November 2016

COLUMBIA SIPA
School of International and Public Affairs

Tech & Policy Initiative

The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance

By: Laura DeNardis, Gordon Goldstein,
and David A. Gross

THE RISING GEOPOLITICS OF INTERNET GOVERNANCE

CYBER SOVEREIGNTY V. DISTRIBUTED GOVERNANCE

LAURA DENARDIS, GORDON GOLDSTEIN, AND DAVID A. GROSS

PRESENTED AT COLUMBIA SCHOOL OF INTERNATIONAL AND PUBLIC AFFAIRS
NOVEMBER 30, 2016

The Political and Economic Stakes of Internet Governance

Internet governance is at a crossroads. The 21st century has given rise to two incommensurable visions for the global Internet and how it is governed. One envisions a universal network that generally supports the free flow of information and whose governance is distributed across the private sector, governments and new global institutions in an approach that has historically been described as "multistakeholder" governance. This vision has materialized, albeit imperfectly, in how the Internet and its coordination has historically progressed and is an approach advocated by the United States government and many other countries. This is the model of Internet governance that has dominated throughout the past decade. The competing vision advocates for greater multilateral and top-down administration of the Internet in the name of social order, national cyber sovereignty, and tighter control of information flows. China and other countries interested in greater administrative control over the flow of information have been vocal proponents of a more multilateral approach to Internet governance. These visions are often debated using the language of abstract theoretical constructs but they involve actual policy choices that have arisen in particular historical contexts and whose future will have tangible effects on American foreign policy interests, American values of freedom of expression and innovation, the global digital economy, and the stability and resiliency of Internet infrastructure itself.

The Internet now ranks high on the policy agendas of governments in countries ranging from Russia and China to the United States and Brazil. In only a decade, concerns about governance of the Internet have transformed from being interesting only to the technical community and a subset of academics to becoming a national policy priority for G20 government leaders. Questions about the control and security of the Internet now rank in global importance alongside topics such as terrorism, climate change, and human rights. Governments and other stakeholders have elevated Internet governance on the global policy agenda because the Internet has become a strategic resource with unprecedented economic, political, and social implications.

The economic stakes of cyberspace are immense. The Internet now contributes more than $4 trillion USD to the global economy. More than this, every sector of the economy from financial services to transportation to health care is completely dependent upon cyber systems for basic day-to-day transactions and functioning. A collapse of the Internet would also be a collapse of the economy. The economic stakes will only increase in the context of the Internet of Things in which every device from cars to medical devices will be deeply integrated with and dependent upon digital systems.

Battles over Internet policy often reflect global interests around geo-economic competition. The Internet is arguably the greatest value creation engine in the history of civilization, with digital technology companies like Apple, Google (Alphabet, Inc.), Microsoft, and Facebook now consistently occupying the upper echelon (within the top ten) of multinational companies in terms of market capitalization. Eventually one will be have a trillion-dollar market capitalization. What complicates global Internet policy is the reality that there is such a diversity of strategic interests around the Internet. The global dominance of American companies emerged in part from the Internet originating in the United States. The globalization and spread of the Internet has seen the rise of even newer companies, such as Alibaba in China, which appropriated aspects of the business models of many US companies such as ecommerce and Internet search.

The rising economic dependency on the Internet exists in a much broader historical context. Globalization and technological change have created deep-seated economic uncertainty about the future of jobs and entire industries. History may demonstrate that the shift from an industrial society to an information society is even more consequential than the shift from agrarian societies to the industrial age. The combination of globalization and industrial transformation that has served as a background context for Brexit and for the election of U.S. President-elect Donald Trump also serves as the context for rising tensions over control of the digital systems on which all economic and political systems now depend. Government interest in cyberspace is in part a response to the rising importance of the Internet but also stems from an interest in providing a stabilizing response to citizen uncertainty over the accelerating pace of technological and industrial change.

The political and social stakes of the Internet may be even higher as control over cyberspace increasingly becomes viewed as a proxy for state power. The 21st century is marked by technical mediation of the public sphere and the condition that cyberspace underpins all functions of government and society. An outage in

cyberspace now equates to an outage of government and society, as was first starkly demonstrated when cyberattacks disrupted government and industry systems in Estonia in 2007. Cyberspace is now the fifth domain of warfare, with the stability and security of critical digital infrastructures high on the policy agenda and control over cyberspace an emerging front for state power. Although data breaches against large multinational companies and government institutions such as Target, Yahoo!, and the United States Office of Personnel Management have potential economic consequences for individuals, cyberattacks are often abjectly political, such as the Sony hack or the alleged Russian cyberattacks breaching private email accounts of American Democratic party leaders during the 2016 U.S. presidential election. Individual civil liberties such as freedom of expression and privacy are now already shaped by arrangements of digital policy, but increasingly democracy itself, is becoming contingent upon the stability and security of cyberspace.

