NEW AMERICA

July 2018

The Idealized Internet vs. Internet Realities (Version 1.0)

Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global Internet

Robert Morgus & Justin Sherman

Cybersecurity Initiative

Last edited on July 25, 2018 at 4:39 p.m. EDT

Acknowledgments

The authors would like to thank Ian Wallace, Jason Healey, Kenneth Rogerson, Alex Grigsby, Jeffrey Ritter, Trey Herr, Adam Segal, and Jaclyn Kerr for their comments on an earlier draft of this paper.

About the Author(s)

Robert Morgus is a senior policy analyst with New America's Cybersecurity Initiative and International Security program and the deputy director of the FIU-New America C2B Partnership.

Justin Sherman is an intern with New America's Cybersecurity Initiative, researching Internet governance and working on the Humans of Cybersecurity project.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

Contents

Contents Cont'd

Abstract

Liberal-democratic nation-states make frequent and explicit reference to five key elements of the global internet in their policy documents and cyber strategies: **free, open, interoperable, secure**, and **resilient**, or some combination of those elements. However, there are two fundamental problems with this approach.

The first is that the global internet never has embodied the absolute of any of these principles—and it is unlikely to in the future.

The second is that these five principles are in tension with one another—for instance, considering that *complete* network openness has some negative effect on network security—but this is not reflected in a vision of the internet where they all exist in harmony.

Recognizing that the principles of freedom, openness, interoperability, security, and resiliency are not representative of the *internet reality*, we have developed an analytical framework for comparing the *idealized* version of the internet—as imagined by liberal-democratic policymakers—with the internet reality. Within this document itself, the framework allows us begin to identify the current divergence from the *idealized* version of the global internet and thus identify gaps, pitfalls, and tensions in the liberal-democratic policy community's approach to the internet. Outside the scope of this document and going forward into future work, this framework enables anyone to plug in a single nation-state's internet policies to track divergence from the *idealized* version and to compare differences between countries. This framework is also an initial version and will be iteratively updated as needed.

Introduction

For the past several decades, the governments of the United States and many other liberal-democratic societies have espoused the benefits of a global internet that is, in some combination, **free**, **open**, **interoperable**, **secure**, and **resilient**. These are what we term the liberal-democratic policy community's five internet principles. As far back as the early 2000s, the U.S. government referenced most of this language in its policy documents,[1] and those ideas have persisted since—most recently in the U.S. Department of Homeland Security's Cybersecurity Strategy (released May 15, 2018)[2] and the U.S. State Department's Recommendations to the President on Protecting American Cyber Interests through International Engagement (released May 31, 2018).[3] The United Kingdom's 2016 cybersecurity strategy called to protect a "free, open, peaceful and secure cyberspace";[4] France's international digital strategy relies on principles of internet openness, net neutrality, and decentralization;[5] and Canada's newly-minted cybersecurity strategy makes similar mention of an open, free, and secure internet.[6] These five terms, while usually not precisely defined, are frequently used by policymakers in liberal-democratic nation-states.[7]

Liberal-democratic societies have espoused the benefits of a global internet that is free, open, interoperable, secure, and resilient.

In contrast, countries like Russia, China, and Iran have gradually developed methodologies for shaping the internet in their borders that do not depend on these five principles. While largely acknowledging and working to maximize the economic benefits of the internet, many of these countries' internet regulatory and legislative structures emphasize and seek to reassert the state's sovereignty over a space not originally designed to recognize sovereign boundaries.[8] In doing so, these countries aspire to forge advantageous, efficient economic environments and leverage the internet's potential to grow wealth, while also managing its capacity to sow instability and create new harms at home and abroad. Many of these countries have developed compelling arguments—to some—for why their nation's model for the internet is the better one. Russia has exported its surveillance technology to encourage compliance with its model of the internet,[9] and China has used assorted mechanisms—such as investment in underwater internet cables in the Asia Pacific[10] and low-cost infrastructure projects in Africa[11]—to push its tightly-controlling, sovereignty-centric internet model as well.

At the same time, the repeal of net neutrality protections in the United States[12] has elevated some discussion of the idealism behind the five principles of freedom, openness, interoperability, security, and resiliency. Not only do liberal-democratic nation-states often challenge their own vision of the global internet through domestic policies, as some commentators are beginning to understand, but some of these characterizations are in tension with one another and in conflict with the architecture of the internet itself.

The internet's physical infrastructure is filled with so-called "choke points" where single companies[13] or governments[14] control massive flows of information —creating single points of failure (SPOFs) that challenge the principle of resilience. In 2017, for instance, private corporation CloudFlare revealed that they handle around 10 percent of all American internet requests.[15] Globally, just four corporations account for upwards of 90 percent of all traffic to content delivery networks (CDNs), challenging the resiliency of dependent systems.[16] Companies and governments have begun reinvesting in control of undersea internet cables,[17] and nations like Iran have built their own internal internets.[18] Centralization, rather than decentralization, is the name of the game.

Not only do liberal-democratic nation-states often challenge their own vision of the global internet through domestic policies, as some commentators are beginning to understand, but some of these characterizations are in tension with one another and in conflict with the architecture of the internet itself.

Further, the internet is certainly not secure; if anything, it was designed for redundancy and constant availability—for protocols to route around failure rather than encrypt data or filter out malicious packets. But even those original principles of redundancy and constant availability have been challenged, with attacks that manipulate data and botnets that shut down entire subsections of a nation's internet.[19] This is perhaps equally true in authoritarian nation-states, where governments restrict public internet access and rigorously police instances in which access is permitted. The web has drastically changed since its inception.

The Five "Ideals"

The U.S. and other liberal-democratic nation-states make reference to an internet that is, in some combination, free, open, interoperable, secure, and resilient. The precise meanings of these terms are unclear. However, as we interpret them based on existing policy documents, these terms mean:

- *Free:* Any user can access and exchange information on and through the internet without unreasonable restriction.
- *Open:* Systems and infrastructure are merely conduits for data transmission; they are net neutral and oblivious to what goes through them.
- *Interoperable:* Parts of the global system (network) work with other parts of the global system (network); *A* can easily move or convert to *B*.
- *Secure:* The system upholds the confidentiality, integrity, and availability (CIA) of its users, its data, and itself.
- *Resilient:* No single points of failure exist in the network; systems do their intended job despite impediments.

Here we provide an elaboration on how we arrived at these definitions and some of the nuance behind them. These definitions are of course subjective, particularly in their original usage by each government, but there is relatively consistent usage among liberal-democratic nation-states which we attempted to extract.

Free

In 2011, the United States' International Strategy for Cyberspace asserted that "the more freely information flows, the stronger our societies become."[21] It also noted that "the ability to seek, receive and impart information and ideas through any medium and regardless of frontiers has never been more relevant."[22] France produced a document that same year which stated, "France condemns all censorship and arbitrary or general restriction of Internet access and seeks to promote freedom of opinion, expression, information, assembly and association on the Internet."[23] A 2012 report to the U.S. House Committee on Energy and Commerce held that any deviation from the "the free flow of commerce and ideas" would harm the internet's "ability to spread both prosperity and freedom." [24] France's 2015 National Digital Security Strategy writes that the internet should remain "a place of free expression for all citizens, where abuses can only be prevented within the limits set by the law and in line with our international agreements."[25] Israel's 2017 National Digital Program says that "freedom of expression and free access to information, which are vitally important for the social resilience of the State of Israel and its democratic nature, must be ensured."[26] Australia explicitly defines internet freedom as a state where "people are not burdened by undue restrictions on their access to and use of cyberspace; and their human rights are protected online as they are offline so that cyberspace remains a vibrant force for economic, social and cultural development."[27] And a 2017 address of the European Commission by the Greek Vice-President even discussed Greece's backing of the free flow of internet data.[28] Our definition is based on these (and many other) references to freedom tying into the ability to access and share information online. Most often, this principle of internet freedom is impacted by laws, regulations, social norms, and political actions.

Open

Australia defines an open internet as "interoperable across borders and accessible to all; it facilitates unrestricted participation and the free flow of information, driving inclusive online collaboration, innovation and growth."[29] France's 2017 international digital strategy discusses the importance of openness and network neutrality, guaranteed by decentralized internet architecture.[30] The Italian government sets "net neutrality, open networks, [and] equivalent and non-discriminatory access conditions" as key goals of its internet strategy, adding the importance of "a technical solution completely open and neutral, deploying only passive infrastructures and laying optic fiber according to a fiber-to-the-building (FTTB) reference architecture to allow the wholesale unbundled access to all operators."[31] The U.S. Federal Communications Commission (FCC) stated in 2016 that openness more or less refers to net neutrality, which ensures that "broadband service providers cannot block or deliberately slow speeds for internet services or apps, favor some internet traffic in exchange for consideration, or engage in other practices that harm internet openness."[32] Our definition is therefore oriented to a non-discriminatory architecture that is net-neutral. What this means in practice is that the internet infrastructure is oblivious to the nature of the data or traffic flowing through it. Regardless of what the data is, it will be treated the same way by the infrastructure. Often, violations of internet freedom (e.g., passage of a censorship law) are what prompt violations of openness in architecture (e.g., corresponding filtering on the part of internet service providers [ISPs]).

