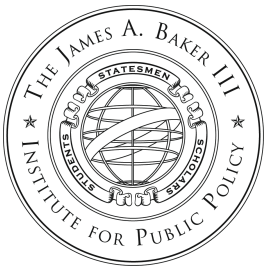

James A. Baker III Institute for Public Policy
Rice University

From Tunis to Tunis: Considering the Planks of U.S. International Cyber Policy, 2005-2011

by

Christopher Bronk, Ph.D.

Fellow in Information Technology Policy
James A. Baker III Institute for Public Policy
Rice University

May 21, 2012

Abstract

How have U.S. policies on the governance of the Internet and cyberspace evolved between the 2005 World Summit of the Information Society (WSIS) in Tunisia and the massive, cyber-fueled uprisings in the Middle East of 2011? The paper develops a framework of possible actions regarding Internet or cyber governance to produce contexts for the timeline of significant policy statements by U.S. government officials and agencies on the topic. In the resulting narrative, Internet governance policy rises from a relatively marginal issue for the foreign policy establishment to a significant component of U.S. grand strategy. Because it covers a brief time period and focuses on a single actor (the United States), this narrative provides input as to how and how rapidly Internet politics and policies have become integral to international affairs.

"Power, before it comes from arms or wealth, emanates from ideas."

—Kenneth Neil Cukier

Introduction

To the agencies of the U.S. government concerned with international affairs and national security, cyberspace has come to matter a great deal. This was not always the case. Interest in the Internet and related environs, labeled "cyber" for simplicity's sake, has grown quickly and for a variety of reasons. A number of events— Internet crackdowns in Burma (2007) and Iran (2009); likely state-sanctioned cyber attacks against Estonia (2007) and Georgia (2009); the impact of the massive WikiLeaks data breach; the Stuxnet worm's apparent damage to the Iranian nuclear enrichment program; and the role of social media in the revolutions of the Arab Spring—have shown foreign policymakers that the Internet and information technology (IT) have a major role in international relations. Cyber, a term that remains a somewhat conceptual moving target, is now important to U.S. foreign policy in areas such as bilateral, multilateral, and public diplomacy as well as military information operations (IO), irregular warfare, and acts of deterrence. In 2012, cyber matters in the foreign policy and national security of the United States, at the State Department ("State") and the Department of Defense (DOD), and in the agencies of the intelligence community. This paper investigates how that came to be.

What is Cyber?

Before studying the historical events that led to what the author considers the rise of U.S. international cyber policy, a practical definition is necessary. So as others have done before, we ask what cyber is and from where it came. The natural point to begin with is the coining of the first element of the lexicon, *cybernetics*, a term made popular by Norbert Wiener[1] in the period immediately following the Second World War in a book described as "a hodgepodge of notions and analysis."[2] It was a beginning, at least, of combining computation and human behavior. Wiener's cybernetics produced a platform for discussion on the intersection of math and logic

[1] Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine* (Hermann & Cie: Paris & MIT Press: Cambridge, MA, 1948).
[2] James Gleick, *The Information: A History, a Theory, a Flood* (Pantheon: New York, 2011), 239.

with social science and human behavior. Cyber's second key text with regard to its conceptual rhetoric is a work of science fiction: William Gibson's science fiction/cyberpunk novel *Neuromancer*,[3] which contains much of the contemporary language regarding the virtual space that interconnects human beings and computers around the globe.

While they could not be more different in many ways, the works of Wiener and Gibson served as touchstones for the imagination in the growing up of computing, networking, and digital interconnection. Both are relevant to the discourse on what defines cyber. Former assistant secretary of defense Joseph Nye offers, "Cyber is a prefix standing for computer and electromagnetic spectrum–related activities."[4] As RAND scholar Martin Libicki constructs it, cyber, or in his parlance cyberspace, holds three layers: physical, syntactic, and semantic.[5]

We may generally agree that cyber is the interconnection of computing that began with the introduction of the Defense Advanced Research Projects Agency's (DARPA) network that connected research computing. The Defense Department had been working with digital computers since the close of the Second World War, but linking those computers together was a key objective of DOD networking research. The protocols, standards, and technology that emerged from the late 1960s ARPANet have become the cyber infrastructure that is the Internet. A series of technologies developed over decades have been incorporated into an infrastructure that is now vitally important; the economic costs of a major disruption are potentially enormous.

[3] William Gibson, *Neuromancer* (Ace: New York, 1984).
[4] Joseph Nye, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly* (Winter 2011): 19, http://www.au.af.mil/au/ssq/2011/winter/nye.pdf.
[5] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press: Cambridge, 2007).

Figure 1. Fundamental Technologies of the Information Revolution

Technology	Year of Development
Digital Computer (ENIAC)	1946
Integrated Circuit (Jack Kilby, Texas Instruments)	1958
Packetized Networking (ARPANET)	1969
Personal Computer (Altair 8800)	1975
Graphical User Interface (Xerox Star)	1981
Cellular Phone (Motorola DynaTAC)	1983

Cyber: Security and Influence

Two interrelated, yet opposing, concepts are part of foreign relations today: cybersecurity and the freedom to communicate via digital means. For the United States, the developer of the Internet, the statecraft of cyber is a relatively new construct. The Department of Defense considers it a domain, standing alongside land, sea, air, and space as a venue for conflict—although the declaration of it as distinct domain may be glossing over information operations (IO) in warfare, a subject that goes back to Thucydides and is at the very core of Sun Tzu's *Art of War*. IO is an area in which practitioners consider how to protect information resources and disrupt the command and control of the enemy. The questions of the moment are how to establish deterrence and understand when actions in cyber permit a physical response of military forces by kinetic means (i.e., bombs and bullets).

Then there is the diplomacy of cyber. Accepting diplomacy as an information-intensive exercise of dialogue, declaration, and demarche, cyber stands alongside previous technologies for connection and interconnection. Before the telegraph, envoys had considerable autonomy and were connected to home capitals by messages sent at the speed of a horse or sailing ship.[6] Telegraphy, telephony, and other analog communication technologies changed the nature of diplomacy, but not the model by which it is practiced. Though advancements in technology

[6] David Nickles, *Under the Wire: How the Telegraph Changed Diplomacy* (Harvard University Press: Cambridge, MA, 2003).

improved communication with senior leadership at home, diplomats still largely spoke for states with states. Only with the rise of public diplomacy—the communication across international boundaries to connect with populations, not leaders—did the number of actors concerned with diplomacy, or at least touched by it, dramatically grow.

