James A. Baker III Institute for Public Policy
Rice University

Between War and Peace: Considering the Statecraft of Cyberspace from the Perspective of the U.S. State Department

By

Christopher Bronk, Ph.D.

Fellow in Information Technology Policy, James A. Baker III Institute for Public Policy
Lecturer, Department of Computer Science
Rice University

52nd Convention of the International Studies Association
Montreal, Quebec
March 19, 2011

These papers were written by a researcher (or researchers) who participated in a Baker Institute research project. Wherever feasible, these papers are reviewed by outside experts before they are released. However, the research and views expressed in these papers are those of the individual researcher(s), and do not necessarily represent the views of the James A. Baker III Institute for Public Policy.

Abstract

This paper considers how cyber-enabled diplomacy may be undertaken by the United States. While cyber warfare has been a popular topic of discussion over the past decade, less has attention has been directed at the use of cyber instruments (information technology, social media, the blogosphere, etc.) in diplomatic engagement. Considered here is the debate regarding cybersecurity issues and how that debate factors into U.S. diplomatic initiatives. Covered are the: (a) framing of the issue; (b) emergence of cyberspace as an issue for diplomacy; (c) coverage of major incidents for consideration; and (d) prescriptive elements for inter-agency and intra-State Department policy development and collaboration.

Considering Cyber Statecraft

Should the United States appoint an ambassador to cyberspace? This question is the starting point for thinking about the elements necessary for diplomatic engagement in cyberspace by the United States. As U.S. Secretary of State Hillary Clinton has reminded audiences in the United States and abroad, the Internet matters to America's diplomatic initiatives around the globe. This is codified in the State Department's organizational plan for the next few years, its sweeping inaugural Quadrennial Diplomacy and Development Review (QDDR). One of the State Department's new capacities to be developed is the position of a "coordinator for cyber issues." This position's incumbent "will lead State's engagement on cybersecurity and other cyber issues, including efforts to protect a critical part of diplomacy—the confidentiality of communications between and among governments."[1]

Broader thinking on the "other cyber issues," however, is desirable for the State Department's first top cyber diplomat, and the capacities and deficiencies of the department must be carefully considered as it moves more deliberately into the international politics of the global digital information space. In a way, this is a paper directed at an audience of one: the cyber coordinator. Topics considered in this study include the an overview of the shaping of the State Department

[1] Hillary Clinton, *The First Quadrennial Diplomacy and Development Review (QDDR): Leading Through Civilian Power*, U.S. Department of State (Washington, D.C., 2010), 7.

on cyber issues; the incident history upon which policy will be constructed; the linkages to other U.S. government entities desired for sharing in the craft of making cyber foreign policy; and the soft and hard power considerations for policy in the cyber domain. Contained here are prescriptive elements for the new coordinator to consider.

Reading Between the Headlines: Issue Framing

Many factors have shaped the secretary of state's decision to install a cyber coordinator, but perhaps none is more important than the WikiLeaks incident in which more than a quarter million diplomatic cables became publicly available in late 2010. But having a coordinator in place to prevent the next WikiLeaks solves a past problem and one that is not entirely cyber in nature. Argued here is the point that the WikiLeaks episode represents a leak, not a cyber attack. If we are to believe the accusations against U.S. Army intelligence specialist Bradley Manning, the WikiLeaks publication of State Department cable traffic is a case that illustrates the enormous vulnerabilities produced by the capacity of digital information to be easily copied and purloined.[2] A trusted insider likely caused the WikiLeaks episode, making it somewhat similar to the leaking of the Pentagon Papers.

While WikiLeaks clearly matters, there have been many episodes to foretell the rising importance of cyber issues at the State Department,[3] from the cyber attacks launched against Estonia and Georgia (ostensibly by Russia) to those reputedly undertaken by North Korea. The Stuxnet worm, which may well be the first precision- targeted cyber attack, appears to have been directed against the infrastructure of Iran's nuclear fuel enrichment program. Thinking about these items in context does not require more consideration of a coordinator role that protects the secure communications channels of diplomacy, but rather a role aimed at using all manner of cyber technologies, from encryption and distributed computing to Facebook and Twitter, to achieve the international policy goals of the United States.[4] Indeed, the entire State Department

[2] "The leaky corporation," *The Economist*, February 26, 2011.

[3] And warnings about information security issues. See Joe Johnson, "Cyber Security at State: The Stakes Get Higher," *Foreign Service Journal*, September 2005.

[4] Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello, "From 'Cyberterrorism' to 'Cyberwar,' Back and Forth: How the United States Securitized Cyberspace," in *International Relations and Security in the Digital Age*, ed. Johan Eriksson and Giampero Giacomello (London: Routledge, 2007).

should well consider how it must retool virtually all of its operations to meet the digitally interconnected, transnational world in which it functions, and it has exhibited behavior that demonstrates that such an activity is underway.

