GPPi
GLOBAL PUBLIC POLICY
INSTITUTE

Getting "Free and Open" Right

How European Internet Foreign Policy Can Compete in a Fragmented World

By MIRKO HOHMANN, THORSTEN BENNER

POLICY PAPER
June 2018

The laissez-faire understanding of a "free and open" internet is facing competition from abroad and is increasingly inconsistent with the regulatory stance of liberal democracies. To counter an emboldened authoritarian approach, address charges of hypocrisy, and carefully guide the fragmentation of content and applications on the internet, the notion of "free and open" must be updated. European policymakers should take the lead in this process and face these challenges head on. To do so, they need to strengthen their own credibility, build new coalitions, and address the effects of fragmentation.

The International Cyber Policy Coordination Staff at the German Federal Foreign Office provided financial support for research for this paper. The authors thank Karsten Geier, Joachim Haupt, Christian Senninger, and Peter Stentzler for sharing their expertise with them. The views expressed in the paper are only those of the authors.

The authors also thank Sophie Barnett, Lukas Feldhaus, Christine Galvagna, and Christian Habla for their help throughout the process of creating the report; Trey Herr, Jonah Force Hill, Josh Kallmer, Robert Morgus, Alexander Pirang, and Isabel Skierka for their constructive criticism; Jacob Lefton and Stephanie Le Lièvre for their editing and proofreading; and Katharina Nachbar for design and overseeing the editing process.

Contents

Executive Summary

The "free and open" approach to internet governance originated in the US and emphasized (self-)regulation through multi-stakeholder governance processes. Using the words of US president Clinton's internet czar Ira Magaziner, this approach argued "against a traditional regulatory role for government."[1] It contributed to the many early advances that the internet and the information and communication technologies (ICT) running on it have made possible, among them the strengthening of human rights and economic growth.

That approach is now under fire on multiple fronts.

Authoritarian governments are quickly gaining ground in their efforts to control the flow of data and information. China in particular has built the technical and institutional capacity to not just limit the threats that the internet poses to the party's authoritarian rule, but to use technology to deepen the state's ability to exert absolute control over the lives of its citizens. China (alongside Russia and others) has also intensified its efforts to promote its approach to internet regulation abroad, directly challenging the "free and open" philosophy espoused by many democratically governed nations.

At the same time, the ultra-libertarian version of "free and open" has also been challenged by liberal democracies, especially in Europe. EU countries had originally supported the US approach to internet (foreign) policy. However, as the internet morphed from a medium for a few to the medium that organizes everyday economic, political, and personal life, democratic governments in Europe realized they had a duty toward their citizens to pursue a stronger regulatory role to guarantee rights and correct market failures. They now face charges of inconsistency, or outright hypocrisy, because their domestic regulatory action is seen as contradicting the original doctrine of an internet that is free and open, with a minimalistic role for government.

The trend of stronger regulation at the national level (in both authoritarian states and liberal democracies) is leading to a more fragmented internet, especially regarding access to applications and content. European democracies need to recast their internet foreign policies in order to tackle these challenges. To do so, they can take action on three fronts: (1) strengthening European and—more broadly—Western credibility and messaging; (2) winning new allies and building coalitions; and (3) making fragmentation work.

[1] Ira Magaziner, "Creating a Framework for Global Electronic Commerce," *The Progress & Freedom Foundation*, July 6, 1999, accessed June 15, 2018, http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html.

Strengthening European Credibility and Messaging

1. **Develop and promote a coherent narrative about the rule of law online:** European policymakers should not shy away from regulatory action because of an unrealistic baseline of non-interference. Free and open societies follow laws, and democratically elected governments write and enforce them. It is crucial that liberal democracies highlight the fundamental differences between them and authoritarian nations when it comes to the motivation for as well as means and effects of internet regulation.

2. **Expose the costs of the authoritarian model:** It is not only necessary to strengthen narratives, but also to highlight the weaknesses of the approach to internet policy pursued by countries like Russia and China. The model of information control can seem attractive at first, but it comes with costs that go beyond the restrictions on individual freedoms. Social tension builds up, and both users and companies must bear the financial burdens of a closed society as well as an internet that is severed from the rest of the world. And the costs of a walled-off internet are particularly high in countries that do not have huge single markets like China.

Winning New Allies and Building Coalitions

3. **Engage key non-Western powers and "swing states":** With a stronger understanding of their own approach, European democracies can effectively engage key non-Western states that do not practice authoritarian digital policy. Countries like India and Brazil stand out as potential partners. Both have the capacity to shape norms and rules internationally. Other such swing states should be identified to help diplomats prioritize who they engage with bi- and multilaterally.

4. **Help create access for and build capacity with selected partner countries:** Capacity building efforts and infrastructure support are a key means to engage new partners. They not only help other countries reap the benefits of digitization, but are also a foreign policy tool. As China expands its infrastructure support at rapid speed, more Western resources should be shifted towards ICT projects, which should, in turn, take human rights implications into account.

5. **Hold corporations accountable:** The private sector is an important intermediary between users and governments, especially in authoritarian countries. Large technology companies should be held to their public claims that they seek to protect users, not just in liberal democracies but globally. Existing legal frameworks should be strengthened to force companies to consider the human rights implications of their work.

Making Fragmentation Work

6. **Take cross-border implications into account:** It is likely that more states will pursue unilateral regulatory action, which increases the risk of fragmentation of the internet, or at least of the applications and content that run on it. There is an overwhelming international interest to properly guide such regulatory efforts at the national level. To increase awareness, lawmakers could add a new category to the evaluation processes in domestic legislative decision-making that deals with the cross-border implications of national efforts to regulate the internet.

7. **Ensure and improve technical and legal interoperability:** Limiting the fragmentary effects of regulation is one step; upholding and increasing interoperability another. Harmonization, standardization and mutual recognition of laws are key mechanisms to improve legal operability. Importantly, such efforts should be issue-specific; for example, to address cybercrime in e-commerce issues. Technical interoperability must be a priority to ensure that different national or regional networks can continue to operate with one another.

For Europe and its allies, it is time to enter the competition on internet foreign policy with a clear understanding of the challenges from abroad and a clear idea of their own goals and ways to shape global (internet) governance. “Free and open,” correctly understood, is still the appropriate guiding star for European internet (foreign) policy; yet it is necessary to re-define these terms for today’s world. The above-mentioned ideas can serve as first steps in that direction.

Introduction

"Good luck," said Bill Clinton in 2000 about Chinese government efforts to regulate and control online communications. "That's sort of like trying to nail Jell-O to the wall."[2] In Clinton's opinion, liberty would "spread by cell phone and cable modem." This assumption neatly captures the approach the US and many Western governments took toward internet regulation in the 1990s and early 2000s: not only was such regulation hard to implement, it was also undesirable. This philosophy led to a hands-off approach domestically and created a clear foreign-policy agenda: to sustain a free, open, and interoperable internet and to limit the role of the state in international internet governance through multi-stakeholder governance processes. "Free and open" became the slogan of Western governments. The extreme position that the activist John Perry Barlow promoted on the role of governments in cyberspace in 1997 resonates well with this approach: "You have no sovereignty where we gather."[3] Of course, the hands-off approach that Clinton promoted was easier to pursue back then, given that many of the relevant for- and not-for-profit stakeholders were American and that Western actors dominated decision-making processes in key technical institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Engineering Task Force (IETF).

This hands-off environment allowed the internet to grow at a phenomenal speed, enabling unprecedented cross-border communication. New business models developed and international trade increased, leading to economic growth and development. Information and communications technology (ICT) also allowed for better access to information and strengthened human rights: users could express their opinions online, journalists were able to receive and share information digitally, and organizing political movements became easier.

But the party did not last. In a way, the internet became the victim of its own success. As it moved from a medium for a few to *the* medium that organizes everyday economic, political, and personal life, governments have increasingly attempted to align online communication with national jurisdictions. These "weary giants of flesh and steel" have sought to reclaim sovereignty online.[4] While the internet was never fully universal, state borders or national laws mattered relatively little. This is changing fast. Almost two decades after Clinton's statements, the Jell-O has long been nailed to the wall—and it stuck. The key question about internet regulation is not whether it can

[2] William J. Drake, Shanthi Kalathil, and Taylor Boas, "Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba," *Carnegie Endowment for International Peace*, October 23, 2000, accessed May 8, 2018, http://carnegieendowment.org/2000/10/23/dictatorships-in-digital-age-some-considerations-on-internet-in-china-and-cuba-pub-531.

[3] John Perry Barlow, "A Declaration of the Independence of Cyberspace," *World Economic Forum,* February 8, 2018, accessed May 8, 2018, https://www.weforum.org/agenda/2018/02/a-declaration-of-the-independence-of-cyberspace/.

[4] Milton Mueller, *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* (Hoboken: Wiley, 2017), p. 3.

be done, but how it will be done and by whom. Authoritarian governments like China, Russia, and Iran have always been at the forefront of internet regulation. They never subscribed to the narrative of a free and open internet, since the free flow of data—or rather, information—poses a distinct challenge to their political system. Over the last couple of decades, they built up the technical and institutional capacity for information control. In parallel, they began promoting an alternative narrative of government-led internet regulation abroad, creating a narrative which competed with that of many Western nations.

As a result, the Western internet governance model is no longer the only game in town. There is an alternative, authoritarian approach to internet governance, promoted by influential countries such as China and Russia. It is competitive, because certain elements are attractive to various nations that currently subscribe to neither an authoritarian model nor the free-and-open model.

In the meantime, democratic governments also realized that no communications medium of such critical importance could remain unregulated, even, or especially, in liberal democracies. After all, the internet is no longer a playground for cypherpunks, but rather the core communications medium of our time. Increasing government engagement is a natural development: offline laws need to be enforced online, users and their data must be protected, and there is the need for a regulatory environment for companies. While the motivations, means, and effects dramatically differ from the efforts of countries like China or Russia, Western governments have nevertheless increased their efforts to nail the Jell-O to the wall.

As a result of these domestic efforts, the foreign policy narrative promoting a free and open internet appears out of step with the limits on the free flow of data that Western governments have pursued, making Western countries vulnerable to charges of inconsistency and outright hypocrisy.

These parallel developments are consequential for Western and, particularly, European foreign policy efforts on several fronts. Most importantly, they threaten many of the recent advances made for human rights and for globally interconnectedness. Internet freedom, and many freedoms with which it is associated, have been declining for years in authoritarian nations, and they are likely to do so in other nations that adopt similar methods for information control.[5] At the same time, the costs of doing business rise with increasing online sovereignty and the “digital borders,” i.e., regulatory national measures, associated with it. This requires governments and other key actors to think about ways to address the effects of fragmentation (for example, by strengthening interoperability between nations and regions).

The charges of hypocrisy further weaken democratic countries’ ability to build alliances and counter authoritarian agendas. Whether the concept has been hollow all along is a different question, but there is a need to build a coherent and consistent narrative on how regulatory measures in liberal democracies differ, what makes for appropriate regulation, and how it could be implemented with partners. In short: the narrative of “promoting a free and open internet” must be updated for today.

[5] Sanja Kelly et al., *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. Freedom House Report. (Washington: Freedom House, 2017), https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf, p. 220.

Finally, various nations' unilateral national regulatory efforts have created a trend towards a more fragmented internet, especially with regards to content and applications. Governments need to take measures to make unavoidable fragmentation work as best as possible.

The European Union and its member states have a key role to play in addressing these challenges. This is an opportunity to use European diplomatic efforts to build momentum toward a new narrative, build alliances with Western and non-Western democratic actors for the promotion of this new narrative, and propose policies to counter fragmentary trends. The EU could step in and fill the diplomatic gap that the US has left since the election of President Donald Trump. Debates on appropriate regulatory action—be it competition or data protection policy—are already taking place in several member states, as well as on the EU level, and these debates could inform suggestions for the international arena.

This paper takes a closer look at the above-mentioned challenges and seeks to provide suggestions to European (foreign-) policy makers on how to approach them. The first part provides a short overview on the traditional internet governance model, before outlining two challenges: the efforts of authoritarian nations like China and Russia to develop a competitive system of information control at home and to promote it internationally, and the changing policy landscape in many Western nations. The second part takes a closer look at the resulting foreign policy challenges. The third part suggests various focus areas for policy-makers to address in order to reinvigorate European foreign policy efforts on internet governance.

The Free-and-Open-Internet Approach Under Pressure

The ARPAnet, which laid the groundwork for the internet, was initially created through a collaboration between university researchers in the United States of America and Europe, backed up by US research and military funding. It was then built upon by a coalition of mainly Western researchers and members of civil society, the technical community, and the private and public sectors. The values and worldviews of these actors have significantly impacted the way in which the internet developed and is governed. The first US International Strategy for Cyberspace naturally stated that "[t]he more freely information flows, the stronger our societies become."[6] The US Department of Defense went even further, stressing that an "open, secure, interoperable, and reliable Internet … reflect[s] core American values—of freedom of expression and privacy, creativity, opportunity, and innovation."[7] Similarly, the UK stresses the need for "international consensus on the benefits of a free, open, peaceful and secure cyberspace" in its cybersecurity strategy, and the German government seeks to "protect and further expand an open, free and secure global internet as a space of opinion variety, participation and innovation as the engine of economic growth and jobs."[8] In general, the adjectives "free", "open", and "interoperable" are recurring themes in Western official documents and speeches alike (alongside "secure" and "resilient").

