet revelations show).[24]

VI. THE GROWING CYBER SECURITY INDUSTRIAL COMPLEX

Not surprisingly a huge industrial sector has sprouted that serves these growing pressures to secure cyberspace, a market now estimated to be on the order of tens of billions of dollars annually.[25] Citizen Lab and its partners have uncovered over the years that many of the countries that censor the Internet rely on products and services developed by western manufacturers: Smart Filter in Iran in 2005, Fortinet in Burma in 2006, Websense in Yemen, Tunisia, and the United Arab Emirates in 2008 and 2009.[26] A more recent Citizen Lab report identified that devices manufactured by Blue Coat were being used in Burma and also Syria possibly to help identify particular types of communication traffic associated with pro-democracy

---

Protection Act of 2001); Raymond Colitt & Fernando Exman, *Google in Deal with Brazil to Fight Child Porn*, REUTERS, Jul. 2, 2008, http://www.reuters.com/article/2008/07/02/us-brazil-google-pornography-idUSN0237672120080702 (signing an agreement with Brazil Prosecutors, Google agrees to help filter access to child porn and gather evidence against perpetrators).

[23] *See, e.g.,* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1115-18, 1128-34, 1139-42 (2005) (arguing that the U.S. government has allowed and supported private sector entities to control the internet and limit free speech); Greenberg, *supra* note 5; Colitt & Exman, *supra* note 22.

[24] *See* Sanger, *supra* note 17*; see also* Gorman & Barnes, *supra* note 18.

[25] *See* Ronald Deibert & Rafal Rohozinski, *The New Cyber Military-Industrial Complex,* GLOBE & MAIL, Mar. 28, 2011, http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/.

[26] *See* Helmi Noman & Jillian C. York, *West Censoring East: The Use of Western Technologies by Middle East Censors 2010-2011*, THE OPENNET INITIATIVE 1-20, (Mar. 2011), http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011.

activists—in the context of what many consider to be crimes against humanity occurring in that country.[27] It has also published several reports about a Canadian company, Netsweeper that sells censorship products and services to ISPs in Yemen, Qatar, and the United Arab Emirates. The Guelph, Ontario based company's product helps block access to human rights information, news, gay and lesbian information, and information critical of the regimes.[28]

But the research has only picked at the surface of a major field. Products that provide advanced deep pack inspection, content filtering, social network mining, cell phone tracking, and even computer network exploitation capabilities are being developed by U.S., Canadian, and European firms, and marketed worldwide to regimes seeking to limit democratic participation, isolate and identify opposition, and infiltrate meddlesome adversaries abroad. A cyber security industrial complex has mushroomed that services the assertion of state power and the growing arms race in cyberspace.

VII. MUTUAL RESTRAINT, NOT OVERREACTION

The growing dark side of cyberspace represents deeply rooted social forces that are not easily reversible. These driving forces now are poised to subvert the domain entirely through a spiraling arms race, the imposition of state-based controls, or by partitioning into walled gardens.

As the imperatives to regulate, secure, and control cyberspace grow daily, we risk degrading or even destroying what made cyberspace so unique in the first place. In the face of these urgent issues and real threats, policymakers may be tempted to adopt extreme solutions that end up throwing out the baby with the bathwater or lowering the normative bar for what is seen as

---

[27] *See* The Citizen Lab, *Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma* (2011), https://citizenlab.org/wp-content/uploads/2012/07/01-2011-behindbluecoat.pdf.

[28] *See* Helmi Norman, *When a Canadian Company Decides What Citizens in the Middle East Can Access Online*, THE OPENNET INITIATIVE (May 16, 2011), http://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online.

acceptable practice in cyberspace. Before extreme solutions are adopted, we need to be careful to premise our actions on core values that underpin cyberspace itself: ensuring that it remains an open and dynamic communications system for citizens the world over. There are alternative approaches to securing cyberspace in this manner that have yet to be fully considered.

VIII. DISTRIBUTED SECURITY FOR A GLOBAL CYBER COMMONS

There is an instinctive tendency related to international security discussions to default to the tradition of Realism, with its accompanying characteristics of state-centrism, top-down hierarchical controls, and a defensive perimeter to the threats outside. As compelling as this tradition may be, it fits awkwardly in a world where divisions between inside and outside are blurred, threats can emerge as easily within as without, and that which requires securing—namely cyberspace—is a globally networked commons of information almost entirely in the hands of the private sector. Moreover, this model privileges state-based agencies, like the National Security Agency, as lead actors in the security of cyberspace, which can create awkward privacy concerns in domestic settings while fueling reciprocal suspicions on an international scale.

