I. Introduction

Just prior to his confirmation as Commander of US Cyber Command (USCYBERCOM), General Keith B. Alexander identified the need to improve cyberspace situational awareness as one of his central responsibilities—and challenges.\(^1\) This mission is rooted in the need to monitor computing activities across the 15,000 networks and seven million devices that compose the Department of Defense (DoD) information and communications technology (ICT) enterprise.\(^2\) Complicating this mission further, USCYBERCOM must also conduct offensive operations in cyberspace and potentially assist the Department of Homeland Security’s (DHS) efforts to defend other information systems across the federal government and US critical infrastructures.\(^3\) These demands help explain what a Defense Information Systems Agency official recently called DoD’s “insatiable desire for situational awareness” in cyberspace.\(^4\)

Unfortunately for those who would seek to assess USCYBERCOM’s progress, no “gold standard” exists for cyberspace situational awareness. It remains challenging to envisage the bounds of future situational awareness capabilities, let alone performance metrics. Thus, analyzing the present state of cyberspace situational awareness for a potential competitor yields a richer understanding of the relative US position. China serves as a sensible counterpart in this comparative analysis for several reasons. Some cite China as a potential military competitor\(^5\) and future conflicts appear poised to spill into (if not originate in) the cyber domain.\(^6\) China’s military, moreover, has a well-documented offensive cyberwarfare doctrine that in some respects appears directed toward the United States.\(^7\)

In parallel, China conducts sometimes “pervasive” internet censorship as part of “one of the largest and most sophisticated filtering systems in the world,” according to the OpenNet Initiative.\(^8\) Policymakers traditionally view internet censorship as a human rights issue.\(^9\) In the past year, however, several technology companies have cogently argued that censorship also acts as a barrier to trade.\(^10\) This article complements these views with a discussion about internet censorship’s security-related implications. Specifically, this analysis argues that some of China’s internet censorship techniques likely improve that nation’s cyberspace situational awareness—which could affect the outcome of a conflict in cyberspace.\(^11\)

This argument advances in section II with an explanation of some key concepts. Section III provides a brief survey of the development and state of cyberspace situational awareness within the United States. Sections IV and V, respectively, explain some key features of the cyber domain in China and gauge their impact for cyberspace situational awareness. Section VI identifies some inherent tradeoffs in the composition of the cyber domain in China. Section VII offers some conclusions and implications for US policymakers.\(^12\)

---

\(^{a}\) This paper presents the author’s personal views and does not reflect those of any institution with which he is affiliated. The author wishes to thank Edward Monan and several anonymous reviewers, whose thoughtful comments on previous drafts helped to greatly improve this paper.
II. Definitions and key concepts

Internet censorship

For the purposes of this analysis, “internet censorship” is any measure enacted to restrict internet accessibility, processes, functions, or content based on sociopolitical imperatives. Such efforts take place in four distinct realms: laws and regulations; norms; markets; and architecture. This paper emphasizes the architectural component, which has the most direct implications for situational awareness. The term “architecture” refers to the physical dimension of cyberspace, described in the National Military Strategy for Cyberspace Operations as “information systems and networks, computers and communications systems, and supporting infrastructures.” Architecture also encompasses network design and layout and the nature of connections with other networks, including those beyond national borders.

States can conduct censorship at four key architectural layers. These include, from least to most centralized: individual computers, organizations, internet service providers (ISPs), and the internet backbone. China has generally succeeded in exerting control at each of these four layers. For example, at the individual layer, Tencent’s popular instant messaging software QQ incorporates a client-based keyword-blocking utility. At the organizational layer, China requires all internet content providers, such as websites, to gain licenses and comply with censorship mandates. China “outsources” some censorship responsibilities to ISPs, the third architectural layer, which must police domestic internet content and enforce website closures. Finally, this article centers on China’s robust filtering activities at the internet backbone layer, specifically at gateways between Chinese networks and the rest of the internet.

Cyberspace situational awareness

The Department of Defense (DoD) has no official, unified definition for “cyberspace situational awareness,” despite the term’s frequent, government-wide usage since the mid-2000s. The 2006 National Military Strategy for Cyberspace Operations, however, sufficiently describes the concept:

Cyberspace situational awareness enables commanders and planners to assess the current situation, collaborate on courses of action, take action, and anticipate opportunities and challenges in the domain. Automated tools must be employed to provide near-real time notification of anomalous activity and properly inject appropriate data into operational views to characterize the cyberspace activity. This situational awareness combined with proper risk assessments, including intelligence loss or gain determinations, will allow commanders to make the best decisions on courses of action.