The way the internet was developed also led to a specific governance model for its relevant infrastructures, rules, and processes, especially on the international level. This was a multi-stakeholder governance model, "whereby a multitude of diverse stakeholders can participate in the collective development and shaping of the evolution and use of the Internet."[9] Relevant stakeholders include the public and private sectors, civil society, the technical and academic communities, and international organizations. This approach is not an end in itself. Rather, the multi-stakeholder model recognizes

[6] White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (2011), accessed May 3, 2018, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[7] Department of Defense, "The DoD Cyber Strategy" (2015), accessed May 7, 2018, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[8] Die Bundesregierung, "Digitale Agenda 2014-2017" (2014), accessed May 3, 2018, https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf;jsessionid=B4CBFD2649B9E36D4E62A1472E1D7B9F.s6t2?__blob=publicationFile&v=6, p. 34.

[9] United Nations Educational, Scientific, and Cultural Organization, *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance* (Paris: 2017), http://unesdoc.unesco.org/images/0025/002597/259717e.pdf.

the relevance of the different actors "in their respective roles"[10] in governing a decentralized network without a clear hierarchy. It seeks to distribute power and add diversity and expertise to decision-making processes. Power imbalances have always existed in this context, yet in contrast to many other policy fields, there has been a much more limited role for governmental actors.

There have been strong arguments for a limited governmental role: Unrestricted internet access, not limited by governments—or private actors—can promote human rights and enable economic growth. An open and free internet has been a boon for human rights. Most notably, it has strengthened the right to freedom of opinion and expression of billions of people, i.e., their right to "seek, receive and impart information and ideas through any media and regardless of frontiers" as granted in Article 19 of the Universal Declaration of Human Rights. More broadly, online communication has had a cross-cutting effect on other fundamental rights, such as the right to education (though a variety of online resources) and the right to assembly and association (enabling people to virtually gather and organize). It also enables journalists to access information and report across borders.

The internet has also had positive economic effects. As the UN Human Rights Council points out: "The global and open nature of the Internet [is] a driving force in accelerating progress towards development in its various forms."[11] In line with this, one of the strong arguments for a free and open internet has always been that it drives economic growth and innovation and increases productivity. Connectivity has been driving down the costs of conducting business across borders, boosting international trade, and cloud-platforms are likely to be "at the heart of innovation and growth" in the next few years.[12] There has been substantial research to link the open character of the internet with its catalytic role in development and economic growth.[13]

While these points hold, it should not be omitted that on both human rights and economic growth the all-out positive story of the impact of the internet has recently been called into question. On the economic front, there are now powerful monopolies emerging that may stifle innovation. On the human rights front, authoritarian governments have turned the internet into a tool of control and oppression.

Rise of a Competitive Model

While the US cybersecurity strategy argues that "the more freely information flows, the stronger our societies become,"[14] the opposite holds true from the vantage point of ruling elites in authoritarian countries. There, the free flow of information is seen

[10] World Summit on the Information Society, "Tunis Agenda for the Information Society," (2005), accessed May 31, 2018, http://www.tjsl.edu/slomansonb/5.2_TunisAgenda.pdf.

[11] United Nations Human Rights Council, Resolution 20/8, *The Promotion, Protection, and Enjoyment of Human Rights on the Internet*, July 16, 2012.

[12] Bertrand de La Chapelle and Paul Fehlinger, "Jurisdiction on the Internet: From Legal arms Race to Transnational Cooperation," *Global Commission on Internet Governance* no. 28 (2016): p. 95.

[13] Organization for Economic Co-operation and Development, "Economic and Social Benefits of Internet Openness" (2016), accessed May 7, 2018, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En.

[14] White House, "International Strategy for Cyberspace."

as a threat to the political system. Those in power seek to tightly control the flow of information.

Information control is not the only reason for disagreement, however: Many non-Western nations have perceived the existing internet governance model as a manifestation of American power. The core technical infrastructure was built in the US and Europe, and the majority of the twelve organizations that run the internet's root servers, comprising the core of the internet infrastructure, are American.[15] Most of the companies that provide this infrastructure and the applications and services that run on it have traditionally been American. Similarly, the technical bodies that set standards for the inner workings of the internet have been Western. A prominent case in point has been the debate about ICANN, a Los Angeles-based nonprofit organization that holds a key technical role in the Internet's global Domain Name System (DNS). Until 2016, ICANN was under contract with the US Department of Commerce until 2016, raising questions about the influence of the US government on its decision-making. Regardless of the actual impact on ICANN, Western actors de facto dominated the membership of key technical organizations like the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE) or the World Wide Web Consortium (W3C) (the IETF, for example, kept no statistics on Chinese attendants to its meetings until 2007 because the numbers were so low)[16].

For these reasons, countries like China and Russia have been developing and promoting a competitive governance and regulatory model. They promote a state-centric narrative of a controlled domestic environment under the umbrella terms "information security" and "cyber sovereignty." On various occasions, Chinese President Xi Jinping has argued for the "right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies."[17] Whether in China, Russia, or Iran, the argument is similar: as with other domains that might be global in nature, "sovereign states have the primary responsibility for maintaining order in cyberspace."[18]

System of Information Control at Home

While many nations, especially in Asia and Africa, have begun to build up domestic efforts to control online communications, China and Russia are leading the way. China has been ranked "the world's worst abuser of internet freedom" by Freedom House for three consecutive years, providing an example of how far "sovereignty online"

[15] Internet Assigned Numbers Authority, "Root Servers," accessed May 3, 2018, https://www.iana.org/domains/root/servers.

[16] Hong Shen, "China and global internet governance: toward an alternative analytical framework," *Chinese Journal of Communication* 9, no. 3 (2016): 304-324, p. 6, http://www.andrew.cmu.edu/user/hongs/files/HongShen_global.internet.governance.WritingSample.pdf

[17] Lu Chuanying, "China's Emerging Cyberspace Strategy," *The Diplomat,* May 24, 2016, accessed May 22, 2018, https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/.

[18] Kamlesh Bajaj, "As Trump Dampens US's Internet Freedom Agenda, the Race to Cyber Supremacy Reaches New Levels," *The Wire,* August 21, 2017, accessed May 7, 2018, https://thewire.in/169461/trump-cyber-diplomacy-nsa-internet-freedom-agenda/.

can be taken.[19] Hundreds of thousands of employees within government agencies and the private sector, together with an advanced technical infrastructure, make up an elaborate system to monitor, censor, and manipulate online content. They routinely block anything from specific words and phrases to entire services and shut down the internet for specific users, or ahead of certain events. Individual users or website operators can easily be charged with subversion or terrorism and imprisoned for days, months, or years.[20]

Russia's system is less elaborate, but the country's hunger for data and information about its citizens is growing.[21] Online media outlets are pressured to report news in a government-friendly manner, and the government has the authority to compel outlets to take specific posts or articles offline. Referencing extremism or incitement, social media accounts have been blocked and users arrested. Censorship is common and targeted, for example around lesbian, gay, bisexual, transgender, and intersex (LGBTI) issues. At the same time, Russia has long operated one of the most extensive surveillance systems. Its System of Operative Search Measures (SORM) requires all telecommunication providers to give the Russian Federal Security Service (FSB) access to all communications, allowing the intelligence agency to monitor telephone calls and internet traffic.[22]

The domestic efforts of both Russia and China share two noteworthy trends: the codification of monitoring, censorship, and surveillance strategies, and the focus on forcing international technology companies into compliance with domestic laws. Data localization laws are a key example. In Russia, the so-called 2016 Yarovaya Law mandates that service providers retain user content for six months and metadata for three years on servers within the country. This way, data that is not captured by SORM is saved on the providers' servers for later access. It also addresses the challenge that encrypted services pose to the surveillance system, as it obliges companies that offer such services to pass on encryption keys to the government.[23] Apple and Google reportedly complied with the data localization laws, while LinkedIn did not and was subsequently blocked in the country.[24] Russian authorities also attempted to block the messenger service Telegram after it failed to share encryption keys.[25] In China, a recent cybersecurity law similarly mandates data localization and forces users to register under real names.[26] The law, which threatens heavy fines to non-compliant companies,

[19] Kelly et al., *Freedom on the Net 2017*, p. 220.

[20] UN Human Rrights Council, Resolution 20/8.

[21] Kelly et al., *Freedom on the Net 2017*, p. 696.

[22] James Andrew Lewis, "Reference Note on Russian Communications Surveillance," *Center for Strategic and International Studies,* April 18, 2014, accessed June 4, 2018, https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

[23] Danny O'Brien and Eva Galperin, "Russia Asks For The Impossible With Its New Surveillance Laws," *Electronic Frontier Foundation*, July 19, 2016, accessed May 8, 2018, https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

[24] Ingrid Lunden, "LinkedIn is now officially blocked in Russia," *TechCrunch,* November 17, 2016, accessed May 8, 2018, https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/.

[25] Sean Gallagher, "In effort to shut down Telegram, Russia blocks Amazon, Google network addresses," *ARS Technica,* April 17, 2018, accessed June 4, 2018, https://arstechnica.com/information-technology/2018/04/in-effort-to-shut-down-telegram-russia-blocks-amazon-google-network-addresses/.

[26] Sui-Lee Wee, "China's New Cybersecurity Law Leaves Foreign Firms Guessing," *New York Times,* May 31, 2017, accessed May 8, 2018, https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html.

seems intentionally drafted to be vague, providing the government with leeway for interpretation and negotiations with non-Chinese companies.[27]

China not only requires the cooperation of foreign companies, it has also managed to build up an impressive public-private partnership at home. Through a mixture of protectionism, government funding, and a thriving domestic market with hundreds of millions of users, Chinese companies have leapfrogged to the forefront of technical expertise and are now able to compete internationally. At the same time, the private sector has become a key resource in implementing many of the censorship and surveillance efforts outlined above. The advanced social credit system is the most recent example of the extent to which governments can take surveillance measures when public and private data on individuals is combined.[28]

The Promotion of Intergovernmental Cooperation Abroad

The domestic regulatory approach also informs these countries' foreign policy agendas. International efforts are a means to legitimize domestic controls and gain international recognition for national policies that are already in place.

Instead of a free, open internet, there are demands for cyber sovereignty. The term information security is used to signal a concern with content control that goes beyond the security and protection of data. Russia and China have also attempted to shift and broaden the definitions of words such as terrorism or (cyber)crime to use them as a justification for stronger governmental information control.[29]

In this approach, sovereign governments are seen as the principal actors in internet regulation at the international level. In contrast to the approach of multistakeholder internet governance, there is a strong focus of the role of governments in multilateral efforts and institutions, i.e., to elevate governments to become the key decision-makers in cyberspace through intergovernmental processes.

There have been efforts to promote this agenda internationally in multiple fora. In 2011, Russia, China and other members of the Shanghai Cooperation Organization (SCO) submitted a draft for an "International Code of Conduct for Information Security" to the UN General Assembly. The text stressed the key role and leading capacity of states to protect the information space, pointing out that "policy authority for Internet-related public issues is the sovereign right of States."[30] It went on to ask for the "the establishment of a multilateral, transparent and democratic international

[27] Chris Mirasola, "Understanding China's Cybersecurity Law," *Lawfare,* November 8, 2016, accessed May 8, 2018, https://www.lawfareblog.com/understanding-chinas-cybersecurity-law. See also Adam Segal, "Year in Review: Chinese Cyber Sovereignty in Action," *Council on Foreign Relations,* January 8, 2018, accessed May 8, 2018, https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action?sp_mid=55724208&sp_rid=bWhvaG1hbm5AZ3BwaS5uZXQS1.

[28] Rogier Creemers, "China's Social Credit System: An Evolving Practice of Control" (University of Leiden, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792.

[29] Mikko Huotari et al., *China's Emergence As A Global Security Actor: Strategies for Europe.* MERICS Papers on China (Berlin: Mercator Institute for China Studies, 2017), p. 45.

[30] United Nations General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359, September 14, 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

management of the Internet."[31] Protecting information space, however, was framed deliberately widely and included curbing "the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability."[32] A slightly updated version was again submitted in 2015, taking into account new developments, but not changing key aspects of the code.[33] Neither of the resolutions found sufficient global support, but demonstrated persistent efforts to suggest new norms and challenge the status quo.

In parallel, the International Telecommunications Union (ITU), a UN organization, has become a battleground for internet governance. Russia's president Vladimir Putin has made it clear that he and his allies seek to establish "international control over the Internet" through the ITU.[34] These goals came to global attention in 2012, when Russia suggested the ITU, instead of ICANN, should take on management of the DNS. According to the proposal, "Member States shall have equal rights to manage the Internet."[35] At the end of week-long negotiations, a coalition of 89 states—led by Russia and China—signed suggested regulations—with 55 opposing them, as seen in Figure 1.[36] While the regulations were binding only for signatories, it was a blow to the US, European states, and their allies, and it was an early indicator for the challenges in building coalitions on internet governance.

It is worth looking beyond traditional international organizations. Since 2014, the Cyberspace Administration of China has held the annual "World Internet Conference" in Wuzhen to promote its vision and understanding of sovereignty in cyberspace. The Wuzhen summit is not only gaining traction regionally, but has also attracted Western business leaders. At the most recent conference in 2017, Apple CEO Tim Cook, Google CEO Sundar Pichai, and Microsoft executive vice president Harry Shum all participated. There, Cook stated that Apple shared China's vision of "developing a digital economy for openness and shared benefits," without stating that China's information control runs counter to any claims of "openness."[37]

[31] UN General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, September 14, 2011.

[32] UN General Assembly, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, September 14, 2011.

[33] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *Citizen Lab,* September 28, 2015, accessed May 8, 2018, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[34] Federal Communications Commission, "Statement of Commissioner Robert M. McDowell" (2012), accessed May 3, 2018, https://apps.fcc.gov/edocs_public/attachmatch/DOC-313082A1.txt.