With economic stability and political and social systems increasingly dependent upon the Internet, tensions over control of the Internet are also rising. Any longstanding views about the Internet being ungoverned or ungovernable are simply not true. The Internet is, and has always been, governed, albeit not necessarily by traditional governance structures but by a combination of actors from the private sector, new global institutions that cross borders, and also traditional laws and policies. Internet governance is not one system, one control point, or one institution, despite how it is often described by the media and policymakers. Keeping the Internet operational requires a large cadre of mostly private companies and institutions performing various administrative oversight functions. Standards-setting institutions such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) establish common technical protocols that enable interoperability among various systems and devices. Network operators make private contractual agreements to interconnect their networks and exchange traffic. Information intermediaries providing services ranging from social media to search establish conditions of free expression and privacy through user terms of service. New institutions like the Internet Corporation for Assigned Names and Numbers (ICANN) oversee critical Internet resources such as the domain names and Internet addresses that serve as globally unique identifiers for online resources. The growth and success of the contemporary Internet has been largely shaped by private sector-led innovations, investments, and administrative coordination.

Some of the most strident and important geopolitical debates over control of the Internet – such as battles over control of the critical Internet resources of names and numbers, interconnection regulation, and encryption – have involved an essential tension between private sector-led versus government-led coordination and control.

This geopolitical tension can be described as multilateralism and Internet sovereignty versus distributed and private-sector-led multistakeholder governance.

One of the most high-profile conflicts reflecting this tension has been the ongoing struggle for control over the Internet names and numbers and the transition of United States Department of Commerce oversight of the "IANA functions" (Internet Assigned Numbers Authority), and particularly the authorization of changes to the root zone file mapping Internet top-level domains to Internet addresses, the binary numbers computers use to route information to its online destination. The transition of U.S. oversight of these functions has taken place and the Internet continues to operate. After a decades-long deliberation, the baton has been passed to a global multistakeholder arrangement within ICANN itself. Unless governments like China and Russia, possibly via the United Nations structure, find a way to inject themselves into a future oversight function around the IANA functions, this transition appears to be at least a short-term win for multistakeholder governance of the Internet.

This paper argues that the transition of American oversight of Internet names and numbers is the beginning, not the end of Internet conflicts between distributed private-sector led governance and multilateral or even unilateral oversight. Battles over Internet governance are also global battles over political and economic power, not unlike control of sea lanes in the 18th and 19th centuries. The transnational and borderless character of the Internet challenges core notions of political power including government sovereignty. The borderless nature of cyberspace is anathema to many governments.

How can the traditional private-sector-led governance of the Internet co-exist in an era in which governments increasingly view control of cyberspace as a proxy for state power, whether for economic advantage, political control over the flow of information, national security, or as a strategic resource in warfare? This paper provides some historical context to the rise of distributed Internet governance, describes some of the key geopolitical conflicts that involve incommensurability between the ideology of national sovereignty and the technical topology and transnational characteristics of private Internet infrastructure, and argues for the preservation of private-sector-led multistakeholder governance rather than a shift to greater government control. Most importantly, the political and economic battles of the future will turn from control of content and largely symbolic power struggles to deeper layers of the Internet's infrastructure, including technical standards, systems of cryptocurrencies, the Domain Name System, cybersecurity systems, and the Internet of Things. It is in the interest of democratic governments to make policy decisions today that resist cyber sovereignty, focus on cybersecurity and Internet

universality, and anticipate emerging battles over Internet infrastructure choke points.

The Evolution of Distributed Multistakeholder Governance

The historical context for the tension between distributed multistakeholder governance and cyber sovereignty models of governance begins with the evolution of the Internet itself, arising in an American setting and, even as the Internet commercialized and expanded internationally, generally reflecting First Amendment values of the free flow of information and private market competition. All technological systems, to a certain extent, reflect the prevailing societal values in which they arise and embed historically specific power structures. Technologies continually evolve and are reciprocally shaped by markets and political dynamics. So too has the underlying technical architecture of the Internet constantly evolved in response to market changes and demographic shifts.

How the Internet is governed is not fixed any more than Internet technical architecture is fixed. Yet, the Internet Society, the institutional home for the Internet Engineering Task Force, has suggested that, even as the Internet has continuously evolved, it has arisen from a set of fundamental design and coordination principles it describes as Internet invariants, the core values that have guided the trajectory of the Internet. While always contested and marked by conflicting interests, these principles have included 1. Global reach/integrity; 2. General purpose; 3. Supporting innovation without requiring permission; 4. Accessibility; 5. Interoperability and mutual agreement; 6. Collaboration; 7. Reusable (technical) building blocks; and 8. No permanent favorites. These principles have resulted in an Internet that, while not universal, has moved toward universality; while not always enabling competition, access, and the free flow of information, providing the potential building blocks for this occur.