An important distinction must be made between enterprise situational awareness and domain situational awareness. Enterprise situational awareness is visibility of the events and activities within a single entity’s networks. This capability would, for example, enable informed computer network defense operations. However, defense against a large-scale, coordinated cyberattack targeting government, private industry, and privately owned infrastructures would require some level of situational awareness across multiple entities. Thus, domain situational awareness is visibility of events and activities spanning national (and ideally international) networks. This analysis addresses certain enterprise-level issues, but focuses on the domain level.

* * *
III. Cyberspace situational awareness in the United States

Policy

In many aspects of the cyber domain, particularly those that relate to computer network attack, US capabilities appear far more advanced than the policies that guide their use. This resembles the early phases of the nuclear age, prior to the advent of deterrence theory and other guiding concepts. Situational awareness is one of the few elements of the cyber domain where policy is more fully developed than enabling technologies and capabilities (discussed below). Several official documents and statements indicate the US government’s policy: more is better.

With respect to enterprise situational awareness, the 2011 US budget states that the Office of Management and Budget should initiate ICT programs and activities that promote the “[m]ove towards Situational Awareness across the Government”. The document asserts that:

More frequent reporting, near or at real-time, is imperative for developing situational awareness across the Federal enterprise. The use of Security Information Management or Security Information Event Management tools will assist in progressing towards real time security awareness and management in the Government.

This echoes two components of the US Comprehensive National Cybersecurity Initiative (CNCI). One specific initiative is to “[d]eploy an intrusion detection system of sensors across the Federal enterprise.” This project aims to bolster the US Computer Emergency Readiness Team’s (US-CERT) situational awareness so it can better develop and distribute security information. A related initiative is to “[p]ursue deployment of intrusion prevention systems across the Federal enterprise.” This step intends to improve situational awareness with more advanced capabilities to “identify and characterize malicious network traffic” in order to prevent its access to protected networks.

Official US government statements also indicate the need to improve domain situational awareness. USCYBERCOM Commander Keith B. Alexander recently characterized the cyber domain as one with “strong adversary capabilities and weak situational awareness.” He described intentions to:

build an effective cyber-situational awareness in real time through a common, shareable operating picture. We must share indications in warning threat data at Net speed among and between the various operating domains. We must synchronize command-and-control of integrated defensive and offensive capabilities, also at Net speed.

The CNCI also addresses the need for domain situational awareness capabilities. Specifically, one initiative is to “[e]ncore current cyber ops [operations] centers to enhance situational awareness.” This element seeks to “support shared situational awareness and collaboration across six centers that are responsible for carrying out US cyber activities,” through “shared analytic and collaborative technologies.” Similarly, DHS’s Information Technology Sector-Specific Plan, an annex to the 2010 National Infrastructure Protection Plan, includes as a primary goal the need to enhance cyberspace situational awareness across the entire ICT sector.

Capabilities

Progress towards these ends is evident, but legal and structural impediments remain. With respect to enterprise situational awareness, DHS Secretary Janet Napolitano recently announced that the Einstein 2 program, which can “automatically detect and disrupt malicious cyber activity,” is almost fully deployed across the “.gov” domain. Development of the program’s third iteration is already
underway. For its part, DoD designated that one of USCYBERCOM’s key missions is to elevate cyberspace situational awareness. Additionally, according to Deputy Secretary of Defense William Lynn, DoD has deployed three layers of protection for US military networks, or the “.mil” domain, of which two relate to industry best practices and appear to enhance situational awareness capabilities. These initiatives appear to have already stemmed malicious activity: security incidents on DoD networks decreased in 2010 for the first time in a decade.

The US government has made other advancements at the domain level. In what probably constitutes the third and outermost layer of protection for its networks, DoD reportedly developed relationships with “tier 1” ISPs to identify and terminate malicious traffic from foreign sources before it reaches DoD networks. DHS operates a “dashboard” that aggregates routing data and other information to provide real-time situational awareness about the state of the internet throughout the country. Critically, it can show when segments of the internet are down, which can help officials diagnose whether the root cause of the outage might be a natural disaster, a power outage, or perhaps an attack. The dashboard can even highlight areas with extreme network congestion, which could draw attention to infrastructure malfunctions.