[35] David P. Fidler, "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations," *ASIL Insights* 17, no 6 (2013). https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision.

[36] Tim Maurer and Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate.* CIGI Internet Governance Paper (Waterloo: Centre for International Governance Innovation, 2014), p. 20.

[37] Simon Denyer, "Apple CEO backs China's vision of an 'open' Internet as censorship reaches new heights," *Washington Post,* December 4, 2017, accessed May 8, 2018, https://www.washingtonpost.com/news/worldviews/wp/2017/12/04/apple-ceo-backs-chinas-vision-of-an-open-internet-as-censorship-reaches-new-heights/?utm_term=.7e7ab9e3ad2b.

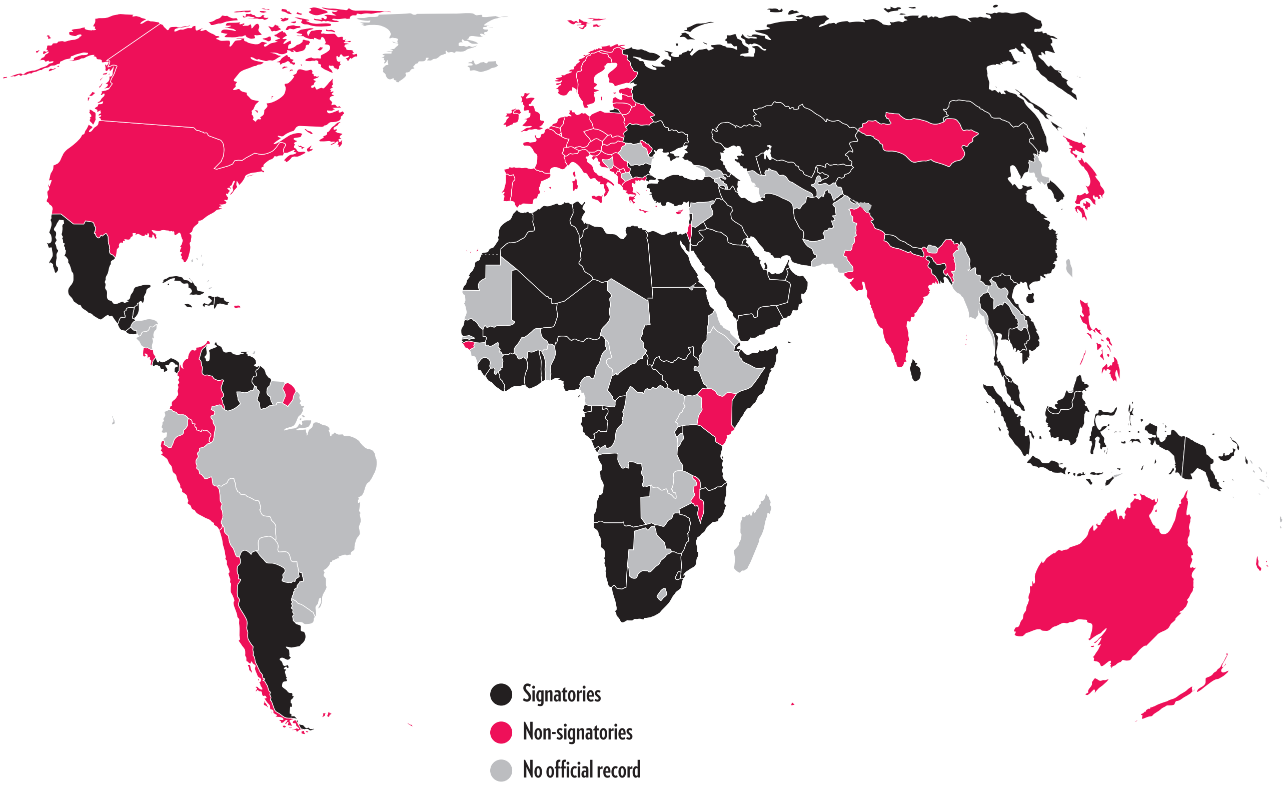


Figure 1: Signatories and Non-Signatories to the International Telecommunications Regulations, 2012 (Source: Broeders, *The Public Core of the Internet*)

In addition to their work in international organizations and with the private sector, China has begun to employ its economic leverage to win allies among other nations. China's Belt and Road infrastructure includes a reference to "an information silk road" to grow digital trade and build communications networks in Asia, Africa and Europe.[38] Chinese officials have openly referred to such a digital or information silk road as a measure to "construct a community of common destiny in cyberspace."[39] While more a catchphrase than a cohesive concept, there is a clear goal, not just of becoming a global technology leader, but also of translating that power into influence. Chinese companies are already leading the development of new (telecommunications) technologies, and they are using their knowledge to build the infrastructure to power the digital silk road, be it fiber optic cable or the BeiDou satellite network.[40] Furthermore, exports are not limited to connectivity-improving technology: the surveillance methods developed and tested at home are attractive to many other nations, and China has begun selling them

[38] Elizabeth C. Economy, "Beijing's Silk Road Goes Digital," *Council on Foreign Relations,* June 6, 2017, accessed May 8, 2018, https://www.cfr.org/blog/beijings-silk-road-goes-digital. See also Huotari et al., *China's Emergence As A Global Security Actor: Strategies for Europe,* p. 98.

[39] State Council of the People's Republic of China, *Digital Silk Road forges strong links* (2017), accessed May 3, 2018, http://english.gov.cn/state_council/ministries/2017/12/05/content_281475965391860.htm.

[40] Economy, "Beijing's Silk Road."

abroad.[41] Finally, the West has been challenged within international standards bodies, like the IETF and the IEEE. On the one hand, efforts to add diversity to a set of bodies that set global standards but have traditionally been dominated by Western (male) experts should be welcomed.[42] On the other hand, China clearly sees "standardization not only as a way to provide competitiveness for their companies, but also as a way to go from being a follower to setting the pace."[43]

Competition to the Western idea of a free, open internet is increasing on various fronts. China, Russia, and other authoritarian nations may not always act in concert, yet they have managed to build and promote an alternative governance model, both regarding domestic regulation and international cooperation. Whether this model works for many more nations remains to be seen, but the promise of additional control is certainly attractive to many governments.

The End of Internet Libertarianism in the West

For Western governments, the initial hands-off approach was a convenient fit. It was in line with Clinton's argument that liberty would spread through cell phones and modems and fit within a broader trend of deregulation and a laissez-faire economic policy that took place during the 1980s and 1990s. The US (and to a lesser extent Europe) dominated the relevant regulatory bodies, with the premise that "the internet" was a separate policy area, one where innovation could take place but that was less important than other traditional policy areas. Mainstream policymakers, to the degree they cared, saw "the internet" as an arena that could safely be left to digital policy wonks. After all, its importance was limited. Through this approach, democratic governments gave the impression that their understanding of free and open corresponded to the libertarian ideals of Barlow and others.

This approach changed when mainstream policymakers realized "the internet" had started to touch on all aspects of the daily lives of citizens, affecting and shaping key areas of public policy. Whether fighting crime, ensuring coherent and fair taxation, or protecting citizens' rights, digitization has affected core government interests and responsibilities. More recent trends have only deepened this realization. For example, foreign influencing efforts have challenged the integrity of election processes, and discussions on the changing public sphere due to social media are dominating the news. The increasing dominance of a few (US-based) technology companies that were able to flourish in an unregulated economic environment has led to conversations, especially

[41] Glyn Moody, "China Exporting Its Surveillance Tech and Philosophy to Other Countries, Helped by Equipment Donations," *TechDirt*, February 1, 2018, accessed May 8, 2018, https://www.techdirt.com/articles/20180124/03425639068/china-exporting-surveillance-tech-philosophy-to-other-countries-helped-equipment-donations.shtml. See also Maya Wang, "China's Dystopian Push to Revolutionize Surveillance," *Human Rights Watch,* August 18, 2017, accessed May 8, 2018, https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance.

[42] Jari Arkko, "IETF Diversity Update," *IETF*, December 4, 2015, accessed June 4, 2018, https://www.ietf.org/blog/ietf-diversity-update/. See also Internet Engineering Task Force, "Meeting Statistics," 2018, accessed June 4, 2018, https://datatracker.ietf.org/stats/meeting/overview/.

[43] Will Knight, "China wants to shape the global future of artificial intelligence," *Technology Review,* March 16, 2018, accessed June 4, 2018, https://www.technologyreview.com/s/610546/china-wants-to-shape-the-global-future-of-artificial-intelligence/.

in Europe, about updating anti-trust policies for application within the technology sector. The disclosures by former National Security Agency (NSA) contractor Edward Snowden showed the public how relevant ICTs are for national security purposes.

As a result, Western governments began to challenge the internet's initial exceptionalism, "at least for matters they cared about,"[44] as had long been predicted by some experts. It turned out that the list of matters they cared about was long. It also became clear that, as in all other areas, a libertarian ideology is not a good fit for a responsible democratic government's approach to the regulation of the central area its economy, security, and public sphere. So democratic governments invested more time and energy in setting the rules of the game – as they do in all other policy areas. In short: they have begun enforcing their sovereignty online and started a process of developing regional or national policies, many of which put constraints on the flow of information or challenged the universal internet experience. It has become clear that that the mantra "the more freely information flows, the stronger our societies become" is not an affirmation of a hyper-libertarian philosophy. [45] Strong, free, and open societies depend on rules that guarantee freedoms for every citizen.

Western regulatory efforts are distinct from those of authoritarian nations. The degree of and motivation for domestic regulations are dramatically different, as are the checks and balances in place to ensure respect for the rule of law. It is not just the processes that are in place that make a difference: the purpose matters, too. Regulations seek to protect individual freedoms instead of limiting them.

Like in all other policy areas, there are competing philosophies over the correct regulatory approach and policy-makers have faced various trade-offs regarding internet policy making. Three examples are worth looking at as part of this discussion: (1) the EU's General Data Protection Regulation (GDPR), (2) Germany's network enforcement law, and (3) Europe's broader efforts to achieve "technological sovereignty" following the Snowden revelations. The GDPR, like many data protection efforts, determines that data should be stored within a specific region. It specifies that "any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation"[46] can only take place under specific conditions. For a company whose headquarters are located outside of the EU, this can mean that the storing of data within the EU becomes necessary, independent from economic or data security considerations. The GDPR creates a different legal regime in the EU compared to the rest of the world, and few challenge the EU's right to enforce such regional policies.

Germany's network enforcement law received much attention globally and falls into the category of creating different provisions for permissible content based on location. One aspect of the law forces social media companies to delete "clearly unlawful" content from their sites within 24 hours. The law has been criticized for

[44] Tim Wu, "Is Internet Exceptionalism Dead?" in *The Next Digital Decade: Essays on the Future of the Internet,* eds. Berlin Szoka and Adam Marcus (Washington: TechFreedom, 2010), p. 180. See also Tim Wu and Jack Goldsmith, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2008).

[45] White House, "International Strategy for Cyberspace."

[46] European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 2016, accessed May 4, 2018, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, art. 44.

outsourcing the tasks of determining what content is “clearly unlawful” to private companies and for failing to provide judicial oversight and remedy.[47] While these aspects could be addressed if the law was written differently, the key idea behind it could not: Germany’s definition of what is unlawful content or speech, which should therefore be deleted, blocked or punished, is different to that of, for example, the US or France. As a result, content on social media will look different for German users than for French or American users.

Across Europe, Edward Snowden’s revelations showed that protectionist impulses can also feed into policy debates on internet regulation. With the purported goal of protecting European citizens’ data from US intelligence agencies and technology companies working closely with the NSA, politicians, government officials, and various private sector and civil society representatives in Europe suggested several measures, ranging from local routing infrastructures over better encryption technologies to new undersea cables. While some of these measures could protect citizens’ data, the strong focus on the location of data (instead of the data security mechanisms that are in place) has led to criticism about the misguided nature of efforts to improve sovereignty online.[48] Many initial proposals were dropped, but other regulations have since been implemented. For example, Germany’s data retention law mandates that all data held by service providers must be stored on servers based in Germany.[49] In this case, the data is not stored on the basis of criteria like data security or efficiency of data flows, but rather on location.

All these measures have been adopted via democratic processes in which there is an open debate on the “right” form of regulation and with a motivation to defend, rather than curtail, open and free societies. In the name of protecting citizens’ rights, these measures regulate online activities within a country’s borders; they restrict information, limit data from flowing freely, and change the user experience based on where one lives or uses the internet. They lead to different national legal environments for companies and users to navigate. These policies mark a departure from the internet’s initial exceptionalism, during which Western governments were seen as promoting a free and open internet in line with an argument for libertarianism both at home and abroad. Democratic governments have realized that guaranteeing freedom and openness requires government intervention online in the same way as is required offline. At home, Western governments are now in the process of identifying the right policy interventions, and the aforementioned measures have been subject to much discussion. Similarly, Western governments must adjust their foreign policy narrative of a free and open internet to reflect these new realities.

[47] Human Rights Watch, “Germany: Flawed Social Media Law,” February 14, 2018, accessed May 8, 2018, https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law. See also Thorsten Benner and Mirko Hohmann, “Internet companies can’t be judges of free speech,” *Politico,* April 27, 2017, accessed May 8, 2018, https://www.politico.eu/article/internet-companies-not-free-speech-judges-facebook-twitter/.