For states, cyber is many things. It is a venue for espionage, both international and domestic. It is a locale for displaying cultural, economic, and political influence. It is a domain in which to extend conflict. Virtually any computer on the planet, from a GPS-enabled mobile phone to the process control machine connected to a water distribution system, is capable of being included in this vast space we call cyber, as each of them may be able to communicate to other computers via Internet Protocol (IP).

Fortunately, we are not grappling with the enormity of cyber, i.e., the billions of IP computers around the world. Here, the issue to be considered is how cyber grew to great importance in the foreign affairs agenda of the United States in a relatively short amount of time. It is a story that is bookended by two events that took place in a relatively out of the way locale in global politics: Tunisia, first in 2005 and again in 2011.

Whose Internet?

In 2005, the United States might have surrendered its considerable control over the Internet.[7] That year, the second convention of the World Summit of the Information Society (WSIS) in Tunis was held, following a large meeting in Geneva two years before. Tunis—Arab, yet still claiming the vestiges of a Francophone past—was as interesting a spot as any to hold a conference on the future of the Internet.

Front and center on the 2005 WSIS agenda was the role that the United States would continue to play in the governance of domain names and addresses. As a core developer of the Internet, the U.S. government had shepherded its development from a Pentagon vehicle for scholarly

[7] See Mueller, Milton, *Networks and States: The Global Politics of Internet Governance* (MIT Press: Cambridge, MA, 2010).

communication to a publicly accessible infrastructure managed and operated primarily by private firms. With the adoption of the High Performance Computing and Communication Act and the opening of the National Science Foundation's NSFNet research network for commercialization in the early 1990s, a series of entities—both for-profit and nonprofit—began filling the role of governing the operation of a rapidly growing Internet and World Wide Web.

Key among the entities was the International Corporation for Assigned Names and Numbers (ICANN), which stood up in 1998 to take over the work that had largely been managed by one University of California, Berkeley, professor, Jon Postel. ICANN's primary function is the management of domain names, the process by which IP addresses are assigned to entities so that they may engage in communications via the Internet. This is a confederated function, as each nation is responsible for its national top-level domain (TLD).[8] Funded by the U.S. Department of Commerce, ICANN was and remains clearly connected to the U.S. government. At issue at the 2005 WSIS was the question of whether ICANN should remain the ultimate arbiter of global standards for domain names and numbers. The alternate choice would be to develop an international organization beholden not to the United States, but to an international body such as the United Nations.

Reasons other countries desired an alternative to ICANN were many. As the manager for the root (see below), the assessor of validity at the highest level in the assignment of domain names, ICANN's sovereign status annoyed or aggravated a variety of constituencies. Run on the Roman alphabet, standards promulgated by ICANN and the Internet Engineering Task Force were viewed as insensitive to the billions on the planet who read and write in Arabic, Cyrillic, Chinese, or other alphabets. Compounding the problem, although not yet fully understood, was the United States' increasingly firm stance on collection and analysis of Internet traffic in its efforts to attack Al Qaeda and other terror groups.

In 2005, the United States was very much the global hub for Internet traffic. Its Internet architecture—the most mature on the world—ensured that U.S. Internet Service Providers (ISPs)

[8] These are noticeable on the Internet as the two letter suffixes to Web addresses, such as .nz for New Zealand, .ly for Libya, .tv for Tuvalu, and so on. The United States is an interesting exception, with its .us suffix rarely used.

were a near-certain intermediate stop for IP data packets passing between Asia and Europe, as well as Latin America. Add to this the dominance of U.S. firms in the Internet space—from hardware to search engines and software—as well as privacy rules considered by others, principally the European Union members, to be lacking, and the case against ICANN and U.S. leadership grew.

Additionally, there was the issue of the "root," the servers distributed around the global topography of the Internet, which stand as the definitive directories of Internet addresses for the purposes of routing data around the world via the Internet. Thirteen organizations, 10 of them in the United States, are responsible for the maintenance of these servers (the remaining three are Swedish, Dutch, and Japanese, although synchronized duplicates of the root servers exist in many additional locations).[9]

Although the United States was heavily distracted by other priorities, including wars in Iraq and Afghanistan, the world did not wrestle control of the "root" away from the United States at the WSIS in Tunis. Essentially, this is because the United States simply did not permit it. On June 30, 2005, the National Telecommunications and Information Administration (NTIA), which reports to the U.S. Department of Commerce, issued a single-page set of principles regarding the domain name and addressing system for the Internet. In it, the NTIA stated that it would: (1) preserve the security and stability of the domain name system (DNS); (2) recognize the national interest regarding their top level domains; (3) maintain the position that ICANN was the "appropriate technical manager of Internet DNS"; and (4) support the continued dialogue on Internet governance in multiple fora.[10]

With the shifting of ICANN from U.S. sovereign control to international management effectively tabled, what then did the U.S. get out of Tunis? Hans Klein argues that while the legitimacy of ICANN was discussed at the 2005 WSIS, the United States failed to achieve its goal of bringing

[9] Kenneth Neil Cukier, "Who Controls the Internet?" *Foreign Affairs* 84, no. 6 (Nov/Dec 2005): 7-13. See also J. Abley and K. Lindqvist, "Request for Comments: 4786" (Internet Engineering Task Force, December 2006, http://tools.ietf.org/pdf/rfc4786.pdf).

[10] National Telecommunications and Information Administration, "U.S. Principles on the Internet's Domain Name and Addressing System," June 30, 2005, http://www.ntia.doc.gov/files/ntia/publications/usdnsprinciples_06302005.pdf.

a comprehensive initiative on information security out of the conference.[11] The Tunis Commitment drafted out of the conference mentioned security, however, and contained firm language regarding a continued effort to bridge the digital divide between Internet-connected haves and have-nots, as well as Internet governance issues. On governance, from the WSIS emerged the framework for a governance forum, what would become the Internet Governancy Forum (IGF). ICANN would remain in charge for the time being.