Recent government efforts reveal imperfect but strengthening capabilities. For example, a DHS-sponsored exercise series called “Cyber Storm” seeks to strengthen preparedness for a contingency in cyberspace, in part by improving enterprise and domain situational awareness. One of the exercise’s four primary objectives is to “validate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information.” One of the key findings of the exercise’s first iteration, held in February 2006, was that “[p]layers were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors.” The following exercise, held in March 2008, cites improvements but maintains that a better “understanding of the interconnectedness and cause/effect relationships between actions taken by each organization would help to maintain broad situational awareness and galvanize a holistic approach to cyber response.”

Several factors, however, may impede the US government’s prospects for improving cyberspace situational awareness. First, with respect to laws, the executive branch operates on the basis of guidelines included in the Foreign Intelligence Surveillance Act, the Electronic Communications and Privacy Act, the PATRIOT Act (which includes provisions for National Security Letters), the Communications Assistance for Law Enforcement Act, and elsewhere. These laws can limit surveillance and other activities related to situational awareness, particularly with respect to data traversing US infrastructures or involving US persons.

Other checks, from a structural standpoint, include the market-driven and generally decentralized development of internet infrastructures. For example, US internet traffic destined abroad (and foreign traffic destined for the United States) may transit any of the approximately 19 undersea cable landing facilities along the US east and west coasts. Moreover, internet access in the United States is multimodal. That is, users may connect in a variety of ways, including by satellite. Finally, there are thousands of ISPs operating in the United States, of which perhaps a half dozen are considered “tier 1” providers. As a corollary, numerous US firms operate the international gateways that connect the internet in the United States to internet infrastructures in foreign countries. This multitude of infrastructure actors severely complicates efforts to establish comprehensive cyberspace domain situational awareness.
IV. Key features of the cyber domain in China

In contrast to the abundance of US policy statements on cyberspace situational awareness, there are few indicators of Chinese views on the subject. In absolute terms, China’s enterprise situational awareness status is probably less robust than its US counterparts. Software piracy—rampant in China—adversely affects software updates and patch implementation, management, and other essential aspects of system hygiene. Microsoft, for example, recently estimated that 90 percent of its software in use in China is pirated. Depending on the vendor, unlicensed server software may not get critical patches and copies of antivirus software may not receive updated definitions. Pirated operating systems, web browsers, media players, and other software may also be affected. Notwithstanding recent efforts to counter the use of pirated software, it remains a common feature of even Chinese government computers. Moreover, China consistently ranks in the top few countries with the most infected computers (although the United States is often in its company).

Less is known about the state of China’s domain situational awareness. However, an analysis of some of the key architectural features of the cyberspace domain in China can inform our understanding of China’s cyber domain situational awareness prospects. Two features in particular—international gateways and filtering capabilities—bear closer examination.

International Gateways

The overwhelming majority of China’s internet communications with the outside world transit just three international gateways located in Beijing in the north, Shanghai in the east, and Guangzhou in the south. By design, this centralization of international internet connections allows Chinese authorities to exert a significant level of control over data traversing China’s national-level networks. As a result, according to an account by journalist James Fallows, Chinese authorities can:

physically monitor all [internet] traffic into or out of the country. They do so by installing at each of these few “international gateways” a device called a “tapper” or “network sniffer,” which can mirror every packet of data going in or out…. “Mirroring” is the term for normal copying or backup operations, and in this case real though extremely small mirrors are employed. Information travels along fiber-optic cables as little pulses of light, and as these travel through the Chinese gateway routers, numerous tiny mirrors bounce reflections of them to a separate set of… computers.

Filtering Capabilities

This separate set of computers, known colloquially as China’s “Great Firewall,” allows Chinese authorities to surveil and filter internet traffic. The system leverages a set of mechanisms to evaluate and analyze data destined for networks outside China. Most of this data is directed to the rest of the internet via undersea cables to transit points throughout East Asia. However, when the Great Firewall identifies data considered offensive by China’s authorities, the system resets the attempted connection in order to terminate the data transmission. Technical research corroborates Mr. Fallows’ account that data transiting between internet destinations in China and abroad are indeed mirrored to “out of band” machines, which are separate and parallel to the core routers that facilitate the transactions. Computer researchers refer to these machines as intrusion detection systems (IDS), defined by the National Institute of Standards and Technology (NIST) as applications or devices for “monitoring the events occurring in a computer system or network and
an analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.”