[48] Jonah Force Hill, “The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders,” *Lawfare Research Paper Series* 2, no. 3 (2014). https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf. See also Tim Maurer et al., *Technological Sovereignty: Missing the Point?* Policy Paper (Berlin: Global Public Policy Institute and Washington, DC: New America, 2014).

[49] Mirko Hohmann, “German Bundestag Passes New Data Retention Law,” *Lawfare,* October 16, 2015, accessed June 4, 2018, https://www.lawfareblog.com/german-bundestag-passes-new-data-retention-law.

Foreign Policy Challenges

An Unclear Western Narrative Faces a Competitive Alternative

For a while, Western foreign policy makers were able rely on a simple assertion that "there is no alternative"[50] to the model of a free and open internet, governed through multi-stakeholder efforts. That era is long over. Authoritarian nations pursue an alternative model of information security and cyber sovereignty that seeks to justify unchecked governmental control on communication. At the international level, they have started to promote the model with increasing success, with signs of support from nations that that subscribe to neither model. This all comes against the backdrop of a successful economic model in China and the country's ability to use ICT as a leverage to gain influence internationally.

Because the internet governance model that puts protecting the rights of citizens first is challenged by a coherent alternative approach that prizes absolute government control over its citizens, it is vital that it is internally coherent and credible. It should communicate how domestic regulation in democracies is consistent with the approach as it is promoted internationally. In their foreign policy, EU democracies express a "commitment to support an open and free Internet"[51] and the multi-stakeholder approach. At the same time, European countries have been leading the way in enforcing new legislation on online communications, as well as the technology sector more broadly, and have set limits to the free flow of data. The shift toward stronger regulation also comes with a more pronounced role for the government. In domestic policy and legislation processes of liberal democracies, civil society, and the private sector generally have only an advisory function.

Liberal democracies appear inconsistent in their domestic policy processes, because they have never clarified that free and open does not mean "no regulation" and that "multi-stakeholder" in a domestic context does not mean that civil society and business have the same level of decision-making power. Authoritarians see a propagandistic opening in this. They refer to Western regulations to justify their own laws that regulate social media companies. Russia, for example, drew on Germany's network enforcement law to justify its own regulation of social media companies. [52]

Democracies should make it clear that as long as their regulations are approved in democratic processes, do not violate human and citizens' rights, and are enforced in systems with appropriate checks and balances, they are in line with the governance

[50] Bruce W. Jentleson and Steven Weber, *The End of Arrogance: America in the Global Competition of Ideas* (Cambridge: Harvard University Press, 2010), p. 11.

[51] European Union External Action Service, "EU-U.S. Cyber Dialogue" (2016), accessed May 4, 2018, https://eeas.europa.eu/headquarters/headquarters-homepage_en/18132/EU-U.S.%20Cyber%20Dialogue.

[52] Reporters Without Borders, "Russia bill is copy-and-paste of Germany's hate speech law," July 19, 2017, accessed May 8, 2018, https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law.

model. They must be vigilant in adhering to these standards in order to be able to point out the differences when other nations invoke laws passed by democracies as inspiration for their own authoritarian designs.

This is the precondition for liberal democracies to regain the initiative in setting an internet governance agenda globally. There still is much to be said about the internet as a tool to promote values that Western—and many non-Western—governments see as guiding their foreign policy. Bill Clinton's hope that liberty would spread "by cell phone and cable modem"—or smartphone and 5G, for that matter—is still relevant, and the internet is undoubtedly crucial for education and economic growth. The West's perceived inconsistency weakens its ability to work toward that goal and to win new partners along the way. This perception hampers Western efforts at a critical point in time: many nations have not yet clearly decided on which kind of internet policies to pursue. At this juncture, it is necessary to have a clear narrative at hand.

Fragmentation Through Increased Governmental Control

Governments' efforts to segment cyberspace into national jurisdictions can pose a foreign policy challenge in themselves. These efforts to "re-align control of communications with the jurisdictional boundaries of national states"[53] have been particularly pronounced over the last several years, as outlined above. A key result of demands for national solutions to internet-related questions has been an increased splintering of an internet with roughly universal characteristics into different local or regional versions with regards to content and applications available to users—a phenomenon also referred to as "fragmentation" or "digital divergence."[54, 55, 56, 57]

Some have warned that the "process of establishing cyber borders and thus states' sovereignty [online] will be non-linear, dangerous and lengthy."[58] There is a need for a sober look at the implications and side effects of this. In particular, it is important to understand where and how fragmentation is occurring. Accordingly, it helps to take a closer look at what is commonly called the internet. While many think

[53] Stanislav Budnitsky, "Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace," *International Journal of Communication* 11 (2017): 4845-4849, p. 4845. See also Mueller, *Will the Internet Fragment*, p. 17.

[54] Budnitsky, "Milton Mueller," 4845. See also Eli Noam, "#BeyondWCIT. Eli Noam (Columbia University: 'A federated internet is the key and cloud is the glue that will hold it together'," *Key4Biz,* March 20, 2013, accessed May 8, 2018, https://www.key4biz.it/News-2013-03-20-Policy-Eli-Noam-Columbia-University-beyond-dubai-216456/19363/.

[55] Tim Maurer and Robert Morgus, "Stop Calling Decentralization of the Internet 'Balkanization,'" *Slate,* February 24, 2014, accessed May 8, 2018, http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html.

[56] This trend is not alone driven by state actors. Business models, for example through dominant social media platforms, can also drive fragmentation. These are not part of the analysis in this text, though.

[57] Jonah Force Hill, *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers*, Research Report (Cambridge: Belfer Center for Science and International Affairs, 2012), https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf.

[58] Chris Demchak and Peter Dombrowksi, "Cyber Westphalia: Asserting State Prerogatives in Cyberspace" in "International Engagement on Cyber III: State Building on a New Frontier" [Special Issue], *Georgetown Journal of International Affairs* (2013): 29-38, p.11.

of it as one global network, it is more accurately described as a network of networks. Established in a time when global infrastructures did not yet exist, the internet has always linked various smaller networks with each other.[59] These networks vary in size and underlying technology and are operated by thousands of different providers, most of which are private companies. Common standards and protocols have ensured the interoperability of these networks, yet the internet is far from universal.[60] One can think of it as a layered system. The most common system has three levels and is further explained in Textbox 1:[61, 62]

- Physical layer (infrastructure e.g., undersea cables, servers);
- Protocol layer (e.g., IP addresses, protocols);
- Application and content layer (e.g., applications, website content).

National (and international) regulations can impact all three layers. Drake, Kleinwächter, and Cerf (2016) described these efforts as governmental fragmentation, i.e., "policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources."[63] These policies range from content control and censorship over privacy and data protection rules to specific data localization or national routing efforts. They seek to keep information either out of or within a country.[64]

The layered model helps to better understand the impact of national policies in cyberspace. Governmental regulatory efforts are creating different online experiences around the world. However, most of these efforts have focused on the regulation of applications and, especially, content. In other words, much of the fragmentation is taking place *on* the internet, yet there is not necessarily a fragmentation *of* the internet, i.e., of the underlying standards and protocols.[65]

This recognition in turn helps to understand Vinton Cerf's statement that "fragmentation isn't necessarily bad in and of itself."[66] Many of these efforts ultimately result in a decrease in uniformity or universality. Given that cultures and norms vary across the globe, even between like-minded nations such as the US and Germany, it is worth asking at which specific points universality online is both possible and desirable. In light of existing differences in online regulation, countries would either need to

[59] Leslie Daigle, "On the Nature of the Internet," *Global Commission on Internet Governance* no. 7 (2015): p.18.

[60] Laura DeNardis, "One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation," *Global Commission on Internet Governance* no. 38 (2016): p. 1-11.

[61] DeNardis, "One Internet," p. 6. See also Dennis Broeders, *The public core of the Internet: An international agenda for Internet governance* (Amsterdam: Amsterdam University Press, 2016).

[62] The layer system has some drawbacks regarding the protocol layer, since some protocols affect the way the infrastructure works, and other affect the applications that run on it.

[63] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, *Internet Fragmentation: An Overview*. World Economic Forum White Paper (Geneva: World Economic Forum, 2016), p. 4.

[64] Anupam Chander and Uyen P. Le, "Breaking the Web: Data Localization vs. the Global Internet," *UC Davis Legal Studies Research Paper Series,* no. 378 (2014): 1-50, p. 3.

[65] Drake et al., *Internet Fragmentation*.

[66] Internet Governance Forum "IGF 2017 – Day 1 – Room XII – WS48 The Future of Internet Identifier: How the DNS Will Function in a Smart Cyberspace," December 2017, accessed May 8, 2018, https://www.intgovforum.org/multilingual/content/igf-2017-day-1-room-xii-ws48-the-future-of-internet-identifier-how-the-dns-will-function-in.

disagree and develop different policy approaches or create unsatisfactory and unstable compromises.[67]

There still is one risk that should be closely examined: fragmentation at the protocol layer. If governments attempt to impose their restrictive policies on content through such technical changes, the potential fragmentation would be more consequential. It would challenge the core assumption of a neutral layer at the core of the internet. Such efforts would be drastic and difficult to implement, but authoritarian nations have definitely begun thinking about them.[68] Drake, Kleinwächter, and Cerf rightly pointed out that "the establishment of an alternate root that has significant government backing arguably would be the mother of all fragmentations."[69]

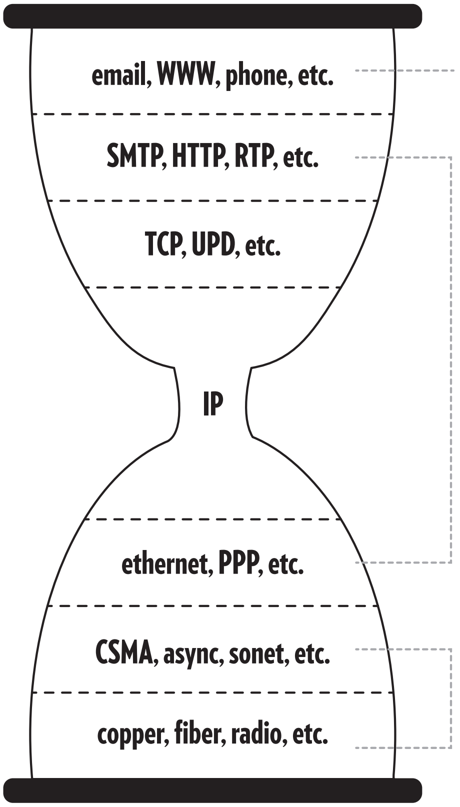
[67] Eli Noam, "Towards the Federated Internet," *InterMEDIA* 41, no. 4 (2013): p. 11.

[68] Kieren McCarthy, "Russia threatens to set up its 'own internet' with China, India and pals – let's take a closer look," *The Register,* December 1, 2017, accessed May 8, 2018, https://www.theregister.co.uk/2017/12/01/russia_own_internet/. See also Dave Burstein, "A Closer Look at Why Russia Wants an Independent Internet," *CircleID,* December 15, 2017, accessed May 8, 2018, http://www.circleid.com/posts/20171215_closer_look_at_why_russia_wants_an_independent_internet/.

[69] Drake et al., *Internet Fragmentation*, p. 29.

Box 1: The Hourglass Model

The Hourglass Model, popularized by Jonathon Zittrain, helps us to understand the classification of layers.[i] The lowest layer makes up the physical infrastructure of the internet, i.e., the cables or waves over which data flows. There is a variety of modes of transportation for data, representing the width of the hourglass: there have always been differences in the hardware that was used, the availability of infrastructure, and the speeds of transmission.[ii] The middle layer refers to the protocols that are in place to transmit data and to ensure "that the sender, the receiver, and anyone necessary in the middle can know the basics of whom the data is from and where the data is going." [iii] These include transport, network, and data-link protocols. The thin waist of the hourglass can be explained by the fewer distinct modes of transmission in place at this level, especially regarding the Internet Protocol (IP), where only two versions exist: IP version 4 and version 6. The top layer refers to applications and content that run on the other layers. This includes a variety of desktop and mobile applications, websites, e-mail clients,and the content that they transfer. In theory, the top of the hourglass should be broader, since there is more diversity on this layer than on any other. There is also the least universality on this layer, since the content that different people can access varies for a variety of reasons.



APPLICATION & CONTENT LAYER
Represents the tasks people might want to perform on the network and the content they access through it.

PROTOCOL LAYER
Establishes consistent ways for data flow so that the sender, the receiver, and anyone necessary in the middle can know the basics of who the data is from and where the data is going.

PHYSICAL LAYER
Constitutes the actual wires or airwaves over which data will flow.

Acronyms

WWW: world wide web
SMTP: simple mail transfer protocol
HTTP: hypertext transfer protocol
RTP: real-time transport protocol
TCP: transmission control protocol
UDP: user datagram protocol
IP: internet protocol
PPP: point-to-point protocol
CSMA: carrier-sense media access

[i] Jonathan L. Zittrain, *The Future of the Internet – And How to Stop It* (New Haven: Yale University Press, 2008), p. 67-68. See also Maurer et al., *Technological Sovereignty*, p. 26, and "Watching the Waist of the Protocol Hourglass," *University of Virginia*, August 2001, accessed May 22, 2018, http://www.cs.virginia.edu/~cs757/slidespdf//////deering-hourglass-london-ietf.pdf.

[ii] DeNardis, "One Internet," p. 2ff.

[iii] Maurer et al., *Technological Sovereignty*. See also John Toon, "Study Shows How the Internet's Architecture Got its Hourglass Shape," *George Tech Research Horizons*, May 3, 2017, accessed May 22, 2018, http://www.rh.gatech.edu/news/69297/study-shows-how-internets-architecture-got-its-hourglass-shape.

