Cyber 2020

Asserting Global Leadership in the Cyber Domain

Booz | Allen | Hamilton

delivering results that endure

Table of Contents

Cyber 2020

Asserting Global Leadership in the Cyber Domain

How should the United States respond as global competitors expand their influence over the Internet and build cyber capabilities? An analysis of four potential scenarios of the Internet in 2020 shows that the United States must develop a strategy that focuses on more than technology to retain its cyberpower status.

Throughout history, the chief source of geopolitical advantage for dominant empires and nation states has been their ability to seize the advantages of new technologies, operational innovations, and organizational models to expand—and ultimately transform—their social, economic, military, and diplomatic capabilities. The domestication of the horse, use of chariots, and new economic models of agro-pastoralism changed society and warfare in the Bronze Age and gave greater significance to armies and "land power" in the Middle Ages. New seafaring technologies and techniques, and economic models of mercantilism and commerce, shifted the geopolitical balance to the maritime world by the sixteenth century, demonstrating the significance of "sea power." Likewise, the invention of the internal combustion engine and the development of the automotive and aerospace industries transformed the economy, society, and national security in the twentieth century, giving rise to the notions of "air" and "space" power. In each of these eras, clearly defined "domains" emerged: land, sea, air, and space. Influence and power shifted to those nations that successfully developed economic concepts, diplomatic rules, military doctrine, and international and national institutions for exploiting new technologies and processes within those domains.

Following this historical course, a new domain has emerged out of the latest technological revolution: the cyber domain. Within this domain, nations with a strong foundation for law and policy, an educated and skilled populace, an entrepreneurial culture of business innovation and investment capital, and a robust information and communications technology (ICT) infrastructure, will emerge as cyberpower nations. For the United States, preserving and furthering our cyberpower posture over the next decade must become one of our most important and enduring national goals.

As with other domains, the emergence of the cyber domain presents the United States with tremendous opportunity and threat. How can we seize the economic and social advantages presented by revolutionary cyber technologies while managing their considerable risks? A viable framework for understanding and governing the new cyber domain will be critical, as will a more holistic vision and definition of cyberspace in a post-convergence world. Cyber policies based on imprecise or inaccurate conceptions of cyberspace will inhibit our ability to develop the strategies and institutions necessary to fully tap the cyber domain's capabilities. At the same time, other national and regional powers now challenging US dominance will be more than eager to fill the leadership void and shape the cyber domain to align with their own interests.

Booz Allen Hamilton recently conducted a series of internal seminars with cyber leaders throughout the firm to define and map the contours of the cyber domain. We found that current models are constrained by legacy definitions of "electronic" technologies and outdated cultural, organizational, and legal boundaries that fail to recognize the convergence of telephone, radio, music, television, satellite, cable, Internet, and other digital technologies into cyberspace. Legacy frameworks are also inadequate to address the global, dynamic nature of cyberspace, where interdependencies cross traditional legal, geographic, and disciplinary boundaries.

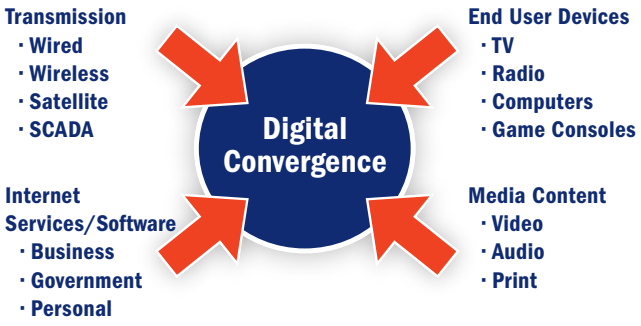
With a goal of challenging status quo precepts, we examined four scenarios of how the cyber domain might develop over the next 10 years. These scenarios

detailed in this paper, offer lessons regarding how the United States can shape the global cyber landscape to promote US economic interests and establish a cyber domain that is transparent, accessible, dynamic, and secure. The goal: Solidify the United States' leadership position as the world's preeminent cyberpower.

Defining the Cyber Domain

Cyberspace is more than just a technology, more than just the Internet. It is a domain—the cyber domain—similar to the domains of land, air, sea, and space, but with its own distinct characteristics and challenges. The cyber domain has national and international dimensions that include industry, trade, intellectual property, security, technology, culture, policy, and diplomacy. At the operational level, it includes the creation, transmission, manipulation,and use of digital information. Technologically, it consists of all converged elements of electronic exchange, including voice, video, and data that involve the movement of electrons and photons across wired and wireless environments. The exchange takes place between devices of varying size and sophistication, such as desktops, laptops, smart phones, mainframes, televisions, radios, supervisory control and data acquisition (SCADA) systems, weapons systems, and communications satellites. Convergence brings together digitized content (e.g., television programs, music, and books), digital devices, digital services, telecommunications, and cable into the increasingly interdependent and complex cyber domain, a domain that has little regard for traditional geographic boundaries.