Interoperable

The United States' FCC discussed interoperability as far back as 2003 in the context of signaling architectures, call control architectures, voice over wireless, inter-provider interfaces, directory services, and safety and security features, broadly referring to features by which different networks and systems interact.[33] Australia's recent international cyberspace strategy links interoperability with the harmonization of global internet standards (e.g., through organizations such as the International Organization for Standardization).[34] A 2014 paper from the U.K.'s Chief Scientific Adviser frames interoperability the same way: compelled by universally-recognized standards.[35] The United States' Computer Emergency Readiness Team (US-CERT) defines interoperability as "the ability of two or more systems or components to exchange information and to use the information that has been exchanged."[36] The European Commission expands upon all of these definitions, asserting that "interoperability is not simply a technical issue concerned with linking up computer networks. It goes beyond this to include the sharing of information between networks and the reorganisation of administrative processes to support the seamless delivery of eGovernment services."[37] Our definition therefore broadly refers to the ability of different components of a given system—in this case, the global internet—to interact without failure.

Secure

Germany's 2011 Cyber Security Strategy defines security in context as "the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyberspace."[38] Australia's government holds that "a secure cyberspace is safe, reliable and resilient; it fosters an environment of trust so that individuals, businesses and governments can engage online with confidence and realise the opportunities and minimise the risks of the digital age."[39] Canada's recent Cyber Security Strategy categorizes cybersecurity as response and mitigation measures to unauthorized data access and electronic attacks.[40] The Spanish government discusses cybersecurity as a broad objective to "ensure that Spain makes secure use of the Information and Telecommunications Systems, strengthening cyber-attack prevention, defence, detection, analysis, investigation, recovery and response capabilities."[41] And US-CERT defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[42] Our definition comes from these and other references, which in aggregate aim to protect the confidentiality, integrity, and authenticity (CIA) of the global internet and its related components —from broad strategy down to highly-technical processes.

Resilient

Israel's previously-mentioned National Digital Program ties the internet directly into the social resilience of the nation-state.[43] The U.S. President's National Security Telecommunications Advisory Committee (NSTAC) issued a 2017 report on resiliency that linked it to network redundancy and the security of communications and infrastructure.[44] The U.S. Department of Homeland Security discusses resilience in context with technical and operational resistance to cyber attacks.[45] Spain's Ministry of Defence defines resilience as "the defensively oriented policy that maximizes the ability of possible target systems to prevent, deter and withstand cyber attacks and, if they occur, to minimize and mitigate their effects" which "is a multidimensional concept and has technical, organizational, political and legal components that need to be combined to be effective."[46] France's Internet Resilience Observatory most recently defined resilience on the internet as "the ability [for the internet] to operate during an incident and return to the nominal state. It can be characterized by measurable indicators, some of which come directly from engineering rules called best practices."[47] Our definition aims to encompass the underlying thread in these and other definitions, which center around the ability of a system to essentially route around failure, regardless of the underlying cause.

An Idealized Picture

Even in an *idealized* version of a global internet, not every dimension or element in our framework necessarily needs to contain or implicate all five of these ideal principles. However, in the *idealized* version of the internet in our framework, we provide a description of a global network that we believe captures the vision of a free, open, interoperable, secure, and resilient global internet. It is our hope that this mapping further clarifies the definitions and our interpretations of free, open, interoperable, secure, and resilient and provides an *idealized* archetype from which we are able to identify real departures.

Ideal vs. Reality: Understanding the Liberal-Democratic Gap

China and Russia do not share the liberal-democratic view of the internet—quite the contrary, in fact. The Chinese and Russian governments have long emphasized security of the state over ideas of openness, resilience, and decentralization (online as much as offline). In addition to censoring content and aggressively cracking down[48] on the ability of foreign companies to operate in and thereby influence their internet, China has clear strategies on internet governance, covering everything from the digital economy to terrorism.[49] Its government and corporations are making significant investments in physical internet infrastructure, gaining control of valuable underwater cables in the Asia Pacific.[50] Further, China's government has begun pushing its policies within international organizations such as the International Telecommunications Union (ITU) and other standards bodies.[51] Chinese policymakers have also made clear their prioritization of "cultural security" and "innovation security," which collectively safeguard the domestic online environment from internal and external threats.[52]

China's cyberspace strategy is "vastly different" from that of its liberal-democratic counterparts—perhaps foremost in its acceptance of the internet reality.[53] Its government addresses security issues, digital and otherwise, head-on.[54] But China's policy is also cohesive: as one scholar puts it, "Beijing has moved to rapidly…[to] construct a policy and regulatory framework spanning cybersecurity, the digital economy, and online media content—all under one mantel."[55]

The Chinese and Russian governments have long emphasized security of the state over ideas of openness, resilience, and decentralization (online as much as offline).

Similar to China, Russia actively seeks to control the internet governance narrative in its favor through the "politicization of global cyber issues"[56] and its use (and export)[57] of SORM-3, a system enabling mass censorship and surveillance.[58] Russia consistently pushes norms in the ITU, the Internet

Corporation for Assigned Names and Numbers (ICANN), and the Internet Governance Forum (IGF) to uphold multilateralism[59] over the West-favored multi-stakeholder approach.[60] And its leadership acknowledges the fundamental use of the internet as a foreign policy tool, viewing cyberspace as a "chaotic domain...which reinforces global anarchy."[61] Russian treatment of the internet ties in visibly with its other economic, social, and political goals.

On the point of multilateralism, China and Russia actively cooperate on international cyberspace issues, signing a joint letter to the UN General Assembly in 2015 on an "international code of conduct for information security." In addition to emphasizing the importance of sovereignty in cyberspace, it called for others "not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security."[62] This comes back to China and Russia's mutually-held idea that online information is "a potential threat to their political stability that demands tight controls."[63]

These countries' visions of the internet may not be desirable, but that does not mean their underlying assumptions (e.g., its insecurity) are flawed. It also does not imply a lack of consistent messaging: China and Russia actively pass laws in support of their own security-centric internet policies, from banning encrypted messenger Telegram[64] and broadly regulating online discourse[65] to controlling gateways to the global internet[66] and punishing search engines that link to banned Virtual Private Networks (VPNs).[67] The same goes for authoritarian countries such as Iran, where violations of net neutrality[68] are consistent with their professed internet strategy.[69]

These countries' visions of the internet may not be desirable, but that does not mean their underlying assumptions are flawed.

In contrast, many liberal-democratic laws and policies—that is, what happens in practice—may not align with their governments' visions. The United States repealed its protection of net neutrality in June 2018,[70] a core element of an open internet. While the European Union is still officially committed[71] to net neutrality, some argue this falls short in practice.[72] National cyber defenses, such as the United Kingdom's filtering of threats at the border,[73] run directly in the face of complete openness, as do the majority of liberal-democratic countries whose surveillance programs aggressively monitor the flow of online information.[74]

In 2015, Freedom House named France as the nation with the second-greatest annual increase in internet censorship, in that case due to blowback from the terrorist attacks against *Charlie Hebdo*.[75] Censorship laws similarly passed in the name of domestic security have gained foothold in the United States,[76] Germany,[77] Canada,[78] and the United Kingdom,[79] to name several others. Again, this may be for legitimate reasons, but the passage of these laws represents at least some shift away from the idea of internet openness, freedom, and interoperability and further toward the idea of the internet's inherent vulnerability and capacity for harm.

The United States permits challenges to internet resilience, allowing only a few internet service providers to control a significant amount of traffic.[80] Some argue this is a byproduct of the United States' capitalist approach to the technology market,[81] but the centralization of control over internet architecture is at least evident. This challenges internet security insofar as single centers hold valuable access to high volumes of traffic (a goldmine for hackers and foreign nation-states wishing to spy on American internet communications).

The passage of these censorship laws represents at least some shift away from the idea of internet openness, freedom, and interoperability and further toward the idea of the internet's inherent vulnerability and capacity for harm.

All of this said, most liberal-democratic nation-states strongly disagree with Russia, China, and other authoritarians on how to govern the internet; the U.S. government, for instance, does not hire citizens to pervasively spread propaganda (as with China[82] and Russia).[83] The Netherlands, to use another example, is known for open sharing of online information rather than aggressive internet censorship.[84] So the challenging of one's own principles does not necessarily (and in this case, does not) constitute full alignment with authoritarian nation-states. However, liberal-democratic countries still need to shift their stances from the total ideal of freedom, openness, interoperability, security, and resiliency to one that is more attuned with today's reality—raising the question of how this should be done.

