Cyber Operations
The New Balance

By STEPHEN W. KORNS

This is no unsolvable problem if we face it wisely and courageously.

—Franklin Delano Roosevelt

A new normalcy is ascendant in cyberspace. What does this mean, and what are the implications for the Department of Defense (DOD) cyber policy? Some characterize cyber new normalcy as hybrid, multimodal Internet conflict, which combines state-level lethality with amorphous cyber formations.[1] Others view cyber new normalcy as a breathtakingly broad and globally inclusive campaign of deliberate cyber penetrations against governments, militaries, and commercial concerns.[2] In a January 2009 *Foreign Affairs* article, Defense Secretary Robert Gates described today's new normalcy as the search for balance in defense capabilities.[3] A few examples might serve to better illuminate the cyber new normalcy concept.

During the August 2008 conflict between Russia and Georgia, cyber attackers used tools from a Web site hosted by a company in Texas to attack a Georgian government Web site that had been relocated—coincidentally—to a Web hosting company in Atlanta, Georgia.[4] In essence, the United States experienced collateral damage during these cyber attacks. Borderless cyber operations confounding border-based paradigms are not a deviation; it is cyber new normalcy.

During the December 2008 attacks in Mumbai, India, the attack teams used cable

Colonel Stephen W. Korns, USAF, is Vice Director for Strategy, Plans, Policy, and International Relations at Joint Task Force–Global Network Operations, Washington, DC.

U.S. Air Force (Lance Cheung)

Airmen discuss operational status at Cyber Command (Provisional) network center, Barksdale Air Force Base

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Operations: The New Balance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 5th Avenue SW Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

television, BlackBerry phones, Google Earth imagery, and global positioning system information to form an integrated, low-cost command and control capability that enabled a modicum of information superiority. As Ralph Peters points out, incidents such as Mumbai demonstrate that nonstate actors "do not fear network-centric warfare because they have already mastered it."[5] Mumbai is not an outlier; it is cyber new normalcy.

Finally, in a subtle yet telling sign of cyber new normalcy, hackers in 2008 attacked the Barack Obama and John McCain campaign Web sites, compromised Mr. Obama's personal Twitter account, hacked Republican Vice Presidential candidate Sarah Palin's email, and falsified a Web account attributed to Vint Cerf, one of the Internet's founding fathers. It leaves us wondering: if hackers have no contrition about sullying national leaders or insulting Internet luminaries, what is next? And thus, we find the essence of cyber new normalcy: what is next in cyberspace? And are we prepared?

The Modern American Experience

New normalcy has become an episodic policy construct in U.S. strategic ideation. National leadership has relied on the new normalcy clarion call to illuminate moments in time when it is understood that the Nation faces not only a severe threat, but also a transcending reorientation. Often invoked in times of national crisis, new normalcy in the American experience signals a cardinal shift in the nature of U.S. security.

For example, in the winter of 1937, the effects of President Franklin Roosevelt's New Deal policies took an unexpectedly negative turn—the "recession within a depression"—with employment falling again to near Depression-era levels. In response, New York Mayor Fiorello LaGuardia despondently observed that "instead of considering the situation as an emergency, we accept the inevitable, that we are now in a new normal."[6] Roosevelt's new normalcy became the reality of Federally guaranteed economic security as the new basis for overall national security.

In 1953, President Dwight Eisenhower viewed the atomic realities of Soviet nuclear weapons as a new and untenable threat. Reflective of this thinking, a White House aide wrote a secret memorandum highlighting the nuclear age of peril as "the new and to all intents permanent normalcy."[7] President Eisenhower believed containment to be inadequate against a nuclear-armed Soviet power; therefore, his new normalcy became the "New Look" defense policy that emphasized mutually assured destruction through massive retaliation using air-atomic power.[8]

On October 25, 2001, echoing a deep national sense of insecurity after the 9/11 terrorist attacks, Vice President Richard Cheney lamented, "Many of the steps we have now been forced to take will become permanent in American life. They represent an understanding of the world as it is, and dangers we must guard against perhaps for decades to come. I think of it as the new normalcy."[9] The Bush-Cheney new normalcy thus became the "New War," instantiated in a fundamental shift to preclusion, or preemptive self-defense, under a permanent state of national emergency.[10]

