The Case for a National Information Strategy

Col. Dennis Murphy, U.S. Army, Retired

Lt. Col. Daniel Kuehl, PhD, U.S. Air Force, Retired

At the end of the previous century, a group of respected analysts and former policy makers called the U.S. Commission on National Security Strategy in the 21st Century, but better known as the Hart-Rudman Commission, produced a series of reports that analyzed the implications of some evolving global forces and trends. The commission's first report, *New World Coming: American Security in the 21st Century*, published in 1999, was clearly influenced by what many would call the *information revolution*.[1] The report was laced with references to "a world brimming with free-flowing information," "deluged with information," and "less hospitable to tyranny" because of that revolution. It pointed out some of the simultaneous

(Image courtesy of Paul Bitler, Facebook intern)

A computer-generated visual representation of raw Facebook data from December 2010 shows the myriad connections among users around the globe. Each thread shows the virtual connection of one "friend" to another.

opportunities and vulnerabilities that this information revolution was presenting to the shapers of national security strategies. The commission's second report, *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom*, published the following year, expanded the discussion into a detailed commentary on the importance of cyberspace.[2]

Subsequent to that time, the United States has developed multiple national strategies, including one for information sharing. Ironically, however, there is still no national strategy for information content.[3] While there are likely myriad reasons for this, it is the authors' intention to recommend just such a strategy. For anyone attempting to develop an approach to the role that the information revolution could play in national security strategy, the Hart-Rudman Commission's work is a critical resource. But if one starts there, one also realizes that more groundwork is required. In fact, one would need to explore in much greater depth the nature of information as an instrument of national power and its historical evolution before attempting to offer a conceptual and organizational model to develop what could be called a national information strategy adequate for U.S. national security requirements in the Information Age.

Probably every curriculum taught at military staff and war colleges around the world attempts to explain and analyze the elements and instruments of national power using a model of some kind. The United States military employs a framework sometimes identified by the simple acronym DIME, representing the diplomatic, informational, military, and economic *instruments of national power*.[4] While the "D, M, and E" instruments are obvious and almost self-defining, such is not the case for the "I" instrument. The proposed definition used here is based on the national security strategies that President Ronald Reagan issued in the late 1980s, to include earlier work of his administration. Simply put, *information power* is the use of informational content and the technologies and

capabilities that enable the exchange of that content, used globally to influence the social, political, economic, or military behavior of human beings, whether one or one billion, in the support of national security objectives.[5]

Every nation-state and strategically important political entity on the face of the earth—including nonstate actors such as Hamas, Greenpeace, or the United Nations—strives to use information as an instrument of power, regardless of how technologically sophisticated or *connected* it might be. Information is used to spur economic productivity and develop new ways of making wealth; to improve the command, control, and effectiveness of military forces and operations; and to conduct diplomacy, both public and traditional. Information power is, and always has been, an essential, perhaps indispensable, foundational component and enabler for the creation and exercise of all other forms of power. Yet, this fact seems to have escaped the attention of most national security strategists in the United States and abroad.

The formal *National Security Strategy [NSS] of the United States*, signed May 2010 by President Barack Obama, is another example of national guidance that is perhaps one-quarter full but three-quarters empty, providing but a glimmer of hope.[6] While this NSS does contain repeated references to information in regard to the need to both share and secure it, there is little if any sense of the power of information content linked to modern information-communication technologies (ICTs) to sustain and grow economic power, which was an important segment of Reagan's first NSS in 1987.

The NSS speaks repeatedly about the right of people to access information, yet there is little if any sense of the power of information to influence populations via public diplomacy as, for example, to sustain America's struggle against violent extremism, and there is no mention at all of the ways that information power and its related ICTs can enhance and magnify American military power and capability. A coherent, comprehensive national information content strategy is needed to provide the focus currently lacking.

The Information Environment: Connectivity, Content, Cognition

Just as nations describe and assess air power or sea power as the ability to use those environments, one measure of information power might be the ability to use the information environment, described as the integration of the three dimensions of *connectivity* (the ability to exchange information), *content* (the actual information), and the *cognitive effect* (the impact of human beliefs and behaviors) resulting from the use of connectivity to deliver the content. Since understanding the information environment is essential to the approach espoused here for information power and an information strategy, the environment itself needs to be explored in more detail.

The first C, connectivity, is most visible in the myriad forms people employ to send, receive, broadcast, disseminate, and share information. Although humans have used various methods throughout history to exchange information—signal fires, smoke signals, semaphore flags, newspapers, even the fabled (although short-lived) Pony Express—modern technology-based connectivity that exploits the electromagnetic spectrum started with the introduction of the telegraph in the mid-1800s. In relatively rapid succession, the telegraph was followed by wireless telegraphy, the telephone, radio, television, and so on to the present. Today, in a world with universally connected cyberspace, people can watch—on a device held in the palm of the hand—the live broadcast of an event on the other side of the world, whether it be sports (e.g., World Cup soccer) or terrorism (e.g., the Mumbai attacks of November 2008 in which hostages were tweeting details while the attacks were underway). This is what modern information technology, the ubiquitous *IT*, has brought us. It is also important to add, however, that the nontechnological forms of connectivity remain critical as well—and are sometimes even more important. In any event, technological and nontechnological connectivity are both crucial components of the modern day information environment.

So what does connectivity offers us without the second C: *content*? Very little. Ultimately, the utility of being able to exchange information depends on what is being exchanged. This is another area in which the impact of modern IT has been profound, sometimes transforming the very way people construct and present complex intellectual and technical information. Gutenberg's printing press began the revolution by enabling the mass production of standardized information, whether as the Bible, Jefferson's Declaration of Independence, or the famous World War I poster of Lord Kitchener with the words "Your Country Needs YOU!"[7] Later, still and then video photography expanded visual content into seemingly exact reproductions of events, from the horrors of

the battlefield to the explicitness of adult movies. Still later, television expanded photography's effect vastly through its ability to broadcast entire events.

