The Strategic Significance of the Internet Commons

What is a global common? Historically, it has been defined as a naturally occurring domain or area not governed by any single political jurisdiction or nation-state. The high seas, Antarctica, air, and outer space have met this definition and have long been accepted as shared and open resources between nations. They bring economic benefits to nations, facilitate the passage of goods, transport people and business opportunities, and advance science and exploration. Every nation depends on the global commons, and every nation benefits from the global commons. The commons work for everyone only if all parties agree on and enforce the rules.

In practice, the designation of these domains as "global commons" is linked to technological developments and strategic interests. Through advancements in technology and increased dependency on global socio-economic interaction, the global commons have strategically evolved through conscious efforts to be a "system of systems" that provides continued equal access, stability, and economic prosperity for the international community. Cyberspace, much like the high seas, air, outer space, and Antarctica should be viewed as the newest global commons. However, managing it presents a unique challenge.

In the twenty-first-century world, cyberspace connects 2.5 billion people, powers more than one trillion devices, and creates more than 2.5 quintillion bytes of data each day. The utility of cyberspace is undeniable, enabling critical functions across commerce, communication, media, and the military while simultaneously connecting governments, private citizens, and corporations through web-based communications. Cyberspace is a strategic resource that is essential to today's global economy yet poses unprecedented risk and vulnerability. Like the development of global governance for the high seas and outer space, cyberspace needs global governance that preserves its freedom and openness while strengthening its security to protect the shared economic and utility value of all nations.

Defining a New Global Commons

Defining rules that govern the global commons is not an easy task. The Law of the Seas Convention took a decade to establish and remains essential to the world's economy and stability. Too much or too little protection can damage the balance between security and economic stability. As evidenced in the continued debates over adoption of the UN Convention on the Law of the Sea (UNCLOS III) by the United States, the balance between national sovereignty and international economic collaboration is controversial. The original UNCLOS was adapted in 1958 and amended in 1960. UNCLOS III is an effort to continue the protection of free trade and safe passage between the high seas by establishing international governance over territorial disputes tied to exclusive economic zones. As of 2013, UNCLOS III has been implemented by 166 counties and the European Union.[1] However, the United States, along with Colombia, Israel, Peru, and Turkey, have not yet ratified this treaty, as opposition in the US Senate fears damage to economic interests and national sovereignty. Under the treaty, the United States would pay a percentage of its profits, less than 10 percent, to an international treaty organization, which would then distribute the funds among poor and landlocked countries. However, even without ratification, the United States still maintains its commitment for open access to the high seas.

Nation-states have long collaborated on an active role in protecting the sea lanes and preserving the economic utility of the high seas. In 2009, nations recognized that Somali piracy costs the global economy $18 billion per year by increasing the cost of trade.[2] As a result, NATO implemented Operation Allied Protector and Operation Ocean Shield to use naval forces to patrol the Somali coast involving collaboration from the British, Greek, Italian, Turkish, and US navies.[3] Similarly, increased piracy and armed attacks against ships in the Malacca and Singapore Straits have indicated the need to holistically address security and safety concerns in that region. Each year, 60,000 vessels utilize these straits, with 30 percent of world trade and 50 percent of world energy passing through each year.[4] Cooperation between national governments, international and regional organization, and the private sector has been essential for both maritime safety and the preservation of global trade. Continuous collaboration and collective police governance of the high seas is essential to preserving the economic stability, safety, and openness of this shared global resource.

Outer space, the global common that knows no bounds, has provided another example of international cooperative effort. By remaining a global common, outer space has allowed the international community to make significant strides in the fields of science and technology. From satellites to GPS naviga-

tion systems to secure telecommunications, outer space technologies collect data faster and more efficiently than any other form of communication.

In 1959, the United Nations created the Committee on the Peaceful Uses of Outer Space (COPUOS) to establish international agreements on the use and access to outer space. The 1967 Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space is the most widely accepted space treaty, with 100 nations as signatories agreeing that the exploration of outer space should benefit all countries, prohibit the placement of nuclear weapons in space, and be free for exploration and use by all nations. In comparison, the 1979 "Moon Treaty" failed to be ratified by any nation that actively engages in self-launched manned space exploration. This controversial treaty places jurisdiction of all celestial bodies under an international community and subsequently limits activities, regulates resources, and threatens territorial sovereignty over activities allowed. Delegate members of COPUOS continue to debate these aspects of space law and the legal framework underpinning activities in space as member states consider their own use of space and international collaboration.