China’s IDS employs deep packet inspection (DPI), described by computer security firm Symantec as the ability “to look within the application payload of a packet or traffic stream and make decisions on the significance of that data based on the content of that data” (emphasis original). This is opposed to less sophisticated utilities that only analyze data labels, such as packet headers, which contain important but less specific information like data origin and destination. In practice, for example, DPI allows the Great Firewall to not only determine when a user in China attempts to establish a connection to www.bbc.co.uk (label), but whether the specific page requested contains keywords related to the Falun Gong (content).

An important caveat here is that DPI technology is generally effective only on data sent “in the clear,” or in unencrypted form. This weakness allows users to leverage virtual private networks (VPN) to “scale” the Great Firewall. Although Chinese authorities could simply block encrypted internet traffic destined abroad, such a move could immediately halt substantial levels of foreign business operations in China, which the government is loathe to do. However, at least one firm with business activities in China advertises DPI suites that use signatures to communicate a “broad range of criteria, header information, actual payload, bi-directional traffic information and the characteristics… even as applications get encrypted.” Such technologies raise questions about how long encrypted traffic can remain a sanctuary from China’s data inspections.

V. Implications for situational awareness

There are at least five components of situational awareness: intelligence, surveillance, reconnaissance, environmental monitoring, and common operating picture. For the purposes of this analysis, reconnaissance is how to find something; surveillance is how to track it; and intelligence is the actionable results of these (and related) efforts. Environmental monitoring involves the attempt to understand natural and unnatural influences and events and their impact on a domain. Common operating picture is a holistic and shared view of information from numerous inputs and sources across a domain. Although complete treatment of how each concept applies to cyberspace is beyond the scope of this paper, all are at least somewhat affected by the architectural features of China’s censorship regime.

Intelligence: The Great Firewall’s main function is traffic inspection and termination, but the system could conceivably employ features designed to collect intelligence. Although it would be infeasible to retain all of the mirrored internet traffic for any longer than it takes to conduct a cursory inspection, some data could be stored for later analysis and exploitation. If such a capability is in place, data could be flagged for retention at the router or IDS level based on predetermined parameters. Rules implemented within this system could direct potentially useful data to a storage device for further review by human analysts. Though the existence of such an inspection regime is purely speculative, the possibility appears within reach of China’s authorities. From a technical standpoint, it would even be less challenging than basic filtering (given that the central obstacle would be the review and manipulation of all data, which China currently does).

These potential intelligence-related features present more cause for concern when viewed in light of China’s ability to essentially import internet traffic from abroad. Although by no means unique—ISPs in other nations have previously done the same thing—China briefly demonstrated this
capability in April 2010. In that incident—which could have been accidental—state-owned China Telecom propagated improper routing information that instructed US and other foreign internet traffic to transit Chinese servers. The event affected traffic to and from, among other things, the web domains associated with the Office of the Secretary of Defense and all four US military services. Affected traffic would likely have transited the Great Firewall and thus could have been censored or exposed to any intelligence collection or analysis features inherent in the system.

**Surveillance:** China’s control of the internet extends beyond censorship and into surveillance. The general trend is well documented, but specific architectural aspects of the Great Firewall enhance these capabilities. In particular, all information that transits the Great Firewall must include origin and destination information, such as Internet Protocol address or domain; these data could conceivably be logged according to rules triggered by keywords or other predetermined specifications. Such information could have numerous applications; for example, it could explain accounts of software used by Chinese authorities that issues reports when specific users in China access banned websites. Of note for people outside China, the Great Firewall reportedly has bidirectional functionality, meaning users outside China can be prevented from viewing content on sites hosted within China. By extension, foreign users who attempt to connect to Chinese nodes may face some level of surveillance, to the extent that it is inherent in the systems that compose the Great Firewall.