Cyberspace and U.S. Diplomacy

If the number of proposed pieces of legislation is any indicator, cybersecurity has again moved up on the Washington policy agenda, with a number of bills introduced before Congress in the past four years.[5] Its importance was heavily discounted after September 11, 2001, as forecasts of cyberterrorism seemed misguided. Al Qaeda's attacks employed the most low-tech of means to achieve the most dramatic of physical results. In response, rounding up jihadists became the order of the day for the Bush administration. To wit, the U.S. Intelligence Community (IC) initiated, in terms of quantity of raw data, an intelligence collection activity likely far outstripping any human capacity to process it.[6]

Interconnectedness became a key issue for Washington agencies engaged in the business of international security. For the State Department, one of the top mandates to arrive before 9/11 from its then-chief Colin Powell was the provision of Internet connectivity to all of the personal computers,[7] both in Washington and the more than 250 diplomatic posts abroad. This was no small feat. The State Department's information technology (IT) overhaul was simultaneously inward looking and externally facing. On the former front, an overhaul of the cable system began in 2004 to more effectively fuse the function and form of e-mail messaging and automated search retrieval.[8] The recently formed Bureau of International Information Programs[9] (IIP), while pushing information outside to foreign audiences, shifted public diplomacy resources to its Internet portal, USINFO.gov. Other State bureaus, for instance Consular Affairs, began

[5] Catherine Theohary and John Rollins, *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*, Congressional Research Service, September 30, 2009.
[6] For a warning regarding this problem from the pre-Internet era, consult: Wendy Lichtenstein, *Managing Operational Intelligence Overload: Guidelines for Avoiding Decision Paralysis*, U.S. Naval War College, Newport, R.I., June 18, 1993.
[7] Jane Perlez, "State Dept.'s Work Rules: Powell's Free and Easy Guide," *New York Times,* January 26, 2001.
[8] Wilson Dizard, "State gears up for SMART messaging," *Government Computing News*, August 15, 2003, http://gcn.com/articles/2003/08/15/state-gears-up-for-smart-messaging.aspx.
[9] Established when the United States Information Agency merged with the Department of State in 1999.

leveraging the Web to perform outreach regarding their roles and services. These parallel activities underscore the dual nature of IT capacity building at the State Department, both internal and external.

Beyond the problems of IT at the State Department are the politics of IT and the Internet itself. Those who have toiled to construct the Internet—a group in the United States that includes the ARPANet[10] pioneers and the Silicon Valley entrepreneurial class—have strong and often conflicting opinions regarding governance and the role of government. Internet politics transcend sovereign boundaries, having gone truly global. At the same time, the stakes have risen considerably.

An interesting coincidence came in the State Department's first serious brush with international policymaking on the Internet in Tunis, site of the 2005 World Summit of the Information Society. There, the question was whether governance of the Internet should be transferred from the U.S.-based International Corporation on Assigned Names and Numbers (ICANN) to a transnational entity. Six years later, Tunisian protests, labeled the Jasmine Revolution, were undertaken in Tunis's streets, but also on Twitter, in blogs, and even on the U.S. Embassy's Facebook page. This last medium cost the State Department almost nothing to create, yet served as a vehicle for direct communication between embassy staff and political activists in Tunisia and beyond the country's borders.[11]

Events in Tunisia and later Egypt underscore the value of information technologies to the conduct of international affairs, not only between states but also publics. Microblogging service Twitter became a vital window into the protests in Iran following the 2009 presidential election.[12] Embassies and consulates unable to open smaller constituent posts to serve the ever growing number of global cities passing the one million inhabitant population threshold have embraced virtual presence via the Web as an alternative. [13] Clearly, the Internet is a tremendous

[10] U.S. Department of Defense Advanced Projects Research Agency Network.

[11] The dialogue is also multilingual, with comments in Arabic and French as well as English.

[12] When a technology update was due to be undertaken by Twitter, a State Department official asked for the work to be delayed so that real-time information would continue to flow from Tehran and other sites of protests against the election results, after internal security forces silenced foreign correspondents and removed them from the country.

[13] Ben Bain, "Chat room diplomacy," *Federal Computer Week*, September 3, 2007.

tool for both collecting information from abroad and also communicating messages from Washington to the world.[14]

For the cyber coordinator, however, three principal functions should stand in relief. First, the cybersecurity task matters, both for the State Department's information systems as well as for policy issues of global cybersecurity. Second, beyond the narrow view of security is a broader set of issues that we place under the heading of Internet politics, including the anticensorship plank that was the central thrust of Secretary Clinton's 2009 Internet Freedom address and the soft power[15] applications of IT.[16] Third, there is the question of diplomatic innovation enabled by IT, a function currently managed in the Office of the Secretary of State, reporting directly to the secretary.[17] All these roles will matter to the cyber coordinator, who will have to assign priority in a world of marked techno-political flux.