Declining Internet Freedom and Rising Economic Costs

The increasing demands for sovereignty online can pose threats to many of the rights, freedoms, and economic gains associated with the internet.

Through regulations at the application and content level, governments have restricted access to information and put pressure on users. This pressure is increasing, as Freedom House's *Freedom on the Net* index reveals. The index measures the level of internet and digital media freedom in 65 countries, looking at obstacles to access, limits on content, and violations of users' privacy in each of them.[70] In 2017, Freedom House found that internet freedom declined in nearly half the countries included in the index, whereas only 13 made—mainly modest—gains.[71] China ranks last despite modest gains, but nations in most regions have experienced declines: Mexico and the US in the Americas, Ethiopia and Egypt in Africa, France and Germany in Europe, Turkey and the United Arab Emirates in the Middle East, and Vietnam and Bangladesh in Asia. All over the world, countries have, to different degrees, blocked access to information or applications, censored or manipulated content, and impeded the work of journalists online.

Clearly, governments have improved their technical and institutional capacity to regulate and control the digital sphere. In parallel, they have begun to put that capacity to use through new laws and regulations. For Western governments, this poses a challenge, since the protection of human rights forms the base of many countries' foreign policy.[72]

Governmental efforts to regulate the internet are likely to introduce friction, potentially reducing connectivity's positive impact on economic growth. Two examples help to explain that correlation. Both Western and non-Western countries have discussed data localization efforts in various forms. Motivations and forms vary,[73] yet all these efforts seek to limit the amount or kind of data that can be stored outside a given country. They would require information providers to build or rent local, domestic server capacity in each of the nations with such legislation, driving up the costs of doing business. [74] Such costs are particularly punitive for small companies or start-ups, introducing barriers to market entry and benefiting large and established companies. Taken together, there are serious concerns that data localization "raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances." [75]

A second example is the different sets of legal requirements for data protection, such as the EU's GDPR. Independently of how one assesses the benefits of such a policy,

[70] "About Freedom on the Net," *Freedom House,* accessed May 8, 2018, https://freedomhouse.org/report-types/freedom-net.

[71] Kelly et al., *Freedom on the Net 2017,* p. 1.

[72] Auswärtiges Amt, "Human Rights – a cornerstone of German foreign policy," accessed May 5, 2018, https://www.auswaertiges-amt.de/de/aussenpolitik/themen/menschenrechte/01-menschenrechte-fundament.

[73] James M. Kaplan and Kayvaun Rowshankish, "Addressing the Impact of Data Location Regulation in Financial Services," *Global Commission on Internet Governance* no. 28 (2016): 35-40, p. 36. See also Force Hill, "The Growth of Data Localization."

[74] Force Hill, "The Growth of Data Localization," p. 31.

[75] Chander and Le, "Breaking the Web," p. 34.

it is fairly easy to identify the costs that are associated with it. Organizations of all sizes are required to carry out audits, streamline their policies for handling data, establish data protection officers, and so forth. While no reliable research is available to put a specific number to these changes, they are definitely raising the costs of doing business. Some have argued that the GDPR will limit the development of future technologies such as artificial intelligence[76] or blockchain technology[77] and thereby limit innovation and productivity.

European legislators were aware of these side effects when they advanced the GDPR as a means to protect user privacy. This is the case with many regulations, and the point here is not to criticize the costs associated with the GDPR. It is instead to emphasize that many of the efforts outlined above are raising the costs of doing business, especially for smaller organizations, with a potential negative impact on development and innovation. This should not be taken lightly by foreign policymakers, who often see seek to promote trade and international business.[78]

A final note on China: the Chinese government has obviously been willing to bear some of the costs outlined above. Not only are there costs associated with implementing the surveillance apparatus, but the apparatus itself has also dramatically limited data flows into and out of the country. The Chinese Government further used protectionist measures to protect their own private sector from foreign competition. These efforts all came with costs that had to be borne by the government, companies, and/or consumers. Still, Chinese economic growth has been astonishing in the last decade, and Chinese companies have become market leaders in many technical fields. What is important to point out here is the difference of the Chinese market, principally its enormous size. The judgement is still out on whether the approach has long-term success, but part of the reasons for its success so far is the massive number of users and consumers within the country. With such a user base, the country was able to seal itself off and still make use of network effects and economies of scale. It seems unlikely that countries with much smaller populations would be able to repeat the success.

[76] Nick Wallace and Daniel Castro, “The Impact of the EU’s New Data Protection Regulation on AI,” *Center for Data Innovation,* March 27, 2018, accessed May 8, 2018, http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

[77] David Meyer, “Blockchain technology is on a collision course with EU privacy law,” *International Association of Privacy Professionals,* February 27, 2018, accessed May 8, 2018, https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

[78] Auswärtiges Amt, “External economic policy,” accessed May 7, 2018, https://www.auswaertiges-amt.de/de/aussenpolitik/themen/aussenwirtschaft.

Reinvigorating the European Internet Foreign Policy Agenda

The model of governmental control promoted by authoritarian actors can be appealing. Many ruling elites are attracted by the promise of enabling the government to comprehensively control the lives of citizens through technological means. China, Russia, and others readily make both the conceptual framework and the necessary hard- and software available to other governments.

These developments are concerning. Not only do they threaten to reverse progress made on human rights such as the freedom of expression and assembly, they also impose economic costs that can limit development and innovation. Democracies, especially in Europe, urgently need to organize to reverse these trends. Their ability to do so is currently hampered by charges of hypocrisy, as many liberal democracies have intensified their efforts to regulate the information space. These policy interventions are driven by (perceived) domestic needs to protect citizens or ensure the enforcement of laws online. At the same time, they strengthen governmental influence and limit the free flow of information, leading to criticism that Western nations are not practicing what they preach.

In our opinion, while this is not the case, these concerns need to be addressed. Doing so is necessary to strengthen Western credibility during times in which various actors promote divergent policy ideas in international fora. If Eli Noam is right that "the standardized Internet is the past but not the future,"[79] it is necessary to have a coherent and useful model to offer.

In the following section we suggest areas of action on which policymakers in Europe and liberal democracies globally could focus in order to strengthen their model. First, it is necessary to begin at home and improve the coherence of our own agenda and the messaging related to it. On that basis, we suggest ideas for how to work with additional partners in order to counter the threat arising from authoritarian states. Finally, we take a closer look at how to address fragmentation, i.e. the the seemingly inevitable trend of governmental regulation and the accompanying turn toward a more segmented internet.

[79] Noam, "#BeyondWCIT."

Strengthening European Credibility and Messaging

(1) Developing and promoting a coherent narrative on the rule of law online

European and, more broadly, Western governments need to self-confidently project a narrative on the democratic rule of law online. This means correcting the misunderstanding that a "free and open internet" precludes responsible government intervention. Some might see it that way or might have seen it that way when the internet first spread. Yet the baseline of absolute non-interference is profoundly misguided. Free, open societies follow laws and democratically elected governments create them. The internet should not be—and has never fully been—a libertarian Wild West where government has no place.

Democratic governments have responsibilities *vis-à-vis* their citizens, such as protecting citizens' rights and providing public goods such as security and safety. To pursue these objectives, it is necessary to make trade-offs between different rights and freedoms. These trade-offs need to be made both online and offline. Even fundamental rights such as the right to freedom of expression can be curtailed, but only on specific grounds. The recognized standard for restrictions is that they are provided for by law, implemented in narrowly defined circumstances, in line with the principles of necessity and proportionality, and ensure appropriate safeguards, such as transparent procedures and avenues for appeal.[80]

Governments have a duty to provide for the rule of law online the same way they do offline, and this is part of the agenda that they should promote abroad.[81] It is important that they follow the same legal processes and standards as they have in the past. Power can be abused, and the necessary checks and balances need to be in place to prevent that.

There should then be more emphasis on these mechanisms and adherence to them. One can also distinguish between the legality of policies pursued by different nations. If Germany mandates data localization as part of a data retention law, one can argue about the appropriateness of the overall law and whether it is overly infringing on individual freedoms. Yet, there are clear legal processes in place for law enforcement to access that data. Independent judges decide on these requests, and there are ways for providers to challenge them. If a country such as Russia were to adopt a similar law, it would do so in a qualitatively different regulatory framework, and this difference needs to be stressed.

[80] Kelly et al., *Freedom on the Net 2017*. See also United Nations General Assembly, *Universal Declaration of Human Rights,* A/RES/217, December 10, 1948, art. 29.

[81] It is important to note that the UN Group of Governmental Experts Developments in the Field of Information and Telecommunications in the Context of International Security has already has already agreed that "[i] nternational law, and in particular the Charter of the United Nations, is applicable, and is essential in maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." See Council on Foreign Relations, "The UN GGE on Cybersecurity: How International Law Applies to Cyberspace" (April 14, 2015), accessed June 4, 2018, https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace.

(2) Exposing the costs of the authoritarian model

Supporters of the authoritarian model of internet governance are not shy about their designs. In April 2018, Chinese President Xi stressed the need to "create a comprehensive cyber governance structure that integrates economic, legal, and technological approaches," and demanded that within it, it will be the "Party Committees who will take the lead, the government that will manage, enterprises that will carry out responsibilities, society that will supervise, and netizens who will self-discipline."[82] He also talked about the need to "strengthen online positive propaganda, unequivocally adhere to the correct political direction, and [guide] public opinion." [83]

China self-confidently promotes the virtues of its approach, as well as the surveillance technologies that underpin it. It is important for Western political actors and NGOs to expose the costs of this approach. The use of technology serves one goal: asserting the state's absolute control over the citizenry. The most draconian form of the surveillance state can be seen in China's western region of Xinjian where "the Chinese Communist Party (CCP) has updated its old totalitarian methods with cutting-edge technology"[84] to monitor the Uighur population: high-tech tools are deployed "in the service of creating a better police state."[85] In addition to blocking services and content, these new tactics include collecting DNA during medical check-ups, installing GPS trackers in all cars, and forcing government-controlled applications onto users.[86] This is one face of the authoritarian surveillance state. The other, seemingly less draconian face, is the social credit system which uses positive incentives to "nudge" citizens to behave in the desired way.

What is missing from this narrative are the costs associated with such high-technology authoritarianism. These costs are, first of all, human. The measures take a toll on basic human rights. That may well not disturb authoritarian elites all that much, but the side-effects of building a high-tech police state may be of greater concern. As *The Economist* points out for China's western provinces:

> "China's Communist rulers believe their police state limits separatism and reduces violence. But by separating the Uighur and Han further, and by imposing huge costs on one side that the other side, for the most part, blithely ignores, they are ratcheting up tension. The result is that both groups are drifting towards violence."[87]

[82] Rogier Creemers et al., "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference," *New America,* April 30, 2018, accessed June 4, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

[83] Creemers et al., "Translation: Xi Jinping's April 20 Speech."

[84] James A. Milward, "What It's Like to Live in a Surveillance State," *New York Times,* February 3, 2018, accessed June 4, 2018, https://www.nytimes.com/2018/02/02/opinion/china-uighurs-xinjiang.html.

[85] Milward, "What It's Like to Live in a Surveillance State."

[86] Milward, "What It's Like to Live in a Surveillance State."

[87] "China has turned Xinjiang into a police state like no other," *The Economist*, May 31, 2018, accessed June 4, 2018, https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other.

In addition, there are indirect financial burdens that incur to companies when they must navigate an internet that is severed from the rest of the world. As mentioned above, China is faring economically well, but the Chinese market is unique due to its size and the capital available to the state and companies. Other nations, even larger countries such as Russia or Iran, have not been able to gain similar successes. If companies are seen as key to maintaining and developing a high-tech authoritarian surveillance society, that may also hamper their ability to do business outside authoritarian countries. This is what we have seen which Chinese technology companies that have come under scrutiny in the US, Europe and Australia. Democratic governments should not shy away from exposing the costs of an approach that puts the absolute control of the state, not the rights and protections of citizens, first.

Winning New Allies and Building Coalitions

When it comes to setting the agenda internationally, an important first step is to ensure coherence among one's own allies, be it within the Organization for Economic Co-operation and Development (OECD), the EU, or an institution like the Freedom Online Coalition (FOC).[88] A starting point should be to share lessons learned and ensure that cross-border side effects remain minimal among like-minded nations. In addition to working within existing partnerships, it will be necessary to cooperate with less traditional partners to address the risks outlined above. This requires steps in various directions, as suggested below.

(3) Engage key non-Western powers and "swing states"

A first step is to ensure the proper framing in various forms. One issue is to address the above-mentioned charges of hypocrisy. This not only improves one's own credibility, but also to increases the attractiveness of the free and open internet approach to other nations. At the same time, it is important to stress the openness of the internet not just in terms of its infrastructure, but also in terms of its values. Although the idea of an open, free internet was developed within the Western circles, it is not a purely Western idea. Many of the actors involved regularly stress the internet's openness to new ideas and concepts—for good reasons. It is therefore equally important not to limit the internet to a specific set of values, as the current US administration has unfortunately done in a recent Executive Order: "the internet is a United States invention, it should reflect American values as it continues to transform the future for all nations and all generations."[89] Statements with strong senses of entitlement do not invite others to contribute, but limit the scope of potential partners.[90]

[88] The Freedom Online Coalition is a group of 30 governments that work to advance internet freedom and protect human right online. See Freedom Online Coalition, "About Us," 2018, accessed June 4, 2018, https://freedomonlinecoalition.com/about-us/about/.