Recognizing that the five characteristics of the *idealized* internet are a departure from the internet reality—what is a series of increasingly restricted, vulnerable, centralized, and often sovereign networks—we have built the following framework[85] to identify pitfalls, gaps, and tensions in the liberal-democratic policy community's *idealized* portrait of the global internet. Importantly, this *idealized* version of the internet is not necessarily the same as that of the initial internet founders, technology companies, or internet users. Instead, it is an interpretation of the picture painted of the internet by liberal-democratic policy statements. It therefore serves as a baseline from which we can analyze current policies towards the internet (e.g., mapping and understanding the divergence from the baseline).

This, we believe, is where our framework proves useful. Highlighting the gap between the ideal and the reality allows us to better understand the challenges and tensions at play, from the physical wires that compose the global internet to the laws and social norms that shape its pervasive impact. Furthermore, understanding this gap helps us better understand the implications of policies and may assist in identifying just how far liberal-democratic societies are willing to push their internet regulations and restrictions in pursuit of cyber and broader security.

Framework Background

In order to better understand and classify the *idealized* version of the internet and the *real* internet, as well as current activities and proposals, we suggest a two-tier analytical framework.

In this section, we provide the framework along with a description of its tiers and elements. In the following section, we then use the framework to construct a baseline *idealized* version of the internet and map todays internet *reality*, to capture the departure from the ideal. Once this baseline is established and the contrast is evident, future work can use the framework to systematically analyze *individual* nation-state policies and practices around cybersecurity and governance of the internet.

To be clear, this is *not* a model for the global internet itself; rather, we introduce an analytical framework for *understanding* the global internet, specifically geared towards helping policymakers with non-technical backgrounds understand the internet reality. The five aforementioned principles—freedom, openness, interoperability, security, and resiliency—are merely a lens, and as such, our perspective in creating the framework remains that of policymakers in liberal-democratic nation-states. In the larger context, highlighting the gaps between the ideal and the reality allows us to guide liberal-democratic thinking on internet governance and cybersecurity policy. For instance: What tensions exist within country *X*'s vision of the global internet? Are their current policies challenging or undermining this goal? What are nation-states like Iran doing under this lens? What are their thresholds for upholding or violating these principles—that is, what gaps do they tolerate between the liberal-democratic ideal and their reality? And so on.

In the larger context, highlighting the gaps between the ideal and the reality allows us to guide liberal-democratic thinking on internet governance and cybersecurity policy.

Our framework integrates softer governance issues such as politics, economics, national security, and international norms with harder architecture issues such as system resilience, protocol interoperability, and network security—factors often isolated from one another in existing internet analysis.[86] Nation-states like China and Russia have set up bureaucratic structures to integrate these ideas,[87] and liberal-democratic nation-states should as well. Further, we believe this integration—that is, a comprehensive and intersectional view of the global internet—will guide the most effective policy creation.

Governance Tier

The first tier (the Governance Tier) breaks out influencers of the internet into four categories: laws and regulations, social norms, standards, and markets. This tier largely examines legal, societal, and economic code rather than technical code.

The Governance Tier is an adaptation of Lawrence Lessig's regulators of behavior in cyberspace[88]—which he identifies as laws, standards/social norms, and markets. His approach is theoretically effective for strategic and policy analysis, but Lessig groups together standards and social norms, two factors which have developed increasingly different roles over time. Standards, developed and maintained by such organizations as the ITU, the Institute of Electrical and Electronics Engineers (IEEE), and the Internet Engineering Task Force (IETF), are formal protocols for device and network activity. They are increasingly necessary to access the global internet; those who do not comply with IP address rules, for instance, will not be able to access Netflix.

The Governance Tier largely examines legal, societal, and economic code rather than technical code.

Social norms, in contrast, differ from standards in both design and enforcement. Norms face the challenge of soliciting and encouraging nation-state agreement—going through mechanisms of the United Nations, for instance, rather than simply saying "comply and connect, or do not comply and stay offline." Incentivizing agreement with norms often is not as black-and-white as it often is with global internet standards.[89] Further, internet norms are typically far less technical than internet standards. For example, IEEE 802.11, the set of standards for wireless local area networks (WLANs),[90] has extreme technical specificity in contrast with a norm such as not interfering in the "internal affairs" of other nations through the internet.[91] Thus, separation between standards and social norms is necessary but nonexistent in Lessig's model.

We therefore have our Governance Tier of laws and regulations, social norms, standards, and markets.

Governance Tier

Dimension
Laws and Regulations
Social norms
Standards
Markets

Architecture Tier

The second tier (the Architecture Tier) describes different layers of internet architecture, using an adaptation of the well-known OSI (Open Systems Interconnection) model.[92]

The OSI model is composed of seven layers:

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

The OSI model is a popular tool for understanding the processes behind the global internet itself, such as IP routing and packet transmission. However, OSI has a problematic omission: content.[93] Although content (information) is not necessarily distinct from presentation (code becoming readable characters, aka data) on a technical level, it must be separated in policy and cultural contexts. Different countries have fundamentally different understandings of terms like "information security," because their fundamental understandings of online information are different—regardless of any technical similarities between systems.[94] Britain, for instance, may use the phrase "information security" in reference to data and network security, whereas Russia may use the term in reference to controlling the flow of information and general public discourse itself.[95] Thus, the particular importance of online information merits a comprehensive analysis of content as its own element.

We refer to these components as elements rather than layers to make clear the interplay between each component. The network cannot route traffic without the support of data link and transport protocols just as there is nothing *to* send without applications and content. "Layer" seems to denote physical separation between components, and we aim to show differently. We also combine OSI's Application and Presentation layers into a single Application and Presentation element, as the distinction is not necessary for our purposes. Minimal policy decisions occur around character code translation (OSI's Presentation layer) but many do occur around applications (e.g., encrypted messaging apps like Telegram and Signal).

We therefore have our Architecture Tier of Content, Application and Presentation, Session, Transport, Network, Data Link, and Physical elements.

Architecture Tier

Element
Content
Application and Presentation
Session
Transport
Network
Data Link
Physical

The Whole Picture

Of course, governance and architecture, while sometimes distinct, can and often do overlap. For example, laws or regulations about the legality of some content (Governance Tier) will necessarily implicate the internet's content element (Architecture Tier) as well as its network element (Architecture Tier). Likewise, markets (Governance Tier)—especially local language information markets—also implicate the content element (Architecture Tier). The separation of tiers, and the separation of dimensions and elements within those tiers, does not mean that each component operates in isolation. Rather, their separation allows for a useful analytical framework for understanding the forces shaping the internet we see today.

The Full Analytical Framework

Our framework for understanding the gaps between the liberal-democratic internet ideal and the global internet reality is below. In the next section, we offer an overview of our mapping of the idealized and real internet. (See **Appendix** for an example of the full mapping)

Governance Tier

Dimension	Idealized	Global Reality	Country A	Country B
Laws and Regulations				
Social norms				
Standards				
Markets				

Architecture Tier

Element	Idealized	Global Reality	Country A	Country B
Content				
Application and Presentation				
Session				
Transport				
Network				
Data Link				
Physical				

Comparing the "Ideal" and Reality

In this section, we offer a mapping of the different elements of our framework through the lens of a *free, open, interoperable, secure, resilient* internet. In doing so, we create two distinct pictures of the internet. The first column—Idealized Version—in each of the below tables describes what an internet built on the absolutes of these five principles would look like. In the second column—The Global Reality—we describe how the current internet departs from this idealized picture.

Governance Tier

Laws and Regulations
Laws and regulations are the primary tools used by states to shape behavior. They impose sanctions or punishment for (defined) undesirable actions or behaviors and/or provide incentives for (defined) desirable actions or behaviors.

In the context of the internet, laws can both shape the behavior of internet users and provide guidelines on how internet architecture should operate.

	"Idealized" Version	The Global Reality
Free	Laws and regulations that enable freedom of access to information and expression via the internet.	All countries have some form of restriction on content, whether bans on child pornography or aggressive censorship of foreign press.[96]
Open	Laws and regulations that enable or ensure openness (oblivious architecture).	Some countries are not protecting net neutrality; many countries have laws that could allow ISPs to throttle traffic based on the content of that traffic.[97]
Interoperable	Laws and regulations that do not negatively impact the network's interoperability.	Some nations mandate data localization and local data routing which can affect resilience.[98]

	“Idealized” Version	The Global Reality
Secure	Laws and regulations that criminalize/penalize (a) illicit use of computers (as we define it: computer network attacks, etc.), but do NOT criminalize (b) content and information, etc.	Most countries have laws that criminalize (a), but many also have laws that criminalize (b). In some cases laws criminalize behaviors that would otherwise positively impact the security of the global network.[99]

Social Norms

Social norms are expectations about “appropriate behavior for actors with a given identity.”[100] They regulate behavior through societal pressure.