Concepts of interoperability, permissionless innovation, no permanent favorites, and global reach may seem self-evident to some in the contemporary context, but were a radical departure from the business models that preceded the Internet in which networks were based on proprietary protocols and designed specifically to only work with equipment made by a single manufacturer (e.g. IBM, DEC, Apple). Even the rise of online consumer systems in the early 1990s, including America Online, CompuServe, and Prodigy, were closed systems designed not to be compatible. For a time, an individual on one system could not send email to an individual on another system. Before the World Wide Web gave rise to the popularization and growth the Internet, there was not yet interoperability, permissionless innovation, or the

potential for a general purpose network. There is nothing preordained about the retention of these design principles. Indeed, it is the contention of this paper that they are being challenged in ways that could change the nature of the Internet itself, compromise its security and stability, and diminish the global flow of information and the pace of technological innovation.

The governance of the Internet, like its underlying infrastructure, also has a historical context. The Internet does not run itself but requires a great deal of coordination to stay operational. At one point in the Internet's history, and in the history of its predecessor ARPANET, the majority of Internet users were American, Internet infrastructure was primarily within US borders, and the coordination of Internet infrastructure was done by Americans. For example, a single individual, Jon Postel working at Stanford Research Institute (SRI) in Menlo Park, California and funded by the U.S. Department of Defense, distributed and kept track of the network's names and numbers, a task over time privatized and internationalized and now overseen by ICANN, regional Internet registries, and domain name registrars.

The term "multistakeholder governance" arose, in part, in conjunction with the evolution of how Internet names and numbers have been overseen. Names refer to domain names, the globally unique alphanumeric names, such as https://sipa.columbia.edu, that identify websites and other virtual locations online. While these are the names that humans use to exchange information online, routers use associated globally unique Internet Protocol (IP) addresses, binary numbers assigned either permanently or temporarily as a globally unique identifier locating an online resource. Each exchange of information on the Internet requires these unique binary numbers, similar to the unique role of a postal address in the material world. This requirement for global uniqueness for each name and number has necessitated a centralized system of coordination for assigning, allocating and tracking all of these virtual identifiers.

Because of the historical condition of the Internet originating in the US with Department of Defense funding, the US government has had a longstanding role in coordinating these resources. As the Internet rapidly grew and internationalized in the 1990s, the US government commenced a process of privatization and internationalization of these coordinating functions, formalized by the incorporation of ICANN and a 1998 memorandum of understanding between the US Commerce Department and ICANN, a non-profit coordinating institution incorporated in the State of California. The agreement formalized ICANN's role in coordinating names and numbers, while still retaining accountability of these functions to the US government during the process of trying to internationalize and privatize this role.

The Commerce Department also arranged a contract with ICANN to handle the tasks known as the IANA functions.

Since the formation of ICANN, the role of the US Commerce Department in holding the contract with ICANN and authorizing root zone changes has been one of the most contentious debates in global Internet governance. International pressure to transition American oversight of names and numbers marked the World Summit on the Information Society in Geneva in 2003 and in Tunis in 2005. Even the formation of the United Nations-sponsored Internet Governance Forum, an annual conference to discuss Internet governance, was a compromise designed to, among other things, allow for the discussion of the possible transition of American oversight.

The disclosures by Edward Snowden of the expansive surveillance practices of the US National Security Agency (NSA) escalated concerns about the unique role of the US government in overseeing Internet names and numbers. Even though this oversight role has no discernable connection to NSA surveillance practices, and despite the knowledge that so many other governments carried out similar surveillance for law enforcement and national security reasons, the disclosures contributed to a loss of trust in US information policy that carried over to name and number administration and, in particular, oversight of changes to the root zone file. An already decade-long international concern about American hegemony in Internet governance became heightened, and international pressure to transition US oversight intensified and was perhaps best reflected in a global gathering in Brazil in May of 2014 called NetMundial to discuss global Internet governance.

In March of 2014, the National Telecommunications and Information Administration of the Commerce Department announced that the US would transition its oversight if the global multistakeholder community could meet a strict five-part test, including ensuring that the IANA functions could not be controlled by another government or intergovernmental organization. Although the original date for the possible transition was extended from September of 2015, it ultimately occurred on October 1, 2016. Key US government oversight functions have essentially been turned over to new structural arrangements within ICANN itself. ICANN, it can be argued, is an example of a multistakeholder governance organization because its processes and structures involve multiple actors – from private industry, government, and civil society. Those concerned about transitioning US oversight of names and numbers to the multistakeholder Internet governance community were not necessarily opposed to the multistakeholder model but rather concerned about a possible future government takeover of names and numbers oversight possibly by the United Nations (including its affiliated entity, the

International Telecommunication Union), or concerns about undue influence of countries like Russia and China with repressive information policies. The question of concern is how oversight will potentially evolve in the future.