Transforming Diplomacy

After the 2004 U.S. presidential elections, former national security adviser Condoleezza Rice took over from Colin Powell as secretary of state. Powell's tenure at the State Department had largely looked inward with regard to information technology and policy. A self-described IT enthusiast and former board member for one-time Internet titan America Online (AOL), Powell had arrived at the State Department shocked to find an information organization without any significant connectivity to the Internet. One of his top institutional priorities for State was simply to push Internet connectivity to all of its employees. But beyond this internal information plumbing effort, the Powell years were marked by the inheritance of relative neglect of the institution (in part remedied by the Diplomatic Readiness Initiative, begun by Secretary of State Madeleine Albright) and the massive U.S. engagement in the Middle East and Southwest Asia undertaken after 9/11.

When Rice took over, she sought to place a mark on her tenure as secretary of state. At an address given at Georgetown University in January 2006, she forwarded the term "transformational diplomacy" to describe a set of fundamental shifts in how the United States would employ its diplomatic resources. While transformational diplomacy was largely related to shifting resources toward conflict areas and emerging world powers such as Brazil, China, and India, a single technological element was incorporated into the strategy—the concept of "virtual presence." Rice described the initiative:

[11] Hans Klein, "ICANN Reform: Establishing the Rule of Law," Georgia Institute of Technology Internet & Public Policy Project, http://www.internetgovernance.org/wordpress/wp-content/uploads/ICANN-Reform-Establishing-the-Rule-of-Law.pdf

> Perhaps the newest and most cost effective way to adopt a more local posture is through a Virtual Presence Post. Here one or more of our young officers creates and manages an Internet site that is focused on key population centers. This digital meeting room enables foreign citizens, young people most of all, to engage online with American diplomats who could be hundreds of miles away.[12]

First conceived to support U.S. outreach into the cities surrounding the U.S. Consulate in Yekaterinburg, Russia, the Virtual Presence Post (VPP) was developed "to combine virtual presence through an embassy-hosted Web site with coordinated outreach, programming, and travel targeted at a particular city or region."[13] Virtual presence represented an important change in the way diplomacy, particularly public diplomacy, could be undertaken. Even before getting noticed by Rice, virtual presence had been identified as a potentially valuable diplomatic innovation.

> The concept, launched by Tom Niblock, the former U.S. Consulate General of Yekaterinburg, Russia, has the potential to stream germane and time sensitive information to audiences in major cities and remote regions where the United States has no physical presence. Additionally, initial anecdotal evidence from Russia suggests that a virtual consulate may be able to perform up to 50 percent of the work of an actual consulate and do it in a timely and cost effective manner.[14]

Major initiatives in cyber strategy were not a core component of U.S. foreign policy at either the State or Defense Departments during the administrations of President George W. Bush. The expanded development of public diplomacy enabled by information and computing technology

---

[12]Condoleezza Rice, "Transformational Diplomacy: Shaping US Diplomatic Posture in the 21st Century" (speech given at Georgetown School of Foreign Service, January 18, 2006), available at http://www.cfr.org/us-strategy-and-politics/transformational-diplomacy-shaping-us-diplomatic-posture-21st-century/p9637.

[13] George Argyros, Marc Grossman, and Felix Rohatyn, *The Embassy of the Future* (The CSIS Press: Washington, DC, 2007), 44.

[14] U.S. Advisory Commission on Public Diplomacy, "The New Diplomacy: Utilizing Innovative Communication Concepts that Recognize Resource Constraints," June 2003, http://www.state.gov/documents/organization/22956.pdf.

(ICT), particularly in the Arab world, was identified as a potential opportunity during Colin Powell's tenure as secretary of state.

In 2003, a Middle East strategy report prepared for the U.S. House of Representatives Appropriations Committee by the Advisory Group on Public Diplomacy for the Arab and Muslim World identified five key policy planks in ICT development in the Middle East: (1) programs to develop sustainable access to ICT and the Internet; (2) widespread dissemination of computer hardware and software; (3) expanded information resources in languages of the Muslim world, including those that would benefit women and bolster public health; (4) incorporation of foreign nationals in U.S. digital outreach efforts; and (5) a push for wider access to information resources and curbs to state censorship efforts.[15]

During the second term of President George W. Bush, Karen Hughes, a longtime political adviser to the president, inherited the task of enhancing public diplomacy in the Middle East region and led State's public diplomacy efforts. Hughes' tenure at State was generally viewed as unsuccessful, with her Middle East travels sounding a particularly sour note.[16] Hughes did, however, establish her understanding of the ways in which the information revolution was changing the business of public diplomacy. In remarks to the Council on Foreign Relations in 2006, she said:

> During the Cold War we were trying to get information into societies that were largely closed, where people were hungry for that information. Well, today in places like the Middle East there's an information explosion and no one is hungry for information. What we are competing for there is for attention and for credibility in a time when rumors can spark riots, and information, whether

[15] *Changing Minds, Winning Peace: A New Strategic Direction for U.S. Public Diplomacy in the Arab and Muslim World* (Report of the Advisory Group on Public Diplomacy for the Arab and Muslim World, Edward P. Djerejian, chairman, prepared for the U.S. House of Representatives Committee on Appropriations, October 1, 2003).
[16] Fred Kaplan, "Karen Hughes, Stay Home!: What on Earth is She Doing in the Middle East?," *Slate Magazine*, September 29, 2005, http://www.slate.com/articles/news_and_politics/war_stories/2005/09/karen_hughes_stay_home.html.

> it's true or false, quickly spreads across the world, across the internet, in literally instants.[17]

Rice elevated the role of public diplomacy at State, and focused resources on engaging the blogosphere of the Middle East. With the aid of newly-established digital outreach teams, the Department of State's Public Diplomacy Bureau made its influence felt in "Arabic language blogs and forums to provide information about U.S. policies and to counter misinformation and myths posted on the blogs."[18] It also funded research on the Iranian/Persian blogosphere, developing a project with the Berkman Center at Harvard Law School that would eventually produce a topical and contextual map of blogging activity in Iran and the Farsi language.[19] Resources were going into connecting with the public in the Middle East, but at the same time interaction on the Internet was undergoing a dramatic change. While virtual presence had forged the concept of diplomacy via websites, new platforms were radically overhauling interaction on the Web.