One alternative approach to security that meshes with the core values and decentralized architecture of an open but secure cyberspace and has a long pedigree in political philosophy might be referred to as the "distributed" approach. Distributed security is not a new concept. It finds roots in political orders reaching back to ancient Greece and the Roman republic, and the late medieval, early Renaissance trade-based systems exemplified by the Venetians, the Dutch, and the English. As the political scientist Daniel Deudny has argued, distributed security finds its fullest expression in the founding of the early United States of America and the writings of the political philosophers associated with it, such as Montesquieu, Publius and others.[29] Although multi-faceted and complex, distributed security starts from the foundation of building structures that help mitigate

[29] *See* DANIEL H. DEUDNEY, BOUNDING POWER: REPUBLICAN SECURITY THEORY FROM THE POLIS TO THE GLOBAL VILLAGE (2007).

unchecked and concentrated political power, both domestically and internationally. It puts forward "negarchy" as an alternative to the twin evils of "hierarchy" and "anarchy."

At the core of the distributed security model are several key principles, which in turn can form the basis for the pillars of global cyber security policy: mixture, division, and restraint. Mixture refers to the intentional combination of multiple actors with governance roles and responsibilities in a shared space. Division refers to a design principle that no one of these actors is able to control the space in question without the cooperation and consent of others. As an approach to global cyberspace security and governance, these can provide a more robust foundation for the empty euphemism of "multi-stakeholderism," and a principle upon which to counter growing calls for a single global governing body for cyberspace. Citizens, the private sector, and governments all have an important role to play in securing and governing cyberspace—but none to the exclusion or preeminence of the others. Mixture and division are the principles upon which this justification can be made.

Principles of restraint are perhaps the most important of those associated with distributed security, and arguably the most threatened by over-reaction today. Securing cyberspace requires a reinforcement of, rather than relaxation of restraint on power, including checks and balances on governments, law enforcement and intelligence agencies as well as the private sector. In an environment of Big Data,[30] in which so much personal information is entrusted to third parties, oversight mechanisms on government agencies are essential.

Principles of restraint—articulated as "mutual restraint" — can also help inform growing discussions at an international level

---

[30] *See* Gillian Tett, *Big Data is Watching You*, FIN. TIMES, Aug. 10, 2012, http://www.ft.com/cms/s/2/97cffaf0-e1b5-11e1-92f5-00144feab49a.html#axzz23GKg7aVr; Michelle X. Zhou, *Big Data: Good for Business, Useful to You*, HUFFINGTON POST, Aug. 7, 2012, http://www.huffingtonpost.com/michelle-x-zhou/ibm-big-data-good-for-business_b_1752210.html; Warwick Ashford, *Big Data Analytics Can Reduce Cyber Risks, Says ISF*, COMPUTERWEEKLY.COM (Aug. 1, 2012, 2:34 PM), http://www.computerweekly.com/news/2240160679/Big-data-analytics-can-reduce-cyber-risks-says-ISF.

concerning confidence and security building measures among states in cyberspace. The dangerous possibilities of escalation in cyberspace are real; to counter them, governments need to self-limit and check each other's behavior in mutually transparent ways. Here, the link in the distributed security model between domestic and international processes is exceptionally clear. The more checks placed on concentrated power at a domestic level, the more adversaries abroad have confidence in each other's intentions.

Distributed security also describes the most efficient and widely respected approach to security in the computer science and engineering circles. Here it is important to remind ourselves that in spite of the threats, cyberspace runs well and largely without persistent disruption. On a technical level, this efficiency is founded on open and distributed networks of local engineers who share information as peers in a community of practice that has its roots in the University system[31] (itself, a product of the liberal philosophy upon which distributed security rests). Rather than abolish this system for another, more top-down approach, we should find ways to buttress and amplify it.

The securitization of cyberspace may be inevitable, but what form that security takes is not. As the securing of cyberspace unfolds, ensuring basic principles of transparency, accountability, and mutual restraint will be critical.

We are at a watershed moment, where decisions could take us down a path where cyberspace continues to evolve into a global commons that empowers individuals through access to information, freedom of speech and association, or down another towards its eventual demise. Developing models of cyber security that deal with the dark side, while preserving our highest aspirations as citizens, is now an urgent imperative on a planetary scale.

---

[31] *See generally* PETER SCOTT, THE MEANINGS OF MASS HIGHER EDUCATION (1995) (explaining the evolution of university education system from an elite and closed off institution to an open forum for the masses).