Defining the Space for Coordination

Cyber issues will continue to surprise American diplomats as the foundations of political power in the Internetworked[18] world change. Mass communication, interaction, and mobilization of political expression via IT are something new.[19] With regard to unfettered access to the Internet, there may be no way for national governments to survive as partially repressive. As we have seen in the Burma 2007 antigovernment protests, it remains possible for the most repressive of regimes to cut Internet links and black themselves out to the world.[20] How Internet connectivity influences the internal politics of states is a rapidly evolving phenomenon. We are unable to know if the cyber cafés of the Middle East and North Africa will serve as forces for political moderation and greater democratization or as digital madrassas, cultivating audiences prepared

[14] Joe Johnson, "The Next Generation," *Foreign Service Journal*, October 2009.

[15] For the initial conceptualization of this concept, which involves fulfilling foreign policy goals through attraction or co-option, see Joseph Nye, *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books 1991).

[16] Hillary Clinton, *Remarks on Internet Freedom*, Washington, D.C., January 21, 2010.

[17] Jesse Lichtenstein, "Digital Diplomacy," *New York Times*, July 16, 2010.

[18] That is, a world interconnected by the Internet.

[19] Clay Shirky, "The Political Power of Social Media," *Foreign Affairs*, January/February 2011.

[20] The Myanmar government severed its outbound Internet service within 24 hours of the killing of Japanese photojournalist Kenji Nagai on September 27, 2007, by a Burmese soldier.

to employ extreme violence as the ultimate form of political expression.[21] This is a world in which we consider Internet freedom issues. But we also increasingly worry about an Internet that will be able to operate as it has for the past 20 years, and how institutions leveraging the Internet are rendered vulnerable by it.

Accepting then, that a cyber coordinator has only a peripheral role in the evolving and potentially enormous job of international information politics, the core job at hand is the management of a secure and stable Internet. This is a task that has largely been left to the technical community. Useful suggestions can be made on securing the technical infrastructure of the Internet without engaging in a political discussion about the job at hand.[22] However, the question remains as to what the international political posture of the United States should be regarding the protection of information systems and conduits from unauthorized access, manipulation, or disruption.

Estonia, Stuxnet, and WikiLeaks: Considering the Anecdotal Exemplars

For more than a decade, a number of individuals have forecast potentially devastating Internet failure scenarios[23] in which the lights go out, banking locks up, planes fall from the sky, and general mayhem ensues. Some in this crowd prognosticated an Electronic Pearl Harbor[24] and remain a factor in the discourse on cybersecurity matters. Perhaps no voice has been more important than Richard Clarke. In his *Cyber War* (2010), Clarke caps prior work on why he considers the cybersecurity problem to be so important. Interesting as well is a review of the book by Bruce Schneier, a leading light in the cybersecurity field with strong technical credentials. Of the book, Schneier opines:

> *Cyber War* is a fast and enjoyable read. This means you could give the book to your non-techy friends, and they'd understand most of it, enjoy all of it, and learn a lot from it. Unfortunately, while there's a lot of smart discussion and good information in the book, there's also a lot of fear-mongering and hyperbole as

[21] Deborah Wheeler, “Empowering publics: Information Technology and democratization in the Arab World: lessons from Internet cafes and beyond,” Oxford Internet Institute Research Report No. 11, 2006.

[22] See Edward Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Burlington, MA: Butterworth-Heinemann, 2011).

[23] Consider James Adams, “Virtual Defense,” *Foreign Affairs*, May/June 2001.

[24] See Neil Munro, “The Pentagon's New Nightmare: An Electronic Pearl Harbor,” *Washington Post*, July 16, 1995.

> well. Since there's no easy way to tell someone what parts of the book to pay attention to and what parts to take with a grain of salt, I can't recommend it for that purpose. This is a pity, because parts of the book really need to be widely read and discussed.[25]

Ultimately this speaks to the core problem for the cyber coordinator: sifting through massive quantities of information to determine the real threats, the points of true international concern that require diplomatic attention and the corralling of partners and stakeholders. There is much bad behavior in cyberspace.[26] Much of it is crime, plain and simple.[27] Other activities revolve around the theft of ideas and intellectual property, from the high crimes of corporate espionage to the more pedestrian problems of peer-to-peer enabled subversion of digital rights management regimes emplaced to protect copyright. Governments, too, have gone from reading the mail of others to reading the e-mail of others, and we are abundantly aware that the signals intelligence piece of the intelligence enterprise is enormously important.[28] There is increasing evidence of a cyber warfare *realpolitik* becoming more a reality than a hypothesis.[29] Finally, it appears that international law on warfare in cyberspace lags behind technical capacity.[30] What is clear is that Internet security politics are increasingly merging with international threat politics.[31]

[25] Bruce Schneier, "Book Review: *Cyber War*," Schneier on Security (blog), December 21, 2010, http://www.schneier.com/blog/archives/2010/12/book_review_cyb.html.