Another Information Revolution: The Participatory Internet

Through the second half of George W. Bush's presidency, the U.S. foreign policy apparatus was largely concerned with its public and bilateral diplomacy with the Middle East. In Iraq and Afghanistan, the U.S. military was heavily engaged in relearning the art of counterinsurgency (COIN) operations and redeveloping its repertoire of capacities for winning the hearts and minds of the public. The U.S. armed forces were forced to cope with the use of new information technologies by its adversaries, particularly in Iraq. By 2005, the Iraqi insurgency's tactics had increasingly embraced the use of what would become by far the most deadly tool in its arsenal, the roadside improvised explosive device (IED). Capable of inflicting a steady stream of casualties against U.S. and coalition forces on the move in Iraq, IEDs also proved to be a formidable propaganda weapon of the Iraqi insurgency and Al Qaeda's Iraq franchise.

---

[17] Under Secretary of State for Public Diplomacy and Public Affairs Karen Hughes, "Remarks at the Council on Foreign Relations," New York City, May 10, 2006, http://merln.ndu.edu/archivepdf/nss/state/66098.pdf.
[18] Kenon Nakamura and Susan Epstein, *CRS Report for Congress—Diplomacy in the 21st Century: Transformational Diplomacy* (Congressional Research Service: Washington, DC, August 23, 2007), CRS-13.
[19] John Kelly and Bruce Etling, "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere," Berkman Center Research Publication No. 2008-01 (Berkman Center for Internet and Society, April 5, 2008).

Insurgent IED attacks were being filmed and posted to the Internet within minutes of their occurrence, and proved a valuable outreach and recruitment tool for groups combating the U.S. military and its allies. The videos sent an important message to the U.S. military and to the larger international affairs establishment involved in combating the Iraqi insurgency and jihadist terrorism: Their adversary was able to use the Internet quite effectively to organize their efforts.[20] Indeed, Al Qaeda's legacy of operational successes led one former FBI official to recently argue that "Al Qaeda is a brand to protect."[21] That brand extended to the Internet and did so during a particularly interesting point in the development of the cyber ecosystem—the period of development for Web 2.0, the participatory Internet.

Web. 2.0, a term coined by Internet and computer book publisher Tim O'Reilly, represented a redefinition of Internet experiences. New software platforms, delivered via an Internet browser, often described under the heading social media, changed the pattern of interpersonal interaction on the Internet. Three platforms in particular—Facebook, YouTube, and Twitter—made it easy for individuals to not only communicate online about political issues, but also to mobilize the public.

Figure 2. Major Web 2.0 Developments

Platform	**Year of Development**
Weblog	1997[22]
Wikipedia	2001
Facebook	2004
YouTube	2005
Twitter	2006

[20] Timothy L. Thomas, "Al Qaeda and the Internet: The danger of 'cyberplanning'," *Parameters* 33, no. 1 (Spring 2003), 112–123.
[21] Steve Moore, "TSA: Fail," *gmancasefile* (blog), January 24, 2012, http://gmancasefile.blogspot.com/2012/01/tsa-fail.html.
[22] Term coined by Jorn Barger in 1997. See Jenna Wortham, "After 10 Years of Blogs, the Future's Brighter Than Ever," *Wired*, December 17, 2007, http://www.wired.com/entertainment/theweb/news/2007/12/blog_anniversary.

Each of the Web 2.0 technologies at work behind the political upheavals of the 2011 Arab Spring was essential, as were widespread blogging and online essays. Each platform became an important tool for a variety of reasons, and permitted activists to share ideas, amplify messages, and ultimately organize efforts to undermine the authority of long-standing governments across the Middle East. It is worthwhile to understand the attributes of each of the platforms.

The blog, or Web log, is in many ways the precursor Web 2.0 technology. Blogging platforms such as Wordpress, Movable Type, and Blogger allow individuals to quickly set up their own multimedia web sites for producing articles, usually fairly limited in length. Blog platforms feature the capacity for readers to respond to posts through moderated or unmoderated comment fields. Facebook, a social network, by design links individuals to one another and also to topics, themes, events, and causes. It is a free and open platform for users,[23] but Facebook aggregates user data and markets it to its clients. YouTube permits the posting of video to the Internet by a highly intuitive, user-friendly method; videos are then indexed by the Google search engine (Google has owned the service since 2006). Coming around full circle, Twitter is a micro-blog, a text publishing platform that restricts the length of posts to 140 characters. Twitter posts, or tweets, typically include free text, hash-tagged metadata, other Twitter identities (handles), and links to Web pages, images, and other resources.

In the United States during the second half of the 2000s, blogging challenged the authority of traditional news publications, while Facebook, YouTube, and Twitter changed the complexion of Silicon Valley. The hottest new companies of the decade were Internet companies, and all of them had firm roots in the United States. Within a few years of their creation, Facebook, YouTube, and Twitter were within the world's top 10 most popular websites.[24] These technology platforms had a pivotal role in U.S. electoral politics, and lessons learned there would eventually be incorporated into American foreign policy.

---

[23] This was not always true, Facebook was once a Harvard-only network and then extended to other elite institutions of higher education. It now has more than 700 million users, which equals the population of the third-largest country on Earth.

[24] According to Alexa, a Web metrics firm, Google is #1, Facebook #2, YouTube #3, and Twitter #9 in global Web traffic. Blogspot, a blog hosting service, also owned by Google, stands at #8. See Alexa, "Top Sites," at http://www.alexa.com/topsites. Also of interest are some of the volume statistics. Twitter claims to transmit an average of 250 million tweets per day and more than 60 hours of video are uploaded to YouTube each minute (see "YouTube, Statistics," at http://www.youtube.com/t/press_statistics).