The digital revolution brought by the Internet and the World Wide Web has expanded this still further, with content in online virtual worlds, such as Second Life, which can create synthetic environments where humans do everything from taking on entirely new personalities and persona to training virtually for terrorist acts.[8]

However, setting aside the effects of technological advances on information exchange, it is still crucial to remember that an enormous amount of information content is transferred through nontechnological means in high-context cultural situations. For example, a raised eyebrow during a conversation in some cultures may convey more content than the actual conversation, and roses delivered to one's lover may express messages from "thank you" to "I'm sorry."

Regardless, whether in a technological or nontechnological realm, the most important form of content is, in fact, an action. The old cliché "actions speak louder than words" comes from this principle, as does the chagrin of parents at hearing their children do or say things that make them wonder, "Where did they learn *that* from?"

Finally, *content* delivered by *connectivity* enables the third and most important C: *cognitive impact*. This is where the human mind applies meaning to the information it has received, where beauty is appreciated, persuasion is accomplished, loss is mourned, and decisions are made. However, this dimension of the information environment is the most difficult to influence because it is rarely quantitatively calculable, and therefore it is difficult to manipulate or even predict. Audiences will respond to information content in ways shaped by cultures, backgrounds, experiences, emotions, and myriad other factors. As former Under Secretary of State for Public Diplomacy and Public Affairs Karen Hughes once told a gathering of members of the military's information operations community, audiences may hear meanings other than intended if their perspectives are very different from those who prepared the content.[9]

One example should make this clear. In 1934, the brilliant young German filmmaker Leni Reifenstahl produced a purported documentary of the Nazi Party congress held in the sports ground in Nuremburg. That film, *Des Triumph des Willens* (The Triumph of the Will), was a masterpiece of propaganda, but it obviously affected different audiences in different ways. German audiences saw it as evidence of the rebirth of German strength and pride after the disasters and humiliations of World War I and life in the 1920s under the demeaning terms of the Treaty of Versailles. Audiences in the countries bordering Germany saw a different, more threatening message; to the more perceptive, it was a dire warning of rising German aggression.

The 3C Model of Information Power

Hence, the medium of connectivity may be technological or human-to-human nontechnological, and the content visual or audio or a deed, but the end result is the same: a human being is affected, internalizes the information, creates a belief, and then behaves a certain way because of it. When the cycle culminates in an observable behavior, it begins anew.

A generation of students has come to know these—connectivity, content, and cognitive impact—as the "3C" model of information. This approach has several attractive aspects. First, it is solidly based on accepted U.S. military information operations doctrine.[10] Second, the three dimensions are surprisingly measurable. Third, it is not totally dependent on technology. Examples of the three Cs can be seen as far back as the Assyrians' use of terrifying stone depictions of the treatment of rebellious prisoners to politically cow their subjects. Fourth, the explosion of modern ICTs has made the use of information power central to the functioning of all other current forms of power. Not only can we identify the organizational aspects of each C, we can also clearly describe some of the partnerships that must be created between the public (government) and private (business and society) sectors.

Therefore, the 3C model demonstrates that information power does not—and cannot—come exclusively from the government or private sector, it must come from both, which suggests an organizational model for how we can best develop a strategy and then operationalize it by employing information power to achieve behavioral change.

Seeking a synergistic balance between securing connectivity and exploiting content to achieve cognitive dissonance leading to behavioral change is not new.

However, efforts to achieve such balance have ebbed and flowed in effectiveness and emphasis in the history of information power as employed by the United States.

An Enduring Problem

One might assume that the issue of securing connectivity while employing it as a means to influence by creating cognitive awareness or change is a recent phenomenon, spurred by the advent of the Internet and the World Wide Web. However, a brief historical look at the industrial age leading up to current issues indicates that the need to balance protection while exploiting the same means to communicate is not new.

At the outset of World War I, both the United States and Germany were already largely dependent on transoceanic telegraph cables for commerce in a rapidly expanding global marketplace. Consequently, these cables, controlled and owned by Britain and Germany respectively, were targeted for exploitation and destruction by both sides. This led the United States to develop an alternate command and control means, the radio, toward the end of the war.

(Associated Press photo by Subel Bhandari, AP Images)