In the context of the internet, social norms typically guide how users interact with the internet and with one another on the internet. However, social norms have in the past also shaped the way infrastructure owners and operators administer internet architecture.

	“Idealized” Version	The Global Reality
Free	Norms that enable freedom of access to information and expression via the internet.	There are some norms in place to protect internet freedom,[101] but many countries challenge them within their own borders. Further, other nation-states push conflicting international norms to restrict internet freedom.[102]
Open	Norms that enable or ensure openness (oblivious architecture).	Net neutrality was a norm, but some nations have already contested that fact.

	"Idealized" Version	The Global Reality
Secure	Norms that dictate responsible behavior of internet users (including individuals, states, and other organizations) to not undermine or exploit insecurity of the global network.	Much time and effort has gone into establishing norms, particularly for responsible behavior of states,[103] but despite these norms, actors persist in exploiting insecurities.

Standards

Standards give "specifications for products, services and systems to ensure quality, safety and efficiency."[104]

In the context of the internet, standards provide guidelines primarily for using and configuring architecture.

	"Idealized" Version	The Global Reality
Interoperable	Standards that ensure interoperability and that devices, systems, and networks are built to connect and interact.	The ideal is mostly the reality. Standards ensure most components of the internet can work with one another.
Secure	Standards exist that promote security.[105]	Governments around the world can undermine national and international security standards.[106]

Markets

Markets regulate behavior through price. "Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates." [107]

In the context of the internet, markets shape the creation, acquisition, and configuration of architecture. They also impact the options available to internet users and the way users react to architectural changes.

	"Idealized" Version	The Global Reality
Free	The market for internet access and content access is not artificially manipulated.	Content laws artificially manipulate the market for information.
Open	Net neutrality.	ISPs violate net neutrality in some countries.[108]
Interoperable	Markets (global) provide economic incentives for developers/owners/ operators to build/manage interoperable infrastructure.	This appears to hold true. Devices that fail to work with other devices are typically not in great demand.
Secure	People will understand what products are and are not secure and make purchases.	This is not the case, as customers continually purchase products with minimal understanding of or care for the security implications.[109]

Architecture Tier

Content

The content element is the result of translating machine-readable code into human-interpretable information. Content is what is presented on the screen of most internet users.

Examples of content include information on websites (not the websites themselves), email messages (not email protocols or applications), text messages, and Voice over Internet Protocol (VoIP).

	"Idealized" Version	The Global Reality
Free	Universally, users can access and share any information they want at will.	Countries and sometimes infrastructure operators put laws or policies in place to censor certain content.

	"Idealized" Version	The Global Reality
Open	Users are guaranteed free, immediate, online availability of information coupled with the rights to use that information fully in the digital environment.[110]	Countries and sometimes infrastructure operators use technical measures to manipulate architecture to block or limit access to certain content.
Secure	Users can trust the validity of the content on the internet.[111]	Fabricated content and manipulated content is rife on the internet. Users are often bereft of ways to verify the truth of a given piece of content.[112]

Application and Presentation

The application and presentation element serves to translate character code representations (machine-readable code, what is often referred to as "data") into physical windows, text, graphics, and other representations that are discernable to an average user. The result of this translation is content.

Examples of application and presentation architecture include internet browsers, websites themselves (search engines, news sites, social media platforms, etc.), email and messaging applications, the Hypertext Transfer Protocol (HTTP), and others, as well as file types (JPG, .doc, .pdf, etc.), encryption protocols (RSA, PGP, etc.), and character code representations (ASCII, Unicode, etc.).

	"Idealized" Version	The Global Reality
Free	Any user can use and access any application.	Governments outlaw some applications.
Open	Applications do not modify what a user of the application sees.	Application owners, operators, and developers willingly design or are compelled by governments to design protocols to discriminate the content their applications present.

	“Idealized” Version	The Global Reality
Interoperable	Translation infrastructure needs to be able to take any coding language and turn it into something an internet user can read.	This generally holds true. Files are fairly interoperable, although encryption can introduce complications.
Secure	Applications are safe to use. In fact, security is built in (secure coding).	Applications are vulnerable to cyberattacks. Files can easily be embedded with malicious code.
Resilient	One type of application breaking doesn’t cause all other types of applications to break.	Sometimes applications break, but their failure has not yet led to the entire system failing. For example, a given web browser could break, but that would not prevent the world from accessing the global internet.[113]

Session

The session element is, for the purposes of the global internet, the interaction between an internet user and a host of internet content. A session is initiated by a user on the user’s own device, sending a signal to a host via the transport element. The host then decides to accept or reject the request for access and sends that signal back to the user. The session remains open for as long as the user maintains access to the host’s content.

For example, when an internet user wants to access *facebook.com*, she enters the URL into her browser, ostensibly sending a session request to a Facebook server. The server chooses whether to accept or deny that request and sends it back to the user.

	"Idealized" Version	The Global Reality
Free	Internet users are not blocked via legal or normative means from opening sessions on the global internet and do not need specific permissions to open specific sessions.[114]	In some places, governments and/or infrastructure operators block users from opening sessions, usually through manipulations of the application element.[115]
Open	Session architecture does not prevent internet users from opening sessions.	In some places, infrastructure operators block users from opening sessions.[116]
Secure	Sessions are alterable only by authorized parties; information is kept secret from other sessions and parties.	Hackers can compromise sessions through such actions as cross-site scripting (XSS) attacks[117] and attacks on mountable networked file system (NFS) shares.[118]
Resilient	Individual sessions can fail (causing failure for the user up the chain), but individual session failures do not cause global session failures.	This generally holds true, but DDoS attacks can prevent users from opening sessions.[119]

Transport

The transport element consists of the processes and protocols that allow devices to communicate to one another over the network (see below).

	"Idealized" Version	The Global Reality
Open	Requests are not discriminated against.	Governments and ISPs throttle traffic by delaying response times of transport protocols.[120]

	"Idealized" Version	The Global Reality
Secure	Message communications are encrypted; CIA is preserved.	Messaging is still vulnerable to attacks like three-way-handshake hacks,[121] TCP spoofing,[122] and others.
Interoperable	It doesn't matter what device a user is using or what query a user is sending; the transport protocols can work with them all.	This largely holds true.
Resilient	Messages are not dropped, duplicated, or corrupted, and arrive in a timely manner while making fair use of the network.	Some failure occurs, but compared to other messaging protocols, and the central challenges that arise with networked messaging, TCP/UDP/etc. are relatively resilient.

Network

The network element is the processes and protocols that help internet traffic identify its intended destination. Network processes and protocols help assign identities to users and hosts.

These most notable of these processes and protocols are the Internet Protocol (IP) and domain name service (DNS) registries.

	"Idealized" Version	The Global Reality
Free	IP addresses are accessible [123] and the range of IPs from which a user can request information is not actively restricted.	Countries control entire blocks of IP or restrict IP access.

	"Idealized" Version	The Global Reality
Open	The network does not discriminate (by limiting speed or bandwidth) when routing IPs.	Government and ISPs identify what traffic to throttle based on IP addresses and other network characteristics.
Interoperable	Protocols work coherently with one another.	ICANN governs a system which ensures that protocols largely do work coherently with one another.
Secure	Routing infrastructure should not be vulnerable to attack.	The network element is vulnerable to some cyberattacks like DNS cache poisoning[124] and replay attacks,[125] which compromise IP and other protocols.
Resilient	There are no SPOFs (single points of failure); systems are configured for redundancy.	Heavy reliance on standard/ universal protocols (IP, for example) creates potential single points of failure.[126] Single system failures can bring down entire subsections of the global internet (e.g., Mirai).[127]

Data Link

The data link element is oriented around packets themselves rather than users and hosts. The data link processes and protocols dictate how packets are sent and received and how they act when delivered to their destination. Data link processes and protocols play a basic role in ensuring the functionality of the internet by detecting and correcting basic errors in transmitted data.Data link processes and protocols include media access control (MAC) addresses.

	“Idealized” Version	The Global Reality
Open	The protocols and access controls in this element will not identify or differentiate between traffic and treat it differently.	This holds true in practice
Interoperable	An international system of standards weaves things together so that links (from/to different manufacturers) interact easily with one another (all of the others, in fact).	This is largely true, but as the need to secure the internet moves further from the end user and closer to the physical hardware, so too do challenges to interoperability.
Secure	Data links uphold CIA.	Links are still vulnerable in their transmission of data, particularly on confidentiality and availability. Techniques for breaking or bypassing encryption (e.g., frequency attacks) also challenge this ideal.
Resilient	Distributed data link infrastructure creates redundancy and resiliency.	This largely holds true. Destroying one data link does not destroy all data links.

Physical

The physical element is the physical infrastructure and hardware that enables all the other elements.