Diplomacy for the 21st Century

By the time the 2008 U.S. presidential election was in full swing, the ground was prepared for a very different sort of political campaign. With the U.S. economy in free fall, presidential candidates vied for their party's nomination using new models for political organization and fundraising. It could be argued that one of the great achievements of the Barack Obama presidential campaign was its capacity to raise money in $100 increments more effectively than competing campaigns that used traditional fundraising mechanisms.[25] Where Howard Dean's campaign had identified the potential of the Internet as a fundraising and mobilization tool, the Obama campaign exploited it.[26]

Obama's arrival in Washington brought more political clout to information technology in the federal executive branch. Among the top technology questions for the new president was whether a federal Chief Information Officer (CIO) position should be created.[27] The Obama administration created positions for both a federal CIO and a federal Chief Technology Officer (CTO). Those officers, Vivek Kundra and Aneesh Chopra, respectively, were assigned roles within the mandate of their organizations, the Office of Management and Budget (OMB) and the Office of Science and Technology Policy (OSTP). They brought with them new ideas about how to run federal IT, the business of government, and transparency levels.

At the State Department, the politics of the Internet assumed a new prominence. Jared Cohen, a Rhodes scholar who had written on youth in the Middle East and came to Condoleeza Rice's policy planning staff in 2006, found an important collaborator and ally in Alec Ross, a key figure in Obama campaign efforts to mobilize support from the U.S. IT sector. Secretary of State Hillary Clinton installed Ross as her senior adviser for innovation. Ross and Cohen's shared

[25] The Obama campaign raised more than $500 million dollars, much of it via the Internet, with 6 million of the 6.5 million donations to the campaign coming from those who gave $100 or less (see Blue State Digital, http://www.bluestatedigital.com/work/case-studies/barack-obama/). Conversely, among individual donors, the John McCain campaign raised the most money from donors who gave $2,300 or more. Indeed, the number of those donating $200-499 and $2300 or more to McCain was roughly equal, about 35,000 people in each category (see OpenSecrets.org, at http://www.opensecrets.org/pres08/donordemCID.php?cycle=2008&cid=n00006424).
[26] Claire Cain Miller, "How Obama's Internet Campaign Changed Politics," *New York Times,* November 7, 2008.
[27] Specified in William J. Clinton, Executive Order 13011: Federal Information Technology (The White House: Washington, DC, July 16, 1996).

efforts bore fruit in new initiatives to reach a technologically savvy audience. They also heavily employed both Facebook and Twitter to connect with others as part of their duties as Clinton's Internet gurus. Traveling widely and often in the company of senior executives from technology companies, the pair came to public prominence with a lengthy feature article in *The New York Times* Sunday magazine. Chronicling the mobile smartphone Twitter postings of both men, and their propensity to intersperse substantive policy views with ordinary pabulum, the *Times* piece made perhaps the fundamental argument for the future of statecraft undertaken via blogs, Twitter, YouTube and Facebook. Perhaps Ross and Cohen's harshest critic, Evgeny Morozov, framed the other side of an argument regarding one of Secretary Clinton's key foreign policy initiatives, regarding Internet freedom.[28]

While Condoleezza Rice had attempted to put her mark on the State Department and international relations via her transformational diplomacy initiative, Hillary Clinton staked out her goals for State through an initiative titled "21st Century Statecraft." Her October 2010 speech on the topic, given to the Commonwealth Club in San Francisco, mentioned several major initiatives for a State Department that was entangled in the realities of working closely with the Defense Department in a number of conflicts, and that was in need of institutional retooling. The precepts of 21st Century Statecraft were underwritten by then-Secretary of Defense Robert Gates, who argued for expanded funding and resources to flow to State rather than the DOD in coping with the soft power tasks in which the United States engaged as it coped with counter-insurgency and counter-terrorism around the globe.

Gates had allegedly made the point that DOD's cadre of band members and musicians outnumbered the ranks of the foreign service, a statement echoed by U.S. Rep. Howard Berman in floor argument regarding the Reconstruction and Stabilization Civilian Management Act of 2008. Berman built upon the idea, pointing out the hollowness of the diplomatic workforce, which was smaller in number than "one carrier battle group."[29] Clinton demonstrated her capacity to think more strategically and along DOD lines with the preparation and publication of

[28] See Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs: New York, 2011).
[29] U.S. Representative Howard Berman (speech on "Reconstruction and Stabilization Civilian Management Act of 2008," March 5, 2008), available at http://www.c-spanvideo.org/appearance/595376794.

an inaugural Quadrennial Diplomacy and Development Review (QDDR), which mated foreign policy goals with institutional capabilities, present or desired.

Published in 2010 and designed to set the tenor for reshaping and developing the State Department and the U.S. Agency for International Development (USAID), the QDDR was built around the identification of key trends in international relations. Among them was recognition that "The information age has accelerated the pace of international affairs and facilitated a new era of connectivity."[30] In the QDDR, the U.S. diplomatic establishment recognized the forces at work in the relationship between digital connectivity and international politics.

> The communications revolution that has swept across the world has had a profound impact on the attitudes, behaviors, and aspirations of people everywhere. Public opinion is influencing foreign governments and shaping world affairs to an unprecedented degree. The advance of democracy and open markets has empowered millions to demand more control over their own destinies and more information from their governments. Even in autocratic societies, leaders must increasingly respond to the opinions and passions of their people. And the tools of technology create unprecedented opportunities to engage foreign publics and advance jointly the interests we share with them.[31]

It is important to remember that this assessment was written in 2010, before the series of events that have come to be known as the Arab Spring. The Clinton State Department was laying the groundwork for diplomatic engagement via the Internet, even as it was about to be buffeted by the largest breach of classified material since the Vietnam War.

The Other Cyber—Military Views of Cyberspace

As it winds down major U.S. military operations in Iraq and Afghanistan, much of what the Department of Defense does has fallen under the scrutiny of the budget cutters. One of the few

[30] "Leading Through Civilian Power," *The First Quadrennial Diplomacy and Development Review* (QDDR), 2010, 16, available at http://www.state.gov/s/dmr/qddr/.
[31] "Leading," *QDDR,*16-17.

areas that has not faced such scrutiny is the Pentagon's set of cybersecurity programs and initiatives. In May 2010, while the State Department was drafting its QDDR, the Defense Department established its newest combatant command or cocom, U.S. Cyber Command (Cybercom). Headquartered at Fort Meade, Maryland, Cybercom was charged with performing military operations in cyberspace—a new, fifth domain of conflict, after land, sea, air, and space.