[89] White House, "President Trump Protects America's Cyber Infrastructure," 2017, accessed May 7, 2018, https://www.whitehouse.gov/briefings-statements/president-trump-protects-americas-cyber-infrastructure/.

[90] Jentleson and Weber, *The End of Arrogance*.

A second step is to decide with whom to work more closely. As in any bureaucracy, there are limited resources within the foreign policy apparatus and thus a need to prioritize. A starting point could be identifying overlapping values—such as internet freedom—and the stances that other governments take toward them. Freedom House provides an overview of this, and the most recent ranking can be found in Figure 2. The country scores of "free," "partly free," and "unfree" are reflected in the colors green, yellow, and red, respectively. Nations ranked "unfree" are the least likely to be to be swayed in their approach, yet continued pressure should still be placed on them. It is the nations ranked "partly free" that should be the focus of these attentions, as they are perhaps more receptive to influence.

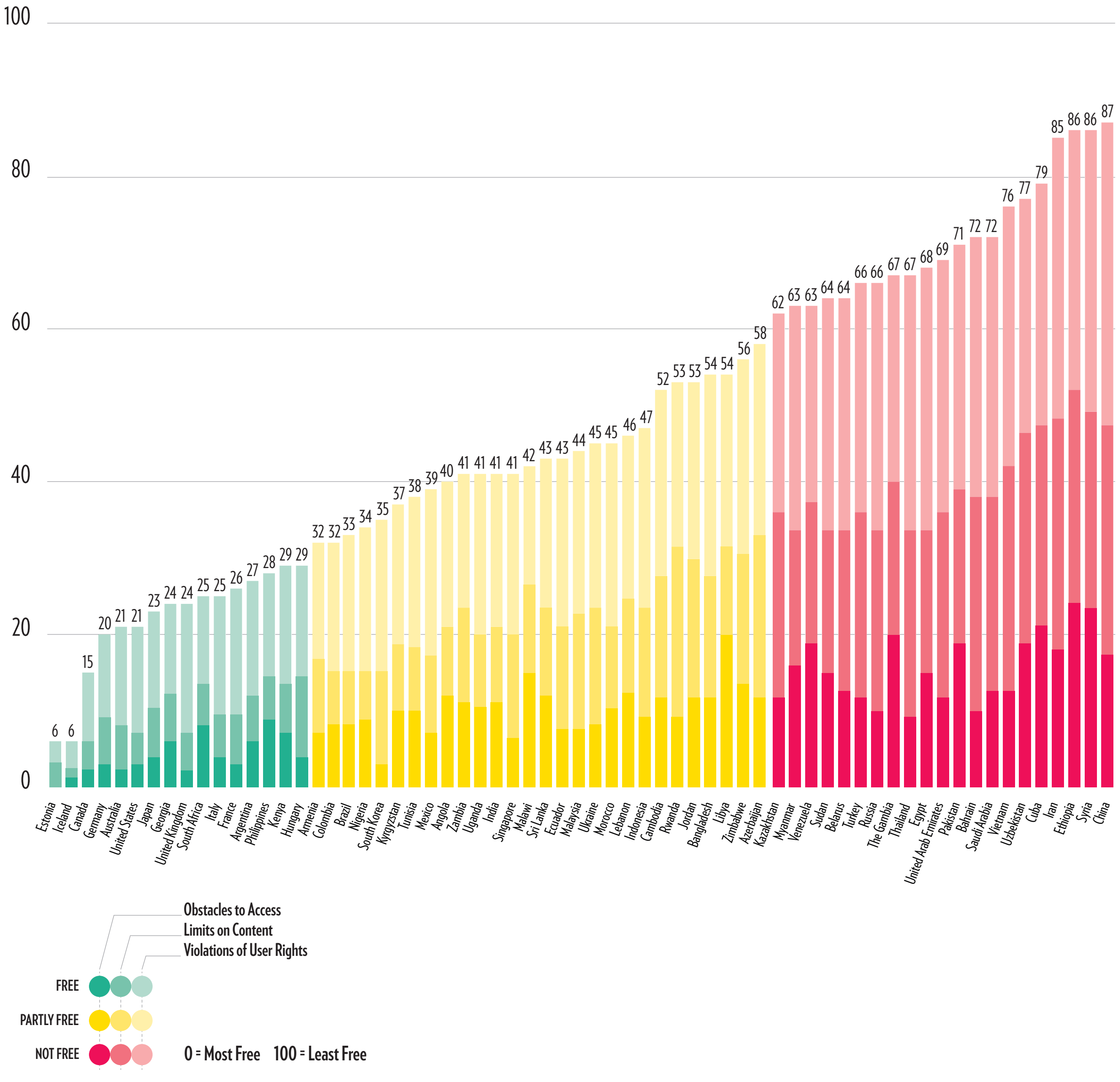


Figure 2: Internet Freedom Country Score Comparison (Source: Freedom House)

An even better starting point is in the analysis of relevant "swing states", i.e., states that fall into neither of the two governance approaches, which could still have a significant diplomatic impact and could therefore "shape what norms and institutions will govern various aspects of international relations in the future, including the Internet."[91] A 2014 study used a systemic approach to point out these states. The analysis was built around nations' voting records at the 2012 World Conference on International Telecommunications and took into account other relevant indicators, such as population size, membership in various international fora, and the ability to influence international debate. [92] The results can be found in Table 1.

Against the ITRs[93]	**For the ITRs, but...**		
I	II	III	IV
	... OECD Member	... FOC Member	... potential swing states based on indicators
Albania	Mexico	Ghana	Argentina
Armenia	South Korea	Tunisia	Botswana
Belarus*	Turkey		Brazil
Colombia			Dominican Republic
Costa Rica			Indonesia
Georgia			Jamaica
India			Malaysia
Kenya			Namibia
Moldova			Panama
Mongolia			Singapore
Peru			South Africa
Philippines			Uruguay
Serbia			

Table 1: Top 30 Swing States (Source: Maurer and Morgus, *Tipping the Scale*)

The results provide relevant insights into which nations to potentially work with. Unfortunately, the overview is based on a one-time voting behavior in 2012. Similar research, if conducted on a regular basis, could provide more up-to-date analysis to decision-makers and better inform policy processes.

Nevertheless, a few key nations stand out even without further analysis. Among them are India and Brazil, who fall into the category of swing states and are ranked as "partly free" on internet freedom. Both nations have the capacity to shape norms and rules internationally. In addition, through multilateral fora such as the BRICS, they engage with Russia and China on a regular basis, including on issues of internet governance. The question is then how to work more closely on these issues with specific nations. The bilateral "cyber dialogues" that Germany, the EU, and other nations are currently pursuing are one way to go about it. These provide a way to learn about each

[91] Maurer and Morgus, *Tipping the Scale*.

[92] Maurer and Morgus, *Tipping the Scale*.

[93] ITRs: International Telecommunication Regulations.

other's positions and address concerns. Such bilateral conversations can be a starting point for cooperation in international fora. One idea is to try and integrate them in the FOC.[94] Membership in such an organization would commit nations to a clear set of principles. The key question will be how to compromise on accepting nations with less-than-stellar human rights records. Yet, within reason and depending on an individual assessment of cases, compromises will be necessary to enlarge the group of members.

(4) Helping to create access and build capacity with selected partner countries

Two important areas of engagement with new partners are capacity building and infrastructure support for creating internet access. These issues are important for several reasons.[95] To begin with, they are a means to help other nations reap the benefits of digitization, enabling development and economic growth. In turn, other nations can benefit from increased cross-border business. A similar argument holds true for building cybersecurity capacity: it is an important tool to protect the potential gains that arise from digitization, but also limits the negative implications of cross-border transactions, such as the rise of international cyber criminality.

Finally, support for building technical infrastructure, as well as cyber capacity, could also be part of the foreign policy toolkit. As outlined above, China has developed a strategic plan to build a digital silk road, and it is not just doing so for the assumed economic benefits. To a degree, these efforts should be welcomed, since they help enhance connectivity. At the same time, they are tools to create market access for the Chinese private sector and are likely to be accompanied by political pressure to adopt a specific model of internet governance.

European foreign policy makers should carefully monitor these developments and improve their own efforts. More development aid can be shifted towards ICT projects, and these should then take human rights implications into account. Such human rights standards would also make it harder for Chinese companies to bid on projects that international organizations, like the World Bank, develop. Otherwise, state-backed companies can and will regularly outcompete Western companies.

(5) Holding corporations accountable

The private sector is a key stakeholder: corporations play an important role not just as providers of core technical infrastructures, but also as an intermediary between users and governments. Much of the data used by governments for law enforcement or intelligence purposes is first gathered by companies. Companies also often develop the tools that are used by governments in these efforts. The private sector therefore

[94] Freedom Online Coalition, "Freedom Online Coalition," 2018, accessed June 4, 2018, https://freedomonlinecoalition.com/.

[95] Mirko Hohmann, Alexander Pirang, and Thorsten Benner, *Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach.* GPPi Policy Paper. (Berlin: Global Public Policy Institute, 2017), p. 4, http://www.gppi.net/fileadmin/user_upload/media/pub/2017/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.

plays an important role in the protection of privacy, especially in countries with a poor human rights record. Some even go a step further, arguing that multinational businesses "provide a counterweight to alignment and a commitment to global access, open markets, and interoperability."[96]

Western technology corporations certainly like to portray themselves as fighting for individual rights. Apple CEO Tim Cook has called privacy a fundamental human right,[97] and Apple challenged the US Federal Bureau of Investigation publicly and legally when it sought to access information saved on an encrypted iPhone following the San Bernardino attack.[98] At the same time, it was Cook who claimed to share China's vision of an open digital economy when talking at the Wuzhen Summit. Apple also just recently removed a variety of Virtual Private Network applications from the Apple Store on order of the Chinese government, making it harder for Chinese citizens to access blocked sites and content.[99] There is a certain hypocrisy to this and it stresses a key point: Tim Cook and other CEOs are ultimately responsible to their shareholders.

Given the key status of the private sector as an intermediary, as well as its ability to provide additional checks and balances in authoritarian nations, Western governments need to strengthen existing frameworks to force companies to consider human rights issues in their business models. After all, companies do not act in a legal vacuum.

International law and norms are a starting point to hold companies accountable. Both the UN General Assembly and the Human Rights Council have called on businesses to "meet their responsibility to respect human rights [...] including the right to privacy in the digital age," to "inform users about the collection, use, sharing and retention of their data," and "to establish transparency policies."[100] The UN General Assembly has also welcomed the voluntary transparency reports that companies have produced to shed light on the ways in which governments around the world seek to access user data.[101] Transparency reports are just one way for companies to live up to their responsibilities. Publishing guidelines on decision-making processes about government requests is another way for them to help protect citizens' rights, as are their terms of services. If companies aligned them more closely with human rights law, "states will find it harder to exploit them to censor content."[102] It is up to international institutions, civil society, and individual governments to monitor the private sector and hold it accountable.

[96] Mueller, *Will the Internet Fragment*, p. 80.

[97] "Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right,'" *National Public Radio,* October 1, 2015, accessed June 4, 2018, https://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right.

[98] "A Message to Our Customers," *Apple,* February 16, 2016, accessed June 4, 2018, https://www.apple.com/customer-letter/.

[99] Brian Fung, "Apple is pulling VPNs from the Chinese App Store. Here's what that means," *Washington Post,* July 31, 2017, accessed June 4, 2018, https://www.washingtonpost.com/news/the-switch/wp/2017/07/31/apple-is-pulling-vpns-from-the-chinese-app-store-heres-what-that-means/?utm_term=.ad6fc6f4c70b.

[100] United Nations General Assembly, Resolution 71/199, *The right to privacy in the digital age,* January 25, 2017, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199. See also United Nations Human Rights Council, Resolution 34/7, *The right to privacy in the digital age,* April 7, 2017, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement.

[101] UN General Assembly, Resolution 71/199, January 25, 2017.

[102] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/38/35, April 6, 2018, accessed June 4, 2018, https://freedex.org/a-human-rights-approach-to-platform-content-regulation/.

Making Fragmentation Work

Fragmentation through governmental efforts to align communications infrastructures with national borders has been mentioned as one of the key challenges. Our assumption is that nations will not stop such efforts any time soon, yet that there is an overwhelming international interest to properly guide them.

(6) Taking cross-border implications into account

Legal standards and processes are the minimum requirement for new national policies. Yet due to the interconnected nature of the internet, policy-makers should also think about the cross-border implications of new laws and regulations. The success of the internet over the past decade has led to a global infrastructure, and any unilateral actions of one nation will almost inevitably have an impact on others.[103] Such externalities are not necessarily considered. This recommendation is reflected in the Council of Europe's agreement that states are responsible for avoiding "adverse transboundary impact on access to and use of the Internet" when enforcing national jurisdictions.[104]

Others have even gone as far as to prescribe a Kantian categorical imperative for Internet regulation: any policy which, if adopted, would incur detrimental outcomes around the world should not be adopted in the first place.[105] It is likely to be impossible to agree on a common understanding of "detrimental outcomes," yet some steps in this direction could be taken. First, lawmakers could add a new category to the evaluation process in domestic legislative decision-making. Just as they usually point out the costs of new legislation, lawmakers should spell out its potential transnational impact. The OECD's Internet Policy-Making Principles can provide a useful starting point for such an evaluation, since they have been specifically designed to "help preserve the fundamental openness of the Internet while concomitantly meeting certain public policy objectives."[106] This could be complemented by a comparison on the international level: Ott and Zylberberg have suggested the creation of a Fragmentation Impact Assessment framework to examine how a specific policy affects the different layers of the internet and whether it constrains private and/or state actors in their operations.[107] Such an assessment could be done by an independent body, helping to focus public attention and provide arguments for affected stakeholders who seek to raise the issue with the respective government.