New normalcy defines a quintessential dichotomy: the urge to return to the comfort and routine of a normal state, confronted by the realization that the prior condition no longer exists. For example, many in the U.S. foreign policy community viewed the collapse of the Soviet Union as an opportunity for a return to normalcy in American foreign policy, allowing the United States to cash in the peace dividend. Yet even as the Belavezha Accords were being signed, effectively dismantling the Soviet Union, the tectonic undertones of terrorism and global fragmentation were already well in place. The notion of an American post–Cold War return to a neo-isolationist normalcy was but a fading ideal, when in fact that prior normal condition had long since vanished under the "New World Order" of Mikhail Gorbachev and George H.W. Bush.

new normalcy in the American experience signals a cardinal shift in the nature of U.S. security

New normalcy can also be seen as a reaction to what author Nassim Nicholas Taleb describes as "black swan" events—those highly improbable occurrences beyond the realm of normal expectations. What was previously accepted as impossible—even preposterous—is suddenly reality, leaving the Nation grasping for comprehension under forced acceptance. In this context, new normalcy becomes an extempore self-interrogatory, compelling the citizenry to unwillingly decipher and assimilate the residue of a perceived calamitous breakdown in the normal way of life. New normalcy thus serves as the tenuous bridge to the reality of an unknown, fundamentally altered future. Perhaps Eisenhower best captured this nuance as "groping to know the full sense and meaning of these times in which we live."[11]

U.S. joint military doctrine includes new normalcy as a central concept. From this perspective, new normalcy is the condition achieved whereby an adversary is rendered unable to oppose U.S. strategic objectives. After achieving the operational endstate, new normalcy becomes a strategic goal in transition from conflict, which disrupts normal life, to a new level of stability. To achieve new normalcy, the U.S. military, supported by interagency and multinational partners, transitions from major combat operations to stabilization, security, transition, and reconstruction. In addition, adaptive force packages counter any insurgency resistance as the new normalcy begins to take shape.

Although primarily understood from a policy development point of view, there is also a socioscientific basis for comprehension of new normalcy. Thomas Kuhn posits that when the current normal condition cannot explain or resolve an anomaly, a crisis ensues, leading to a fundamental paradigm shift, concluding in a new state of normalcy. In Kuhn's normative transformation theory, a professional community "alter[s] its conception of entities with which it has long been familiar, and . . . shift[s] the network of theory through which it deals with the world."[12]

Cyber New Normalcy

At a 2005 hearing, Senator Olympia Snowe alluded to waking up one morning to "yet another new normalcy, just as we did on September 12, 2001."[13] These words symbolically parallel growing national sentiment regarding the fear of a major cyber disaster—thus, the dramatic rise in predictions of a "cyber Pearl Harbor" or an "e-9/11" event. Vint Cerf even likens the rampant spread of malware to a "pandemic . . . that could undermine the future of the Internet."[14] In the end, Cerf reflects circumspectly, "It seems every machine has to defend itself. The Internet was designed that way. It's every man for himself."[15]

Some in the national security community question whether current U.S. cyber

strategy can meet the challenges of modern cyber threats. For instance, a December 2008 Center for Strategic and International Studies (CSIS) report on cybersecurity concludes that protecting cyberspace is "a battle we are losing."[16] In testimony before Congress, Jim Lewis, a member of the panel that wrote the CSIS report, stated that "the U.S. is disorganized and lacks a coherent national [cybersecurity] strategy."[17] Similarly, a 2008 Defense Science Board report concludes that "there is scant real progress to better secure our information infrastructure."[18] The former Director of National Intelligence believed the country is "not prepared to deal with current cybersecurity threats."[19] A former special assistant to the President for critical infrastructure protection warns: "Are we ready for a large-scale cyber disruption or attack? I believe the answer is clearly no."[20]

The daily tidal wave of ever more shocking revelations threatens to overwhelm, as if we are witnessing a recession in cybersecurity capabilities. Cyber attacks have resulted in government-wide computer infections and loss of information. The Department of State admits to losing terabytes of information. Likewise, DOD has lost a volume of information equivalent to twice the number of printed pages in the Library of Congress. Hackers so pervasively penetrated the U.S. Bureau of Industry and Security that the agency completely disconnected itself from the Internet. The White House itself has had to deal with unidentified intrusions into its network, and malware has even infected laptops aboard the International Space Station. Due to the overwhelming nature of these cyber threats, a 2008 Senate report indicated the cost to defend government networks could rise to as much as $17 billion.[21]