**Reconnaissance:** If Chinese authorities leverage the Great Firewall to analyze traffic, the limited number of international gateways would simplify the process. That virtually all internet traffic between China and the outside world transits three locations would significantly bind the complexity of information mining. Consider a scenario where Chinese authorities sought to locate a user based on a unique identifier, such as email address: the fewer the transit points, the more efficient the search. For people and systems within China, it would be far more pragmatic to conduct reconnaissance activities at the ISP level, but the gateway level would serve to identify the correct ISP to approach in the event that that information was not already known to authorities. Again, bearing in mind the Great Firewall’s bidirectional nature, such reconnaissance activities may also have implications for users outside China communicating with users or connecting to sites inside China. China’s network infrastructure abroad may also have a suite of features that, though perhaps harmless, could facilitate reconnaissance. China Telecom Americas Corporation’s promotional materials call its network “traceable,” with “real-time monitoring and reporting.”

**Environmental Monitoring:** One of the unique features of the cyberspace domain is the relative indivisibility of the domain itself from a given system within that domain. In the space domain, the evaluation of space weather and events to determine how they might affect space systems, such as satellites, is fairly straightforward (though certainly not simple). In cyberspace, enterprises should similarly seek to understand significant “environmental” events, such as viruses and malfunctions in exterior networks. But in the sense that the government has a vital interest in ensuring that the cyber domain itself—and all domestic segments in particular—remain operational, it would be arbitrary to separate a system of interest from other networks and infrastructures. For example, a key government entity might perfectly defend its networks, but if an attack disrupts upstream systems—such as the entity’s ISP—key systems could still be denied access to the internet. In this light, environmental monitoring should include any substantial event in the cyber domain.

Some evidence suggests that Chinese authorities previously configured routers on national-level networks to filter virus-related traffic. To bolster this capability, gateway filtering could operate in a similar capacity. The limited number of gateways creates comprehensive vantage points that could
help inform battle damage assessment across networks and enable mitigation efforts, particularly if an attack lacks a readily identifiable signature to block. For example, monitoring bandwidth might help administrators estimate the effects of distributed denial of service (DDoS) attacks targeting numerous sites across multiple ISPs. Other “sensors” at the gateways could monitor routing data to provide reports on route hijacking or other unusual events.

Common Operating Picture: The confluence of all traffic at just three international gateways could also help enable threat characterization analysis. China has an active marketplace for data mining utilities, frequently used for surveillance applications, which may offer efficient ways to identify and parse events and trends on the internet. Unity of effort is another imperative related to common operating picture, and these “hubs” could facilitate a coordinated response by various Chinese entities in the event of a cyberattack or counterattack. Moreover, any of the monitoring scenarios described above could have implications for tracking “red” and “blue” forces (in China’s usage, friendly and adversary, respectively), which is a key component of traditional common operating picture requirements.

VI. Balancing equities

Although situational awareness is clearly a desirable end in the cyber domain, the means employed by China imply some important tradeoffs. Three in particular merit consideration. First, states must determine how to allocate resources in the cyber domain, and skilled personnel might well be the key constraint. Second, states may have an interest in the topology of their networks, particularly the extent to which infrastructure should be centralized. Third, if states view cyberspace as a potential domain of conflict, infrastructure and force structure should be optimized to address contingencies based on threat assessments.

Resource allocation: China’s censorship system is rooted in the Chinese Communist Party’s (CCP) perception about how best to maintain regime stability. Thus, from a defense planning perspective, derivative gains in situational awareness are essentially free. However, it is unclear that Chinese investments in ICT architecture reflect risk analyses that weigh censorship against the potential implications of a cyberwar, which could also affect the CCP’s ability to maintain social control. Assuming a finite pool of human capital with the advanced skills required to operate in the cyber domain, man-hours expended on censorship activities—even with their ancillary benefits for cyberspace situational awareness—come at the expense of other cyberwar-related capabilities. These could include, among other things, cyber defense, cyber offense, command and control in cyberspace, and cyberspace reconstitution capabilities.