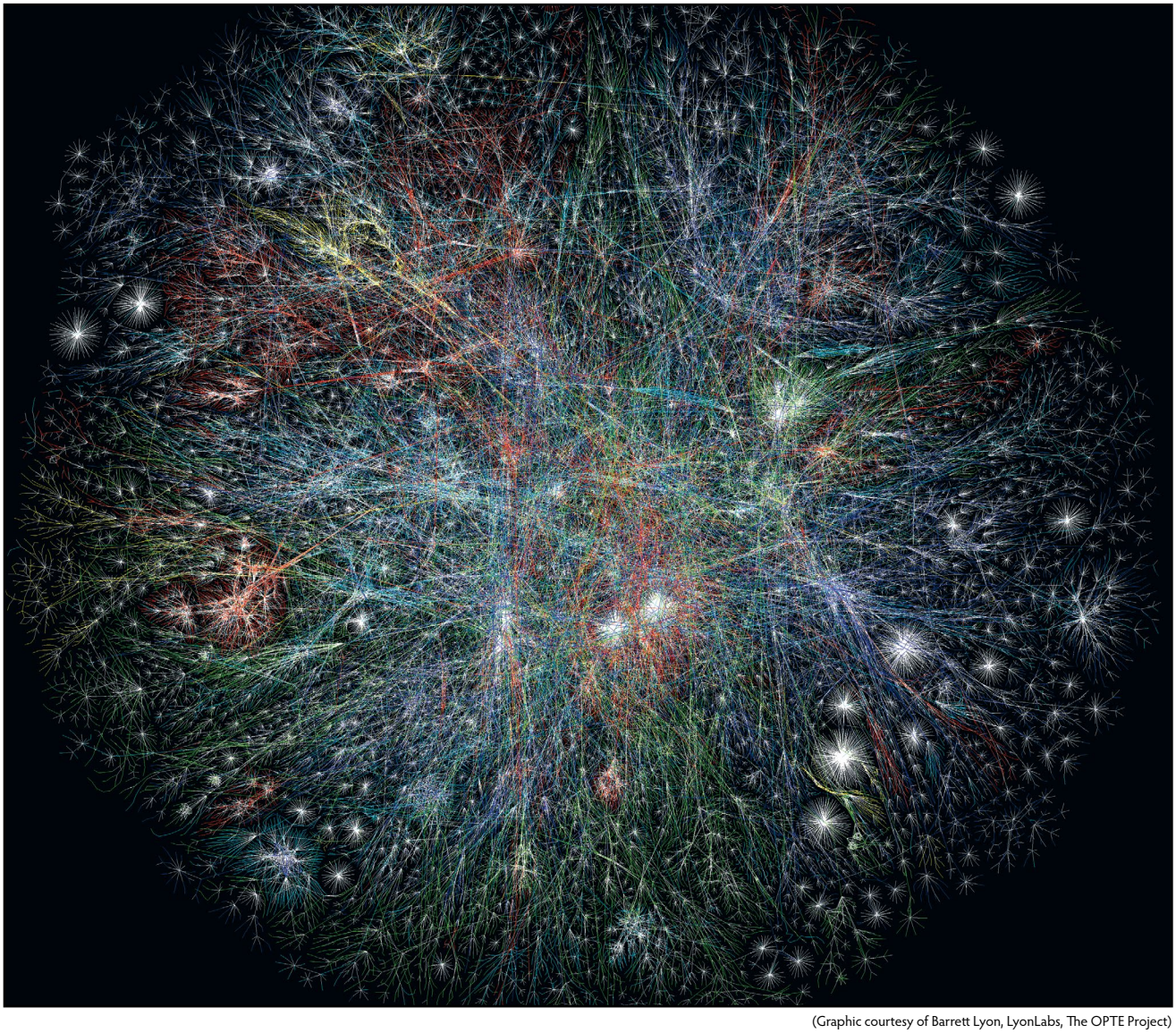
Afghan cleric Sadschad Mohsini holds a smartphone 24 October 2014 in Bamian, Afghanistan. Mohsini routinely uses social media to advise young people in matters of faith and religion. Mohsini's son taught him how to navigate search engines and explained how Facebook works.

The problems the United States faced in terms of maintaining connectivity through both means are eerily familiar to those we face today. The capacity to move and establish a priority for information content over the limited cable system became strategically significant. Today we face limits on capacity bandwidth. Similarly, the nascent development of radio encountered electromagnetic-spectrum issues in terms of usable and deconflicted frequencies; this is another issue of importance today. And of course, the significant dependency on transoceanic telegraph lines to daily business and economic intercourse became a vulnerability. All of these challenges have significant parallels to Internet capacity and vulnerability issues today.[11]

Additionally, during that time, President Woodrow Wilson saw the benefit of persuasion and influence in employing information as an instrument of national power in the war. As a result, Wilson established the Committee on Public Information (CPI) to inform and engage the world while influencing enemy publics, leaders, and militaries. CPI, led by journalist George Creel, met with mixed results, but it was clear that Wilson could see the great benefit of using the same global information means—the transoceanic telegraph—to rapidly disseminate his diplomatic messages worldwide. In their *Parameters* article "Propaganda: Can a Word Decide a War?" Dennis M. Murphy and James F. White describe Wilson's reaction:

> When Wilson gave his "Fourteen Points" speech in January 1918, CPI representatives in Saint Petersburg and Moscow received the text by way of transatlantic radio and telegraph, and were able to pass it to the Russian man on the street via posters and handbills just four days later .... Wilson was taken aback by this effective dissemination of his peace aims and the world's reaction. He remarked to George Creel in December 1918, "I am wondering whether you have not unconsciously spun a net for me from which there is no escape."[12]

In Wilson's time, much as today, the reliance of the United States on one vulnerable connectivity system for command, control, and economic prosperity,



(Graphic courtesy of Barrett Lyon, LyonLabs, The OPTE Project)

A computer-generated map is overlaid on a picture of the world, depicting Internet connections on 23 November 2003 emanating from regions around the globe. They are coded by color: Asia Pacific—red; Europe, the Middle East, Central Asia and Africa—green; North America—blue; Latin America and the Caribbean—yellow; other regionally localized concentrations—white.

while at the same time using it as a means for achieving cognitive effects among both allies and enemies, became evident. Even then, many asserted a need to develop a holistic national information strategy—one that considered both the protection of that connectivity and the exploitation of it to influence a targeted audience—to manage and direct this new technology effectively. However, no comprehensive policy was fully developed either in Wilson's time or thereafter. Consequently, the United States stumbled along for the remainder of the twentieth century with piecemeal policy efforts largely resulting from Cold War competition with the Soviet Union.

Information Power during the Cold War

At the outset of the Cold War, U.S. policy makers broadly conceived of it as a competition between ideologies to be contested primarily through information power, albeit strategically supported by the threat of military force and mutually assured destruction. Recognizing this, the Smith-Mundt Bill of 1948 established the United States Information Agency (USIA). The purpose of the law was to "promote the better understanding of the United States among the peoples of the world and to strengthen cooperative international relations."[13] USIA was to act as the agency responsible

(Photo courtesy of the Lyndon B. Johnson Presidential Library)

Carl T. Rowan, then director of the U.S. Information Agency, discusses support of U.S. involvement in Vietnam at a National Security Council meeting in the Cabinet Room at the White House in July 1965. At that time, USIA had more than thirteen thousand employees. It coordinated and distributed strategic themes and information through the international Voice of America broadcasts together with daily communiqués to U.S. embassy personnel. USIA also maintained a system of libraries in foreign countries featuring American literature and philosophical thought pertaining to democracy throughout the world.

for achieving strategic cognitive information effects globally in support of U.S. strategy and policy.