The unprecedented growth in cyber threats has led policymakers and analysts alike to assert with increasing frequency that the United States is experiencing a new normalcy in cyberspace. As early as 2003, the Gilmore Commission's report on *Forging America's New Normalcy* predicted the onset of cyber new normalcy conditions, including cyberterrorism.[22] In commenting on the increasing sophistication of cyber attacks, the state of Michigan's chief information security officer recently noted: "I don't think this is just hype—this is the new normal."[23] Perhaps the clearest, most unambiguous recognition of cyber new normalcy is the CSIS 2008 report on cybersecurity, which invokes the spirit of Roosevelt's national emergency, Eisenhower's nuclear threat, and Bush's war on terror: "The U.S. must treat cybersecurity as one of the most important national security challenges it faces. . . . [T]his is a strategic issue on par with weapons of mass destruction and global jihad."[24] The following trends provide compelling evidence of this new normalcy condition in cyberspace.

new normalcy is the condition achieved whereby an adversary is rendered unable to oppose U.S. strategic objectives

Commoditization. Under old normalcy, individuals developed malware. Under cyber new normalcy, anyone can obtain malware at the "cyber drive-through window." The Internet is a profit-generating machine for criminal syndicates that have perfected malware-as-a-service. The Organisation for Security and

Airman monitors servers for unauthorized activity on Ali Air Base, Iraq

U.S. Air Force (Jonathan Snyder)

Co-operation in Europe estimates that the cyber underground now rakes in a staggering $100 *billion* per year.[25] Reflective of this trend, during the Georgian-Russian conflict, hackers posted downloadable malware on public Web sites with instructions on how to join in the cyber attack against Georgia. An Internet journalist investigating the issue concluded: "All I needed to do was to save a copy of a certain web page to my hard drive and . . . voilà: my browser was now sending thousands of queries to the most important Georgian sites, helping to overload them. . . . [I]n less than an hour, I had become an Internet soldier."[26]

Identification. Under old normalcy, when bombs and bullets flew, identification of the adversary was relatively easy. In cyber new normalcy, identification is the exception. In *Here Comes Everybody*, author Clay Shirky attributes "ridiculously easy group formation" as the Internet's defining characteristic.[27] The Estonian and Georgian cyber events serve as the quintessential examples of this state versus ad hoc cyber assemblage phenomenon. Although some initially declared the events as cyberwar, most in the international community now characterize these incidents as cyber crime via a proxy apparatchik of instantaneous cyber militia-mobs. At best, according to Estonian officials, it is terrorism.[28]

Distrust. Under old normalcy, we trusted but verified. Under cyber new normalcy, there is no trust, and verification is highly suspect. Malware can spoof and effectively nullify antivirus and firewall systems. Even worse, a team of Dutch and Swiss researchers have broken the MD5 encryption algorithm used by nearly all Internet Web browsers.[29] With MD5 compromised, it is now possible that Web browsers could erroneously verify forged digital signatures or software certificates, compromising previously trusted Internet transactions with little indication of foul play.

Symmetry. Under old normalcy, cyber was seen as an asymmetric capability. Under cyber new normalcy, cyber attacks are no longer asymmetric; they are *expected*. As Verisign analyst Eli Jellenc points out: "We are witnessing . . . the birth of true, operational cyber warfare."[30] Similarly, Representative Jim Langevin of the House Homeland Security Committee asserts, "Never again will we see major warfare without a strong cyber component."[31] Cyber today is ubiquitously many-to-many: weak attack weak, strong attack weak, and weak attack strong. Asymmetric warfare is generally considered the domain of the weaker party in applying unconventional methods to exploit vulnerabilities of the strong. Given this, it is questionable if the asymmetry precept still applies to cyber. Russian-inspired hackers have in succession attacked Estonia, Lithuania, and Georgia. These are the attacks of the cyber strong against the cyber weak. Iranian Shi'a and Arab Sunni hackers carry out "Koranic retaliation" cyber attacks against each other. Indian and Pakistani patriotic hackers engage in sustained cyber skirmishes. When the Lebanese government tried to prevent Hizballah from operating its own fiber optic network, Hizballah declared the affront as tantamount to war and responded by taking over West Beirut. Cyber operations are now the very definition of modern conventional tactics.