[26] Charney's four categories—espionage, cybercrime, intellectual theft, and cyberwar—are a useful heuristic. See Scott Charney, *Rethinking the Cyber Threat: A Framework and Path Forward*, Microsoft Corporation, May 2010.

[27] For a trenchant take, see David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Malden, MA: Polity Press, 2007).

[28] Setting aside the Zimmerman Note and Enigma cases as exemplars of First and Second World War signals intelligence exploits, respectively, signals intelligence (SIGINT) rose to become a fundamentally important area for intelligence collection during the Cold War (see Matthew Aid and Cies Wiebes, "Introduction on the Importance of Signals Intelligence in the Cold War," *Intelligence and National Security* 16, No. 1 (2001): 1-26) and remains so in global intelligence operations by the U.S. and its allies today (see James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008).

[29] Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54, no. 2 (2010): 381-401.

[30] Thom Shanker, "Cyberwar Nominee Sees Gaps in Law," *New York Times*, April 14, 2010.

[31] Myriam Dunn Cavelty, *Cybersecurity and Threat Politics: U.S. Efforts to Secure the Information Age* (London: Routledge, 2008).

Bordering on Cyberwar: Some Hard Power Cases[32]

While cyber operations as a component of warfare between states or in civil conflicts is a real and growing prospect, we can look to a series of events to serve as guideposts for policy on cyber misbehavior falling somewhere short of war. The cyber attacks launched against Estonia in April-May 2007[33] certainly mark an escalation of seriousness in the level of impact wrought upon the function of a highly Internetworked, digital society. While there is no definitive proof of Moscow's involvement in directing or initiating the broad denial of service attacks against Estonia, a NATO member, the fact remains that the attacks against Estonia were politically motivated. Whether one of Russia's cybercrime syndicates, a phenotype exemplified by the Russian Business Network (RBN), was to blame, or the Russian security or intelligence services remains unknown. But Estonia's cyber incident capped more than a decade of denial of service attacks and web page defacements made between rival and belligerent states or groups, including China-Taiwan (as a corollary to cross-Straits issue), Israel-Palestine (as part of the continuing Intifada movements), and Japan-South Korea (over language regarding Korea's occupation appearing in Japanese school textbooks).

Estonia's neighbors and NATO allies rendered assistance, essentially rebooting the country's information infrastructure, but the process to full restoration of electronic services was neither rapid, nor without difficulty. But other than some rioting in Tallinn by members of the Russian minority, there was no significant violence. A year later, cyber attacks were launched against Georgia, another of Russia's neighbors, as part of a full spectrum of military attacks by the Russian state in response to Georgian military moves in South Ossetia. Although the Georgian government was probably far more preoccupied with the armored columns streaming south in Abkhazia and South Ossetia and the bombs falling on Tbilisi's airport, it also fell victim to denial of service and web page defacement attacks. The attacks included a photo-montage defacement of the Georgian parliament's website in which images of President Mikheil

[32] That is, cases that involve coercion or the use of force.

[33] Cyber attacks against institutions in Estonia including telecommunications, banking, and government services were precipitated by the Estonian government's decision to move the Soviet Bronze Soldier of Tallinn, a monument in remembrance of the Great Patriotic War, from a location in the city's core to a military cemetery in Tallinn's suburbs.

Saakashvili's were juxtaposed with those of Adolf Hitler.[34] Actors operating under the title "South Ossetia Hack Crew" took credit for the parliament's defacement. Once again, the computer security community was left to ponder whether the cyber attacks against the Georgians could be considered part of the military action against Georgia by Russia or the patriotic acts of Russian hacker gangs. However, the use of force by Russia against Georgia shows ample evidence that Russia can generate a cyber capability, whether civilian, military, or both, when the need of state arises.[35]

This confusion over laying blame and the problem of attribution are of course one of the key challenges for international cybersecurity policy.[36] The personal computer and an Internet connection are the weapons of the cyber activist, cyber criminal or cyber warrior, just as the Kalashnikov assault rifle and the rocket-propelled grenade are the cheap, readily available tools of the insurgent. Because the platform by which to launch a cyber attack is inherently democratic, the source of an attack can be almost any machine, located anywhere. Worse, major distributed attacks, which involve botnets,[37] pay little, if any, respect to sovereign geography. That means that politically motivated cyber attacks may enlist computing cycles from millions of "zombie" Internet hosts, including those within the targeted country. Technical countermeasures to this type of attack thus far appear unsuccessful, and international policy has yet to address the issue with a treaty instrument to ban denial of service attacks or bot-delivered e-mail spam.