As of October 2013, 52 nations operated or planned to operate one of the 1,071 satellites currently in orbit around the earth.[5] While the United States is a dominant figure in space technology, operating 42 percent of those satellites in orbit, outer space cannot become the domain of an exclusive few. Space must continue to be governed by the standard of equal access and shared responsibility of protection to all nations.

Cyberspace is new, vast, and its full potential is still unknown. But to protect it as a global common, like outer space and the high seas, requires international cooperation and respect. Cyberspace must have standards to preserve continued global exploration, access, and information sharing.

Cyberspace has no borders and does not fall under any one nation's sovereignty. The 2010 *Quadrennial Defense Review Report* stated that "Although it is a man-made domain, Cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space." Opponents to this perspective argue that since it is run through physical entities located in sovereign states, nations are entitled to ownership and control over its entity. But again, don't all global commons have a physical component? Outer space has satellites, the high seas have ships. Why should cyberspace be any different? Without the shared domain, the physical elements provide no utility.

Threats and Consequences

When first established, the architecture of the World Wide Web was based on the assumption of inherent trust. The Internet was intended for universities and national labs to move large volumes of information across a limited number of trusted nodes. Cyberspace has evolved well beyond what the original creators envisioned it to be and is now a risky domain—susceptible to threats, attacks, diffusion, and conflicts over authority. The Internet was not originally designed to be a global infrastructure for hundreds of millions of people to access in a secure environment. However, we are now connected and able to deliver critical operations and transactions across the world. New policy solutions for the Internet must work in this new global environment.

In the twenty-first century, global communications through proliferation of access to the Internet is changing and blurring technological, economic, political, and cultural boundaries. Moreover, accelerating technological advances and their worldwide dissemination is changing the rules of international relations. Science, technology, information, and ideas are moving from their respective centers to global peripheries. Global information is shared at the local level; local information is shared globally.

As the Internet has grown and innovation continued, so have those seeking to exploit this new domain harmfully. These actors vary in size, scope, and motivation from nation-states stealing intellectual property to cyber criminals seeking financial gain; from internal threats by disgruntled employees to hactivists with a political motivation or personal grudge. Exploitation of global networks, as well as the attack tools being used to carry out these events, are increasing rapidly, and no industry or single organization is fully protected.

At the same time, with the rise of economic activity and market dependency on the Internet, many policymakers are rightly distrustful of heavy governmental control. The Chinese and Russian governments argue that nations must safeguard and control the Internet to protect their sovereignty. As a result, they have become increasingly vocal about rethinking Internet governance and placing it under the United Nations' International Telecommunications Union (ITU) as a means of providing greater control. The United States and the European Union continue to oppose this structure and aim to preserve the Internet's democratic characteristics of openness, speed, flexibility, and efficiency. Similarly, structural investments must be implemented to counter emerging threats and cyber challenges from both state and nonstate actors.

While it is fair to say that the Internet is not a war zone, it could certainly become one. War-like activity has been experienced as recently as 2007, when the Estonian government and financial institutions were the objects of massive denial-of-service attacks aimed at disrupting and denying their ability to function. When Russia invaded Georgia in 2008, ground movements were accom-

panied by cyber attacks aimed at disrupting Georgian command and control functions.[6] Indeed, the United States–China Security Commission, a congressionally mandated body, has identified cyber warfare as an explicit part of Chinese military doctrine.

A Global Governance Strategy

Early Internet governance was designed to be an ad hoc, multi-stakeholder, and self-regulatory approach. The intrinsic value of the Internet is only actualized under this multi-stakeholder environment where freedom and open access are attainable to all participating nations. The global economic and communicative value of the Internet is defined by these very principals of equal access and inherent protection.