USIA was organized during a time when the means to connect globally in the post-World War II world was rapidly expanding with technological advances. While television was still emerging as a technology, radio became the dominant global capability to transmit the U.S. message to targeted audiences. One result was that *Voice of America* became the preeminent program of USIA during the Cold War. It exploited the reach of radio technology to communicate effective messages aimed at influencing and persuading intended audiences behind the Iron Curtain.

Recognizing the necessity of competing effectively in the ideological struggle, the Reagan administration made the first attempt to develop a comprehensive national security document on information in 1984, with National Security Decision Directive (NSDD) 130, *U.S. International Information Policy*. The focus of this directive is what today could be called strategic communication, but there is discussion within the document of securing and using the connectivity aspects of the information environment as well. The document states, "More systematic thought needs to be given to the opportunities offered by international television broadcasting …. New technologies (particularly in the area of audio and video tape cassettes) have created new instruments whose potential should be explored."[14]

NSDD 45, released in 1982, also recognized the overarching requirement to balance expansion and protection of connectivity to allow transmission of the message: Acquisition of new transmitting sites and facilities should be a priority matter … [with] priority given to protecting and where possible expanding the frequencies available to the U.S. for international short wave broadcasting …. A major coordinated effort should be undertaken to press the jamming issue diplomatically in all appropriate international and bilateral fora.[15]

The last sentence refers to countering Soviet activity to electronically jam *Voice of America* signals to prevent the programs from reaching the intended audiences behind the Iron Curtain. This Russian desire to control the flow of information can be seen in the strategic policy issued by the Kremlin in late 2011, which aims first and foremost to use that control of information to achieve political effects—both domestically and internationally.[16]

The next major advance toward a U.S. national information power policy came in during the second Clinton administration with recognition of the exponential growth of the Internet in the United States.[17] In a press release in September 1998, the White House hinted at the increasingly apparent importance of the Internet to commerce and the economy as well as its vulnerability to criminal elements. The administration would "strengthen its support for electronic commerce by permitting the export of strong encryption when used to protect sensitive financial, health, medical, and business proprietary information in electronic form."[18] In 1999 Presidential Decision Directive 68, *Concerning International Public Information*, separately recognized the need to influence foreign audiences in support of policy.[19] However, as the twentieth century ended, there was no indication of a requirement to provide a strategic linkage to protect the Internet while exploiting it to influence and persuade in an ever-increasingly transparent world. This was the situation as the United

States sluggishly transitioned to the information age during the George W. Bush administration [not to be confused with the administration of his father, George H.W. Bush].

(Image courtesy of Michael Hogg, Visual Information Specialist)

An Islamic State recruitment and funding website found in the *darknet*, the portion of Internet content that cannot be indexed with standard search engines. ISIS has also been known to use other social media, such as message services WhatsApp and KIK, to solicit donations in the form of what it calls "humanitarian charity."

The Twenty-first Century Dilemma: Achieving Balance

George W. Bush, throughout his two terms, recognized the strategic impact of the Internet and the World Wide Web across all instruments of national power. Perhaps this was in part because of the effective use of these technologies by emergent adversaries, but also it was because of the significant reliance on the Internet that U.S. business and government interests had developed for daily business, commerce, and command and control.

Additionally, information as a strategic tool of influence or as a weapon was no longer the exclusive province of government. Where technological costs and infrastructure formerly limited information power to the purview of nation-states, multinational corporations, and global nongovernmental organizations such as the Red Cross, which had sufficient resources to operate information systems, the power of the low-cost, ubiquitous Internet and World Wide Web could also be wielded by individuals or small groups of people. Therefore, policy makers were forced to recognize that strict government control of a message was no longer possible. They were compelled to recognize that careful management of the information environment was henceforth essential to proactively compete with adversaries who exploited the Internet to disseminate their messages.

Just as important, the economic dependency due to extensive use of the Internet by business concerns to conduct daily commerce made the economy of the United States increasingly vulnerable and subject to attack.

Cognition, the Internet, and Strategic Focus

The attacks on the United States on 11 September 2001 further shaped George W. Bush's information power strategy. No one could argue that the attacks were not lethally devastating of themselves. However, the almost instantaneous exploitation of the images and subsequent global propaganda communications by U.S. enemies became the loud and clear precursor to the nature of war in the information age. Exploitation of this event by perpetrators signaled the beginning of the extensive use of the Internet to conduct warfare in the era of "new" media.[20] The psychological impact of the images of airplanes striking U.S. symbols of economic and military power spread instantaneously and globally, received in different ways by various audiences—some with shock and horror, others with adulation and praise; it was a sober indication of the increasing power of information to achieve strategic ends using the ICT, such as satellite and cable television and the Internet, as a means.

Moreover, rapid exploitation of the images of the attacks by adversaries revealed that the United States was not prepared to deal effectively with the exigencies of warfare in the new dimension of the global information battlefield. The bureaucratic nature of government was shown to be an impediment to strategic policy regarding information in an era where speed and nimbleness were essential to compete proactively and responsively.