[103] De La Chapelle and Fehlinger, "Jurisdiction on the Internet," p. 84.

[104] Council of Europe, "Recommendation CM/Rec (2011) 8 of the Committee of Ministers to Member States on the Protection and Promotion of the Universality, Integrity and Openness of the Internet" (2011), quoted in de La Chapelle and Fehlinger, "Jurisdiction on the Internet," p. 85.

[105] De La Chapelle and Fehlinger, "Jurisdiction on the Internet," p. 83.

[106] Organization for Economic Co-operation and Development, "COMMUNIQUÉ on Principles for Internet Policy-Making" (2011), accessed May 7, 2018, https://www.oecd.org/internet/innovation/48289796.pdf.

[107] Nikolas Ott and Hugo Zylberberg, "Cyber Sovereignty and Online Borders Do Not Improve International Security," *Council on Foreign Relations,* October 2, 2017, accessed June 4, 2018, https://www.cfr.org/blog/cyber-sovereignty-and-online-borders-do-not-improve-international-security.

(7) Ensuring and improving technical and legal interoperability

Limiting fragmentary trends is one step; keeping and increasing interoperability another. Instead of focusing the conversation on the universality of the internet at the content and application level, a focus should be on legal and technical interoperability to maintain global connectivity.

With regards to legal interoperability, the harmonization, standardization, and mutual recognition of laws (e.g., agreeing on and institutionalizing common principles and standards, or recognizing the equivalence of different laws) are the three key mechanisms.[108] In order to bring these about, conversations will need to be much more issue-specific. The Budapest Convention is a step in the right direction in its efforts to fight cybercrime and increase cooperation and harmonization among signatories. Many more conversations are taking place regarding economic questions. The EU's Digital Single Market (DSM) is a great example of an effort to enable free flow of data and information, and the Association of Southeast Asian Nations (ASEAN) has also announced plans to intensify corporation.[109] Similarly, e-commerce has been discussed in various fora that deal with trade more broadly: The Trans-Pacific Partnership (TPP) includes provisions on the limitation of data localization and cross-border data flows, for example, for the finance industry.[110] There are also discussions at the World Trade Organization (WTO) about how to adapt its frameworks to e-commerce.[111] Such issue-specific agreements can be fostered in a variety of settings and institutions and provide a way to counter some of the ongoing fragmentary trends.

With regards to technical interoperability, it is important to keep in mind that the internet has always been a "network of networks." Its original purpose was to link different local networks through interoperable protocols, and various actors shared resources to achieve global reach.[112] The key here is that the narrow middle of the hourglass model deserves special attention. A fragmentation at the protocol layer would be the "mother of all fragmentations,"[113] and any efforts in this direction should therefore be monitored closely. The Dutch Scientific Council has even proposed a norm to safeguard the internet's main protocols and infrastructure—what they call the internet's public core—"against unwarranted intervention by states."[114] Defining

[108] Rolf H. Weber, "Legal Interoperability as a Tool for Combatting Fragmentation," *Global Commission on Internet Governance* no. 4 (2014): 5-13, p. 10.

[109] European Commission, "Digital single market" (2018), accessed June 4, 2018, https://ec.europa.eu/commission/priorities/digital-single-market_en. See also Vivien Shiao, "Innovation, digital economy key areas for Singapore's Asean chairmanship: Lim Hng Kiang," *Straits Times,* March 1, 2018, accessed June 4, 2018, https://www.straitstimes.com/business/economy/innovation-digital-economy-key-areas-for-singapores-asean-chairmanship-lim-hng.

[110] Ron Cheng, "Open E-Commerce Data Flows in the New Non-US TPP," *Forbes,* March 14, 2018, accessed June 4, 2018, https://www.forbes.com/sites/roncheng/2018/03/14/open-e-commerce-data-flows-in-the-new-non-us-tpp/#770f1fa6663e.

[111] Angelica Mari, "Brazil demands rules on data flows from WTO," *ZDnet,* April 16, 2018, accessed June 4, 2018, https://www.zdnet.com/article/brazil-demands-rules-on-data-flows-from-wto/.

[112] Daigle, "On the Nature of the Internet," p. 18.

[113] Drake et al., *Internet Fragmentation*.

[114] Dennis Broeders, "Aligning the international protection of 'the public core of the internet' with state sovereignty and national security," *Journal of Cyber Policy* 2, no. 3 (2017): p. 367.

unwarranted interventions in such a setting would be a challenge, but the idea points in the right direction: The internet's core is key to technical interoperability and must be protected from governmental efforts to impose national policies on their citizens.

Outlook

Earlier this year, US academic Jack Goldsmith decried the "failure of internet freedom."[115] We need to be more precise. It is the ultra-libertarian version of "free and open" that originated in the US more almost 30 years ago that has not withstood the test of time.

Authoritarian nations, who could never reconcile the free flow of information with the closed societies that they pursue, have self-confidently pursued the approach of an "unfree and closed" internet. Over the past decade, countries like China and Russia have built up the technical capacity and legal frameworks to control content and applications. In parallel, they have been offering these capacities and rules abroad, together with a sovereigntist model of internet governance that places governments clearly in control of the information space. At the same time, liberal democracies, especially in Europe, have moved away from a laissez-faire approach to internet governance and taken a stronger regulatory stance to fulfil their responsibility to shape policy online, just as they do offline.

From a European foreign policy perspective, this parallel trend of a strengthened authoritarian narrative and growing regulatory action at home creates several challenges. To begin with, the perceived hypocrisies between what we preach and what we practice weakens our diplomatic efforts and therefore the ability to win allies internationally. Second, global governmental efforts to align communications infrastructures with national borders have led to the increasing fragmentation of the internet at the content and application level and could affect the technical infrastructure of the internet. Finally, the increasing ability of authoritarian nations to technically implement the state-centric governance model has led to a continued decrease of internet freedom and limited international data flows, which has a negative economic impact.

These developments have several implications for European foreign policymakers. First of all, in order for them to be able to assert themselves in this competition for global order, there is a need to better understand the agendas of authoritarian nations. In parallel, credibility and messaging from liberal democracies should be improved to offer a coherent narrative. On that basis, it is possible to strengthen cooperation and coordination with existing partners and establish new partnerships, both governmental and non-governmental. Finally, the challenge of further fragmentation of the internet should be taken seriously and countered where possible, for example, through improved legal and technical interoperability.

Most importantly, the developments as outlined in this study should not be seen as separate from broader geopolitical challenges: there is a competition for global order

[115] Jack Goldsmith, *The Failure of Internet Freedom*. Knight Institute Emerging Threats Paper. (New York: Knight First Amendment Institute, 2018), https://knightcolumbia.org/sites/default/files/content/Emerging_Threats_Goldsmith.pdf.

in which authoritarian states like China and Russia have begun to present their own ideas. At the same time, many other non-Western nations also do not just want to be socialized into a Western-dominated order. For Europe and its allies, it is time to enter the competition with a clear understanding of the challenges from abroad as well as a clear idea of their own goals and ways to shape global (internet) governance. “Free and open” — if correctly understood — is still the appropriate guiding star for European internet (foreign) policy.

References

Apple. “A Message to Our Customers.” February 16, 2016. Accessed June 4, 2018. https://www.apple.com/customer-letter/.

Arkko, Jari. “IETF Diversity Update.” *IETF,* December 4, 2015. Accessed June 4, 2018. https://www.ietf.org/blog/ietf-diversity-update/.

Auswärtiges Amt. “External economic policy.” Accessed May 7, 2018. https://www.auswaertiges-amt.de/de/aussenpolitik/themen/aussenwirtschaft.

Auswärtiges Amt. “Human Rights – a cornerstone of German foreign policy.” Accessed May 5, 2018. https://www.auswaertiges-amt.de/de/aussenpolitik/themen/menschenrechte/01-menschenrechte-fundament.

Bajaj, Kamlesh. “As Trump Dampens US’s Internet Freedom Agenda, the Race to Cyber Supremacy Reaches New Levels.” *The Wire,* August 21, 2017. Accessed May 7, 2018. https://thewire.in/169461/trump-cyber-diplomacy-nsa-internet-freedom-agenda/.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *World Economic Forum,* February 8, 2018. Accessed May 8, 2018. https://www.weforum.org/agenda/2018/02/a-declaration-of-the-independence-of-cyberspace/.

Benner, Thorsten and Mirko Hohmann. “Internet companies can’t be judges of free speech.” *Politico,* April 27, 2017. Accessed May 8, 2018. https://www.politico.eu/article/internet-companies-not-free-speech-judges-facebook-twitter/.

Broeders, Dennis. “Aligning the international protection of ‘the public core of the internet’ with state sovereignty and national security.” *Journal of Cyber Policy* 2, no. 3 (2017): p. 366-376.

Broeders, Dennis. *The public core of the Internet: An international agenda for Internet governance.* Amsterdam: Amsterdam University Press, 2016.

Budnitsky, Stanislav. “Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace.” *International Journal of Communication* 11 (2017): 4845-4849.

Burstein, Dave. “A Closer Look at Why Russia Wants an Independent Internet.” *CircleID,* December 15, 2017. Accessed May 8, 2018. http://www.circleid.com/posts/20171215_closer_look_at_why_russia_wants_an_independent_internet/.

Chander, Anupam and Uyen P. Le. “Breaking the Web: Data Localization vs. the Global Internet.” *UC Davis Legal Studies Research Paper Series,* no. 378 (2014): 1-50.

Cheng, Ron. “Open E-Commerce Data Flows in the New Non-US TPP.” *Forbes,* March 14, 2018. Accessed June 4, 2018. https://www.forbes.com/sites/roncheng/2018/03/14/open-e-commerce-data-flows-in-the-new-non-us-tpp/#770f1fa6663e.

“China has turned Xinjiang into a police state like no other.” *The Economist,* May 31, 2018. Accessed June 4, 2018. https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other.

Chuanying, Lu. “China’s Emerging Cyberspace Strategy.” *The Diplomat,* May 24, 2016. Accessed May 22, 2018. https://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/.

Cook, Tim. “Apple CEO Tim Cook: ‘Privacy Is A Fundamental Human Right.” *All Things Considered,* interviewed by Robert Siegel, October 1, 2015. Accessed June 4, 2018. https://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right.

Council on Foreign Relations. "The UN GGE on Cybersecurity: How International Law Applies to Cyberspace." April 14, 2015. Accessed June 4, 2018. https://www.cfr.org/blog/un-gge-cybersecurity-how-international-law-applies-cyberspace.

Creemers, Rogier. "China's Social Credit System: An Evolving Practice of Control." University of Leiden, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792.

Creemers, Rogier, Paul Triolo and Graham Webster. "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference." *New America,* April 30, 2018. Accessed June 4, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

Daigle, Leslie. "On the Nature of the Internet." *Global Commission on Internet Governance* no. 7 (2015): 1-16.

de La Chapelle, Bertrand and Paul Fehlinger. "Jurisdiction on the Internet: From Legal arms Race to Transnational Cooperation." *Global Commission on Internet Governance* no. 28 (2016): 81-96.

Deering, Steve. "Watching the Waist of the Protocol Hourglass." *University of Virginia*, August 2001. Accessed May 22, 2018. http://www.cs.virginia.edu/~cs757/slidespdf//////deering-hourglass-london-ietf.pdf.

Demchak, Chris and Peter Dombrowksi. "Cyber Westphalia: Asserting State Prerogatives in Cyberspace." In "International Engagement on Cyber III: State Building on a New Frontier" [Special Issue], *Georgetown Journal of International Affairs* (2013): 29-38.

DeNardis, Laura. "One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation." *Global Commission on Internet Governance* no. 38 (2016): 1-11.

Denyer, Simon. "Apple CEO backs China's vision of an 'open' Internet as censorship reaches new heights." *Washington Post,* December 4, 2017. Accessed May 8, 2018. https://www.washingtonpost.com/news/worldviews/wp/2017/12/04/apple-ceo-backs-chinas-vision-of-an-open-internet-as-censorship-reaches-new-heights/?utm_term=.7e7ab9e3ad2b.

Department of Defense. "The DoD Cyber Strategy." 2015. Accessed May 7, 2018. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Dewey, Caitlin. "Merkel calls Internet 'unchartered territory,' earns Web's endless mockery." *Washington Post*, June 20, 2013. Accessed May 8, 2018. https://www.washingtonpost.com/news/worldviews/wp/2013/06/20/merkel-calls-internet-uncharted-territory-earns-webs-endless-mockery/?noredirect=on&utm_term=.dc770eeaf0c7.

Die Bundesregierung. "Digitale Agenda 2014-2017." 2014. Accessed May 3, 2018. https://www.digitale-agenda.de/Content/DE/_Anlagen/2014/08/2014-08-20-digitale-agenda.pdf;jsessionid=B4CBFD2649B9E36D4E62A1472E1D7B9F.s6t2?__blob=publicationFile&v=6.

Drake, William J., Shanthi Kalathil, and Taylor Boas. "Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba." *Carnegie Endowment for International Peace,* October 23, 2000. Accessed May 8, 2018. http://carnegieendowment.org/2000/10/23/dictatorships-in-digital-age-some-considerations-on-internet-in-china-and-cuba-pub-531.

Drake, William J., Vinton G. Cerf, and Wolfgang Kleinwächter. *Internet Fragmentation: An Overview.* World Economic Forum White Paper. Geneva: World Economic Forum, 2016.