Even more vexing for the cyber coordinator will be coping with clandestine measures undertaken by the United States or its allies. What are we to make of a former In-Q-Tel[38] administrative officer and counsel's statement that the Central Intelligence Agency was involved in the shipment of faulty computer controller systems to the Soviet Union that would later be involved

[34] Travis Wentworth, "You've Got Malice: Russian nationalists waged a cyber war against Georgia. Fighting back is virtually impossible," *Newsweek*, August 12, 2008, http://www.newsweek.com/id/154965.

[35] John Leyden, "Russian spy agencies linked to Georgian cyber-attacks," *The Register*, March 23, 2009, http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/.

[36] Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (2010): 384-410.

[37] A botnet is a network of compromised computers that perform instructions clandestinely at the direction of an unauthorized party.

[38] "Launched in 1999 as an independent, not-for-profit organization, In-Q-Tel (IQT) was created to bridge the gap between the technology needs of the IC and new advances in commercial technology." In-Q-Tel website, accessed March 24, 2011, http://www.iqt.org/mission/our-aim.html.

in the largest natural gas pipeline explosion in history?[39] With this as background, the Stuxnet attack must be further scrutinized. Stuxnet reputedly involved the installation of malicious software code on the process control computers running the high-speed centrifuges employed by the Iranian government to enrich uranium at its Natanz facility. Additional detail on Stuxnet's functionality, drawn from its source code, is worth considering as described on a trade publication website:

> In a nutshell, Stuxnet can be thought of as a stealth control system that resides on its target controllers along with legitimate program code. The ultimate goal of the attack is not the controller; it is what the controller controls. Attack code analysis reveals that the attackers had full knowledge of project, installation and instrumentation details. The attackers took great care to make sure that only their designated targets were hit. It was a marksmen's job. On target, the attack is surgical and takes advantage of deep process and equipment knowledge. The attack is not performed in a hit-and-run style, where it would be executed immediately after attaching to the controller or at the next best opportunity. Instead, the attack code carefully monitors the hijacked process for extended periods of time before executing the strike. Outputs are then controlled by Stuxnet, with neither legitimate program code nor any attached operator panel or SCADA system noticing. Stuxnet combines denial of control and denial of view, providing for the ultimate aggressive attack.[40]

This "marksmen's job," a covert action by cyber means, proved an attractive option for a state or states, but which ones? Stuxnet was an activity not without scale, complexity or considerable planning. If we are to believe the hypotheses laid out in one piece of news analysis,[41] the purported Stuxnet attack on Iran's nuclear enrichment program connects the German electronics

[39] Jody Westby, comments to the First Worldwide Cybersecurity Summit, Dallas, TX, May 4, 2010. See also: William Safire, "The Farewell Dossier," *New York Times*, February 2, 2004.

[40] Ralph Langner, "How to Hijack a Controller: Why Stuxnet Isn't Just About Siemens' PLCs," *Control Global*, January 13, 2011, http://www.controlglobal.com/articles/2011/IndustrialControllers1101.html.

[41] William Broad, John Markoff and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

conglomerate Siemens,[42] who the authors conjecture collaborated with the U.S. Department of Energy on security issues in its process control computing systems, and Israel, which possesses the infrastructure required to integrate and test a cyber attack against an enrichment complex (the country has been enriching nuclear fuel at Dimona for several decades).

All of this is speculation, of course, but for the cyber coordinator, the question must be asked, "To what degree will that individual be keyed into whatever offensive or clandestine cyber operations undertaken by the U.S. military or agencies of the Intelligence Community?" Cyber operations may serve as a highly useful alternative to overt and covert uses of military force, but rendering the United States invulnerable to cyber attack, by state-sponsored groups or those without state affiliation, is an accomplishment not yet achieved (and perhaps unachievable).[43] The United States may possess unrivaled offensive cyber capabilities, but no doubt any would-be attacker will have plenty of targets from which to choose impacting its interests. It will be hard for the international community to take seriously American leaders who scold rivals for engaging in cyber espionage as reports emerge of major U.S. cyber attacks against threatening states or transnational groups. How the offensive use of cyber force complements diplomacy will be perhaps be the thorniest of issues for a State Department cyber coordinator to sort out.

Not so important for the long haul will be the problem set presented by the WikiLeaks episode. WikiLeaks is a tactical information security failure with strategic diplomatic implications. However, the organization came into the massive trove of SIPRNet[44] distribution-labeled cables,[45] we can be fairly certain that such a breach will not ever again occur in exactly the same way, with the same type of information. In consideration of the cable channel data breach, policy response should be directed at continued protection of that channel by all technical means possible. In addition, the State Department, and those agencies with which it collaborates, will

[42] Despite numerous news stories detailing the vulnerability Stuxnet exploits in the Siemens S7-series process controllers, shares of Siemens AG rose from US$60 to more than US$90 over the 52-week period ending January 21, 2011.