The longstanding and high-profile tension over US oversight of Internet names and numbers has sometimes created the misperception that these functions comprise the totality of all Internet governance tasks. Governance of the Internet is not at all a single function, although it is sometimes discussed in this way, but rather an entire ecosystem of tasks necessary to keep the Internet's infrastructure operational and to enact public policy around this infrastructure. There are many taxonomies that explain the various layers of Internet governance tasks. The administration of domain names and Internet addresses is just one area, which itself disaggregates into numerous tasks including the distribution of IP addresses, the assignment of domain names, the authorization of changes to the root zone file mapping top-level domains and Internet addresses, the operation of the Internet's root servers, the task of resolving billions of Domain Name System queries a day to translate domain names into numbers, and the approval of top-level domains (TLDs). This non-exhaustive list of tasks around name and number administration serves to explain the number of coordinating responsibilities required in this one area alone. Other activities of Internet governance include the establishment of technical protocols by standards-setting institutions, access and interconnection coordination, cybersecurity governance, the policy-making role of private intermediaries, and intellectual property rights enforcement. Cybersecurity governance alone involves many heterogeneous tasks ranging from cybersecurity regulation and enforcement, software patch management, routing and DNS security, encryption design, and the role of trust intermediaries authenticating websites.

What becomes obvious in describing these few tasks of Internet governance is that the administration of the Internet is distributed over a variety of actors, including the private sector, new global institutions, and traditional governance structures. Some tasks, such as international treaties or the establishment of information laws around intellectual property rights are the purview of governments, some, such as private interconnection arrangements, are private-sector led, and still others, such as the administration of names and numbers, are performed by institutions like ICANN that involve a combination of actors from civil society, private industry, and government. Taken together, these collective tasks that have developed over decades and necessary to keep the Internet operational, are called distributed "multistakeholder governance."

In some ways, multistakeholder governance is also the privatization of governance, with many functions formerly handled by the state in the material world now overseen by private industry in the digital world. For example, large information intermediaries like Google and Facebook establish the conditions of privacy and speech via their user terms of service, essentially private contractual agreements for how personal data and metadata is handled, collected, and shared, when user accounts are terminated on speech grounds, how to handle cyberbullying and hate speech, and how and when to comply with government requests to take down content or turn over user account information for law enforcement or other reasons. This technical mediation and, in many ways, privatization of individual civil liberties, does not exist in a vacuum because information intermediaries are constrained by the laws of the countries in which they operate, and influenced by market forces and civil society pressure. The Internet's technical community has an influence over architecture-based policy; global institutions like WIPO and the United Nations help shape approaches; civil society exerts pressure on the private sector, such as the boycotts over the Stop Online Piracy Act (SOPA) in the US; and governments have the ability to pass laws, including Section 230 of the Communications Decency Act.

Technically and institutionally mediated Internet policy decisions about conditions of speech, privacy, decency, and government requests, is significantly complicated by the geopolitical reality that cultural norms, technological capabilities, and statutory contexts vary widely from country to country. Navigating context-specific constraints, particularly around content, is complicated. For example, German law requires information intermediaries to block access to Nazi content. Brazil has strong hate speech prohibitions. The European Union has strong consumer privacy protections. The United States imposes strong intellectual property rights enforcement requirements, such as the notice and take down provisions of the Digital Millennium Copyright Act (DMCA). Lese-majeste laws prohibiting insults against a monarch or member of a royal family are in effect, for example, in Thailand and Malaysia. Private companies make determinations every day about how to comply with, or not comply with, requests to block information or turn over user data.

The multistakeholder model arose in the American Internet context but now the vast majority of Internet users are not in the US or even in the West. Overall, there are more than three and a half billion global Internet users, and this will soon reach five billion with the majority of growth in emerging markets and countries like India with most users accessing the Internet on mobile phones. The Internet is growing rapidly across the world, but the majority of Internet users are in China, with the number of

Chinese Internet users far exceeding the entire population of the United States. Both demographic changes and technocultural heterogeneity have provided the backdrop for the Internet governance conflicts of the modern era.

Inflection Points in Cyber Sovereignty vs. Distributed Governance

It has long been established that the distributed architecture and governance of the Internet is subject to national statutory contexts, but this is complicated to implement in practice. That legal borders matter became crystalized in the 2000 French court case *LICRA v. Yahoo!* addressing the sale of Nazi memorabilia on the Internet. Yahoo! was sued because French citizens were able to purchase memorabilia via this platform. Even though the company's servers (at the time) were housed in the US and the company incorporated in the US, and despite the strong US constitutional protections of free expression, the ability to purchase Nazi memorabilia via Yahoo! was ruled to be illegal under French law and would require technical blocking. This more than a decade-old case helps to capture the challenges private companies face in navigating heterogeneous legal contexts and how jurisdictional questions are complicated by the transborder nature of technical architecture. It also provides an example of an Internet policy issue quite distinct from the question of control of Internet names and numbers.