Just two years earlier, in 1999, USIA had been dismantled as a "peace dividend" following the Cold War, and its activities parceled out across the State Department. Nominally, the position of under secretary of state for public diplomacy and public affairs had assumed the responsibilities for international

information programs, while the international broadcasting efforts of the U.S. government had been transferred to a semi-independent Broadcasting Board of Governors.[21] This greatly diminished, decentralized, and politicized arrangement proved to be inefficient and ineffective following the 9/11 attacks. Additionally, the problems of policy and a clunky process were compounded by a lack of continuity in leadership as four under secretaries of state for public diplomacy and public affairs were appointed during the eight years of George W. Bush's presidency—and, more telling, the position was vacant for more than one-third of that time.[22] It was not until 2007 that Karen Hughes, the third of Bush's four under secretaries and a close confidante of the president, published a National Strategy for Public Diplomacy and Strategic Communication. While this document focused on informing, engaging, and influencing, it recognized the importance of the Internet to that effort:

> All agencies and embassies must … increase use of new technologies, including creative use of the Internet, web chats, blogs, and video story-telling opportunities on the Internet to highlight American policies and programs.[23]

During the same period, terrorists, recognizing the strategic importance of communication to achieve their objectives though influence, increased their numbers of sponsored websites from twelve at around the start of this millennium to more than seven thousand as of May 2010.[24]

In the absence of a process of effective policy formulation and a mechanism for central management, other agencies of the executive branch of the Bush administrations filled the policy vacuum by acting independently in accordance with their missions and priorities. The Department of Defense (DOD) in its 2006 Quadrennial Defense Review highlighted strategic communication as a key wartime effort, spinning off a separate study to consider how best to inform, engage, and influence while establishing a DOD-level office to spearhead the effort.[25] Less than a year later, the same office within DOD published an extremely limiting policy on the use of the Internet as a means for this purportedly important strategic communication effort.[26]

Later, Bush's *National Strategy to Secure Cyberspace*, published in 2003, focused exclusively on the need to protect the Internet and the associated critical infrastructure dependent on it. While recognizing the critical

interdependencies of both the public and private sectors in the security effort, it provided a framework for information sharing, a means of responding to incidents after the fact, but no standards for creating a more secure system that would be less vulnerable to the increasing threat. Additionally, there is no mention of the Internet as a means to influence through using strategic communication or public diplomacy. In fact, the word "influence" is not mentioned at all in the document, since it was focused on connectivity, not the cognitive impact of information.[27]

While these efforts recognized the necessity of competing in the information environment to achieve cognitive effects while protecting the connectivity to communicate, they also reflected a dichotomy in purpose, which is not surprising given the lack of any overarching national information strategy. The result was different agencies of government—and different offices within the same agency—focused on different dimensions of the information environment. This trend continues today with the Obama administration.

The Obama Administration: More of the Same … but a Glimmer of Hope

If any group should understand the power of the Internet to communicate and influence audiences, it is

(Official White House Photo by Pete Souza)
President Barack Obama discusses strategy on Syria with his national security advisors 31 August 2013 in the White House Situation Room.

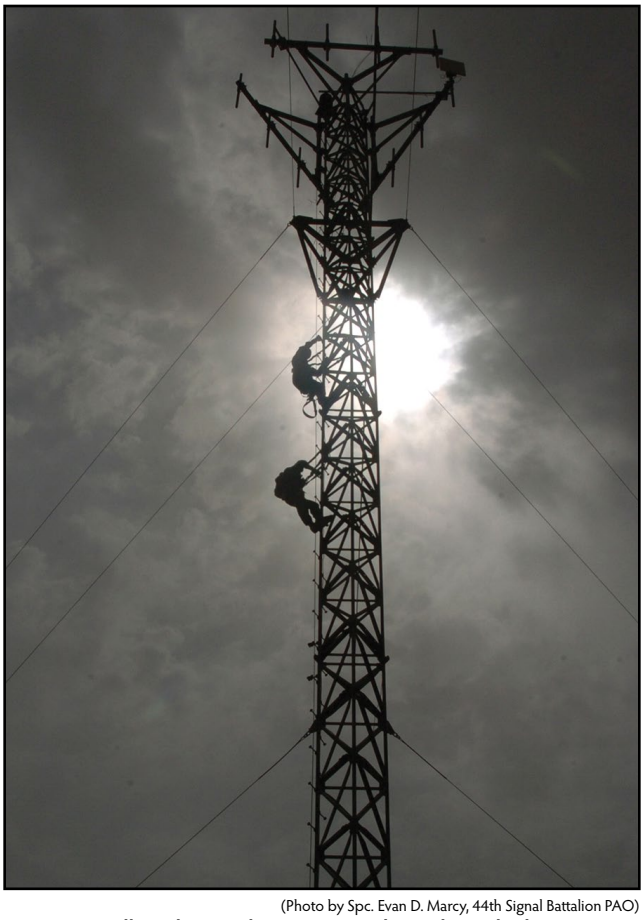
the Obama administration. As a presidential candidate, former Senator Obama adroitly used the Internet to raise funds and spread his political message as never previously seen in the lead-up to his first-term presidential election. This carried over into his administration when the traditional weekly address moved from radio to streaming Internet video. Obama used short-message service text messaging, podcasts, and online transcripts in a variety of languages to communicate his landmark "New Beginnings" Cairo speech in June 2009 throughout the Middle East and Africa.[28] He also understood the significant requirement to protect the Internet by calling for a cyber security review within three weeks of assuming office.[29]

Later in Obama's administration, the White House responded to a congressional requirement by providing the *National Framework for Strategic Communication*, which focused on the cognitive aspects of information as power but principally covered the mechanisms used to coordinate that effort.[30] The White House also announced a program to build upon the Bush administration's "Comprehensive National Cybersecurity Initiative." This effort focused entirely, however, on securing the Internet—with no mention of its use as a means to strategically communicate.[31] These documents and policies approach content and cognition separately and apparently toward distinctly different ends: to protect the connectivity (Internet) or to exploit it to leverage cognitive effects. However, there are indications that the Obama administration understands the need to achieve balance toward both objectives. The Department of Defense released a social media directive in February 2010 ordering military commands to open access to social media sites and to allow individual service members to inform and engage while simultaneously cautioning leaders to "continue to defend against malicious activity."[32] As previously stated, the overarching *National Security Strategy* of 2010 provided a glimmer of hope by addressing both cybersecurity and strategic communication. While strong calls for security of the Internet abound in this strategy, there is also recognition of the need for balance so that communication can be exploited:

> We support the dissemination and use of these technologies [the Internet, wireless networks, mobile smart-phones] to facilitate freedom of expression, expand access to information, increase governmental transparency and accountability, and counter restrictions on their use. We will also better utilize such technologies to effectively communicate our own messages to the world.[33]

Interestingly, in January 2010, then Secretary of State Hillary Clinton gave a highly touted speech on Internet freedom, offering that the freedom to connect is like the freedom of assembly. Continuing, she said, "It allows individuals to get online, come together, and hopefully cooperate. Once you're on the Internet, you don't need to be a tycoon or a rock star to have a huge impact on society."[34] Events in the Middle East, popularly dubbed the "Arab Spring," seemed at first glance to support this position. But the continuing turmoil in that region offers a cautionary tale about any attempt to establish a monocausal explanation for meaningful political change, especially when that single focus is information technology.[35] This points to the complexity and interrelationship of connectivity, content, and cognition.

Perhaps the best way forward yet published by the Obama administration is its *International Strategy for Cyberspace* that the president signed in May 2011 and



(Photo by Spc. Evan D. Marcy, 44th Signal Battalion PAO)
Pvt. Justin Hill, 44th Expeditionary Signal Battalion, climbs a training tower 23 August 2008 while Sgt. Joseph Raymond Chavis waits above at Camp Victory, Iraq. Hill and Chavis are part of a cable team training to install Radio over Internet Protocol equipment on top of towers to improve military communications in Iraq.

publically released at the State Department. This is the most comprehensive approach yet seen towards the strategic implications and use of this new domain. It cites key objectives in economic development, Internet freedoms, network governance, and other wide-ranging areas that are being dramatically shaped by cyberspace, and thus it establishes links to information power.[36]

However, the fact remains that no single executive government agency is in charge of the information instrument of national power overall. Therefore, there will continue to be conflict between agencies seeking to protect the technology and agencies seeking to exploit it to compete cognitively on the world stage. Exacerbating the problem is that the information environment—in its connectivity, content, and cognitive dimensions—is wholly shared, and sometimes dominated by, the private sector. Nor is this dilemma limited to the connectivity represented by information-communication technologies. The executive branch does not control what a senator says … or what an entertainer such as Lady Gaga does.

Having evolved little in terms of policy toward content from where it was in World War I, the United States remains at a crossroad that requires an overarching national information strategy incorporating connectivity, content, and cognition in all its forms. As Bruce Hoffman, a professor at Georgetown University, notes, "Our adversaries have a communications strategy. We, unfortunately, don't."[37]

Strategic Modeling, Organization, and the 3Cs: An Approach to a National Information Strategy

Author Harry Yarger, in *Strategic Theory for the 21st Century: The Little Book on Big Strategy*, describes strategic thinking as "a sophisticated intellectual process seeking to create a synthesis of consensus, efforts, and circumstances to influence the overall environment favorably while managing the risks involved in pursuing opportunities or reacting to threats."[38]

This intellectual process, as related to an information strategy, is best considered by reviewing the definition of the information instrument of national power, which we previously described as "the use of informational content and the technologies and capabilities that enable the exchange of that content, used globally to influence the social, political, economic, and/or military behavior of human beings, whether one or one billion, in the support of national security objectives." From this definition, the *ends*, *ways*, and *means* are evident, and the opportunity to examine them from the perspective of connectivity, content, and cognition emerges.

Ends are the desired effects that enable achievement of objectives. Consequently, a national information strategy should seek to "influence the social, political, economic, and/or military behavior of human beings, whether one or one billion, in support of national security objectives."[39]

Ways reflect the processes applied that most efficiently support achievement of the ends, while *means* are the capabilities and resources synergistically employed by the processes that are inherent to the ways.

In the case of a national information strategy, this paper argues that the 3C model must be applied considering connectivity, content, and cognition to provide strategic focus and to wholly address the application of information power by the United States.

The key words "influence … the behavior" within our definition point to the cognitive nature of the ends. The connectivity necessary to influence human behavior in support of national security objectives runs the entire gamut from the personal interaction of soldiers on the ground to the use of social media by the Departments of State and Defense. Any information strategy must consider all of these possibilities when resourcing and integrating capabilities.

For example, while funding of the DOD's transregional web initiative is important, so are cultural and educational exchanges sponsored by the Department of State.[40] Additionally, given the decentralized execution of these programs and interactions, a key to success is defining a process (a way) to ensure that a lead U.S. government agency provides broad guidance that allows the application of information power while ensuring communication occurs at all levels in ways that enable the stated ends. This approach will drive the appropriate content that, in turn, will impact cognition by influencing to affect behavior.

As previously noted, the power of information and modern information-communication technologies sustains and grows economic power, while enhancing and magnifying American military power and capability as well. The United States is dependent upon that power for success, yet extremely vulnerable to attacks against it based on that very dependency. Thus, cyberspace strategies understandably stress the security aspects of the connectivity without addressing a balanced approach to exploiting it to provide content that affects cognition.

Since information as power is woven through and enables the diplomatic, military, and economic instruments of national power, failure to define a lead U.S. government agency for the information instrument becomes problematic at best. Exacerbating the problem is that, for the most part, private industry controls the connectivity and is not necessarily open to sharing vulnerabilities with the government. This is above and beyond a national psyche that equates information power to propaganda and its pejorative implications, and thus the Nation is unlikely to allow a "Department of Information."[41] However, an extant model may hold the key to the successful development of a holistic U.S. information strategy and any subsequent policy implementation of that strategy.