Exhibit 1 | Digital Convergence



Source: Booz Allen Hamilton

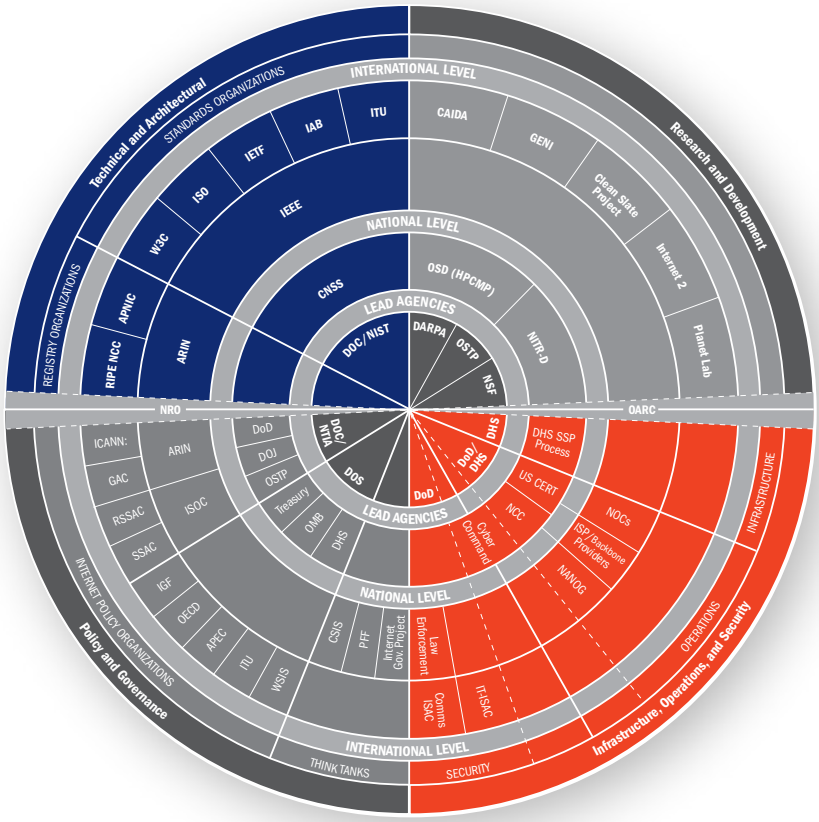
Our public regulatory and policy institutions treat these various elements not as a single, converged cyber domain but as separate and only tangentially related pieces. This approach stems largely from the reality that the relevant policies were developed over a lengthy evolution of electronic communications, beginning with the telegraph in the 1840s, the telephone in the 1880s, radio technologies in the 1890s, and electronics in the 1940s and 1950s. When the digital technologies and communications that we now refer to as "cyber" arrived in the 1960s and gained prominence in the 1980s, there existed more than 100 years of laws, governance models, institutions, and operating concepts dictated by legacy technologies. The International Telegraph Union (now the International Telecommunication Union [ITU]) was created in 1865 to manage international telegraphic communications; the Federal Communications Commission (FCC) was created in 1934 to manage the electromagnetic spectrum congestion created by the proliferation of electronic devices. The Internet Engineering Task Force (IETF) was formalized in 1986 to develop standards around Internet technologies. The Internet Corporation for Assigned Names and Numbers (ICANN) was established by the US Department of Commerce and its partners in 1998 to manage the domain name system. The US Department of Defense, which recently created a new Cyber Command, recognizes cyberspace as a domain but manages its computers and digital networks separately from electromagnetic spectrum and other space-based assets (where the overwhelming majority of satellite assets create, process, and transmit information). At the same time, numerous independent organizations such as the World Wide Web Consortium (W3C) also play key governance roles within the cyber domain. Thus, cyberspace has become governed by a complex, multilayered web of international organizations,

national entities, and industry and volunteer associations, each with its own set of authorities, agendas, and areas of focus.[1]

To date, the decentralized cyber landscape has helped drive the innovative, dynamic development of the Internet and related technologies and services. However, this fragmented approach is also leading to increasing tensions as global business leaders and policy makers wrestle with cyberspace challenges ranging from cybersecurity, content filtering, intellectual property theft, and privacy to e-commerce taxation, net neutrality, Internet Protocol version 6 (IPv6) deployment, and cyber standards. Many of the disputes within the United States concern who should wield authority within the cyber domain. Outside the United States, foreign governments are asserting sovereign rights to control cyberspace within their nations while also pressing for greater influence in shaping the international cyber domain. For example:

- The FCC, US courts, and industry are debating what regulatory authority the FCC has over high-speed Internet companies such as AT&T and Comcast. Obama administration officials contend that the FCC authority is crucial to implementation of many White House cyber initiatives, such as universal broadband access and net neutrality. But many industry stakeholders oppose what they regard as an expansion of FCC authority into a separate domain.
- In May 2010, Congress was reviewing more than 35 different legislative measures for cybersecurity alone, according to a study for Harvard University's

Exhibit 2 | Cyber Governance Environment



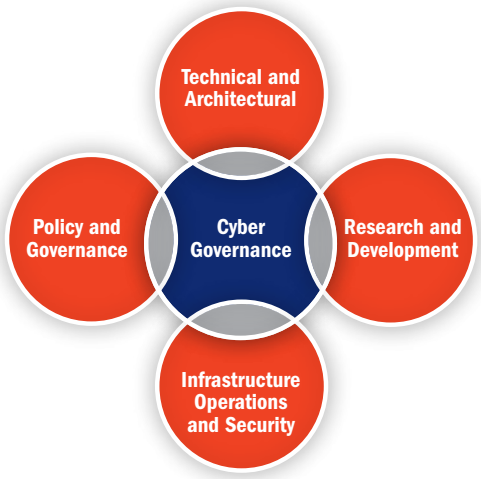
Source: Booz Allen Hamilton

Belfer Center for Science and International Affairs.[2] The proposed bills reflect the organizational and jurisdictional prerogatives of House and Senate lawmakers, each with different aims and oversight authority. Lawmakers are well intentioned, said one observer regarding the numerous bills, but nevertheless "there's a lot of jurisdictional land-grabbing around this topic."[3]