Questions abound regarding the role and mandate of Cybercom, which is run by the director of the National Security Agency. Certainly, a "priority will be to improve the defenses of military networks," according to one senior U.S. officer.[32] Cybercom is an establishment designed to engage in cyber operations, but very little is known about it. The amount of official public information on Cybercom, nearly two years after its inception, remains quite limited.[33] It has no public doctrine and a publicly stated budget of approximately $3.2 billion[34]—a significant sum, but a small slice of the $553 billion FY 2012 defense budget.[35]

Despite its small public and budgetary footprint, Cybercom—along with the DOD's role in cybersecurity issues—is part of an upward trend in defense and the defense industry. At the DOD, information security issues have generally been the closely held discipline of a small community of cryptography and communications security professionals. But through the late 1990s and into the 2000s, the threat politics of cyberattacks received considerable attention in the Pentagon and in the defense industry press that covers many of its activities.[36] While the DOD was largely preoccupied with the business of fighting counterinsurgencies and engaging in operations against terror groups, a small but growing constituency among its ranks argued for a role in the militarization of cyberspace.

---

[32] "War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?" *The Economist,* July 1, 2010, http://www.economist.com/node/16478792.

[33] Most informative is a DOD media fact sheet regarding the command. See "US Cyber Command Fact Sheet," May 25, 2010, available at http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

[34] Cheryl Pellerin, "'Investing in People is Key' at Cyber Command," *American Forces Press Service*, March 17, 2011, http://www.defense.gov/news/newsarticle.aspx?id=63205.

[35] Not including $117 billion for ongoing combat operations. See "United States Department of Defense Fiscal Year 2012 Budget Request, Overview," Office of the Undersecretary of Defense (Comptroller), U.S. Department of Defense, February 2011.

[36] Myriam Dunn Cavelty, "Cyber-Security and Threat Politics" (London, New York: Routledge, 2008).

Although Cybercom is today a fully joint subcommand—reporting to U.S. Strategic Command, the part of the DOD responsible for maintaining and operating the forces that compose the national strategic nuclear triad—it is hardly the original idea for a cyber force. The U.S. Air Force (USAF) initially floated the concept of a cyber force in an announcement from its then-secretary, Michael Wynne, in November 2006.[37] As part of a publicity campaign that included computer animated television commercials, Wynne made moves that appeared to set the USAF as the lead, or perhaps even the sole, service for cyber operations, of both offensive and defensive nature.[38] The proposal, which was interpreted as a bureaucratic land grab outside the Air Force, was withdrawn by 2008.[39] Some time after his retirement, Marine Gen. James Cartwright, commander of Strategic Command at the time of Wynne's announcement, indicated his misgivings on housing cyber entirely in one service and not at the NSA.[40]

With the arrival of the Obama administration, the DOD's position on cyber issues, primarily regarding the development of a cyber force, continued to evolve. The White House initiated a 90-day cybersecurity review under the leadership of Office of the Director of National Intelligence executive Melissa Hathaway; eventually, a cyber coordinator position was created and filled by Howard Schmidt, a former law enforcement officer who had spent time in the Bush administration as well as in information security positions at Microsoft and eBay. In 2010, the Pentagon published its cybersecurity concerns and ambitions in the form of an article for *Foreign Affairs* penned by Deputy Secretary of Defense William J. Lynn.

Lynn's article revealed a highly classified information security incident regarding the DOD's Secret Internet Protocol Router Network (SIPRNet), code-named Buckshot Yankee. Buckshot

---

[37] C. Todd Lopez, "8th Air Force to become new cyber command," *Air Force Print News*, November 3, 2006, http://www.af.mil/news/story.asp?storyID=123030505.
[38] Christopher Bronk, "Off We Go…: Cyberspace, the Air Force And the New Face of Battle," (paper published by the James A. Baker III Institute for Public Policy at Rice University, August 8, 2008, http://bakerinstitute.org/publications/TSPP-WWT-CyberCommand-080808.pdf.
[39] Wynne's vision for an Air Force-dominated cyber force evaporated after his dismissal by Secretary of Defense Robert Gates in the wake of a scandal regarding his service's management of nuclear weapons; to wit, several W-88 warheads flew across the United States inside cruise missiles aboard a B-52 bomber without its crew knowing they were there.
[40] Webcast of a talk by Gen. James Cartwright at the Hudson Institute Center on Economics of the Internet, February 13, 2012, http://www.hudson.org/index.cfm?fuseaction=hudson_upcoming_events&id=909.

Yankee and the Pentagon's response to it,[41] Lynn contended, "marked a turning point in U.S. cyberdefense strategy."[42] He outlined the missions of the DOD Cybercom (not the Air Force version, which was shelved and eventually replaced with its 24th Air Force), including: (1) the day-to-day protection of the DOD's networks; (2) the provision of a chain of command for mobilizing cyber resources; and (3) cooperation with external stakeholders and partners across the U.S. federal government.

Despite Cybercom's best efforts, the DOD's security efforts regarding the protection of classified information from unauthorized disclosure eventually led to one of the most significant diplomatic crises at the Clinton State Department. Allegedly at the hands of an enlisted intelligence analyst deployed in Iraq, the contents of a DOD system containing more than 250,000 diplomatic cables, many of them carrying a classification level of "Secret," were copied and eventually made public. The actions of that analyst, Army Specialist Bradley Manning, and his reputed confederate, Julian Assange, would come to be known by one word, the name of the radical transparency organization Assange helmed: WikiLeaks.

In November 2010, five major newspapers, *El Pais, Le Monde, Der Spiegel, The Guardian,* and *The New York Times*, revealed following months of rumors that a large number of diplomatic cables purloined from a U.S. government network was in the hands of WikiLeaks. The revelation was met with an indication of deep concern by the State Department. Clinton characterized the dynamics of the transgression in a public statement:

> There have been examples in history in which official conduct has been made public in the name of exposing wrongdoings or misdeeds. This is not one of those cases. In contrast, what is being put on display in this cache of documents is the fact that American diplomats are doing the work we expect them to do. They are helping identify and prevent conflicts before they start. They are working hard every day to solve serious practical problems – to secure dangerous materials, to

[41] Public revelation of Buckshot Yankee represented the first public revelation of a cyber espionage operation undertaken against a DOD classified computer network.
[42] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (September/October 2010), 97.