Similar to information power, the economic instrument of power straddles the private and public sectors. Thus, the National Economic Council, established in 1993 within the executive office of the president, may provide a useful model to emulate in developing a similar system of managing national information power. The council's four principal functions are "to coordinate policy-making for domestic and international economic issues, to coordinate economic policy advice …, ensure that policy decisions … are consistent with the president's economic goals, and to monitor implementation… ."[42] The council consists of numerous department and agency representatives within the administration whose policies affect the U.S. economy.

Establishing a national information council with a similar mandate seems a reasonable approach to strategy development and subsequent policy implementation based on the previous discussion. The council would engage and involve the private sector, bring together all executive agencies with a stake in the strategy and policy, and develop a holistic and balanced approach that considers connectivity, content, and cognition. It would employ the ways and means that most effectively and efficiently allow achievement of defined ends in support of national security objectives while considering and mitigating risk. Importantly, it would directly advise and answer to the president. The composition of such a council would, of course, be up to the president and could easily grow so big as to be unmanageable but, at a minimum, should include representation from government, business, and from all three Cs of the information environment. Its work would emphasize cooperation and coordination toward common national security and strategic goals as expressed in the *National Security Strategy*.

Conclusion

In the past, the United States was able to muddle along using information as power without a strategy to define and direct its use. However, an increasingly connected and complex world demands a national information strategy. Information power is woven throughout the diplomatic, military, and economic instruments of national power as a key enabler of their synergistic success. The obvious importance of information as power demands that the United States develop a holistic national strategy that considers all aspects of the information environment: connectivity, content, and cognition. Only when this occurs will

the United States effectively and efficiently manage and compete in an increasingly muddled and complex information environment.

Author's note: Dan Kuehl passed away on 28 June 2014. He was the consummate selfless educator and leader. He taught and mentored thousands of senior leaders of the U.S. government and its allies on the information element of national power. I was proud and honored to be his friend.

—Dennis Murphy

Col. Dennis Murphy, U.S. Army, retired, is a senior analyst for cyberspace operations at IHS Jane's. He previously served as director of the Information in Warfare Group at the Center for Strategic Leadership, U.S. Army War College. He served in a variety of command and staff positions over his twenty-seven years of U.S. Army service and as the George C. Marshall Fellow for Political-Military and Diplomatic Gaming at the Department of State's Foreign Service Institute. He is accredited in public relations and military communication by the Public Relations Society of America.

Lt. Col. Dan Kuehl, PhD, U.S. Air Force, retired, was a professor of information operations at the National Defense University for eighteen years. At NDU, he helped create the Department of Defense's first major educational effort in what was then called information warfare and, until his retirement in June 2012, served as the director for NDU's program on information operations. Dr. Kuehl received his PhD from Duke University.

Notes

1. U.S. Commission on National Security Strategy in the 21st Century, *New World Coming: American Security in the 21st Century*, 15 September 1999, 1, 4, and 8, accessed 22 June 2015, http://govinfo.library.unt.edu/nssg/Reports/NWC.pdf.

2. U.S. Commission on National Security Strategy in the 21st Century, *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom*, 15 April 2000, accessed 22 June 2015, http://govinfo.library.unt.edu/nssg/PhaseII.pdf.

3. A Google search conducted by the authors of the phrase "National strategy for" resulted in more than 17 million hits, with links to strategies for "suicide prevention," "trusted identities in cyberspace," "prevention and control of Hepatitis," and "combating terrorism," to cite just four on the first results page.

4. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: U.S. Government Printing Office [GPO], 25 March 2013). There are other analytical frameworks, such as PMESII (political, military, economic, social, infrastructure, and information); the use of DIME is not intended to exclude other frameworks.

5. Dan Kuehl, "Defining Information Power," Strategic Forum #115, June 1997, Phil Taylor's papers website (University of Leeds), accessed 22 June 2015, http://media.leeds.ac.uk/papers/vp015a5f.html; originally published by the National Defense University in June 1997.

6. Barack Obama, *National Security Strategy*, May 2010, accessed 22 June 2015, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. This strategy was superseded in 2015, accessed 15 June 2015, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. It should be noted that the 2015 *Strategy* continues the theme of the 2010 version with a section devoted to cybersecurity but little mention of the value of cyberspace to convey content to achieve cognitive effects.

7. British Library, "Your country needs you" advertisement in *London Opinion*, XLII (546), 5 September 1914, accessed 22 June 2015, http://www.bl.uk/collection-items/your-country-needs-you.

8. "Second Life," Linden Lab website, accessed 22 June 2015, http://www.lindenlab.com/products/second-life. Second Life is a three-dimensional online virtual world that allows users to role play and interact with other avatars in a free-play environment.

9. Karen Hughes, remarks made during a worldwide Department of Defense information operations conference, 2005. Both authors were present.

10. JP 3-13, *Information Operations* (Washington, DC: U.S. GPO, 20 November 2014), I-1–I-2.

11. Dennis M. Murphy, book review of Jonathan Reed Winkler, *Nexus: Strategic Communications and American Security in World War I*, *Parameters* 38(4) (Winter 2008-2009): 147–148.

12. Dennis M. Murphy and James F. White, "Propaganda: Can a Word Decide a War?" *Parameters* 37 (3) (Autumn 2007): 18–19.

13. Matt Armstrong, "The Smith-Mundt Act: Myths, Facts and Recommendations," 24 November 2009, Mountain Runner homepage, accessed 19 June 2015, http://www.mountainrunner.us/search?q=The%20Smith-Mundt%20Act%3A%20Myths%2C%20Facts%20and%20Recommendations&f_collectionId=55324e8de4b0323bd730fa5a; The United States Information and Educational Exchange Act, Pub. L. No. 80-402 (1948).