[43] Chris Bronk, "Treasure Trove or Trouble: Cyber-Enabled Intelligence and International Politics," *American Intelligence Journal* 28, no. 2 (2010).

[44] SIPRNet is the United States Department of Defense Secret Internet Protocol Router Network, a computer network employed to transmit classified information from computer workstations via Internet Protocol (IP).

[45] Joby Warrick, "WikiLeaks cable dump reveals flaws of State Department's information-sharing tool," *Washington Post*, January 31, 2010.

need to work out practical data monitoring, retention, and destruction policies for digital information.[46]

Considering each of the major incidents mentioned above, U.S. diplomacy will doubtlessly cope with cyber attacks launched by international actors against one another, including allies and perhaps the United States itself. In addition, the United States, including the agencies of its federal government, will continue to be targeted by actors wishing to purloin, manipulate, or deny access to information. While the worst- case scenarios of cyber-launched chaos will likely remain worst-case scenarios, the pattern of incidents reported over the last few years indicates significant vulnerability without remedy immediately at hand. Technical currents are merging with those of politics and policy. For U.S. international policy, this confluence of heterogeneous phenomenon will necessitate collaboration across a broad expanse of government agencies, into the private sector, and reaching institutions of international governance and civil society around the globe. Foggy Bottom or the Pentagon alone cannot manage the international security issues of global information infrastructure.[47]

Relationships of Cyber Command, Control, Cooperation, and Collaboration

The State Department's cyber coordinator will not only need to coordinate activity and effort across the organization's regional and functional bureaus, but also with partners in the Intelligence Community (IC), Department of Defense (some of which also fall under the auspices of the IC), and other concerned U.S. agencies. How will bridge building take shape? Will the State Department assign a political adviser to U.S. Cyber Command[48] as it does the other Department of Defense combatant commands? Will "cyber officers" fill portfolios in U.S. embassies and consulates abroad? There are likely many more questions of this variety to be considered.

[46] Artificial intelligence able to detect anyone accessing more pages of textual information than could be read in a realistic timeline is a necessity, and does not represent an insurmountable technical issue.

[47] Peter Sommer and Ian Brown, "Reducing Systemic Cybersecurity Risk," *Future Global Shocks,* Organisation for Economic Co-operation and Development, 2011.

[48] Established in 2009 and formally opened in May 2010, Cyber Command is a subunified combatant command reporting to U.S. Strategic Command, a full unified combatant command.

Developing diplomatic cyber policy, however, should not be an activity of augmenting military or intelligence activities alone. Thus, in framing partnerships with other U.S. agencies, the State Department should be reminded of how control of information impacts the foreign governments with which it interacts on a daily basis. If a preliminary response to all internal instability within foreign regimes is to cut access to the Internet, social media, and mobile voice and digital communications, then the cyber coordinator must be engaged on this front as well, seeking remedy on cybersecurity issues, both for diplomatic communications and broader incident response. Obviously, this set of wants likely vastly exceeds any existing well of resources to be tapped. Therefore the cyber coordinator will have to forge a number of key relationships with other actors, both in the State Department and inside other agencies, to craft elements of the United States's hard and soft power cyber strategies.

Viewing malicious software code as an armament aids development of a language diplomat and soldier may share. It is no secret that the Department of Defense (DoD) has set cybersecurity as a key function, likely to grow considerably. In establishing a U.S. Cyber Command (USCYBERCOM) in 2010, headquartered at Fort Meade, Maryland, the longtime home of the National Security Agency, the DoD expressed a pivotal shift in priorities.[49] Fighting wars without air-to-air or ship-to-ship combat, the U.S. military is left to cope with asymmetric threats posed by a body of actors including national intelligence agencies, criminal hacker gangs, and political hacktivists. But what is USCYBERCOM's international mandate?

Doctrinally, little is known about it. Unlike the other combatant commands, it has no public website. DoD public affairs said of it in a May 2010 press release:

> USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure

[49] And one the U.S. Air Force had sought to develop semi-independently from the other services only a few years before. See T. Michael Moseley, *The Nation's Guardians: America's 21st Century Air Force*, CSAF White Paper, December 29, 2007.