Media and policy discussions around the transition of United States oversight of names and numbers nevertheless often portray governance of the Internet as a single functional area – the administration of the Domain Name System - and view control struggles over this system through the prism of traditional governmental institutions. For example, United States Senator Ted Cruz framed the IANA transition as President Obama surrendering the Internet to authoritarian regimes and instead advocated that the Commerce Department retain its oversight. Operationally, governance of the Internet is not a single task that can be relinquished but an entire constellation of distributed responsibilities necessary for keeping the Internet operational and for establishing relevant public policy. The following describes some of the more high-profile global debates over control of the Internet that collectively portray Internet governance as much broader than control of the Domain Name System and that illustrate the essential tension between governmental versus distributed control.

Interconnection Conflict

One conflict between multistakeholder versus multilateral approaches to Internet governance emerged around the 2012 International Telecommunication Union

(ITU) World Conference on International Telecommunications (WCIT) convened in Dubai. The objective of the meeting was to revisit an international interconnection treaty on telecommunication pricing known as the International Telecommunication Regulations (ITR), an intergovernmental treaty dating back to the late 1980s to address cross-border operation of telecommunication carriers. The conference was convened by the ITU, a specialized sub-agency of the United Nations to address telecommunication policy. Regulatory questions regarding interconnection have historically addressed issues of compensation and pricing related to how telecommunication companies interconnect and exchange traffic.

At issue in Dubai was the question of a possible expansion of the multilateral treaty to include Internet connectivity (rather than primarily voice telecommunication issues, although the two overlap considerably), a greater call for government intervention in facilitating interconnection among private companies, and also the prospect of extending the treaty to include content-specific issues such as regulating spam. The conference exposed a fundamental divide between countries wanting greater government control and oversight of the Internet's infrastructure and of content, and those countries opposing an expansion of the ITRs to include Internet infrastructure, opposing greater government control of content, and generally wanting to preserve multistakeholder, rather than multilateral approaches to interconnection governance arrangements. This fundamental divide was captured by divisiveness leading up to and during the conference, as well in the fractured vote on the proposed new telecommunications regulations, in which 55 out of 152 countries opposed the proposed treaty changes, including the United States, Japan, Canada, German, India, the United Kingdom, and others.

Data Localization Policies

One area in which governments are seeking to assert national sovereignty in cyberspace involves so-called data localization laws, often framed in terms of technological sovereignty or data sovereignty. Data localization policies involve a range of specific requirements and prohibitions on how and where private companies may handle and store customer data. For example, they often mandate that content intermediaries store data within the country in which the customer resides. In other cases, they impose restrictions on how data "crosses borders," require consumer consent, or require taxation on "data exports." These laws are in place in many countries – from Russia to Brazil - that span a range of ideological approaches to information policy. For example, Russia's law requiring companies to store data of Russian citizens within the nation's borders took effect in late 2015. Some countries, like China, have industry specific data laws in areas such as

restrictions on storing financial services and healthcare data offshore or requiring that cloud computing services housing government data reside within China.

Some of these policies, citing privacy concerns for citizens, arose in the aftermath of disclosures about the expansiveness of the NSA surveillance program. In other cases, motivations appear to be providing market advantages to home-grown companies. Some civil society groups have advocated for legal restrictions on the transfer of personal data across borders to comply with privacy and personal data laws.

From an engineering and business model standpoint, and possibly even a civil liberties standpoint, these laws create new challenges. They not only apply to technology companies, such as social media platforms, but usually to other industries that store data, such as banks and retail companies, and these multinational companies can be forced to retool their computer networks to comply with requirements. Newer companies can be shut out of markets because they might not be able to locate their physical infrastructure and servers within every potential market in which they do business. The concentration of data can also make it easier, not harder, to protect data privacy by concentrating personal information. Data sovereignty does not match up with the multinational market approaches of many companies, nor with the distributed technical design that crosses borders and could potentially store data in several locations, house a customer service center in another nation, and have a corporate headquarters in still another country.

Cyber Sovereignty and Multilateral "Cyber Order"

The Internet is not yet a universal network. Much of the world does not yet have access and, where there is Internet penetration, users have different experiences based on language, technical expertise, access speeds, and different technical characteristics. But the rapid growth and innovation of the network creates conditions in which, in most of the world, the network can be thought of as having at least a technological affordance of universality. In other places, like Cuba, Iran, China, and North Korea, networks are walled off from the universal Internet using a variety of control mechanisms. In Iran and Cuba, for example, there are firewalls that strictly control interoperability with other networks and control the flow of content, both in and out of the country, as well as within borders. The Great Firewall of China is perhaps the best example of an efficient, nation-wide system of content restrictions and censorship and a prime example of an exertion of cyber sovereignty in which governments require private industry, as well as the institutions of Internet

governance, such as Internet Exchange Points (IXPs), standards bodies, and registries, to carry out various forms of restrictions to content and infrastructure.