> fight international crime, to assist human rights defenders, to restore our alliances, to ensure global economic stability.[43]

Following Clinton's remarks, the State Department moved to more deeply address cybersecurity issues with the installation of a coordinator for cyber issues. But before that position could be filled, the fallout from the WikiLeaks cable breach was already being felt, first with the dismissal of the U.S. ambassador to Libya, Gene Cretz, after the release of a cable detailing the eccentricities of life inside the inner circle of Col. Moammar Gadhafi. But already, across the Maghreb a storm was brewing, and WikiLeaks was but one element.

Facebook, YouTube, Twitter, and Revolution

In late 2010, the world's attention once again fixed upon Tunisia—but far more intensely than at the 2005 World Summit on the Information Society. Pressures building across the Middle East since the departure of colonial powers in the wake of the Second World War and through the 1960s exploded with the suicide of a single produce vendor, Mohamed Bouazizi, who set himself on fire to protest political corruption in Tunisia and his inability to make a living. Suddenly, discontent in the government and institutions of the Middle East boiled over.[44] In just a few weeks, a tectonic political shift, labeled an Arab Spring, radically changed the political complexion of the region.

While leaders across the region had flirted with ideas of reform, democratic representation, and economic liberalization, to the man on the street in most Arab cities, the pace of change appeared glacial. Between demographic pressures of populations growing far more rapidly than their economies could possibly produce jobs, the rise of social service institutions largely outside the auspices of the state[45] (which in many cases appeared ineffectual at providing them), and the outright kleptocracy of ruling families, there was a recipe for discontent. With Presidents Zine

[43] U.S. Secretary of State Hillary Rodham Clinton, "Remarks to the Press on Release of Purportedly Confidential Documents by Wikileaks," Washington, DC, November 29, 2010, available at http://www.state.gov/secretary/rm/2010/11/152078.htm.
[44] With early experiments in post-colonial democracy completely sidelined by revolutions and coup d'etats across the Arab world, by 2011 nations from the Maghreb to the Arabian Peninsula fell into three categories: monarchy, dictatorship, and Israel.
[45] Largely undertaken by religious organizations.

al-Abidine Ben Ali (Tunisia), Hosni Mubarak (Egypt), Ghadafi (Libya), and Bashar Assad and his father, Hafez Assad (Syria) holding between them more than a century of executive power, those they ruled were left to wonder whether their successors would provide any sort of roadmap for increased prosperity or expansion of democratic institutions.

Causes of the revolutions and uprisings in Tunisia, Egypt, Libya, Yemen, and Syria will continue to be the subject of debate as scholars move beyond the earliest drafts of history regarding those events. Corruption, rising prices for staple goods, and a lack of economic mobility were all contributing factors to the overthrow of regimes in the Middle East in 2011. But these events have been labeled Facebook, Twitter, or social media revolutions. The power of social media and its utility to the youth at the core of the Arab Spring movement have received attention. In a February 2012 town hall with students in Tunis, Clinton considered the hyperconnectivity available to them:

> [Y]ou are living in a world that your parents, and certainly your grandparents, could never have imagined—satellite television, the Internet, Facebook. My late mother used to say, "What is this about faces on the Internet?"… And new communications technologies shrink your world but expand your horizons. Now everybody can see how others are living—living in prosperity, dignity, and freedom, and they rightly want those things for themselves.[46]

Facebook did matter in Tunisia as individuals organized resistance movements against the Ben Ali government. So, too, did WikiLeaks, with one British tabloid calling events there the "First WikiLeaks Revolution," after leaked cables revealed the country's corruption.[47] But via Twitter, the State Department's then-spokesman, Philip J. Crowley, asserted, "Tunisia is not a Wiki

[46] Transcript and online video of Secretary of State Hillary Rodham Clinton at "Town Hall with Tunisian Youth," Palais du Baron d'Erlanger, Tunis, Tunisia, February 25, 2012, available at http://www.state.gov/secretary/rm/2012/02/184656.htm.

[47] "'First Wikileaks Revolution': Tunisia descends into anarchy as president flees after cables reveal country's corruption,"*Daily Mail Online,* January 15, 2011, http://www.dailymail.co.uk/news/article-1347336/First-Wikileaks-Revolution-Tunisia-descends-anarchy-president-flees.html.

revolution. The Tunisian people knew about the corruption long ago."[48] Some felt WikiLeaks had everything to do with the Tunisian uprising while others believed the opposite.

However, it appears fairly clear that the Ben Ali regime was threatened by the use of Facebook by those who opposed the ruling government. In early January 2011, thousands of Facebook accounts accessed in Tunisia were compromised. Facebook's information security team realized that "the country's Internet service providers were running a malicious piece of code that was recording users' login information when they went to sites like Facebook."[49]

As discontent spread, first to Egypt and then elsewhere in the Middle East, the speed at which political discontent morphed into viable and sustained protest movements overtook the capacity of well-established regimes to maintain order and isolate opponents. Where the Ben Ali government had attempted to monitor discontent on social media by logging ISP data, Egypt went for a wholesale shutdown of Internet connectivity on January 26, 2011.[50] Despite the shutdown, protests continued unabated. Social media–based organization was swapped for the mobilization of people power in the streets. Internet tools and mobilization tactics had served a purpose, but were unnecessary to maintain sustained pressure on the Mubarak government. On the afternoon of Friday, February 11, 2011, Egyptian Vice President Omar Suleiman announced Mubarak's resignation. Further resistance in the Middle East became bloodier, subject to far more harsh state responses and international intervention.