Physical elements of the global internet include servers, undersea cables, satellites, routers, Ethernet cables, internet exchange points (IXPs), cellphones, tablets, and computers themselves.

	"Idealized" Versions	The Global Reality
Free	Any user can plug into any component of the infrastructure and use it to access the global internet.	Governments and corporations can and do purchase/own physical cables and exert control over how and by whom they are used.
Open	The physical infrastructure does not identify or differentiate between traffic and treat it differently.	The physical infrastructure itself does not breach openness.
Interoperable	Physical components interact easily with one another.	Design standards for physical infrastructure ensure interoperability, for the most part.
Secure	Physical components of the global internet are physically secured (e.g., strong access control), and physical infrastructure (hardware) is not hackable.	Physical security of physical infrastructure varies widely. Hardware is also hackable.[128]
Resilient	If one wire fails, the system still survives.	Because physical infrastructure is not necessarily equitably distributed, physical infrastructure failures have led to internet blackouts across entire nations.[129] However, one cable failing does not shut off the global network. The fact that 4 corporations account for 93 percent of CDN traffic poses potential challenges to the resiliency of the global internet.[130]

Analysis: Tensions

One of the primary values of this framework is its ability to highlight tensions inherent in the *idealized* internet. These inherent tensions partly explain some of the incoherence in liberal-democratic nation-state approaches to cyberspace policy. The absolutes of the five principles—freedom, openness, interoperability, security, and resiliency—may not be compatible with one another. For instance, a network cannot be *completely* open and *completely* secure.[131] However, the absolutes of these principles are not implemented in practice; in other words, they are not the reality, which in fact lies somewhere on a spectrum. Thus, there are tensions between these five principles which must be explored to determine the right balance. Some are starting to realize this fact, as demonstrated by a report from the U.S. National Security Telecommunications Advisory Committee, which in 2017 noted that "as networks become more open and interconnected, [the current] trust model can no longer be the sole foundation for Internet security."[132] Others have begun to point to inherent tensions and problems with this approach as well.[133] However, most liberal-democratic policymakers are still reluctant to consider the tensions at play. Here, we identify some such tensions and identify key considerations and challenges for liberal-democratic policymakers as they devise future cyberspace policies.

Secure and Open

There is certainly some tension between internet security and internet openness, as we just referenced. Firewalls, email filters, and other components of a network defense are in fact designed to *restrict* the open flow of information for purposes of security. These technical interventions on the network's architecture explicitly make infrastructure aware (or otherwise the opposite of oblivious) of the traffic traversing it. Even at the internet's content level, allowing anything to be transmitted anywhere, by any user, empowers the spread of propaganda and disinformation in addition to child pornography and other illegal or undesirable information. This raises a key question for liberal-democratic policymakers: how closed are they willing to make the internet in the name of security? Some democracies, notably the United Kingdom, are beginning to realize the value in nationally-coordinated cyber defenses, in this case through national filtering of low-level threats like phishing emails.[134] While authoritarian approaches to internet openness, like China's Golden Shield and Great Firewall, similarly manipulate the openness of architecture to filter out malicious traffic, the operative difference is in the definition of malicious traffic—or essentially the instructions for the national firewall. This is a prime example of how liberal-democratic policymakers must examine the tensions between internet security and internet openness in order to find their ideal balance in policies and processes.

Resilient and Secure

The resilience of data may similarly be in tension with security. Ensuring the persistence of all packets sent across a network enables a version of all worms, viruses, and other malware to indefinitely reside on the global internet. On the other hand, ensuring resilience of internet routers can prevent botnets like Mirai [135] from disabling large components of a nation's internet. Resilience harms security in the former case but supports security in the latter, indicating that different elements of the Architecture Tier may therefore expose different tensions or compatibilities between resilience and security. Again, no network is going to be entirely resilient or entirely secure. The objective, instead, should be striking an optimal balance between the two.

Interoperable and Secure

Interoperability can arguably help and harm security at once. Having interoperable communications (e.g., network protocols) can enable stronger security between devices and thus across entire networks and systems (e.g., through standardized encryption). Within single government or corporate systems, interoperability of devices and programs enables integrated security defenses such as packet filtering and secure data management. Conversely, wireless interoperability that enables device and network communication permits hackers to easily hop from one to device to the next, essentially using a single entry point to seamlessly cascade down a string of networks and devices. As smartphones and the internet of things (IoT) increase interconnectivity, for example, the risk of remote and/or data-based attacks that exploit interoperability also grows. This is by definition a tension as both realities exist in tandem. The interoperability of the global network is also what allows nation-states to attack one another from within their own countries.

Interoperable, Free, Open, and Resilient

Interoperability supports openness insofar as it enables the flow of data through neutral systems, and it supports resilience insofar as it allows devices, systems, and networks to rely on each other for resource protection and thus maintain constant availability. But to what extent does interoperability allow content restriction through centralized surveillance, thus harming the principle of internet freedom?

Free and Open

Freedom and openness are intertwined. Laws and regulations that restrict freedom of access to or expression of information will often be implemented via architectural interventions that limit openness. In other words, nation-states often approach the same organizations to censor content (restricting freedom) as they allow to violate net neutrality (restricting openness): ISPs and IXPs. Further, once an organization begins filtering content for purposes of censorship, it’s not a far step to scan the content for purposes of speed throttling or price discrimination (e.g., violating net neutrality). There is a clear distinction between the two in nation-states like Iran, which slow connections to foreign sites rather than censoring them entirely,[136] but the challenges to freedom and openness are again closely related. This perhaps explains the frequent grouping of a free and open internet in liberal-democratic policy documents.[137]

Conclusion and Future Work

The goal of this framework is to help build greater understanding of where the current internet departs from the *idealized* version in liberal-democratic foreign policy. We highlight a number of tensions here, but there are a lot more to be explored. Notably, complete security appears to clash with each and every one of the other principles at various levels of architecture and in the governance tier. In part for this reason, the urgency with which liberal-democratic governments must start with these types of questions, even if at high levels, is great. Understanding what stance to take towards each of these five characteristics is contingent upon an understanding of the underlying tensions. If we want better security, for instance, we have to sacrifice some openness.

The purpose of this exercise—and the tensions identified herein—is not to highlight contradictions for the sake of highlighting contradictions. Rather, the goal is to help liberal-democratic policymakers understand where the internet is currently, where it could be headed, and the implications of those directions. The ultimate goal is to help policymakers understand these tensions so they might be effectively balanced in a more cohesive and coherent strategy.

Appendix: Full Framework Mapping

In order to demonstrate our methodology to inform the analysis of this report and provide an example of how the framework could be applied by others we are providing our full mapping in this attachment: **Appendix - The Idealized Internet vs. Internet Realities**.

Notes

[1] Network Reliability and Interoperability Council VI: Focus Group 3, “Network Interoperability,” 2003, https://transition.fcc.gov/nric/nric-6/fg3-report.pdf, 3.

[2] U.S. Department of Homeland Security, “Cybersecurity Strategy,” 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf, 4.

[3] U.S. Department of State, “Recommendations to the President on Protecting American Cyber Interests through International Engagement,” 2018, https://www.state.gov/documents/organization/282224.pdf, 1.

[4] Government of the United Kingdom, “National Cyber Security Strategy 2016-2021,” 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 63.

[5] Government of France, “Stratégie Internationale de la France pour le Numérique,” 2017, https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf, 4.

[6] Government of Canada, “National Cyber Security Strategy,” 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf, 32.

[7] To be clear, not every liberal-democratic nation-state uses all five of these terms at once in their policy documents, or perhaps at all. Further, even with different languages aside, nation-states may use different words to refer to these terms—preferring, for instance, to say “redundant” or “decentralized” rather than “resilient.” Nation-states may also use these in different combinations in different documents. All of that said, most liberal-democratic nation-states do refer to these general five ideas when discussing internet governance and cyber strategy.

[8] For further discussion of this phenomenon, see: Henry H. Perritt, “The Internet as a Threat to Sovereignty? Thoughts on the Internet’s Role in Strengthening National and Global Governance,” 1998, https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1128&context=ijgls, 423-442.

[9] Peter Bourgelais, “Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia,” 2013, https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf, 2-3.

[10] Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure,” 2017, https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228, 241 & 261.

[11] See, for example: The Infrastructure Consortium for Africa, “Africa’s ICT Sector in China,” n.d., https://www.icafrica.org/en/topics-programmes/ict/africa%E2%80%99s-ict-sector-and-china/; and The Chinafrica Project, “For Better or Worse, Africa’s Digital Future is Tied to China,” May 5 2018, https://chinaafricaproject.com/china-africa-information-digital-technology-iginio-gagliardone/.

[12] Jeremy B White, “Net Neutrality Rules Officially Repealed in the United States,” June 11 2018, https://www.independent.co.uk/news/world/americas/net-neutrality-us-repeal-takes-effect-what-changes-ajit-pai-discharge-petition-a8394266.html.