An emerging narrative closely related to national Internet sovereignty is the discourse of cyber order, in which countries are advocating for stronger multilateral, rather than multistakeholder approaches as a way of bringing about social order. In late 2015, for example, this multilateral approach was a significant theme at the World Internet Conference convened by China. As the Internet has become more economically and politically important in China, the government has had an increasing interest in global Internet governance and has advocated for greater multilateral oversight in which governments primarily oversee the coordination of Internet infrastructure and the policies around this infrastructure. This philosophy is clearly evident in the June, 2016 *Joint Statement between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development* which declares support for creating a multilateral Internet governance system in which the United Nations plays a very important role. The changing narrative from multistakeholder to multilateral Internet governance is a sea change in how the technical community, civil society, industry, and policymakers in the West have both carried out and talked about the administration of the Internet.

Cybersecurity Versus National Security

Points of pressure toward national Internet sovereignty also exists in Western countries, especially around questions of government access to online content, personal information and metadata about citizens for purposes of national security and law enforcement. The need for strong cybersecurity, particularly encryption, so economically necessary for instantiating trust in the digital economy, often comes into conflict with law enforcement and national security requirements for accessing data to fight crime and carryout intelligence functions. After learning about the extent of NSA surveillance, for example, the Internet's multistakeholder technical community, particularly the Internet Engineering Task Force (IETF) called for "hardening the Internet" with greater end-to-end encryption that makes it more difficult, or more expensive to carry out pervasive surveillance. Similarly, private industry has made encryption the default in email and web access.

One government response to trends toward greater encryption, most visibly in the US, has been a discussion of building in "backdoors" into encryption protocols and systems so that law enforcement can readily access data. The issue emerged in the wake of a terrorist attack in San Bernardino, California when authorities sought access to an encrypted Apple smartphone belonging to the attacker and Apple CEO

Tim Cook resisting attempts to circumvent device encryption because it potentially builds in an inherent security vulnerability that could be exploited by foreign governments, hackers, and cybercriminals. In the context of massive data breaches, such as potentially 500 million users' data compromised in the Yahoo! hack, the idea of building in security vulnerabilities for national sovereignty is in direct tension with the multistakeholder technical community's efforts to increase rather than decrease the security of the Internet infrastructure that underlies all industrial, political, and social systems in the modern era.

Four Problems with Cyber Sovereignty Models

These examples of conflicts involving the rise of cyber sovereignty share several characteristics that help explain the problems these trends present for the future of the Internet, the pace of innovation, and human rights online.

1. Cyber Sovereignty Tampers with Internet Technical Infrastructure and Business Models

The Internet's core infrastructure can be taken for granted because of the network's ongoing growth and success. Indeed, policymakers and users alike are often not aware of the massive infrastructure of telecommunication transmission systems, switches, interconnection facilities, and cloud computing server facilities comprising the global Internet. In using the Internet, one only sees content, applications, and the end device (e.g. smartphone, laptop) used to access the content and applications. More than 99% of the Internet's infrastructure lies beneath what is visible at these end points.

Internet infrastructure has grown organically in the contemporary era, led by private sector investment and innovation. There has not been a centralized or hierarchical system that has shaped infrastructure which, despite challenges associated with cyber security breaches, anti-competitive forces, and movements toward proprietary enclosure, has been relatively stable and secure. Decisions about infrastructure arrangements, while reflecting public interest concerns, have been shaped in part by consideration of engineering efficiency, redundancy, and security.

Cyber sovereignty approaches seek to tamper with technical architecture, raising questions about how these alterations will affect the Internet itself. For example, data localization requirements impose politically motivated constraints on configurations of technical architecture. Under the mantel of cyber order, government censorship efforts sometimes involve local DNS redirection techniques that compromise

universally consistent name and number resolution. Referring back to the Internet Society's articulation of the design values that have shaped the Internet, the core design values of interoperability, global reach, and permissionless innovation, in particular, are challenged. Cyber order approaches seek to limit global reach, place politically motivated limits on interoperability and interconnection, require layers of permissions for the introduction of new services, and place restrictions on the organic configuration of networks based primarily on market demands or engineering efficiency. If these top down infrastructure modification requirements had arisen decades ago, it is very likely that the world would not have experienced the rapid growth and innovations of the Internet that have provided so many opportunities for freedom of expression and economic growth.

Part of this infrastructure tampering arises from incommensurability between national borders and transnational technology. For example, data localization requirements do not match how networks are designed. Engineering efficiency and performance objectives are often predicated upon distributing data closer to end points and creating distributed redundancy rather than having more centralized repositories. The flow of information crosses borders. Servers are distributed around the world. For a private company, a domain name can be registered with a registry in one area, a call center located in another part of the world, and the company incorporated in yet another region. While national laws apply within borders, cyber sovereignty models are often incompatible with how technology works in practice.

2. Cyber Sovereignty Models Impede Civil Liberties

Tensions between cyber sovereignty and distributed governance are often flashpoints that mediate what counts as human rights in the online environment. For decades, considerations about human rights online have included freedom of expression, privacy, the right to assembly, the right to participate in cultural life, the right to access knowledge, the freedom to innovate, and a host of economic liberties such as the freedom to innovate and participate in technological and scientific advancement. Civil liberties in the digital sphere have long also included the protection from online harms such as cyberbullying, censorship, unwarranted invasive surveillance, identity theft, and theft of intellectual property, among others. In many public policy areas, governments are viewed as necessary for creating the statutory and market conditions necessary for the promotion of human rights. The United Nations Human Rights Council has asserted that the same rights citizens are entitled to offline are applicable online.