> US/Allied freedom of action in cyberspace and deny the same to our adversaries.[50]

What this means in more practical terms involves a number of policy decision items. As mentioned above, the presence of cyber arms begets discussion of cyber arms control. In addition, there is the issue of how deterrence may be conveyed in cyberspace, where attribution is a consistent problem.[51] Ostensibly, USCYBERCOM is aimed at waging offensive operations during times of war and preparing for such operations, as well as defending the Department of Defense's networks and information resources at all times. Certainly, the State Department could learn from USCYBERCOM's massive defensive efforts, and also would need to know what sorts of cyber arms might be in the wings to demonstrate as sticks for diplomacy.

But there is a complicating wrinkle. USCYBERCOM's chief is also wears a "dual-hat" as director of the National Security Agency (NSA). Any discussion of the State Department's relationship with the IC obviously turns on its relationship with the NSA. However, the thorny issue at high levels is to what degree the cyber coordinator will be speaking to the commander of USCYBERCOM, or the director of NSA, at any given moment (although staffing arrangements below the top position should hopefully work much of that confusion out). Despite this potential confusion, the relationship between NSA and the State Department will matter deeply, as no other agency in the federal government holds the depth of knowledge and understanding of information security threats, vulnerabilities, and mitigation strategies. How NSA intelligence products become a part of U.S. cyber foreign policy will be delicate. However, it is one that will build on a longstanding set of protocols involving incorporation of NSA products in foreign policy decision-making.

Far shallower are the relationships between the State Department and the other major U.S. cybersecurity agency, the Department of Homeland Security (DHS). Standing as the lead civilian agency on cybersecurity matters and holding responsibility over cyber-incident response deemed

[50] "Cyber Command Fact Sheet," U.S. Department of Defense, accessed February 2, 2011, http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

[51] "U.S. Cyber Command Goes Online," discussion by the editors of *Democracy Arsenal* (blog), National Security Network, October 1, 2009, http://www.democracyarsenal.org/2009/10/us-cyber-command-goes-online-.html.

to fall below the threshold of military action, DHS has been characterized as an agency with mandates far beyond its capabilities.[52] Though this asymmetry of capability versus portfolio may not persist indefinitely, its integration into the policy process with regard to cybersecurity has been at times rocky. Former DHS cyber chief Rod Beckstrom (now running ICANN) lamented the agency in starving its cybersecurity activity of resources. [53] While that problem has largely been remedied, DHS has not yet published anything beyond a draft National Cyber Incident Response Plan. If a major national cyber incident should occur, the State Department and DHS will need to collaborate, and this is something for which the cyber coordinator must lay the groundwork.

In addition to relations with the lead civilian cybersecurity agency, the State Department must have a link to the lead civilian intelligence agency as well. Especially because of the potential for clandestine action via cyber means, the State Department must retain linkages to the Central Intelligence Agency's National Clandestine Service, as well as its analytical and technical organs. If the CIA is going to engage in what might be labeled "offensive" cyber operations in conditions other than war, continuity of connection to diplomatic initiatives, including even public diplomacy programs, should be maintained.

Reaching Inside State

In addition to reaching beyond the boundaries of the State Department, the cyber coordinator will need to maintain relationships with stakeholders within it. There are obvious interior linkages that will help and provide value to the Department of State. Obviously, the Bureau of Diplomatic Security (DS) is a necessary partner, as is the Bureau of Information Resource Management (IRM), as the two share duties in defending the State Department's data processing and messaging systems. Indeed, DS and IRM hold exactly the mandate and capabilities to

[52] Gregory Wilshusen, "Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information" (General Accountability Office testimony before the Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives, June 25, 2009), http://www.gao.gov/new.items/d09835t.pdf.

[53] Rod Beckstrom, "Letter of Resignation" (Department of Homeland Security National Cybersecurity Center director's letter of resignation, March 5, 2009), http://epic.org/linkedfiles/ncsc_directors_resignation1.pdf.

prevent future major data breaches, a core directive established for the cyber coordinator in the QDDR. But more complicated will be the relationships on matters of international policy.

For decades, the United States has espoused as a significant plank of its foreign policy the belief that foreign publics should hold unfettered access to information. This global extension of the Constitutional rights to assembly and speech was employed heavily in the Cold War and has been echoed in the Bush and Obama administrations. Significantly figuring in the Bureau of Democracy, Human Rights, and Labor (DRL), has been policy designed to influence repressive regimes toward opening their presses and permitting political expression.[54] The presence of the Internet, of course changes the vehicles of dissemination for news, political speech, and indeed assembly. As the events in Egypt and Tunisia show, people power still matters, but the people need not publish newspapers or storm state-run media outlets. Perhaps most importantly, IT has and will continue to significantly alter the means by which political groups organize and aggregate their efforts. Hopefully, a lesson will be learned that suicide bombs don’t work in changing the system, but flash mobs do.