[13] Russell Brandom, “We Have Abandoned Every Principle of the Free and Open Internet,” December 19 2017, https://www.theverge.com/2017/12/19/16792306/fcc-net-neutrality-open-internet-history-free-speech-anonymity.

[14] Center for Human Rights in Iran, “Guards at the Gate: The Expanding State Control Over the Internet in Iran,” 2018, https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf, 8.

[15] Matthew Prince, “Why We Terminated Daily Stormer,” August 16 2017, https://blog.cloudflare.com/why-we-terminated-daily-stormer/.

[16] Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure,” 2017, https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228, 242.

[17] The Economist, “Tech Companies Are Laying Their Own Undersea Cables,” October 9 2017, https://www.economist.com/graphic-detail/2017/10/09/tech-companies-are-laying-their-own-undersea-cables.

[18] Berkman Klein Center for Internet & Society, “Iran’s National Information Network: Faster Speeds, but at What Cost?” February 21, 2018, https://cyber.harvard.edu/node/100145.

[19] BBC, “Hack Attacks Cut Internet Access in Liberia,” November 4 2016, https://www.bbc.com/news/technology-37859678.

[20] This does not necessarily mean that internet access is free of monetary cost.

[21] The White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf, 4.

[22] Ibid., 5.

[23] Government of France, “France and the Global Challenges of Information and Communications Technologies,” 2011, https://www.diplomatie.gouv.fr/IMG/pdf/BR_TIC_version_anglaise-3.pdf, 3.

[24] United States House Committee on Energy and Commerce: Majority Committee Staff, “Hearing on International Proposals to Regulate the Internet,” 2012, https://archives-energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CT/20120531/HMTG-112-HHRG-IF16-20120531-SD001.pdf, 2.

[25] Government of France, “French National Digital Security Strategy,” 2015, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy, 3.

[26] Government of Israel, “The Digital Israel National Initiative: The National Digital Program of the Government of Israel,” 2017, https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf, 63.

[27] Government of Australia, “Australia’s International Cyber Engagement Strategy,” 2017, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf, 57.

[28] European Commission, “Speech by Vice-President Ansip in Athens on ‘A Digital Strategy for Greece: Path to Growth,’” May 10 2017, https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/speech-vice-president-ansip-athens-digital-strategy-greece-path-growth_en.

[29] Government of Australia, “Australia’s International Cyber Engagement Strategy,” 2017, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf, 57.

[30] Government of France, “Stratégie Internationale de la France pour le Numérique,” 2017, https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf, 4.

[31] Government of Italy, “The Italian Strategy for Next Generation Access Network,” 2015, https://www.agid.gov.it/sites/default/files/repository_files/documentazione/next_generation_access_network_-_english_version.pdf, 17 & 62.

[32] Federal Communications Commission, “Consumer Guide:
Open Internet,” 2016, https://transition.fcc.gov/cgb/consumerfacts/openinternet.pdf, 1.

[33] Network Reliability and Interoperability Council VI: Focus Group 3, “Network Interoperability,” 2003, https://transition.fcc.gov/nric/nric-6/fg3-report.pdf, 4.

[34] Government of Australia, “Australia’s International Cyber Engagement Strategy,” 2017, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf, 17.

[35] Government of the United Kingdom, “The Internet of Things: Making the Most of the Second Digital Revolution,” 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf, 30.

[36] National Initiative for Cybersecurity Careers and Studies, “A Glossary of Common Cybersecurity Terminology,” n.d., https://niccs.us-cert.gov/glossary#C.

[37] Commission of the European Communities, “Linking Up Europe: The Importance of Interoperability for eGovernment Services,” 2003, https://administracionelectronica.gob.es/pae_Home/dam/jcr:b17d4af0-6be9-46ed-a2d8-edc68c3ba528/Administracion_Electronica_Documento_de_trabajo_sobre_interoperabilidad.pdf, 3.

[38] Government of Germany, “Cyber Security Strategy for Germany,” 2011, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, 4.

[39] Government of Australia, “Australia’s International Cyber Engagement Strategy,” 2017, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf, 57.

[40] Government of Canda, “Canada’s Cyber Security Strategy,” 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, 3.

[41] Government of Spain, “National Cyber Security Strategy,” 2013, http://www.lamoncloa.gob.es/lang/en/Documents/20131332EstrategiadeCiberseguridad_ingl%C3%A9s.pdf, 3-4.

[42] National Initiative for Cybersecurity Careers and Studies, “A Glossary of Common Cybersecurity Terminology,” n.d., https://niccs.us-cert.gov/glossary#C.

[43] Government of Israel, “The Digital Israel National Initiative: The National Digital Program of the Government of Israel,” 2017, https://www.gov.il/BlobFolder/news/digital_israel_national_plan/en/The%20National%20Digital%20Program%20of%20the%20Government%20of%20Israel.pdf, 2 & 63.

[44] U.S. National Security Telecommunications Advisory Committee, “NSTAC Report to the President on Internet and Communications Resilience,” 2017, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf, 18.

[45] U.S. Department of Homeland Security, “Cybersecurity Strategy,” 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_0.pdf, 23.

[46] Spanish Institute for Strategic Studies, “Strategic Dossier 162 B: Economic Intelligence in a Global World,” 2013, https://publicaciones.defensa.gob.es/media/downloadable/files/links/c/e/ce_162_b.pdf, 191.

[47] Agence Nationale de la Sécurité des Systèmes d'Information, “Internet Resilience in France: 2015,” 2015, https://www.ssi.gouv.fr/uploads/2015/06/internet-resilience-in-france-report_2015_anssi.pdf, 5.

[48] Greg Wilford, “China Launches Internet Crackdown to Make it Harder for People to Avoid Its ‘Great Firewall,’” August 6 2017, https://www.independent.co.uk/news/world/asia/china-internet-crackdown-virtual-private-networks-vpns-facebook-twitter-youtube-google-whatsapp-a7879641.html.

[49] Tian Shaohui (ed.), “International Strategy of Cooperation on Cyberspace,” March 1 2017, http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

[50] Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure,” 2017, https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228, 241 & 261.

[51] China has used its growing participation in international standards bodies to promote its vision of the global internet, a clearly-defined goal in Chinese internet strategy. [See: Elsa Kania, Samm Sacks, Paul Triolo, and Graham Webster, “China’s Strategic Thinking on Building Power in Cyberspace,” September 25 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.] Russia has done the same, “blurring the lines between internet governance and cyber security” in pursuit of its preferred cyber policies. [See: Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance,” 2015, https://www.chathamhouse.org/publication/ia/contest-and-conquest-russia-and-global-internet-governance, 121.]

[52] Jan Fell, “Chinese Internet Law: What the West Doesn’t See,” October 18 2017, https://thediplomat.com/2017/10/chinese-internet-law-what-the-west-doesnt-see/.

[53] Gabi Siboni and Ofer Assaf, “Guidelines for a National Cyber Strategy,” 2016, http://www.inss.org.il/wp-content/uploads/systemfiles/INSS%20Memorandum%20153%20-%20Guidelines%20for%20a%20National%20Cyber%20Strategy.pdf, 32.

[54] Rogier Creemers, Paul Triolo, Samm Sacks, Xiaomeng Lu, and Graham Webster, “China’s Cyberspace Authorities Set to Gain Clout in Reorganization,” March 26 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

[55] Samm Sacks, “China’s Emerging Cyber Governance System,” n.d., https://www.csis.org/chinas-emerging-cyber-governance-system.

[56] Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance,” 2015, https://www.chathamhouse.org/publication/ia/contest-and-conquest-russia-and-global-internet-governance, 112.

[57] Peter Bourgelais, “Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia,” 2013, https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf, 2.

[58] Andrei Soldatov and Irina Borogan, “Inside the Red Web: Russia’s Back Door onto the Internet - Extract,” September 8 2015, https://www.theguardian.com/world/2015/sep/08/red-web-book-russia-internet.

[59] Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance,” 2015, https://www.chathamhouse.org/publication/ia/contest-and-conquest-russia-and-global-internet-governance, 121-123.

[60] The multilateral model of internet governance, while argued on the basis of inclusive, transnational consensus-building around internet issues, risks centralizing control of the internet in the hands of governments. As Vint Cerf, a founder of the net, noted over 10 years ago, “Internet is used by a billion users around the world, it’s not strictly a purely governmental thing to control, and that’s why you need this multi-stakeholders structure to make sure all the prospects are respected.” [See: Pedro Fonseca, “Cerf Sees Government Control of Internet Failing,” November 14 2007, https://www.reuters.com/article/us-internet-cerf/cerf-sees-government-control-of-internet-failing-idUSN1420689320071114.] The Federal Communications Commission and others have also documented problems with a multilateral approach. [See: Michael O’Rielly, “International Efforts to Regulate the Interent Continue,” April 21 2017, https://

www.fcc.gov/news-events/blog/2017/04/21/international-efforts-regulate-internet-continue.]