- Cybersecurity legislation introduced by Sens. Jay Rockefeller (D-W.Va.) and Olympia Snowe (R-Maine) ignited a firestorm of opposition to a provision that would give the president authority to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network."[4] Although the Rockefeller-Snowe provision mirrors Section 706(c) of the Communications Act of 1934 in intent, which gives the President control over "communications systems" (but not "information systems") in the event of a national crisis, opponents forced the senators to amend their legislation and publicly avow that "the Rockefeller-Snowe bill will not empower a 'government shut down or takeover of the Internet.'"[5]
- Disputes over electronic privacy and censorship are becoming more frequent as governments seek to impose limits on Internet content providers. Google fought with China over the country's policy of restricting access to information, while YouTube and Facebook have been temporarily blocked by nations that objected to content regarded as anti-Islamic. More recently, the United Arab Emirates said it would suspend BlackBerry mobile services such as e-mail and text messaging because the U.A.E. cannot effectively monitor BlackBerry's highly encrypted data system.[6] The United States struggles with how to establish effective rules for cyber privacy and security, especially those related to monitoring of suspected terrorist activities and the publication of highly sensitive documents.
- Numerous federal entities participate in international efforts aimed at cybersecurity and governance, according to the Government Accountability Office (GAO).[7] These include organizations within the Departments of Commerce, Justice, Defense, and Homeland Security, along with the Federal Trade Commission and US Trade Representative, which collectively share many responsibilities and often participate in the same international bodies addressing cybersecurity. However, the GAO said these federal organizations "have not demonstrated an ability to coordinate their activities and project clear policies on a consistent basis," nor has the federal government "forged a coherent and comprehensive strategy for cyberspace security and governance policy" to guide its activities in the international realm.[8]
- China's Information Office of the State Council issued a white paper on "The Internet in China" in June 2010 asserting that "the UN should be given full scope in international Internet administration" and "all countries have equal rights in participating in the administration of the fundamental international resources of the Internet."[9] Participants in international groups that are shaping cyber governance and standards note that China's delegations are becoming much better organized, and present a unified, coordinated front at working group meetings and conferences, helping to expand China's influence and promote its interests within the cyber domain.

These and other ongoing controversies illustrate the obstacles policy makers face in establishing a coherent national strategy for addressing cyber challenges and shaping the cyber domain to our strategic advantage. Although the White House and Congress are responding to demands for greater broadband, cybersecurity, education and training, Internet governance, and other pressing needs, our nation's leaders have not clearly defined the cyber domain, which is still viewed, organized, and managed in

Exhibit 3 | The Cyber Domain



Source: Booz Allen Hamilton

essentially the same legislative and executive branch silos of the past 50 years. Each agency presses ahead with its own plan based on its own narrow writ; each corporation pushes for policies that satisfy its own narrow needs. Tensions between the public and private sectors over the US government's proper role in cyber governance further complicate efforts to craft a comprehensive plan that ties together US cyber-related activities and encourages stakeholders in the public, private, and civil sectors to work together toward common goals. We still have time to develop and assert a unified vision of the cyber domain. But if we hesitate, other nations are more than prepared to step in as global leaders to define the domain based on their values, interests, and agendas.

Embracing the Cyber Domain

The United States has been and continues to be the dominant player in developing Internet technologies, assigning domain names, routing traffic, and developing international protocols and standards. However, in recent years, Brazil, China, India, Russia, and other nations have sought a stronger role in Internet governance. They want to treat the Internet as an international cyber domain, not as a network owned and controlled by US interests. Their growing technical capabilities—such as their rapid adoption of IPv6, their manufacturing prowess, and their rapidly expanding markets of Internet users—will make it difficult if not impossible to ignore their efforts to be included in cyber governance. In fact, these nations, acting collectively or alone, could establish rival Internet systems that give the United States and other Western powers only limited access and influence. Rather than trying to shut out these potential rivals, our policies should be aimed at bringing them into a more inclusive cyber governance framework, with the goal of retaining our pre-eminence while sharing authority and promoting US economic and political values.

Promoting international agreement and collaboration within the cyber domain will require greater public sector involvement. This does not necessarily mean more government regulation and control. There are other avenues for advancing US cyber interests. Similar to government activities relative to the sea, air, land, and space domains, the government should become involved in both domestic and international cyber initiatives. These could include efforts such as negotiating international agreements addressing cyber risk reduction; seeking common ground on privacy; enforcing intellectual property rights in cyberspace; convening and participating in international standards bodies; supporting technical training programs at home; identifying, preserving, and promoting critical industrial base components; leading global governance institutions in developing proper frameworks for a post-convergence environment; being a catalyst for high assurance industries; and spearheading national cybersecurity planning. Recognizing cyber as a unique domain provides a starting point for understanding the instruments of power available to promote US cyber interests, as well as for discerning government's proper role in applying its authority.