In the online sphere, the historical record suggests that government interventions in cyberspace, under the guise of cyber sovereignty, are increasingly in direct conflict with human rights. For example, governments with repressive information policies use the Internet to monitor activists and censor information. They use distributed denial of service attacks to disrupt alternative media sources. They engage in expansive surveillance and information gathering practices that challenge basic norms of individual privacy. In the case of the Egyptian Internet outage, for example, they sometimes cut off citizen access entirely. The Internet is clearly recognized as a significant site of power in which economic and political objectives can be carried out.

Indeed, some tension points between cyber sovereignty models and distributed governance are actually tension points over human rights online. Models of cyber sovereignty in China include systems of filtering and censorship. Cyber order in Russia includes repression of free speech for LBGTQ and other communities. Attempts to weaken Internet security for expansive surveillance practices in the West raise profound privacy questions. Even data localization laws designed to protect privacy, concentrate data in a way that could make it easier to compromise privacy and make it easy for foreign surveillance to be carried out. Questions about the protection of human rights online are becoming increasingly complicated.

4. Cyber Sovereignty Approaches Weaken the Stability and Security of the Internet

Cyber sovereignty tools that tamper with the core infrastructure of the Internet often carry negative externalities for cybersecurity. Attempts to weaken or place limits on encryption are obvious examples of government interventions that, intentionally or not, can compromise the Internet's stability and security. Attempts to modify non-security-related core infrastructure of the Internet can also have affects. Politically motivated modifications to the Internet's Domain Name System are an example, such as local DNS redirection techniques that require local institutions residing within national borders, such as ISPs or non-authoritative DNS operators, to ignore the universally consistent record mapping names and numbers and instead modify address resolution data locally. In other words, when an Internet user attempts to access a website or page being blocked, the local DNS server would redirect the request to another site, or the lookup would fail. Local redirection has been used to block entire social media applications, such as when Iran banned Twitter.

Billions of address resolution lookups happen daily and the stable functioning of this system requires universal consistency. Local redirection can create problems when it does not remain local but rather cascades globally. The most well-known example

occurred in 2008 when the Pakistan government order Pakistani Telecom to block YouTube using local redirection but the routing information was extended up the DNS technical hierarchy resulting in a more global inability to access YouTube.

Local redirection, and also DNS injection techniques that cause DNS servers to lie about associated IP addresses, create security complications, such as impeding the implementation of DNSSEC, an important protocol designed to cryptographically authenticate domain name lookup processes so that users can be assured that a server returns the webpage requested rather than a counterfeit or malicious site. DNSSEC would be unable to distinguish between local redirection and cybercrime designed to carry out identity theft, disseminate malicious code, or sell counterfeit products.

This example is emblematic of the values tensions between the economic and public interest need for cybersecurity and government interest in content control, whether for intellectual property rights enforcement, censorship, or other objective. Attempts to exert bordered, top-down policies on technical infrastructure must understand and consider the complex technical substructures that preserve Internet stability and security.

5. Cyber Sovereignty Approaches Fragment the Internet

A significant theme in global Internet policy discussions is whether the Internet will continue to grow into a universal network or fragment into networks divided by national borders, proprietary ecosystems or other divisions. Bringing the next billion users (and objects) online requires the ongoing growth of the Internet. Ongoing growth in the digital economy requires interoperability among systems and the free flow of information across borders. This potential for universality and interoperability has been a taken for granted assumption for the enjoyment of expressive rights and for economic development. The United Nations Human Rights Council statement on The Promotion, Protection, and Enjoyment of Human Rights on the Internet describes the global and open characteristics of the Internet as a driving force of development.

It is important to acknowledge that the Internet is not yet a universal network. There are barriers to access, digital knowledge divides, language divides, interoperability challenges among protocols, and other kinds of technical fragmentation. But the Internet has continued to become more universal. Cyber sovereignty models are attempts to overlay geographical borders on the cross border Internet, raising questions about the effects of these policy approaches on the question of whether the Internet will become more fragmented or move toward greater universality. Data

localization laws, in particular, impose these national borders around the transnational Internet.

The universal nature of the Internet has brought about considerable economic growth and development and new opportunities for access to knowledge and expression. Imposing new techniques to assign national borders on this infrastructure may have significant implications for access to knowledge, business autonomy, and the digital economy.

Beyond cyber sovereignty approaches, there are also private industry efforts to limit Internet universality and interoperability through protocol fragmentation and the development of proprietary ecosystems designed to limit competition and interoperability for market advantage. Indeed, many of the problems caused by cyber sovereignty approaches would be similar with "industry sovereign approaches." It is exactly the relative balance of powers among various stakeholders in distributed Internet governance models that creates conditions for universality and innovation.