61 Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance,” 2015, https://www.chathamhouse.org/publication/ia/contest-and-conquest-russia-and-global-internet-governance, 116-117.

62 See: United Nations General Assembly, “International Code of Conduct for Information Security,” January 9 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf, 4.

63 Geoff Van Epps, “Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain,” 2013, https://www.jstor.org/stable/26326340?seq=1#page_scan_tab_contents, 27.

64 Vlad Savov, “Russia’s Telegram Ban is a Big, Convoluted Mess,” April 17 2018, https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban.

65 ChinaFile, “Document 9: A ChinaFile Translation,” November 8 2013, http://www.chinafile.com/document-9-chinafile-translation.

66 Freedom House, “Freedom on the Net 2017: China,” 2017, https://freedomhouse.org/report/freedom-net/2017/china.

67 Mohit Kumar, “Russia to Fine Search Engines for Linking to Banned VPN Services,” June 9 2018, https://thehackernews.com/2018/06/russian-vpn-services.html.

68 Freedom House, “Freedom on the Net 2017: Iran,” 2017, https://freedomhouse.org/report/freedom-net/2017/iran.

69 For greater discussion of Iranian cyber strategy, see: Collin Anderson and Karim Sadjadpour, “Iran’s Cyber Threat: Espionage, Sabotage, and Revenge,” 2018, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf, 11 & 25; Brad D. Williams, “Iran’s Cyber Strategy: A Case Study in Saudi Arabia,” February 7 2017, https://www.fifthdomain.com/home/2017/02/07/irans-cyber-strategy-a-case-study-in-saudi-arabia/; and Michael Eisenstadt, “Cyber: Iran’s Weapon of Choice,” January 29 2017, https://www.thecipherbrief.com/cyber-irans-weapon-of-choice-2.

70 Jeremy B. White, “Net Neutrality Rules Officially Repealed in the United States,” June 11 2018, https://www.independent.co.uk/news/world/americas/net-neutrality-us-repeal-takes-effect-what-changes-ajit-pai-discharge-petition-a8394266.html.

71 Saleem Bhatti, “Net Neutrality May be Dead in the US, But Europe is Still Strongly Committed to Open Internet Access,” January 5 2018, https://theconversation.com/net-neutrality-may-be-dead-in-the-us-but-europe-is-still-strongly-committed-to-open-internet-access-89521.

72 Andrei Khalip and Agnieszka Flak, “False Paradise? EU is No Haven of Net Neutrality, Say Critics,” December 15 2017, https://www.reuters.com/article/us-usa-internet-eu-analysis/false-paradise-eu-is-no-haven-of-net-neutrality-say-critics-idUSKBN1E92SC.

73 See: Ian Levy, “Active Cyber Defence - Tackling Cyber Attacks on the UK,” November 1 2016, https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk; and Government of the United Kingdom, “National Cyber Security Strategy 2016-2021,” 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 10 & 63.

74 Dustin Volz, “Trump Signs Bill Renewing NSA’s Internet Surveillance Program,” January 19 2018, https://www.reuters.com/article/us-usa-trump-cyber-surveillance/trump-signs-bill-renewing-nsas-internet-surveillance-program-idUSKBN1F82MK. Also see: Ryan Gallagher and Henrik Moltke, “The Wiretap Rooms: The NSA’s Hidden Spy Hubs in Eight U.S.

Cities," June 25 2018, https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.

75 Freedom House, "Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015," 2015, https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf, 2 & 3.

76 Sarah Jeong, "A New Bill to Fight Sex Trafficking Would Destroy a Core Pillar of Internet Freedom," August 1 2017, https://www.theverge.com/2017/8/1/16072680/cda-230-stop-enabling-sex-traffickers-act-liability-shield-senate-backpage.

77 Patrick Evans, "Will Germany's New Law Kill Free Speech Online?" September 18 2017, https://www.bbc.com/news/blogs-trending-41042266.

78 Aaron Mackey, Corynne McSherry, and Vera Ranieri, "Top Canadian Court Permits Worldwide Internet Censorship," June 28 2017, https://www.eff.org/deeplinks/2017/06/top-canadian-court-permits-worldwide-internet-censorship.

79 Matt Burgess and Liat Clark, "The UK Wants to Block Online Porn. Here's What We Know," May 8 2018, http://www.wired.co.uk/article/porn-block-ban-in-the-uk-age-verifcation-law.

80 Sascha Segan, "Exclusive: Check Out the Terrible State of US ISP Competition," December 15 2017, https://www.pcmag.com/news/357972/exclusive-data-shows-the-terrible-state-of-us-isp-competitio.

81 Rick Karr, "Why is European Broadband Faster and Cheaper? Blame the Government," June 28 2011, https://www.engadget.com/2011/06/28/why-is-european-broadband-faster-and-cheaper-blame-the-governme/.

82 Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army,'" 2015, https://journals.sub.uni-hamburg.de/giga/jcca/article/view/850, 111-114.

83 Daisy Sindelar, "The Kremlin's Troll Army," August 12 2014, https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/.

84 Freedom House, "Freedom on the Net 2017: Netherlands," 2017, https://freedomhouse.org/report/freedom-press/2017/netherlands.

85 This is the first version (1.0) of the framework and will be iteratively updated as needed.

86 For more on the exclusion of politics, economics, and other types of influence from digital and internet analysis, see: Laura DeNardis, "The Global War for Internet Governance," 2014, 8; Jacques Bughin, Tanguy Catlin, Martin Hirt, and Paul Willmott, "Why Digital Strategies Fail," January 2018, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-digital-strategies-fail; Dan Schiller, "Geopolitical-Economic Conflict and Network Infrastructures," 2011, https://www.tandfonline.com/doi/abs/10.1080/17544750.2011.544085?journalCode=rcjc20&, 90-107; and Dwayne Winseck, "The Geopolitical Economy of the Global Internet Infrastructure," 2017, https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228.

87 For instance, see: Jack Margolin, "Russia, China, and the Push for 'Digital Sovereignty,'" December 2 2016, https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/ for discussion on Russian and Chinese views of the internet playing into national sovereignty and regime stability.

88 Lawrence Lessig, "The Laws of Cyberspace," 1998, https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf, 2-3.

89 This is not to say that internet norms are impossible to achieve or necessarily ineffective, as such assertions would be incorrect; rather, we believe this difference simply merits a distinction between standards and social norms that Lessig's approach does not provide. For more discussion on international norms in cyberspace, see: Martha Finnemore,

“Cybersecurity and the Concept of Norms,” November 30 2017, http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870; Tim Maurer and Kathlyn Taylor, “Outlook on International Cyber Norms: Three Avenues for Future Progress,” March 2 2018, https://www.justsecurity.org/53329/outlook-international-cyber-norms-avenues-future-progress/; and Tim Maurer, Ariel Levite, and George Perkovich, “Toward a Global Norm Against Manipulating the Integrity of Financial Data,” March 27 2017, https://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

[90] See technical specifications at: IEEE, “IEEE 802.11, The Working Group Setting the Standards for Wireless LANs,” n.d., http://www.ieee802.org/11/.

[91] See: United Nations General Assembly, “International Code of Conduct for Information Security,” January 9 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf, 5.

[92] This dimensional separation between “softer” elements of governance and architectural “code” conforms with Lessig’s notion of code as a separate regulator of cyberspace behavior. [See: Lawrence Lessig, “The Laws of Cyberspace,” 1998, https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf, 3-4.] Our framework, though, goes into detail of what that “code” actually means.

[93] The presence of a “content layer” is based on Jonathan Zittrain’s idea of a conceptualized internet layer that contains “actual information exchanged among the network’s users.” See: Jonathan Zittrain, “The Future of the Internet -- And How to Stop It,” 2008, https://dash.harvard.edu/bitstream/handle/1/4455262/zittrain_future%20of%20the%20internet.pdf?sequence=1, 67.

[94] Because information—both network data and the idea itself—plays such a critical role in nation-state crafting of international cyber policies, particularly in Russia and China, it is essential to leverage content as a mechanism for comparing different models of internet governance. For more information on the semantic differences surrounding such words as “cyber,” see: Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance,” 2015, https://www.chathamhouse.org/publication/ia/contest-and-conquest-russia-and-global-internet-governance; Rogier Creemers, Graham Webster, Paul Triolo, Katharin Tai, Lorand Laskai, and Abigail Coplin, “Lexicon: 网络强国 Wǎngluò Qiángguó,” May 31 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/; and Keir Giles and William Hagestad II, “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English,” 2013, https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf.