Our strategy must address the non-technical aspects intrinsic to the cyber domain—such as diplomacy, education, culture, economics, and standards—because these issues will determine how

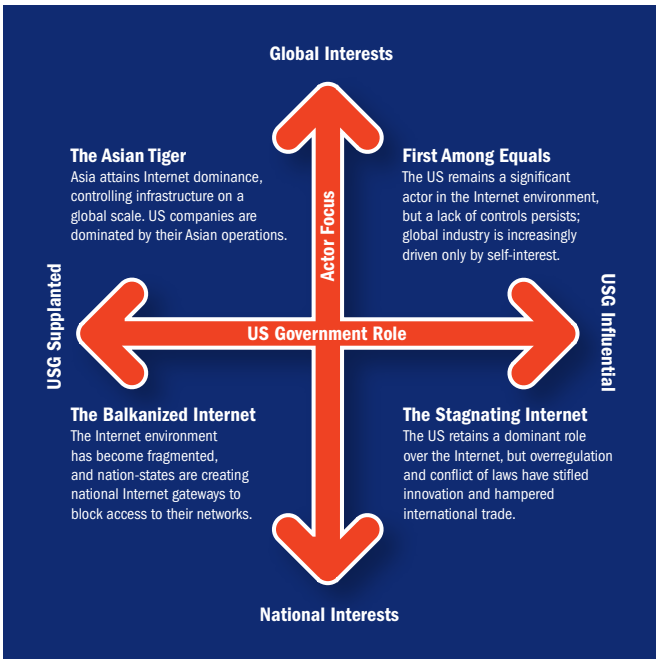
emerging applications and networks are used, whether networks remain private and secure, and who uses them and for what purposes. The cyber domain is more than just technology, more than just electrons and photons moving across networks. It is a multi-dimensional domain. An effective strategy requires a comprehensive framework that captures the complex, dynamic interplay among its many dimensions. Building the network is not enough—we must govern, operate, and protect it, including its data and users—across a global landscape.

Ultimately, our nation's goal is cyberpower. Just as we strive for pre-eminence as a sea power, land power, air power, and space power, so too should we strive for preeminence in the cyber domain. Cyberpowers will be those nations that strategically use information and communications technologies to spur economic growth, empower civil society, and enhance national security. The cyber domain holds the promise not just of huge gains in economic performance but also of promoting social and political values such as transparency, democratic participation, and the open exchange of ideas. We want to position ourselves to shape the development and use of cyber by all nations and world users, so that all may share in its benefits.

Shaping the Cyber Domain

Although the future state of the cyber domain is difficult to predict, our understanding of cyber as a domain, coupled with our understanding of the current issues and tensions, provides insight into how the domain may evolve during the next decade. Toward that end, Booz Allen Hamilton explored potential scenarios that could play out as nations compete for influence and advantage. Specifically, we examined scenarios that move from a strong US role to a weak US role along one axis; and, at the same time, we examined scenarios that move from exclusionary (nationally focused) cyber policies to inclusive (globally focused) cyber polices along the other axis. (See Exhibit 4 for an illustration of scenarios). Each of the four major scenarios presented different challenges, policy choices, risks, and rewards for the United States.

Exhibit 4 | Scenarios



Source: Booz Allen Hamilton

Scenario 1: A Foreign-Dominated Internet.

A single nation or a coalition of nation states becomes the dominant power within the cyber domain, where 75 percent of Web sites map to non-Latin character domains. US companies gradually become dominated by their foreign operations and rely on equipment manufactured overseas. As the spread of inexpensive Internet-enabled mobile devices strains the infrastructure, the United States fails to invest to build out its infrastructure due to arcane legal, policy, and institutional regimes that act as barriers to competition. As a result, engineering and design expertise follows manufacturing to Asia, which adds new product innovation to its manufacturing dominance and sets the standards for the rest of the world.

How it occurs. Brazil, China, India, Russia, and other nations are already positioning themselves as world leaders in cyberspace, not necessarily through confrontation, but by executing comprehensive national strategies aimed at developing technical expertise,

building robust infrastructures, supporting cyber industries, and expanding their cyber governance influence. China, for example, has already become the manufacturing leader for critical Internet components. In addition, some nations are looking to move beyond manufacturing into other high-value activities, particularly innovation, where the United States is the world leader. Similarly, some nations, especially those in Asia, are moving to IPv6 more rapidly than the United States, thus enabling them to leverage its advantages sooner by "leap-frogging" existing technologies and taking a lead in defining next generation standards and products for this enhanced network environment. In contrast, the United States is saddled with legacy infrastructure that could hinder cyber growth. These nations may well form a coalition to counterbalance a perceived Western bias in many cyber institutions and norms. In particular, Asia has the benefit of an overwhelming market size, which can have significant influence on defining the future of cyberspace.

Implications. Under such a scenario, the cyber domain would likely adopt a non-Western bias toward content, language, and technology. Increasingly, infrastructure would be designed, engineered, and built outside the United States, increasing supply chain risk and network traffic flows through other regions, impacting the bottom line of US-based ISPs and limiting law enforcement access to that traffic. The United States probably would not be totally supplanted because of its market size, general leadership role, and ability to innovate, but Europe's influence and relevance could dramatically fall. Even if these other nations became responsible stakeholders, they would likely establish international cyber organizations that are predicated on their interests rather than ours.

Scenario 2: A Fragmented Internet.

The cyber domain becomes fragmented as nation states or regions create independent Internet networks with gateways to control access to their networks. Each nation or region has its own laws and regulations for its networks; as a result, Internet companies, in some instances state-owned or controlled, focus on national and regional services rather than on reaching consumers throughout the world. An alternative communications protocol to TCP/IP gains widespread adoption to counter the Western-dominated Internet. As a security measure, the United States bans alternative protocols but cannot enforce the ban. Overall, interoperability is hampered on a global scale, as is the ability of the United States to exploit e-commerce, promote US values, and protect US interests by gathering electronic information abroad.