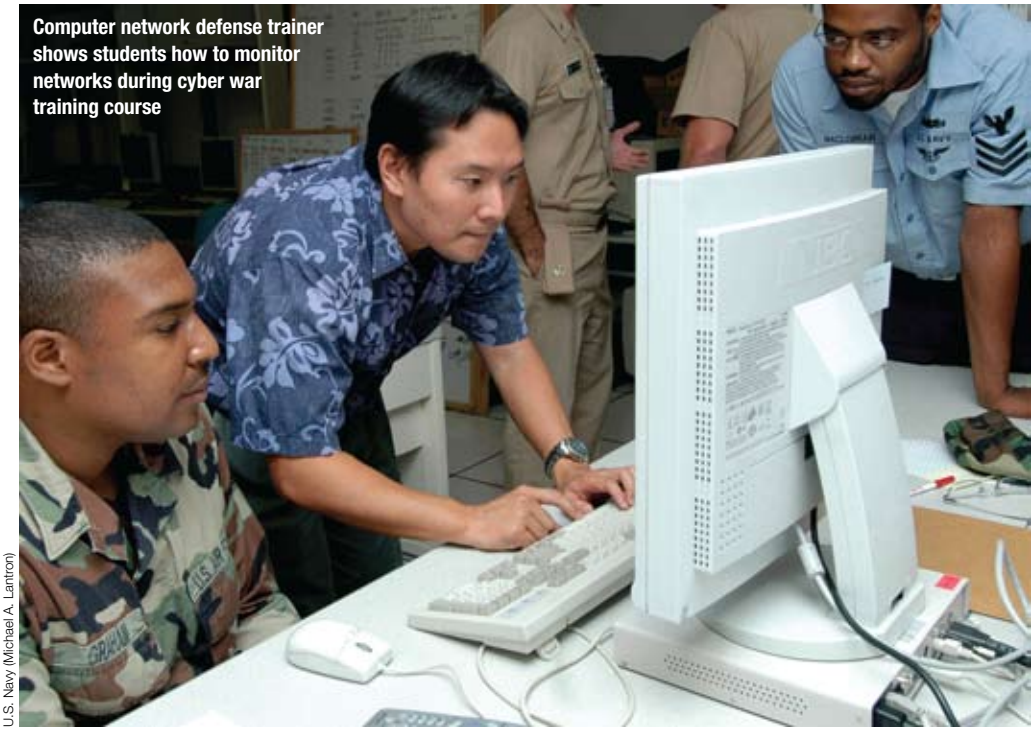
under cyber new normalcy, cyber attacks are no longer asymmetric; they are expected

Deterrence. Under old normalcy, "deterrence by denial" defined the core U.S. cyber policy.[32] Cyber new normalcy admits that deterrence has failed to substantively alter the motivational calculus of determined cyber attackers. As Jim Gosler points out in "Digital Dimensions," cyber defenses are mismatched against the offensive efforts of cyber adversaries. Over a decade ago, Richard Harknett argued that deterrence models developed during the Cold War will provide "poor guidance" for strategic thinking about cyber deterrence.[33] The well-regarded Cyber Conflict Studies Association indicates that to date there is no compelling evidence refuting Harknett's position. This situation will likely continue unabated until the penalties for cyber attacks begin to outweigh the gains.

The New Balance

In facing the new normalcy of today's complex defense environment, Secretary Gates offers an insightful way ahead. In January 2009, he established "balance" as the defining principle of the Pentagon's new National Defense Strategy.[34] In effect, the Secretary's vision can be seen as the call for a New Balance in DOD capabilities, and it establishes a practical framework for addressing cyber new normalcy. In line with joint doctrine, cyber New Balance could be defined as the quest to attain a new level of stability in the DOD cyber environment in order to better support U.S. strategic objectives.