Network topology: The CCP’s perceived need for censorship influenced the development of China’s internet architecture, resulting in considerable centralization. Though helpful for filtering and situational awareness, this comes at the expense of robust redundancy. This may be an acceptable trade-off at the enterprise level. However, centralized architecture at the domain level raises questions about the sustainability of internet access in a conflict scenario. This could have implications for China’s ability to retaliate in cyberspace, which raises two key concerns. First, the absence of an assured second strike capability in cyberspace could give China a destabilizing incentive to strike preemptively. Second, denied access to the cyber domain could promote escalation into other domains of war.
China’s international gateways connect its six national-level networks to one or more of seven international land-submarine cables that link China to the rest of the internet. Causing a power outage in the three cities that host international gateway facilities, a conceivable objective in the context of conflict in cyberspace, could substantially isolate China from the rest of the internet. The physical disruption of one or more of the China’s international submarine cables could cause even greater damage. Attacks on such cables would be a severe measure, as their disruption would adversely affect the internet throughout the region. Moreover, US cyberspace operations have been canceled in the past for fear of unknown or uncontrollable effects. Still, while global telecommunications interdependence may be more entrenched today than ever before, the precedent for targeting undersea communications cables dates back to the First World War. Such assets could be targeted again in a serious contingency.

**Domain optimization:** The discussion above suggests that China’s domain configuration yields some benefits for cyberspace situational awareness at the expense of other features. Although China’s internet architecture probably evolved independently of these considerations, the Chinese government is nonetheless left with forces and infrastructure that appear better equipped to handle limited rather than total conflicts in cyberspace. For example, in a constrained engagement, situational awareness might be the primary consideration, as it could enable smart defense and mitigation techniques. By contrast, in a more intense scenario, emphasis might shift to favor
offensive actions. To the extent that resources available for each mission are drawn from the same pool, this would relatively diminish the importance assigned to domain situational awareness activities. Of course, it remains unknown whether this orientation aligns with the Chinese government’s threat perception regarding the relative likelihood of limited versus severe conflict in cyberspace.

VII. Policy Implications

The United States must consider the security implications of internet filtering activities. This may influence the urgency and means with which US policy seeks to address internet censorship and related activities abroad. By extension, a policy that accounts for the nexus between certain censorship activities and cyberspace situational awareness could alter present views about the permissibility of US firms’ assistance to foreign countries’ censorship activities. In particular, situations that involve technology transfer could require some sort of regulation or oversight.

The United States must also “balance equities” in cyberspace. One of the defining characteristics of the United States’ approach to the cyber domain, particularly when compared to China, is the numerous limitations on the US government’s ability to collect information that might aid situational awareness. While the United States requires improved cyberspace situational awareness, it remains unclear whether this end necessitates or justifies drastic adjustments to legal and structural checks. Alternative technologies or systems—perhaps even administered by private entities, such as a consortium of ISPs—might yield sufficient domain-level situational awareness capabilities. Such a mechanism might eventually serve as the foundation for a wider application of what appears to be DoD’s approach to stopping malicious traffic at the “tier 1” ISP level.86 Policymakers must recognize, however, that such activities are not costless and could require government support through subsidies, tax breaks, or other incentives.

In the event that improvements do require alterations to existing legal and structural checks, each change should reflect a deliberate, inclusive, and transparent review process. Moreover, each potential change ought to be justified through cost-benefit analyses related to resource allocation, network topology, and domain optimization, as described above, or another compelling rationale. Finally, on a tactical level, internet architecture should be a central factor in the context of defensive and offensive cyberspace operational planning.
About the Author

Robert Sheldon is a Policy Analyst for Military and Security Affairs at the US-China Economic and Security Review Commission. He previously worked on various cyber issues in law enforcement, intelligence, and defense-related capacities. Sheldon has an MA in Security Policy Studies and a BS in Computer and Digital Forensics. He can be reached at x@longtelegrams.com.

Notes

2 Lynn III, William F. "Defending a New Domain." Foreign Affairs 89, no. 5 (September/October 2010): 98.
11 This article discusses cyberspace situational awareness primarily as it relates to potential cyber conflict between the U.S. and China. This article does not take a position on the likelihood of such a scenario. For a nuanced take on how China might seek to employ offensive cyber attacks in a contingency against the U.S., see Libicki, Martin C. “Chinese Use of Cyberwar as an Antiaccess Strategy: Two scenarios.” Testimony to the U.S.-China Economic and Security Review Commission, January 27, 2011. http://www.uscc.gov/hearings/2011hearings/written_testimonies/11_01_27_wrt/11_1_27_libicki_testimony.pdf. Of course, general cyberspace situational awareness capabilities would also be of value for combating cyberterrorism, an arguably more likely contingency.
12 This paper does not include specific policy recommendations, a discussion about the desirability of “cyberwar” as a tool of statecraft, or meaningful treatment of privacy issues or the human rights implications of either censorship or conflict in cyberspace. Each merits due consideration, but are outside the scope of this analysis.