How it occurs. Under this scenario, we would see enclaves of influence and power as nations and regions seek to maximize cyberpower with beggar-thy-neighbor policies that enable them to capture home markets and bolster cyber industries at the expense of competitors. Nations would pursue cyber growth as a zero-sum game. However, economic motivation might not be the only driver behind a fragmented cyber domain. For example, the United States might limit access to keep networks secure, perhaps after being victimized by a series of attacks; conservative elements within the Middle East might want to expand the blocking of Western content for cultural reasons; the Chinese government might be concerned about political instability; and Europe might be driven toward regional isolation to protect itself from incendiary racial content or the weak privacy rules of other enclaves. The regions would remain interconnected; it is not possible to completely shut off the Internet. But cross-regional traffic would be severely limited and would slow in comparison to today's data flow, likely due to substantial deep packet inspection and content filtering.

Implications. As in the first scenario, US influence would be greatly diminished. However, no single nation or coalition would dominate. A fragmented Internet would significantly diminish cyber efficiencies and could profoundly hinder global economic growth. Furthermore, the importance of the English language throughout the world would be reduced substantially. The constricted flow of ideas would impair innovation, although this

negative impact could be offset to some degree by competition between regions and states. Likewise, global organizations and cross-regional alliances would disappear, but bilateral or small regional alliances would likely strengthen considerably. These strengthened alliances would be driven not so much by geographic borders and political entities but by shared norms, values, language, etc., thus suggesting a more fragmented political as well as cyber landscape. Internet companies would focus on national markets due to the complexity of regional cyber laws.

Scenario 3: A Stagnating Internet.
Unlike the first two scenarios, the United States retains a dominant role over the cyber domain. But government regulations and laws stifle innovation and hamper international trade instead of facilitating commerce. The US adopts a heavy regulatory hand, creating greater costs, uncertainty, and complexity for companies wishing to invest in infrastructure or provide innovative new services. The United States implements strict trade and security laws for Internet technologies because of poor intellectual property rights enforcement and concerns over transfers of leading edge technology. Because of attacks on the nation's Smart Grid and other systems, all Internet traffic flowing into the country is now filtered at four regional gateways. This heavy-handed US governance—aimed at both enhancing US economic competitiveness and bolstering cybersecurity—generates significant global opposition, further inhibiting commerce and cyber development. Foreign competitors coalesce to wrest power from the United States.

How it occurs. If the US government continues to devise cyber practices and policies without formulating an overarching strategy—or, at least, a coherent approach to cyber standards and policy—we risk developing uncoordinated, conflicting regulations and laws that ultimately could weigh down industry and private users. A haphazard approach, driven by a lack of consensus about the government's proper role, could result in heavy regulation in some areas but too little in others. The lack of overarching strategy also could lead to dramatic over-regulation following a major Internet disruption or attack where the response is mismanaged due to a lack of clear guidelines around roles/responsibilities of the federal and private sectors. This too could have significant impact on the US cyber industry and international cooperation.

Implications. In addition to its negative economic consequences, this scenario would likely trigger efforts by competitors to supplant the United States, perceived as an ineffective, nationalistic steward of the cyber domain. Thus, this scenario could be a precursor for scenarios No. 1 (Foreign-Dominated Internet) or No. 2 (Fragmented Internet). In the latter scenario, a dominant actor fails to emerge and the cyber domain devolves into competing enclaves; and in the former, a nation or coalition supersedes the United States as the key player.

Scenario 4: A US-Led Global Internet.
The United States remains the most significant actor in the cyber domain as the US government takes the lead with partners in establishing a new international organization to set standards and govern the Internet. However, US industry continues to be the driving force behind cyber innovation and economic growth, and US regulatory agencies have become increasingly irrelevant. As the Cyber Age enters its fifth decade, a massive wave of mergers and acquisitions results in industry consolidation around a handful of global ICT giants, similar to the consolidation around the big three automakers in the 1950s. A few dominant global Internet service providers compete ferociously, causing occasional outages as they repeatedly de-peer. They gradually gain a monopoly over daily life as wired consumers rely on the Internet for everything from groceries to doctors' appointments.

How it occurs. In many respects, this is a natural extension of the United States' current implicit policy supporting free-market principles. It envisions that the US government will lead efforts to establish new international alliances and institutions governing the cyber domain. By taking a leading role, the

United States would be able to shape international programs and approaches that encourage access, transparency, privacy and security, free enterprise, and other principles aligned with our national interests. But this scenario also highlights the need for the US government, in collaboration with private- and civil-sector stakeholders, to adopt coordinated, comprehensive policies and safeguards to protect citizens, consumers, and infrastructure by addressing issues such as cybersecurity, Internet openness, privacy/civil liberties, and equal access.

Implications. This scenario would provide the United States with major economic opportunities by virtue of the nation's central role in setting major cyber standards and other governing initiatives, which would give US companies a natural competitive advantage. However, a coordinated cyber strategy that includes industry and international partnership components is necessary to avoid potential negative outcomes such as the one in the scenario. The role of multi-stakeholders (industry, government, and civil society) in this scenario must be balanced to ensure overlapping vital interests prevail, rather than the prerogatives of any one stakeholder group. All nations, including strategic competitors, would benefit from an inclusive approach to governance that allows wider participation and voice, but also strengthens common economic and political values across the cyber domain.