Secretary Gates' call for a New Balance is strikingly reminiscent of the new normalcy



Computer network defense trainer shows students how to monitor networks during cyber war training course

U.S. Navy (Michael A. Lantron)

experiences of the Roosevelt, Eisenhower, and Bush administrations. For example, in his first inaugural address, Roosevelt called for a frank and honest discussion regarding the Nation's economic ills. Secretary Gates' New Balance similarly calls for a blunt assessment of the current U.S. defense posture. In line with this thinking, cyber new normalcy warrants a frank, realistic assessment of the New Balance needed in DOD cyber capabilities. A fundamental premise of cyber new normalcy is that a New Balance is required in culture, conduct, and capabilities in order to better operate and defend in and through cyberspace. A judicious cyber New Balance policy would reassess DOD-wide priorities in areas such as offense balanced with defense, personal use balanced with official use of military networks, compliance balanced with accountability in network usage, and permitting versus restricting unfettered Internet access from the global information grid. As Kuhn warned, these changes may be difficult to accept for those entrenched within the current paradigm. It may unfortunately take a Billy Mitchell moment—a "cyber Ostfriesland"—to truly convince skeptics of the reality of cyber new normalcy.

Secretary Gates' call for a renewed focus on U.S. deterrence policy evokes President Eisenhower's New Look emphasis on strategic deterrence. An enlightened cyber strategy would seek an appropriate balance between secrecy and openness. While working at RAND in the early 1960s, Paul Baran conceived the digital packet switching concept used to establish a survivable U.S. nuclear command and control system. Significantly, Baran openly published his work, with the U.S. Government's implied consent, under the premise that "deterrence only works if the other guy knows."[35] Harknett similarly argues that deterrence is contingent on the challenger and the deterrer possessing shared knowledge about each other.[36] A perceptive cyber New Balance protocol would openly communicate certain capabilities and intentions in order to strengthen cyber deterrence. Credible deterrence will also require balanced resourcing for identification and authentication; data hardening and network resiliency; cyber intelligence, surveillance, and reconnaissance; and cyber early warning and response.

Mindful of the Bush New War, Secretary Gates' New Balance seeks solutions to hybrid conflict. Cyber new normalcy reflects Ralph Peters' notion of a "counter-revolution in military affairs."[37] In essence, an evolving "counter-revolution in cyber affairs" defines cyber new normalcy. An adroit New Balance cyber policy would encourage an honest assessment of the military means for engaging in cyber conflict and determine the relevancy to cyber new normalcy conditions. As witnessed in the cyber attacks on Estonia, Lithuania, and Georgia, non–mirror-imaging adversaries have a well-honed grasp of operating within the grey area of cyber, below the threshold of use of force. Deterritorialized attackers target territorialized infrastructure, frustrating border-based orthodoxy. These hybrid cyber militia-mobs clearly demonstrate that adversaries will not fight the U.S. military on its own terms in cyberspace. In fact, military-on-military in cyberspace may become the exception, rather than the norm, with relatively few "lawful combatants" in the traditional sense. An astute strategy would seek to refine the understanding of how "military affairs" fits within a cyber world where predominantly industry and noncombatant civilians establish and control the core operational theater of conflict. The counterrevolution in cyber affairs will necessitate development of alternative tactics against this global amalgam of state, state-sponsored, and nonstate actors.

In addition to the above, a wise cyber New Balance would prudently avoid the "10-foot-tall Ivan" syndrome that some analysts argue symbolically represented overstated Soviet Cold War capabilities. A thoughtful approach would seek a conscientious balance between cybersecurity and openness, and inclusively engage the public. The Gilmore Commission succinctly captured the essence of this tension by suggesting that any new normalcy policy should include "heightened security but not with such an obsessiveness that it would destroy the economic base or the civil freedoms of the country."[38]

Finally, a sensible New Balance policy would rationally approach the issue of cyberwar. Cyber weapons may offer the advantage of low cost in terms of human life and physical damage. In fact, a growing line of thought suggests that the potentially nonlethal and discriminative nature of cyber weapons should motivate international law to accommodate and even encourage the judicious application of cyber operations.[39] However, while some have asserted that the United States is at war in cyberspace today, there must also be follow-through in articulating the strategy and conditions for a discernible end. Implying an undefined and unending cyberwar could lead to the misperception that the United States seeks militarization of the Internet. In addition, international law remains immature for determining when a cyber event crosses the threshold triggering use of force. Cyber New Balance would seek to avoid unproductive discourse of endless, boundless cyberwar while constructing a methodology for discriminating between cybercrime, cyberterrorism, and the conduct of legitimate military cyber operations.