Global rules need to be established to preserve the balance between protection of privacy and national security while safeguarding against cyber theft, hacking, and spam. The creation of national and international norms in cyberspace will help protect citizens' safety and privacy, while also thwarting cyber attacks and the malicious use of Internet and cyber communications. The right approach can ensure the protection of civil liberties while preserving the uncontested definition of a global common. However, there must be enforcement of these policies to ensure that those who break them are disciplined and those who consider breaking them are deterred.

The protection of civil liberties and freedoms is not guaranteed under a government-regulated Internet. Some nations consider the spread of democratic ideals and public dissent as a threat to their own national security and are actively seeking ways to replace innovation, openness, and connectivity with international controls and censorship. Under their proposed regulations to the ITU, international norms could sanction comprehensive and unfettered government surveillance of Internet activity, control or repress unwelcome content, and allow political agendas to drive allocation of Internet resources, such as IP addresses. For example, Russia proposed a 2012 treaty provision which would allow governments to shut down Internet access whenever someone in their territory uses the Internet to "interfere in the internal affairs" of that country.[7] Similarly, Iran has laid the technical foundations and garnered support from China to establish a "national Internet" that diminishes Western influence by fragmenting their nation's access to the Internet through a tightly controlled digital portal. In this light, some national efforts to amend current International Telecommunications Regulations and make new legal grounds for Internet control is alarming.

For this reason, the United States made a strategically wise move when on 14 March 2014, the National Telecommunications and Information Admin-

istration (NTIA) announced that it will transfer US government oversight of the Internet Corporation for Assigned Names and Numbers (ICANN). The US government conditioned its move by observing that the transition must not replace "the NTIA role with a government-led or an inter-governmental organization solution."[8] The goal is that a new multi-stakeholder system of governance will develop. The United States is exhibiting trust that the ICANN and the global community will protect the ideals of a free and open internet that is user driven. By adjusting its authority over the Domain Name System, (DNS), the United States is setting a precedent that the Internet should be governed by stakeholders, not by any single government entity.

The United States does not need be the owner of the Internet, but it must play a leadership role in ensuring that Internet openness is maintained and continues to reward innovation, entrepreneurship, and forwarding of diplomatic communication across borders.

A Necessary Path Forward

The world of cyberspace is vast and still largely uncharted. However, as a global community we must commit to preserve the utility and economic value of a global common. The Internet cannot be governed by one. Safeguarding the global commons demands a code of conduct universally supported by a global community. By relinquishing control of the Internet directory "root zone file," the United States demonstrated its commitment to cyberspace as a global common which cannot be owned or ruled by one.

As of February 2013, 65–70 percent of the world's population is not yet online. The need for a new standard of Internet governance will only increase. Without collective leadership to establish these rules, nations may lead to a less open Internet where ideas and discourse are hindered. The US goal, and the goal of most other nations, should be to ensure the Internet remains open and true to the many benefits it provides citizens around the world today. SSQ

Michael Chertoff
Former Secretary of Homeland Security (2005–09)
Co-Founder and Chairman, The Chertoff Group
Member, Global Commission on Internet Governance

Notes

1. "The Global Oceans Regime," Council on Foreign Relations issue brief, 19 June 2013, http://www.cfr.org/oceans/global-oceans-regime/p21035.
2. Ibid.
3. Michael Horowitz, "A Common Future? NATO and the Protection of the Commons," Chicago Council on Global Affairs, http://www.thechicagocouncil.org/userfiles/file/task%20force%20reports/Trans-Atlantic_Papers_3-Horowitz.pdf.
4. "World Oil Transit Chokepoints," US Energy Information Administration, 22 August 2012, http://www.eia.gov/countries/regions-topics.cfm?fips=wotc&trk=p3.
5. Kevin Coleman, "Digital Conflict," *DefenseSystems.com*, 25 July 2013, http://defensesystems.com/blogs/cyber-report/2013/07/satellite-security.aspx.
6. "The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," Armed Forces Communications and Electronics Association (AFCEA), 24 May 2012, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.
7. Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," World Policy Institute, Fall 2013, http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.
8. "NTIA Announces Intent to Transition Key Internet Domain Name Functions," National Telecommunications and Information Administration press release, 14 March 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

Disclaimer