Cyberpower: Mastering the Cyber Domain

Both globally focused scenarios—"Foreign-Dominated Internet" and "US-Led Global Internet"—would likely provide the largest economic benefit to the United States and, in fact, to all nations in terms of greater innovation and lower prices. However, some US policy makers might prefer the "Stagnating Internet" scenario to the "Foreign-Dominated Internet," because the United States would still be the cyber domain's global leader, though much less prosperous under the "Stagnating Internet" scenario. Clearly, the "US-led Global Internet" scenario could place the United States in the strongest economic and political position within the cyber domain. However, even this scenario carries with it negative consequences unless: 1) the US government seeks strengthened collaboration with the private and civil sectors towards setting a robust, rational cyber policy; 2) the United States works with foreign competitors to cooperatively address global cyber governance and security challenges; and 3) foreign countries find it in their best interest to cede to the general principles of transparency, openness, and free-market enterprise that we regard as essential to a secure, vibrant cyber domain.

Achieving this ideal state would be challenging for several reasons:

- The US government today is poised to lead the establishment of international standards, norms of behavior, and rules of engagement for the cyber domain. However, US government and industry have failed to evolve a truly productive public-private relationship around cyber that boosts security and leadership without sacrificing industrial competitiveness. Industry questions the value of government involvement and is reluctant to provide propriety data. Consequently, the US government will have to develop its own national policy regime—with stakeholder buy-in—before trying to work with other nations.
- Although the US government could take the lead in forming new international alliances and institutions, these structures would differ from previous ones (particularly the alliances) and may have some unusual participants. Moreover, the new alliances would not be predicated on traditional threats, nor on traditional notions of communications that do not address the realities of a converged environment. (For example, the basis for NATO was a massive, imminent geopolitical and military threat.) New alliances might be built around common interests such as culture or economics. Differences such as the US predilection towards openness versus other nations' desire for more content filtering are likely to pose continuous challenges for any alliances.

- The United States is ripe for accusations of cyber imperialism. The US government would be in the forefront of setting the standards and establishing alliances, as well as developing and implementing regulatory policies. Being so influential could lead other actors to resent the US far more than they do today.
- A slow economic recovery or a relapse into recession could push the United States toward protectionism, which could include a movement to assert greater unilateral control over cyber governance policies, practices, and institutions.
- A massive cyber attack on the United States—one that leads to heavy economic damages or loss of life—might force the government to impose stronger controls on Internet traffic, limiting commerce and information exchange.

Realistically, it is unlikely that any scenario above will develop to the exclusion of the others. Today, in fact, we see the cyber domain being pushed and pulled toward each of the scenarios by a vast array of competing activities and interests among the world's nations. However, the sharp distinctions between scenarios we have drawn in this paper can help us better understand the potential impact of US policies—and, in some cases, lack of policies—in shaping outcomes within the cyber domain.

Next Steps

Our ultimate objective is cyberpower. Cyberpower is not a military objective, nor is it synonymous with military might. Cyberpower is capturing the advantages of cyber technologies, process innovations, and governance models to significantly improve our nation's social, economic, military, and diplomatic capabilities. It is about optimizing both our economic and national security posture within the new cyber domain.

The scenarios above provide a range of possible futures for cyberspace. The primary instruments of power and change in any scenario boil down to three elements: policy, strategy, and governance.

- **Policy.** Some might argue that the United States can retain its current leadership position without expanding government involvement beyond the status quo. After all, the federal government is not completely inactive. The Bush administration initiated the National Strategy to Secure Cyberspace and the Comprehensive National Cybersecurity Initiative (CNCI) to dramatically increase resources to combat the growing cyber threat. The Obama administration and Congress have launched numerous programs and initiatives aimed at strengthening the nation's cyber posture in areas such as cybersecurity, broadband, open government, the Smart Grid, digital health, secure online transactions, Internet governance, and cybersecurity education and training. But if these efforts are not united by a coherent, overarching policy and legal framework, and well thought-out economic incentives, many will fail to gain the momentum or support required to become permanently enabled.
- **Strategy.** The US government spends over $100 billion annually on ICT, which, combined with its ability to develop laws, enter into treaties, drive standards, create tax policies, and provide overall leadership, gives the government enormous influence in shaping the cyber domain. The US government cannot sustain its cyber dominance with its current uncoordinated approach; cyber is a multidimensional domain that requires a national strategy and strong government leadership. Without a robust cyber strategy, we could be slowly pushed toward one of the less desirable scenarios by nations that are crafting comprehensive cyber policies that favor their interests over our own.
- **Governance.** The United States must develop new governance models that recognize the full breadth of a distributed yet converged cyber domain. Legacy institutions with lines of authority created for the pre-digital age hinder our ability to effectively address cyber challenges. As the GAO noted, agencies with overlapping authority must develop effective mechanisms for collaborating on

shared mission activities. But even more important, agencies must learn to collaborate proactively with global stakeholders from the private sector, civil society, and foreign governments. Private sector organizations, including foreign-controlled entities, own and control the majority of assets in the cyber domain. Consequently, the federal government will need to rationalize authorities and streamline processes as it develops a new governance model that includes robust and meaningful participation by the international "megacommunity" of stakeholders from governments, business, and civil society.

Conclusion

Currently, the United States is the global leader in the cyber domain. Our overall ability to create innovative technologies and services, start new businesses, invent efficient processes, and stimulate economic growth remains second to none. This is what has allowed us to maintain our special status as the leader in global cyber governance over the past two decades. But the environment is showing signs of change. Although we provided the world with the original Internet protocols and institutions, today's cyber challenges have grown to a size and complexity that overwhelm our fragmented legacy approach. As the infrastructure and our reliance upon it have matured, our policy and regulatory approaches have remained static, uncoordinated, overlapping, and too often conflicting, with business and government leaders unable to agree on a cohesive strategy for maintaining growth and security. Through innovation, long range strategic planning, and the persuasive force of an exploding user base, our foreign competitors are challenging our economic preeminence and earning a greater voice in cyber governance. Collectively, these challenges threaten to erode our lead in cyberspace and, by extension, our economic standing and national security.