Economy, Elizabeth C. "Beijing's Silk Road Goes Digital." *Council on Foreign Relations,* June 6, 2017. Accessed May 8, 2018. https://www.cfr.org/blog/beijings-silk-road-goes-digital.

European Commission. "Digital single market." 2018. Accessed June 4, 2018. https://ec.europa.eu/commission/priorities/digital-single-market_en.

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. Accessed May 4, 2018. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

European Union External Action Service. "EU-U.S. Cyber Dialogue." 2016. Accessed May 4, 2018. https://eeas.europa.eu/headquarters/headquarters-homepage_en/18132/EU-U.S.%20Cyber%20Dialogue.

Federal Communications Commission. "Statement of Commissioner Robert M. McDowell." 2012. Accessed May 3, 2018. https://apps.fcc.gov/edocs_public/attachmatch/DOC-313082A1.txt.

Fidler, David P. "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations." *ASIL Insights* 17, no 6 (2013). https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision.

Force Hill, Jonah. *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers*. Research Report. Cambridge: Belfer Center for Science and International Affairs, 2012, https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf.

Force Hill, Jonah. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders." *Lawfare Research Paper Series* 2, no. 3 (2014): 1-41. https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

Freedom House. "About Freedom on the Net." Accessed May 8, 2018. https://freedomhouse.org/report-types/freedom-net.

Freedom Online Coalition. "About Us." 2018. Accessed June 4, 2018. https://freedomonlinecoalition.com/about-us/about/.

Freedom Online Coalition. "Freedom Online Coalition." 2018. Accessed June 4, 2018. https://freedomonlinecoalition.com/.

Fung, Brian. "Apple is pulling VPNs from the Chinese App Store. Here's what that means." *Washington Post,* July 31, 2017. Accessed June 4, 2018. https://www.washingtonpost.com/news/the-switch/wp/2017/07/31/apple-is-pulling-vpns-from-the-chinese-app-store-heres-what-that-means/?utm_term=.ad6fc6f4c70b.

Gallagher, Sean. "In effort to shut down Telegram, Russia blocks Amazon, Google network addresses." *ARS Technica,* April 17, 2018. Accessed June 4, 2018. https://arstechnica.com/information-technology/2018/04/in-effort-to-shut-down-telegram-russia-blocks-amazon-google-network-addresses/.

Goldsmith, Jack. *The Failure of Internet Freedom*. Knight Institute Emerging Threats Paper. New York: Knight First Amendment Institute, 2018, https://knightcolumbia.org/sites/default/files/content/Emerging_Threats_Goldsmith.pdf**.**

Hohmann, Mirko. "German Bundestag Passes New Data Retention Law." *Lawfare,* October 16, 2015. Accessed June 4, 2018. https://www.lawfareblog.com/german-bundestag-passes-new-data-retention-law.

Hohmann, Mirko, Alexander Pirang and Thorsten Benner. *Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach.* GPPi Policy Paper. Berlin: Global Public Policy Institute, 2017, http://www.gppi.net/fileadmin/user_upload/media/pub/2017/Hohmann__Pirang__Benner__2017__Advancing_Cybersecurity_Capacity_Building.pdf.

Human Rights Watch. “Germany: Flawed Social Media Law.” February 14, 2018. Accessed May 8, 2018. https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

Huotari, Mikko, Jan Gaspers, Thomas Eder, Helena Legarda, and Sabine Mokry. *China’s Emergence As A Global Security Actor: Strategies for Europe.* MERICS Papers on China. Berlin: Mercator Institute for China Studies, 2017.

Internet Assigned Numbers Authority. “Root Servers.” Accessed May 3, 2018. https://www.iana.org/domains/root/servers.

Internet Engineering Task Force. “Meeting Statistics.” 2018. Accessed June 4, 2018. https://datatracker.ietf.org/stats/meeting/overview/.

Internet Governance Forum. “IGF 2017 – Day 1 – Room XII – WS48 The Future of Internet Identifier: How the DNS Will Function in a Smart Cyberspace.” December 2017. Accessed May 8, 2018. https://www.intgovforum.org/multilingual/content/igf-2017-day-1-room-xii-ws48-the-future-of-internet-identifier-how-the-dns-will-function-in.

Jentleson, Bruce W. and Steven Weber. *The End of Arrogance: America in the Global Competition of Ideas*. Cambridge: Harvard University Press, 2010.

Kaplan, James M. and Kayvaun Rowshankish. “Addressing the Impact of Data Location Regulation in Financial Services.” *Global Commission on Internet Governance* no. 28 (2016): 35-40.

Kelly, Sanja, Mai Truong, Adrian Shahbaz, Madeline Earp, and Jessica White. *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy.* Freedom House Report. Washington: Freedom House, 2017. https://freedomhouse.org/sites/default/files/FOTN_2017_Full_Report.pdf.

Knight, Will. “China wants to shape the global future of artificial intelligence.” *Technology Review*, March 16, 2018. Accessed June 4, 2018. https://www.technologyreview.com/s/610546/china-wants-to-shape-the-global-future-of-artificial-intelligence/.

Lewis, James Andrew. “Reference Note on Russian Communications Surveillance.*” Center for Strategic and International Studies*, April 18, 2014. Accessed June 4, 2018. https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

Lunden, Ingrid. “LinkedIn is now officially blocked in Russia.” *TechCrunch,* November 17, 2016. Accessed May 8, 2018. https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/.

Magaziner, Ira. “Creating a Framework for Global Electronic Commerce,” *The Progress & Freedom Foundation*, July 6, 1999. Accessed June 15, 2018, http://www.pff.org/issues-pubs/futureinsights/fi6.1globaleconomiccommerce.html.

Mari, Angelica. “Brazil demands rules on data flows from WTO.” *ZD net*, April 16, 2018. Accessed June 4, 2018. https://www.zdnet.com/article/brazil-demands-rules-on-data-flows-from-wto/.

Maurer, Tim and Robert Morgus. “Stop Calling Decentralization of the Internet ‘Balkanization.’” *Slate,* February 24, 2014. Accessed May 8, 2018. http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html.

Maurer, Tim and Robert Morgus. *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate.* CIGI Internet Governance Paper. Waterloo: Centre for International Governance Innovation, 2014.

Maurer, Tim, Robert Morgus, Isabel Skierka, and Mirko Hohmann. *Technological Sovereignty: Missing the Point?* Policy Paper. Berlin: Global Public Policy Institute and Washington, DC: New America, 2014.

McCarthy, Kieren. “Russia threatens to set up its ‘own internet’ with China, India and pals – let’s take a closer look.” *The Register,* December 1, 2017. Accessed May 8, 2018. https://www.theregister.co.uk/2017/12/01/russia_own_internet/.

McKune, Sarah. “An Analysis of the International Code of Conduct for Information Security.” *Citizen Lab,* September 28, 2015. Accessed May 8, 2018. https://citizenlab.ca/2015/09/international-code-of-conduct/.

Meyer, David. “Blockchain technology is on a collision course with EU privacy law.” *International Association of Privacy Professionals,* February 27, 2018. Accessed May 8, 2018. https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

Milward, James A. “What It’s Like to Live in a Surveillance State.” *New York Times,* February 3, 2018. Accessed June 4, 2018. https://www.nytimes.com/2018/02/02/opinion/china-uighurs-xinjiang.html.

Mirasola, Chris. “Understanding China’s Cybersecurity Law.” *Lawfare,* November 8, 2016. Accessed May 8, 2018. https://www.lawfareblog.com/understanding-chinas-cybersecurity-law.

Moody, Glyn. “China Exporting Its Surveillance Tech and Philosophy to Other Countries, Helped by Equipment Donations.” *TechDirt,* February 1, 2018. Accessed May 8, 2018. https://www.techdirt.com/articles/20180124/03425639068/china-exporting-surveillance-tech-philosophy-to-other-countries-helped-equipment-donations.shtml.

Mueller, Milton. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Hoboken: Wiley, 2017.

Noam, Eli. “Towards the Federated Internet.” *InterMEDIA* 41, no. 4 (2013): 10-14.

Noam, Eli. “#BeyondWCIT. Eli Noam (Columbia University): ‘A federated internet is the key and cloud is the glue that will hold it together’.” *Key4Biz,* March 20, 2013. Accessed May 8, 2018. https://www.key4biz.it/News-2013-03-20-Policy-Eli-Noam-Columbia-University-beyond-dubai-216456/19363/.

O’Brien, Danny and Eva Galperin. “Russia Asks For The Impossible With Its New Surveillance Laws.” *Electronic Frontier Foundation,* July 19, 2016. Accessed May 8, 2018. https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

Organization for Economic Co-operation and Development. “COMMUNIQUÉ on Principles for Internet Policy-Making. 2011. Accessed May 7, 2018. https://www.oecd.org/internet/innovation/48289796.pdf.

Organization for Economic Co-operation and Development. *Economic and Social benefits of Internet Openness.* 2016. Accessed May 7, 2018. https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En.

Ott, Nikolas and Zylberberg, Hugo. “Cyber Sovereignty and Online Borders Do Not Improve International Security.” *Council on Foreign Relations,* October 2, 2017. Accessed June 4, 2018. https://www.cfr.org/blog/cyber-sovereignty-and-online-borders-do-not-improve-international-security.

Reporters Without Borders. “Russia bill is copy-and-paste of Germany’s hate speech law.” July 19, 2017. Accessed May 8, 2018. https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law.

Segal, Adam. “Year in Review: Chinese Cyber Sovereignty in Action.” *Council on Foreign Relations,* January 8, 2018. Accessed May 8, 2018. https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action?sp_mid=55724208&sp_rid=bWhvaG1hbm5AZ3BwaS5uZXQS1.

Shen, Hong. “China and global internet governance: toward an alternative analytical framework.” *Chinese Journal of Communication* 9, no. 3 (2016): p. 304-324. http://www.andrew.cmu.edu/user/hongs/files/HongShen_global.internet.governance.WritingSample.pdf.

Shiao, Vivien. “Innovation, digital economy key areas for Singapore’s Asean chairmanship: Lim Hng Kiang.” *Straits Times,* March 1, 2018. Accessed June 4, 2018. https://www.straitstimes.com/business/economy/innovation-digital-economy-key-areas-for-singapores-asean-chairmanship-lim-hng.

State Council of the People’s Republic of China. *Digital Silk Road forges strong links*. 2017. Accessed May 3, 2018. http://english.gov.cn/state_council/ministries/2017/12/05/content_281475965391860.htm.

Toon, John. “Study Shows How the Internet’s Architecture Got its Hourglass Shape.” *George Tech Research Horizons,* May 3, 2017. Accessed May 22, 2018. http://www.rh.gatech.edu/news/69297/study-shows-how-internets-architecture-got-its-hourglass-shape.

United Nations Educational, Scientific, and Cultural Organization. *What if we all governed the Internet? Advancing multistakeholder participation in Internet governance* (Paris: 2017), http://unesdoc.unesco.org/images/0025/002597/259717e.pdf.

United Nations General Assembly. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. A/66/359. September 14, 2011. https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

United Nations General Assembly. Resolution 71/199. *The right to privacy in the digital age*. January 25, 2017. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199

United Nations General Assembly. *Universal Declaration of Human Rights.* A/RES/217. December 10, 1948.

United Nations Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* A/HRC/38/35. April 6, 2018. Accessed June 4, 2018. https://freedex.org/a-human-rights-approach-to-platform-content-regulation/.

United Nations Human Rights Council. Resolution 20/8. *The Promotion, Protection, and Enjoyment of Human Rights on the Internet*. July 16, 2012.

United Nations Human Rights Council. Resolution 34/7. *The right to privacy in the digital age.* April 7, 2017. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement.

Wallace, Nick and Daniel Castro. “The Impact of the EU’s New Data Protection Regulation on AI.” *Center for Data Innovation,* March 27, 2018. Accessed May 8, 2018. http://www2.datainnovation.org/2018-impact-gdpr-ai.pdf.

Wang, Maya. “China’s Dystopian Push to Revolutionize Surveillance.” *Human Rights Watch,* August 18, 2017. Accessed May 8, 2018. https://www.hrw.org/news/2017/08/18/chinas-dystopian-push-revolutionize-surveillance.

Weber, Rolf H. “Legal Interoperability as a Tool for Combatting Fragmentation.” *Global Commission on Internet Governance,* no. 4 (2014): 5-13.

Wee, Sui-Lee. “China’s New Cybersecurity Law Leaves Foreign Firms Guessing.” *New York Times,* May 31, 2017. Accessed May 8, 2018. https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html.

White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. 2011. Accessed May 3, 2018. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

White House. “President Trump Protects America’s Cyber Infrastructure.” 2017. Accessed May 7, 2018. https://www.whitehouse.gov/briefings-statements/president-trump-protects-americas-cyber-infrastructure/.

World Summit on the Information Society. "Tunis Agenda for the Information Society." 2005. Accessed May 31, 2018. http://www.tjsl.edu/slomansonb/5.2_TunisAgenda.pdf.

Wu, Tim. "Is Internet Exceptionalism Dead?" In *The Next Digital Decade: Essays on the Future of the Internet,* edited by Berlin Szoka and Adam Marcus, 179-188. Washington: TechFreedom, 2010.

Wu, Tim and Jack Goldsmith. *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press, 2008.

Zittrain, Jonathan L. *The Future of the Internet – And How to Stop It.* New Haven: Yale University Press, 2008.

Global Public Policy Institute (GPPi)
Reinhardtstr. 7, 10117 Berlin, Germany
Phone +49 30 275 959 75-0
Fax +49 30 275 959 75-99
gppi@gppi.net

gppi.net