Beyond DRL, several other functional bureaus probably will be of some importance to the cyber coordinator. The Bureau of Economic, Energy, and Business Affairs (EEB) has long had a role in global telecommunications regulation. The Tunis World Summit on the Information Society (2005) marked the beginning of what is likely a major re-allocation of attention in EEB to Internet policy and a host of other digital issues. Arms control and political military affairs offices are also likely partners, as is the department’s public diplomacy bureau, and in particular its Office of International Information Programs, which dedicates considerable effort to Internet-based communications of the U.S. government to publics abroad. Other elements of the State Department, from the policy planning staff and global affairs to international law enforcement and narcotics, also will matter.

However, it is the relationship between the cyber coordinator and the State Department’s undersecretary for political affairs will be most important for the cyber coordinator to make serious

[54] Daniel McCarthy, “Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet,” *Foreign Policy Analysis* 7, no. 1 (2011).

headway in the promulgation of policy goals. This is because the regional bureaus responsible for managing the bilateral relationships and staffing the embassies and consulates abroad work for the undersecretary. To make the cyber coordinator's goals stick, real positions and portfolios inside the regional bureaus will be needed. Such a process will require the reformulation of duties and competencies in an organization still struggling to overcome an internal structure that largely caters to the business of maintaining bilateral relationships with nation states. The concern is that cyber tasks will take their place as requests for reports, along the lines of mandated reports regarding human rights, religious freedom, or state sponsorship of terrorism.

Ultimately, cyber issues will require a home inside the State Department and the broader foreign affairs community. Needed is an answer for the following question: Does the State Department foresee the cyber coordinator's office as leading to an eventual component of another bureau, a free-standing organization reporting to the secretary, or as a temporary entity to be dissolved when the problem of cybersecurity is well-managed as a global issue?

Engaging in the Business of Cyber Statecraft

While proffering the idea that cyber issues may be resolved may seem naïve and unsophisticated, it begs the additional question of when, how, and where cyber political strategies, tools, and policies—a framework of cyber statecraft—will take hold in Washington. For the moment, there appear two general strains of cyber power with which policymakers will contend: hard and soft. Hard or soft cyber power may appear genuinely unreal and abstract, but when considering the cases above, from the role of social media in the Middle Eastern revolutions of 2011 to the application of malicious software code against the Iranian nuclear program via the Stuxnet worm, there seems little dispute in acknowledging that both concepts are real and relevant.

The question then must be, "How relevant?" Consider Stuxnet, a malware attack on physical infrastructure that is reputed to have significantly damaged the Iranian enrichment capacity. Does such an attack qualify as an act of terrorism, war, or international crime? Conversely, do the services provided by U.S. firms that may aid those wishing to overthrow foreign governments represent a serious threat to national sovereignty?

These are hard questions, but ones needing attention at the Departments of Justice, State, Defense, and Homeland Security, as well as the National Security Council. There remains a dearth of international agreement on the running or policing of cyberspace, and not a single treaty regarding the use of cyber means in or outside of war. We are left to wonder if cyber attacks, as long as they do not kill or maim, will be illegal, but generally considered fair game—a requisite for espionage and option for covert action.

Painting such a picture appears bleak, and for good reason. The Internet has transformed human capacity for communication at a distance. Statements from U.S. officials retain a high-minded view of how it should be employed to enable transparency, combat corruption, and diffuse American or Western ideals regarding speech and expression. While the causality is unclear and weighting of variables difficult, arguments that the diffusion of IT may lead foreign publics to question their political and economic surroundings appear valid. Cyber soft power, just as information-based soft power before it, is a real consideration for diplomacy, both bilateral and multilateral, and not just to be placed under the heading of public diplomacy.[55] But there are unanticipated consequences of local interpretation of U.S. messages and content delivered by networks: digital, informational, and social. Constructively considering concepts of some complexity, such as the merits of representative or direct democracy, in 140-character blocks seems unlikely. But, nonetheless, the political pamphleteers of the coming decade will likely be bloggers of one sort or another.

Bringing this back to the job of Secretary Clinton's cyber coordinator, Christopher Painter, the author counsels to consider statecraft over security in rendering advice. Much thinking has gone into how nations and others might wage cyberwar, but far less is locatable on digital diplomacy.[56] Perhaps this will change if the countries, corporations, and the multiplicity of others who employ, value, and enjoy the Internet as a global entity are not able to do so. As boundary gateways align with sovereign boundaries, we may yet observe a fracturing of the Internet into many non-contiguous pieces. Bearing in mind Internet freedom and cybersecurity, such a fragmentation may be the most important consequence of U.S. policy that is poorly designed to pursue such lofty goals.

[55] Joseph Nye, "Cyber Power," (paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA, 2010).

[56] For the exemplar, consult: Wilson Dizard, *Digital Diplomacy: U.S. Foreign Policy in the Information Age*, (Washington, D.C.: Center for Strategic and International Studies, 2001).