We believe the United States can successfully resolve these cyber challenges and retain its leadership position by adopting a strategic approach that recognizes cyber as a unique domain of converging digital technologies and legacy policy doctrines. This includes developing a strategy that addresses all dimensions of the cyber domain and coordinates roles and responsibilities across cyber's key stakeholders. Current government policies suggest that US leaders are committed to developing our cyber capabilities. We must develop an overarching vision and plan for how we want to shape and manage the cyber domain. Wise choices will not only enhance US cyberpower; they will also promote policies and values within the emerging cyber domain that will benefit all global users and citizens of all nations.

Appendix

History's Lesson: How the Maritime Domain Developed Over Time

The US Department of Defense recently established the US Cyber Command, essentially recognizing cyber as one of its military domains, joining the domains of air, land, sea, and space.[10] But what does it mean to be a domain, and how does a domain develop? And how do nations exert influence and become dominant forces within a domain? The development of the sea domain provides an instructive comparison.

Background. While the sea domain has been important since ancient times, it took a maritime revolution in the 15th and 16th centuries to make sea power both global and an important component of economics and geopolitics. This revolution crystallized in Portugal under the leadership of Prince Henry the Navigator, who improved upon and combined existing technologies and techniques (magnetic compass, astrolabe, lateen sail, oceanographics) into a fleet built around the caravel—an agile and powerful ship that paved the way for oceanic travel and created the foundation for an economy based on global maritime trade. From the 16th to mid-19th centuries, the Age of Sail transformed the global economy and power centers as waves of successive maritime powers—Portugal, Spain, Dutch, French, and English—competed in the "sea" domain.[11]

Governance. Initially, control and governance over the sea was determined by the policies, economies, and technologies of the dominant powers. Beginning in the 1600s, nations followed the principle of "Freedom of the Seas," in which national maritime boundaries and controls were determined by a boundary of three nautical miles from the shoreline—the maximum range of a cannon shot. Everything else was considered international waters. However, as the sea became more important to global commerce due to its abundant resources (e.g., fish, oil, gas, minerals), a series of international conventions began to create norms, provide definitions, identify boundaries, and establish rules for the seas. These United Nations Conferences on Law of the Seas, held between 1956 and 1984, spurred a whole host of treaties, agreements, and regimes: port authorities, navies, coast guards, rules of engagement, fishing rights, whaling laws, environmental regulations, maritime research institutions, and maritime industries.

Impact. Today, no single nation owns the oceans or maritime domain, though a nation may control its own coastal waters as well as rivers and tributaries that flow into the ocean. Vessels at sea in international waters display the flag of their "flag state," the jurisdiction they are subject to for legal purposes. We have given authority to local, national, and international organizations to oversee compliance, adjudicate disputes, and develop new regulations and policies as they arise. We still have problems and disputes, but for the most part, the world's seas represent a vibrant domain that provides nations, businesses, and people with economic prosperity, recreation and

leisure, and security. Nations that successfully exploit ocean resources—economically as well as militarily—are recognized as sea powers. Over the years, the United States has established the public and private sector institutions necessary to ensure our standing as the world's leading sea power. The US Navy, US Coast Guard, and Department of Transportation Maritime Administration (MARAD) have integrated their efforts through a series of policies, strategies, operating concepts, and initiatives under the rubric of Maritime Domain Awareness.

Relevance. The emergence of a new cyber domain has instigated disagreements and competition among nations (and stakeholders within those nations) who are vying to exploit it. The Law of the Seas governing the ocean domain evolved slowly over time; it would be unrealistic to expect nations to reach immediate agreement on protocols and rules for the highly complex cyber domain. This will be difficult, contentious work. But it also would be unrealistic to expect this work to be accomplished without strong US government involvement in international governing institutions. Similarly, it would be unrealistic to expect the United States to develop into a cyberpower without comprehensive policies aimed at strengthening all dimensions of its activities within the cyber domain—just as the United States became a sea power by adopting maritime policies that fostered a strong shipbuilding industry, merchant marine, ports and harbors, education and scientific research about the oceans, weather stations, and a Navy and Coast Guard to protect ships and shipping lanes. Although nations may seek military dominance within a domain, the real source of a domain's transformative power lies within the economic and social realm.