14. Ronald Reagan, "U.S. International Information Policy," National Security Decision Directive 130, 6 March 1984, accessed 19 June 2015, http://www.reagan.utexas.edu/archives/reference/Scanned%20NSDDS/NSDD130.pdf.

15. Ronald Reagan, United States International Broadcasting," National Security Decision Directive 45, 15 July 1982, accessed 19 June 2015, http://www.reagan.utexas.edu/archives/reference/Scanned%20NSDDS/NSDD45.pdf.

16. Russian Ministry of Defense, "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space," 2011, accessed 19 June 2015, http://www.pircenter.org/media/content/files/9/13480921870.pdf. An unofficial translation is available on the NATO Cooperative Cyber Defence Centre of Excellence website, accessed 19 June 2015, https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf. Note that it does not say "cyberspace" but rather "information space." This is not about the technology; it is about the cognitive impact.

17. Pew Research Center, "Internet Use Over Time," Pew Research Center website, accessed 19 June 2015, http://www.pewinternet.org/data-trend/internet-use/internet-use-over-time/.

18. William J. Clinton, "Administration Updates Encryption Policy," Press Release (Washington, DC: The White House, 16 September 1998).

19. William J. Clinton, Presidential Decision Directive 68, *Concerning International Public Information*,1999, available through the Clinton Presidential Library, accessed 19 June 2015, http://www.clintonlibrary.gov/_previous/Documents/0207.pdf.

20. New media as used here are any capabilities that empower a broad range of actors (individuals through nation-states) to create and disseminate real-time or nearly real-time information that can affect a broad (regional or worldwide) audience.

21. Dennis M. Murphy, "Strategic Communication: Wielding the Information Element of Power," *U.S. Army War College Guide to National Security, Volume I: Theory of War and Strategy*, ed. J. Boone Bartholomees, Jr. (Carlisle, PA: Strategic Studies Institute, 2008), 181-182.

22. Matt Armstrong, "Whither Public Diplomacy? Sixty-six Days (and Counting) Without an Undersecretary," Mountain Runner homepage, 23 March 2009, accessed 19 June 2015, http://mountainrunner.us/2009/03/whither_public_diplomacy/.

23. George W. Bush, *U.S. National Strategy for Public Diplomacy and Strategic Communication* (Washington, DC: The White House, March 2007), 6.

24. Bruce Hoffman, *Internet Terror Recruitment and Tradecraft: How Can We Address an Evolving Tool While Protecting Free Speech?,* written testimony submitted to The House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, 26 May 2010: 7, accessed 19 June 2015, http://chsdemocrats.house.gov/SiteDocuments/20100526101502-95237.pdf.

25. U.S. Deputy Secretary of Defense, *2006 Quadrennial Defense Review (QDR) Strategic Communication (SC) Execution Roadmap*, Memorandum for Secretaries of the Military Departments (Washington, DC: U.S. Department of Defense, 25 September 2006), accessed 19 June 2015; http://www.defense.gov/pubs/pdfs/QDRRoadmap20060925a.pdf.

26. On June 8, 2007, the Deputy Secretary of Defense published a memorandum entitled *Policy for Department of Defense Interactive Internet Activities*. This policy allowed only public affairs personnel to interact with the media over the Internet and designated authority for Internet activities be held at the four-star level.

27. George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), accessed 19 June 2015, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

28. Barack Obama, "Remarks by the President on a New Beginning," speech presented at Cairo University, 4 June 2009, accessed 19 June 2015, http://www.whitehouse.gov/blog/NewBeginning/.

29. The White House, Office of the Press Secretary, "President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review, Melissa Hathaway Selected to Lead the Review" White House Press Release, 9 February 2009, accessed 26 March 2015, https://www.whitehouse.gov/the-press-office/president-obama-directs-national-security-and-homeland-security-advisors-conduct-im.

30. Barack Obama, *National Framework for Strategic Communication* (Washington, DC: The White House, February 2010).

31. Barack Obama, *The Comprehensive National Cybersecurity Initiative,* White House White Paper, May 2009, accessed 22 June 2015, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

32. U.S. Deputy Secretary of Defense, *Responsible and Effective Use of Internet-Based Capabilities*, Memorandum for Secretaries of the Military Departments, 25 February 2010, accessed 22 June 2015, http://www.defense.gov/NEWS/DTM%2009-026.pdf.

33. Barack Obama, *National Security Strategy*, May 2010: 39, accessed 22 June 2015, https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

34. Hillary Rodham Clinton, "Remarks on Internet Freedom," speech at the Newseum, Washington, DC, 21 January 2010, accessed 22 June 2015, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

35. Evegny Morozov, *The Net Delusion* (New York: Public Affairs, 2011), 48-49.

36. Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, accessed 22 June 2015, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

37. Bruce Hoffman, quoted in Stew Magnuson, "Futile to Control Internet Terrorist Recruitment, Witnesses Say," *National Defense Magazine*, July 2010, accessed 22 June 2015, http://www.nationaldefensemagazine.org/archive/2010/July/Pages/FutiletoControlInternetTerroristRecruitment.aspx.

38. Harry R. Yarger, *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2006), 36.

39. Kuehl, "Defining Information Power."

40. Senate Report 112-026, National Defense Authorization Act for Fiscal Year 2012, Library of Congress, accessed 22 June 2015, http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp11268Jt5&r_n=sr026.112&dbname=cp112&&sel=TOC_800764&.

41. Murphy and White, "Propaganda: Can a Word Decide a War?" 15.

42. "National Economic Council, Overview" The White House website, accessed 18 June 2015, http://www.whitehouse.gov/administration/eop/nec.