A Sea Change in Internet Governance

Cyber policy is a critical domain of foreign policy. The balance of control over the Internet is now inextricably linked to the state of the digital economy, critical infrastructure protection, human rights, and even job markets. The rising importance of cyber governance is increasingly recognized by governments as they acknowledge the Internet as a site of conflicts around political and economic power. From a foreign policy perspective, including in the U.S., Internet policy inherently contains tremendously conflicting interests, such as cybersecurity and the promotion of democracy and Internet freedom, on one hand, and intelligence and cyber warfare concerns, on the other.

The great myth of Internet governance in the past decade has been that it is a single system over which control can be wrested. The term Internet governance sounds singular. The media and policymaker overemphasis on the IANA transition and the stakes of the transition is an example of monolithic approach to control of the Internet. This sense of a cohesive, uniform Internet governance framework may have had some truth decades ago, but in the contemporary era, as the Internet becomes more globalized and heterogeneous and becomes so fundamentally important to the world, Internet governance has morphed into a large number of interrelated areas. Intersections between national security and critical infrastructure protection are one set of issues that have a certain set of players and its own set of different decision

making processes. Concerns related to the free flow of information on the Internet, often framed as "Internet freedom" issues, embody a different set of foreign policy and public interest concerns. The Domain Name System and its global institutional governance structure embodies yet a different set of concerns. Politically, one of the contextual backdrops that created so much anxiety around the IANA transition is this discursive aggregation of more than a hundred Internet governance functions into a single control point. There is not one stop shopping for cyber issues and unpacking the various issues and their unique public interest and technical considerations most precede policy discourses. There are policy areas in which national sovereignty concerns, especially national security, trump other considerations, but in most areas, distributed multistakeholder governance approaches have contributed to the ongoing success of the coordinating functions necessary to keep the Internet operational.

The transition of American power over the DNS is the beginning, not the end of geopolitical conflict. The IANA transition resolves nothing about the broader geopolitical conflicts involving the essential tension between multilateral or sovereign control and the distributed multistakeholder approach to administering the Internet. There is a sea change in the philosophy of Internet governance around this tension. This paper has described a small subset of global inflection points that reflect this transformation. The same tension will play out on different game boards as technological, cultural and market forces continue to shape the Internet.

Internet governance questions now exist in a post-Washington-consensus world. Because of its historical origins in the US and the West, the Internet came of age in a certain political and cultural context. Liberalization, privatization, and globalization were the hallmarks of this Washington consensus world. There has been a sharp turn away from this, including increased interest in regulation, distrust of globalization, and movement away from privatization. In the same way a certain set of democratic and free market values shaped the constitution of the Internet in its opening decades, where will this emerging context have the greatest implications for the future of Internet architecture and governance?

The policy battles of the future will be around the co-option of infrastructure rather than control of content. Already, governments recognize infrastructure control points as points of power, whether seeking modifications to the Domain Name System, approaches to data storage, or interconnection agreements. This turn to infrastructure will only increase. The most complex and overwhelming of infrastructure issues, and one with profound implications for security, privacy and economic competition, exists around the Internet of Things. Already, Distribute

Denial of Service Attacks have exploited security vulnerabilities in IoT devices like baby monitors and surveillance cameras to carry out extensive and disruptive attacks on specific targets and even on the DNS itself. The Internet constantly changes and policy changes today have to anticipate the diffusion of the Internet into material objects of our social and economic systems. It would be a difficult process to create international norms and enforceable agreements to not attack the core infrastructure of cyber physical systems or to agree on common privacy laws around the Internet of Things. Getting ahead of future cybersecurity problems around the Internet of Things will require strong security and accountability, a public policy challenge because there may not be adequate incentives for individual users or markets to address security.

In the context of cyber physical systems, another major policy battleground likely to reflect tensions between distributed multistakeholder governance and cyber sovereignty will involve government surveillance. There will also be infrastructure battles over technical standards and the open question of whether cyber physical systems will rely on the universal Internet address space or seek alternative address spaces controlled by governments rather than by the global multistakeholder communities. The question of involvement of the ITU in technical architecture and governance questions around IoT standards and names may be as contentious a debate as the decades-long battle over control of the IP address space and associated standards. Will the Internet remain a universal system based on the common IP address space or transform to other name and number systems, and therefore new governance structures? There is nothing fixed about Internet governance arrangements in the same way there is nothing fixed about Internet architecture. The process of Internet governance has been contentious but fairly stable – however there is nothing preordained about this. Geopolitical tensions will only rise as states increasingly view points of control over Internet infrastructure as sites of power, even while every aspect of political, social and economic life increasingly depend upon this infrastructure to function. How these tensions are resolved and the values inherent in the way Internet governance operates will likely determine whether the Internet continues to be an engine for material economic, social, political and cultural change, or if the Internet begins to splinter and become just another technology that did not meet the hype and its promise to change the world permanently for the better.