Internet Legacies in U.S. Foreign Policy

With the lead up to and onset of the Arab Spring, we have witnessed, in roughly five years' time, the United States manage the impact of an enormous shift in the politics of digital international communications on international statecraft, in foreign policy, national security, and international policing efforts. U.S. federal agencies have made an important pivot, recognizing the value of

[48] Philip J. Crowley, Twitter post, January 16, 2011, https://twitter.com/#!/pjcrowley.
[49] Alexis Madrigal, "The Inside Story of How Facebook Responded to Tunisian Hacks," *The Atlantic,* January 24, 2011, http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/.
[50] James Cowie, "Egypt Leaves the Internet," *Renesys* (blog), January 27, 2011, http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

what remains a vague catchall term, cyber, and new capacities are being developed. We are witnessing a sovereign response to the issues produced by a global infrastructure that is, at times, difficult to confine to the sovereign boundaries of an international system assembled in Europe in the wake of the last information revolution, which was spurred by the development of the printing press.

Nonetheless, the United States is responding. The FBI provides an example, citing the work of its rapid-response Cyber Action Teams in aiding the governments of Turkey and Morocco in their joint investigation of the Zotob worm, a piece of malware that disrupted computers running the Microsoft Windows 2000 operating system.[51] With U.S. assistance, perpetrators in both countries were located and arrested.[52] This illustrates how the bureaucratic institutions of the state are adapting to the issues created by the global cyber infrastructure. The FBI has developed a cadre of cyber agents who must understand international and domestic law, as well as how IT may be abused or employed to violate those laws. Agents who successfully collect evidence are able to work with prosecutors to successfully take the cases to trial, enhance their careers, and rise in the organization. This demonstrates that pre-Internet bureaucratic edifices may exert their influence and have a measurable impact. Cyber crime fighting is a very real and growing activity.

Moving to the world of cyber conflict, we must raise the question as to what sorts of cyber conflict have actually occurred and what sorts of conflicts will occur. The ostensibly Russian actions against Estonia in 2007, which may be summarized as a variety of persistent distributed denial of service (DDoS) attacks against the country's digital infrastructure, was characterized as a form of cyber conflict.[53] Russia went on to employ cyber means as a component of its military operations against Georgia in 2009. Due to the Russian cyber attacks as well as state-launched cyber espionage operations, mention of cyberwarfare is a staple in the threat politics around the topic of cyber security.

---

[51] "FBI Cyber Action Teams: Traveling the World to Catch Cyber Criminals," Federal Bureau of Investigation news stories, March 6, 2006, http://www.fbi.gov/news/stories/2006/march/cats030606.
[52] "Turk, Moroccan nabbed in huge worm case," *CNN Money,* August 26, 2005, http://money.cnn.com/2005/08/26/technology/worm_arrest/.
[53] Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *SelectedWorks of Scott Shackelford,* July 2008, http://works.bepress.com/cgi/viewcontent.cgi?article=1004&context=scott_shackelford.

The United States continues to develop military cyber capacity to both defend its own command and control resources, and to also engage in the broad spectrum of activities lumped under the term "information operations." However, in the national defense space, despite the purported impact of the Stuxnet worm on Iranian nuclear enrichment capability, we can generally assess that in areas where cyberspace and national security intersect, "what if?" scenarios are more plentiful than real cases open to general consideration and examination.

That leads us, finally, to diplomacy. Here, a significant transformation has occurred. Official statements from U.S. embassies around the globe are increasingly transmitted by Twitter, a tool of seemingly great value in crisis situations where the information picture may be highly fluid and filled with incorrect or specious inputs. The March 2012 coup d'etat in Mali is yet another case of such activity, with the Twitter feed from the U.S. Embassy in Bamako serving as perhaps the definitive information tool for the U.S. government in-country. The post's first tweet, "Contrary to rumors, #Mali's president #ATT is not at @USEmbassyMali,"[54] also indicates just how rapidly a U.S. diplomatic post can develop a virtual presence and communicate its message to a global audience. So, much like the FBI, the State Department finds itself rapidly moving from theory to practice.[55]

There are, however, a variety of diplomacies to consider. First, there is the State Department's emphasis on Internet freedom, which may be interpreted as a de facto extension of U.S. freedoms regarding expression, press, and speech. Second is consideration of the diplomacy of cybersecurity, in which sovereign states attempt to sort out the legality of their own actions in conflict, as well as their efforts to support other stakeholders in coping with crime undertaken via cyber means. A third area of development is cyber-enabled public diplomacy, which may increasingly overtake the more broad brush of international broadcasting the United States has developed under the Voice of America brand. All of these areas are of far greater importance now than they were at the middle of the last decade.

[54] AmEm Bamako, Twitter post, March 12, 2012, Twitter post, https://twitter.com/#!/USEmbassyMali.
[55] Fergus Hanson, "Revolution @State: The Spread of Ediplomacy," *Lowy Institute for International Policy*, March 2012, http://lowyinstitute.richmedia-server.com/docs/Hanson_Revolution-at-State.pdf.

The growth of international cyber policy has another set of considerations. A common refrain is that cyber issues represent an erosion of state power and the decline of effective sovereignty, and an amplification of non-state actor institutional capability.[56] Furthermore, there is a blurring of lines between the state, the individual, the NGO, and the corporation. Consider Jared Cohen, the de facto Internet expert on the policy planning staff at the State Department, who left that institution in 2010 but brought with him more than 200,000 Twitter "followers" to his new position as the head of Google Ideas (a corporate-run policy think tank) and to a parallel appointment at the Council on Foreign Relations.[57]

Because of the ambiguities of digital diplomacy, we are left to wonder what is the policy of states, the sentiments of individuals, or the behavior of corporations. With more horizontal, non-hierarchical networks as a prevailing form of organization, pre-existing norms, rules, and modes of understanding undoubtedly float upon a choppy sea.

The temporal span from the 2005 WSIS to the first revolution of the Arab Spring, both of which happened to occur in Tunis, represents bookends of an interesting time in the international affairs of the United States. It was a period in which international cyber politics bloomed. Finally, we should momentarily ponder to what degree, if any, a connection exists between the events of the WSIS and Tunisia's revolution. While there may not be any, it is at the very least a novel coincidence.

[56] Ronald Deibert, "International Plug 'n Play: Citizen Activism, the Internet, and Global Public Policy," *International Studies Perspectives* 1, no. 3 (December 2000).
[57] That said, foreign policy celebrity is hardly new, but the rapid rise to prominence of new digital media has created a window for new forms of that celebrity.