Strategic Insights • Spring 2011 Volume 10, Issue 1
"About Filtering." OpenNet Initiative. Accessed January 30, 2011. http://opennet.net/about-filtering/. This analysis substitutes the term “organizations” for the original “institutions” to avoid conflation with the traditional social science definition of the latter. I am indebted to an anonymous reviewer for identifying the potential for confusion.


17 In 2010, following revelations about the Aurora exploitations, Chinese authorities used a license renewal application as a lever to force Google to stop automatically redirecting mainland Chinese users to its uncensored Hong Kong site. See Lee, Melanie, and Emma Graham-Harrison. "UPDATE 4-Google Tweaks China Site in Bid to Keep License." Reuters, June 29, 2010. http://www.reuters.com/article/idUSN2914697820100629.


19 This article focuses specifically on architecture because of its relatively static nature. Control at other levels could be intensified or moderated on a more rapid basis.

20 Specifically, the term does not appear in JP1-02 DOD Dictionary of Military and Associated Terms (as Amended through September 2010).


35 Specifically, “DOD, working with DHS, has begun an approach currently named ‘Active Defense’ that can be described as working with tier 1 service providers to intercept malware from foreign sources.” Representative Langevin, James R., Michael T. McCaul, Scott Charney, and Lt. General Harry Raduege,
http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf. Findings from Cyber Storm III (September
2010) had not been released at the time of this writing.
40 Most fundamentally, situational awareness-enabling technologies lag behind threats (in other words, “necessity is the
mother of invention”). This lag is consistent with other weapons technologies: intercontinental ballistic missiles, for
example, came before the early warning satellites used to detect launches. However, this dynamic also affects China (and
all other actors in cyberspace), and will therefore not be treated here.
41 This analysis excludes Hong Kong and Macau Special Administrative Regions, which have fairly open ICT
environments.
42 Brodkin, Jon. "Ballmer to Hu: 90% of Microsoft Customers in China Using Pirated Software." Network World,
44 The author has not established causation between software piracy and compromised machines, although the variables
may correlate. For one report about the volume of China’s infected machines, see Nakashima, Ellen. “China leads the
http://www.washingtonpost.com/wp-dyn/content/article/2010/02/14/AR2010021403817.html. Caveat lector: these
figures probably do not represent a scientific sample. Moreover, the data appears to be in absolute terms, whereas
infections as a percentage of total online systems may be a more instructive measure for the purposes of this analysis.
45 There are several important qualifications. China Telecom operates terrestrial cables to Vietnam, Laos, Myanmar, India,
Kazakhstan, Russia, and Europe (via Russia). With the exception of the latter, these cables carry marginal levels of traffic
(for example, the China-India cable’s capacity is 44.21 mb/s, or about 0.22 percent of the firm’s capacity to Japan), and
likely employ some variation of the same gateway-level filtering mechanisms described below. China Telecom Americas.
http://www.chinatelecomusa.com/content.asp?pl=627&sl=637&contentid=727&id=1&indexid=0. Similarly, China
Unicom, which also has a stake in the notable China-Europe cables, operates low bandwidth terrestrial cables to
once robust mode of Internet access in China, now carry little or no Internet traffic, according to recent routing data and
traceroute measurements. Contractor to the U.S. Department of Homeland Security. E-mail message to author. January
2011.
48 Consistent with popular usage, this paper uses the term “Great Firewall” in place of the proper term, “Golden
Shield.” For information about the latter, see Walton, Greg. International Centre for Human Rights and Democratic
49 For a general explanation of these mechanisms, see Fallows, “The Connection Has Been Reset.” 2008. For a technical
explanation, see Clayton, Richard, Steven J. Murdoch, and Robert N. M. Watson. "Ignoring the Great Firewall of
aspects of the Great Firewall.

29, 2009. p. 28. http://www.tracking-ghost.net. These examples were enabled by means other than the architectural

http://www.nartv.org/2005/06/03/censorship-is-in-the-router/.

Dam, and Herbert S. Lin. about cyberspace doctrine, which is comparatively underdeveloped. See, for example, Owens, William A., Kenneth W.