[95] And in this way, Russia’s government doesn’t just use “information security” in the context of cyberspace or the internet, but it also attaches deeply political and philosophical meanings to the phrase as well, in ways that relate to newspapers, radio, and television. For more on this, see: Julien Nocetti, “Contest and Conquest: Russia and Global Internet Governance,” 2015, https://www.chathamhouse.org/publication/ia/contest-and-conquest-russia-and-global-internet-governance, 126; and Keir Giles and William Hagestad II, “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English,” 2013, https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf, 3-4.

[96] This is not to say that all countries have equivalent laws; whereas the United States may ban the resale or redistribution of copyrighted content, China may punish any internet user criticizing a government policy online. It is to highlight, though, that virtually every country in the world has laws and regulations that limit or restrict the creation and/or dissemination of online content.

[97] Iran is a prime example of a nation-state that “throttles” (slows) traffic based on the nature of the traffic itself. This violates an open internet

architecture. See: Collin Anderson, “Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran,” June 18 2013, https://arxiv.org/abs/1306.4361, 1.

98 Laws and regulations that require internet service providers and other administrators of internet architecture to store citizens’ data locally (data localization) and/or prioritize domestic internet traffic (local data routing) violate the non-discriminatory nature of an open internet. For examples of data localization laws see: Bret Cohen, Britanie Hall, and Charlie Wood, “Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy,” 2017, https://www.americanbar.org/content/dam/aba/publications/antitrust_magazine/anti_fall2017_cohen.authcheckdam.pdf. For discussion on how routing protocols can influence internet resilience on technical levels, see: Government of France, “Internet Resilience in France: 2015,” 2015, https://www.ssi.gouv.fr/uploads/2015/06/internet-resilience-in-france-report_2015_anssi.pdf.

99 For instance, see the United States’ so-called Computer Fraud and Abuse Act: Legal Information Institute, “18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computer,” n.d., https://www.law.cornell.edu/uscode/text/18/1030.

100 Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” 1998, https://www.jstor.org/stable/2601361, 891.

101 United Nations Human Rights Council, “The Promotion, Protection and Enjoyment of Human Rights on the Internet,” https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/082/83/PDF/G1408283.pdf?OpenElement.

102 United Nations General Assembly, “International Code of Conduct for Information Security,” January 9 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

103 See earlier endnote regarding international norms.

104 This definition is taken from the International Organization for Standardization (ISO). See: International Organization for Standardization, “About ISO,” n.d., https://www.iso.org/about-us.html.

105 Widely-implemented internet protocols such as HTTPS and TCP are continually updated with stronger encryption and more robust security processes.

106 Governments often expect law enforcement and intelligence agencies to maintain some violation of security standards under the banner of fighting crime and protecting national security. This could also be argued in an intelligence-gathering context (e.g., breaking an adversary’s security standards for espionage purposes). In other words, policymakers around the world permit or even encourage the violation of internet security standards for assorted reasons.

107 Lawrence Lessig, “The Laws of Cyberspace,” 1998, https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf, 3.

108 As previously referenced, the United States federal government just officially repealed its protections of net neutrality.

109 This reality is the impetus for numerous organizations working to provide security metrics for software and/or hardware products, such as the Cyber Independent Testing Lab (CITL) and Consumer Reports. See: Cyber Independent Testing Lab, “About Us,” n.d., http://cyber-itl.org/about-us/; and Consumer Reports, “Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security,” March 6 2017, https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/.

110 This definition is an adapted version of the Open Access definition. See: SPARC, “Open Access,” n.d., https://sparcopen.org/open-access/.

[111] From the "idealized" perspective of liberal-democratic policymakers, the value of the internet relies on this notion.

[112] This is perhaps one of the most accepted characteristics of the "internet reality" in recent years.

[113] More blatantly, the global internet is not reliant on a single web browser for end user communication just as all users do not rely on a single messaging app.

[114] In the context of freedom and the session element, it's important to recall that we are concerned with the global (i.e., the publicly-accessible) internet. Thus, while some networked technology (like corporate networks) will require certain permissions to open certain sessions, in essence posing a prohibition as described in the framework above, this is not within the purview of our discussion of the publicly-facing, global internet.

[115] In China, for instance, the government has explicitly banned certain VPNs as well as prohibited citizens from using those VPNs. Thus, service providers cannot allow Chinese citizens to open sessions with an outlawed VPN. See: Freedom House, "Freedom on the Net 2017: China," 2017, https://freedomhouse.org/report/freedom-net/2017/china. Similar practices, as previously referenced, occur in Russia.

[116] See previous endnote, which also implicates the openness of the internet architecture.

[117] Cross-site scripting attacks occur when "an untrusted source is allowed to inject its own code into a web application," after which point the malicious code seeps into another session on the device. See: TechTarget, "Cross-Site Scripting (XSS)," n.d., https://searchsecurity.techtarget.com/definition/cross-site-scripting.

[118] Attacks on mountable NFS shares occur when a user gains unauthorized, remote access to a networked file system without administrative privileges. See: Beyond Security, "Finding and Fixing Mountable NFS Shares, a High Risk Vulnerability," n.d., https://www.beyondsecurity.com/scan_pentest_network_mountable_nfs_shares_vulnerability.html.

[119] There are many examples of DDoS attacks preventing users from opening sessions with a given service, perhaps most notably the Mirai botnet that struck American service provider Dyn in 2016. See: Ben Herzberg, Dima Bekerman, and Igal Zeifman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," October 26 2016, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

[120] See previous reference to Iran, which provides a potent example of internet traffic throttling.

[121] "Three-way handshakes" occur when two devices initiate a network connection (through the transport element). Because this process can often reveal information about the devices, however, it can be used by attackers to later compromise the devices' connection.

[122] While perhaps less common than it was several years ago, TCP spoofing enables a malicious actor to send seemingly-legitimate traffic to a victim through masking or "spoofing" their machine's identity. See: Matthew Tanase, "IP Spoofing: An Introduction," March 11 2003, https://www.symantec.com/connect/articles/ip-spoofing-introduction.

[123] Again, this does not mean free of financial cost. There are certainly financial costs involved with the acquisition and use of IP addresses.

[124] DNS cache poisoning occurs when an attacker compromises the database of a Domain Name System (DNS) server. This can lead the server to inadvertently reroute traffic to malicious destinations through seemingly-legitimate means. See: Veracode, "DNS Cache Poisoning Attack Solutions," n.d., https://www.veracode.com/security/cache-poisoning.

[125] Replay attacks occur when an attacker duplicates and resends a stream of legitimate traffic already sent

between two parties. This can cause assorted failures and/or security complications. See: Microsoft Corporation, “Replay Attacks,” March 30 2017, https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks.

[126] The Internet Protocol has not broken to date, but such an event would mean failure in a fundamental building block of the global internet. Dan Geer discusses this general idea in a 2018 paper, citing the Domain Name system root as an example of a critical service “which by the very definition of [its] mission must create a single point of failure.” See: Dan Geer, “A Rubicon,” 2018, https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf, 2.

[127] See earlier endnote on the Mirai botnet, which rendered numerous internet services completely unavailable along the eastern coast of the United States.

[128] Israeli cybersecurity researchers have developed numerous attack techniques to compromise computer hardware through physics, such as reading computer data through the heat generated from a processor. See: Jesse Emspak, “A Computer’s Heat Could Divulge Top Secrets,” July 1 2015, https://www.scientificamerican.com/article/a-computer-s-heat-could-divulge-top-secrets/.

[129] In 2011, for instance, Egypt cut off nearly all access to the global internet from within its borders. See: Matt Richtel, “Egypt Cuts Off Most Internet and Cell Service,” January 28 2011, https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?mtrref=www.google.com.

[130] Figure from: Dwayne Winseck, “The Geopolitical Economy of the Global Internet Infrastructure,” 2017, https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228, 242.

[131] Total security is obviously impossible online, but the point here is to highlight the fundamental incompatibility of these two principles in absolute form.

[132] U.S. National Security Telecommunications Advisory Committee, “NSTAC Report to the President on Internet and Communications Resilience,” 2017, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20DRAFT%20-%20508%20compliant.pdf, 5.

[133] See, for example: Mirko Hohmann and Thorsten Benner, “How European Internet Foreign Policy Can Compete in a Fragmented World,” June 28 2018, http://www.gppi.net/freeandopen; and Robert Potter, “Is Cyberwar Politics by Other Means?” June 27 2018, https://www.policyforum.net/cyberwar-politics-means/.

[134] Ian Levy, “Active Cyber Defence - Tackling Cyber Attacks on the UK,” November 1 2016, https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk.

[135] Elie Bursztein, “Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis,” December 14 2017, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/.

[136] Collin Anderson, “Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran,” June 18 2013, https://arxiv.org/abs/1306.4361, 1.

[137] For instance, see many of the previously-referenced government strategies, such as: Government of France, “Stratégie Internationale de la France pour le Numérique,” 2017, https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.