Cyber Organizations

- APNIC: Asia-Pacific Network Information Centre
- ARIN: American Registry for Internet Numbers
- CAIDA: Cooperative Association for Internet Data and Analysis
- CNSS: The Committee on National Security Systems
- Comms ISAC: Communications Information Sharing and Analysis Center
- CSIS: Center for Strategic and International Studies
- CYBER COMMAND: United States Cyber Command
- DARPA: Defense Advanced Research Projects Agency
- DOC: Department of Commerce
  - NIST: National Institute of Standards and Technology
  - NTIA: National Telecommunications and Information Administration
- DoD: Department of Defense
- DHS: Department of Homeland Security
  - SSP: Sector Specific Planning Process
- DOJ: Department of Justice
- DOS: Department of State
- Treasury: Department of Treasury
- GAC: Government Advisory Committee (ICANN)
- GENI: Global Environment for Network Innovations (NSF)
- IAB: Internet Architecture Board (IETF)
- ICANN: Internet Corporation for Assigned Names and Numbers
- IEEE: Institute of Electrical and Electronics Engineers
- IETF: Internet Engineering Task Force
- IGF: Internet Governance Forum
- ISO: International Organization for Standardization
- ISOC: Internet Society
- ISP: Internet Service Providers
- IT-ISAC: Information Technology – Information Sharing Analysis Center
- ITU: International Telecommunication Union
- NANOG: North American Network Operators Group
- NCC: National Coordinating Center for Telecommunications
- NITR-D: National Coordination Office for Networking and Information Technology Research and Development
- NOCs: Network Operations Centers
- NRO: Number Resource Organization
- NSF: National Science Foundation
- OARC: DNS Operations, Analysis, and Research Center
- OECD: Organisation for Economic Co-operation and Development
- OMB: Office of Management and Budget
- OSD (HPCMP): Office of the Secretary of Defense (High End Computing Infrastructure and Applications)
- OSTP: Office of Science and Technology Policy
- PFF: Progress and Freedom Foundation
- RIPE NCC: Réseaux IP Européens Network Coordination Centre
- RSSAC: Root Server System Advisory Committee (ICANN)
- SSAC: Security and Stability Advisory Committee (ICANN)
- US CERT: United States Computer Emergency Readiness Team
- W3C: World Wide Web Consortium
- WSIS: World Summit on the Information Society

Notes

[1] The Government Accountability Office (GAO) identified 19 international organizations that it regarded as the most influential in the realm of cybersecurity and governance of cyberspace. "Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance," (GAO-10-606), pp. 8-9.

[2] Melissa E. Hathaway, "Cybersecurity: The US Legislative Agenda," Belfer Center for Science and International Affairs, Harvard University, May 10, 2010.

[3] Ben Bain, "Cyber policy snared in legislative tangle," *Federal Computer Week*, June 3, 2010.

[4] Cybersecurity Act of 2009, S. 773, April 1, 2009, Section 18, Cybersecurity Responsibilities and Authority.

[5] Roy Mark, "Presidential Internet Kill Switch May Still be Alive," eWeek.com, Sept. 20, 2009.

[6] Barry Meier and Robert F. Worth, "Emirates to Cut Data Services of BlackBerry," *New York Times*, August 1, 2010.

[7] "Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance." Rutherford, "Rockefeller's Office Responds to Cyberterrorism Bill."

[8] "GAO, Cyberspace," (GAO-10-606), pp. 33, 39.

[9] "Full Text: The Internet in China," People's Daily Online, June 8, 2010; Evan Osnos, "Can China Maintain 'Sovereignty' Over the Internet," *The New Yorker*, June 11, 2010.

[10] William J. Lynn III, "Defending a New Domain," *Foreign Affairs,* September/October 2010.

[11] The Chinese actually had an early lead in sea power during the 14th and 15th centuries, expanding maritime trade in East Asia and dispatching imperial fleets to the Indian Ocean between 1405 and 1433. However, internal opposition to outside contact led the Ming Dynasty to cease expeditions in 1433, leading to a power vacuum in the Indian Ocean which was filled by Portuguese, Dutch, French, and English traders.

Contacts

Cyber Strategy

Patrick Gorman
Senior Executive Advisor
gorman_patrick@bah.com
703/377-0016

David Sulek
Principal
sulek_david@bah.com
703/984-1085

Cyber Advanced Analytics

Suzanne Storc
Principal
storc_suzanne@bah.com
703/984-0925

Cyber Policy and Governance

Evelyn Remaley Hasch
Lead Associate
hasch_evelyn@bah.com
703/984-0818

Cyber Futures and Scenarios-based Planning

Lisa Heald
Senior Associate
heald_lisa@bah.com
703/377-6386

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, the firm is a major provider of professional services primarily to US government agencies in the defense, security, and civil sectors, as well as to corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning strategy and organization, technology, operations, and analytics—which it combines with specialized expertise in clients' mission and domain areas to help solve their toughest problems.

The firm's management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. By combining a consultant's problem-solving orientation with deep technical knowledge and strong execution, Booz Allen helps clients achieve success in their most critical missions—as evidenced by the firm's many client relationships that span decades. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cyber-security, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 23,000 people, and has annual revenues of approximately $5 billion. *Fortune* has named Booz Allen one of its "100 Best Companies to Work For" for six consecutive years. *Working Mother* has ranked the firm among its "100 Best Companies for Working Mothers" annually since 1999. More information is available at www.boozallen.com.

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.

Booz | Allen | Hamilton

Principal Offices

ALABAMA
Huntsville

CALIFORNIA
Los Angeles
San Diego
San Francisco

COLORADO
Colorado Springs
Denver

FLORIDA
Pensacola
Sarasota
Tampa

GEORGIA
Atlanta

HAWAII
Honolulu

ILLINOIS
O'Fallon

KANSAS
Leavenworth

MARYLAND
Aberdeen
Annapolis Junction
Lexington Park
Linthicum
Rockville

NEBRASKA
Omaha

NEW JERSEY
Eatontown

NEW YORK
Rome

OHIO
Dayton

PENNSYLVANIA
Philadelphia

SOUTH CAROLINA
Charleston

TEXAS
Houston
San Antonio

VIRGINIA
Alexandria
Arlington
Chantilly
Charlottesville
Falls Church
Herndon
McLean
Norfolk
Stafford

WASHINGTON, DC

The most complete, recent list of offices and their addresses and telephone numbers can be found on www.boozallen.com by clicking the "Offices" link under "About Booz Allen."

www.boozallen.com