Chapter II-7-8. The official definition for each, albeit for the purposes

http://www.fas.org/irp/doddir/dod/jp3_14.pdf . Chapter II-7-8. The official definition for each, albeit for the purposes

of space, are contained within. There is precedent for the use of existing air and space doctrine to inform discussion


51 Clayton, Murdoch, and Watson. "Ignoring the Great Firewall of China," 2006. Section 4. However, there is also

reason to believe that some blocking occurs at the router level, thus obviating the need to pass data to an IDS.


http://www.nartv.org/2005/06/03/censorship-is-in-the-router/.

52 U.S. Department of Commerce. National Institute of Standards and Technology. Guide to Intrusion Detection and


http://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection. However, there is some

confusion about whether China’s DPI efforts occur at the ISP level or at international gateways, or both. Rhodes,


http://online.wsj.com/article/SB124562668777335653.html#ixzz1B8feczNwz.


http://www.fas.org/irp/doddir/dod/jp3_14.pdf. Chapter II-7-8. The official definition for each, albeit for the purposes

of space, are contained within. There is precedent for the use of existing air and space doctrine to inform discussion

about cyberspace doctrine, which is comparatively underdeveloped. See, for example, Owens, William A., Kenneth W.

Dam, and Herbert S. Lin. Technology, Policy, Law, and Ethics regarding U.S. Acquisition and Use of Cyberattack Capabilities.


57 This is adapted from a pithy formulation by then-secretary of defense Donald Rumsfeld. See Deptula, David A., and R.


For this section, the author has attempted not to overstate the potential significance of international gateways. Readers

should bear in mind, however, that the hypotheticals described here (subject to included qualifications) could probably

occur at the ISP level, albeit in a more fragmented and thus less effectual fashion.


59 For this section, the author has attempted not to overstate the potential significance of international gateways. Readers

should bear in mind, however, that the hypotheticals described here (subject to included qualifications) could probably

occur at the ISP level, albeit in a more fragmented and thus less effectual fashion.


counterpoints to this account, see Cowie, James. "China's 18-Minute Mystery." Renesys Blog (web log), November 18,


63 See, for example, Villeneuve, Nart. BREATCHING TRUST: An Analysis of Surveillance and Security Practices on China’s


29, 2009. p. 28. http://www.tracking-ghost.net. These examples were enabled by means other than the architectural

aspects of the Great Firewall.

64 China’s ISPs and ICPs have data retention obligations. Deibert, Palfrey, Rohozinski, and Zittrain. Access Controlled: the


469.


73 Granted, in a country with over 1.3 billion citizens, the labor pool is probably quite robust. Still, as more and more of those citizens gain access to communications technologies, and as those technologies become more data-intensive, evermore people will probably be required to maintain the censorship regime. Also, although this does not necessarily indicate a labor shortage in the Chinese government, China’s military has for years appropriated civilians, in the form of Information Warfare Militias, for use in potential cyberwar scenarios. U.S.-China Economic and Security Review Commission. 2009 Annual Report to Congress. Washington, DC: Government Printing Office, 2009. pp. 173-4. http://www.uscc.gov/annual_report/2009/annual_report_full_09.pdf.


75 This assumes that an effectual second strike would need to be launched domestically, which may not be the case. China could well have capabilities “forward deployed.” In particular, Hong Kong (again, not treated in this analysis) is a regional Internet hub that probably could not be forcibly isolated from the Internet without catastrophic spill-over effects throughout Asia and the Pacific. Forces could also be deployed to foreign countries. For example, authoritative Chinese military writings call for cyber attacks against the United States to be launched from within the United States. Mulvenon, James. “Information Warfare and China’s Cyber-warfare Capabilities.” Speech, Carnegie Endowment for International Peace, Washington, D.C. February 10, 2011.


77 This figure, which is undated, does not include the international terrestrial cables referenced above.


80 The same may apply for the coastal cities that host the cable landing facilities: Qingdao in the north, Chongming and Nanhu in the east, and Shantao in the south.


84 This is an exceedingly delicate matter. Different countries (even throughout the West) have different standards of free speech, and U.S. firms operating abroad ought to have some degree of latitude to comply with local laws and regulations.

85 Best practices developed—and strictly adhered to—by industry itself could obviate the need for governmental regulation.
Any such activities must offer sufficient protections to both users (especially with respect to expression) and ISPs and other operators (especially with respect to liability). “Threading the needle” on this issue socio-politically will be well more challenging than the technical requirements.