a perceptive cyber New Balance protocol would openly communicate certain capabilities and intentions in order to strengthen cyber deterrence

Lessons from the Roosevelt, Eisenhower, and Bush new normalcy cases provide compelling evidence to suggest that enlightenment, rather than retrenchment, is the path for cyber New Balance. The economic calamity of the Great Depression directly confronted Roosevelt, as the Soviet nuclear arsenal did Eisenhower and terrorism did Bush. The threats were known and real. Similarly, cyber threats are real and have evolved. In the face of fractious cyber challenges, an insightful reevaluation of DOD cyber policy is advisable.

With Secretary Gates' New Balance as the fundamental underpinning, DOD has a compelling opportunity to rebalance cyber priorities in line with the realities of cyber new normalcy. A comprehensive cyber New Balance effort recognizes that action must be taken across the entirety of the defense community, including defense industrial base partners. Progress necessitates identification and resolution of entrenched technical and cultural impediments that hamper progress. A New Balance strategy can attain true cyber new normalcy through change in culture and conduct, improved technical capabilities, and altered policy constructs that deliver meaningful deterrence. Failing these, DOD cyber capabilities will undoubtedly remain ossified under old normalcy. **JFQ**

NOTES

[1] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, December 2007), 28, available at <www.potomacinstitute.org/publications/Potomac_HybridWar_0108.pdf>.

[2] James R. Langevin et al., *Securing Cyberspace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, December 2008), 12, available at <www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf>.

[3] Robert M. Gates, "A Balanced Strategy," *Foreign Affairs* 88, no. 1 (January-February 2009), 1, available at <www.foreignaffairs.org/20090101faessay88103-p0/robert-m-gates/a-balanced-strategy.html>.

[4] Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2008), 13, available at <www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>.

[5] Ralph Peters, "The Counterrevolution in Military Affairs," *The Weekly Standard*, July 2, 2006, 1, available at <www.weeklystandard.com/Content/Public/Articles/000/000/006/649qrsob.asp>.

[6] Ronald Edsforth, *The New Deal* (New York: Blackwell Publishing, 2000), 152.

[7] Ira Chernus, "The National Insecurity State," November 3, 2002, available at <http://hnn.us/articles/1102.html>.

[8] John Lewis Gaddis, *We Now Know: Rethinking Cold War History* (New York: Oxford University Press, 1997).

[9] Richard B. Cheney, remarks to the Republican Governors Association, Washington, DC, October 25, 2001, available at <www.whitehouse.gov/vicepresident/news-speeches/speeches/vp20011025.html>.

[10] George W. Bush, conversation with Rudolph Giuliani and George Pataki, September 13, 2001, available at <www.whitehouse.gov/news/releases/2001/09/20010913-4.html>.

[11] Dwight D. Eisenhower, first inaugural address, Washington, DC, January 20, 1953, available at <http://millercenter.org/scripps/archive/speeches/detail/3356>.

[12] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago: University of Chicago Press, 1962).

[13] Olympia J. Snowe, prepared statement, Hearing on Current and Projected National Security Threats, Senate Select Committee on Intelligence, Washington, DC, February 16, 2005, 71, available at <http://intelligence.senate.gov/threats.pdf>.

[14] Will Sturgeon, "Botnets Could Eat the Net," ZDNet Asia, January 29, 2007, 1, available at <www.zdnetasia.com/news/security/0,39044215,61985344,00.htm>.

[15] Vint Cerf, in Jack Schofield, "It's Every Man for Himself," *The Guardian*, October 1, 2008, available at <www.guardian.co.uk/technology/2008/oct/02/interviews.internet>.

[16] Langevin, 11.

[17] James Lewis, "Cyber Security Recommendations for the Next Administration," testimony before House Subcommittee on Emerging Threats, Cyber Security, and Science and Technology, Washington, DC, September 16, 2008, available at <http://homeland.house.gov/SiteDocuments/20080916142057-24561.PDF>.

[18] Defense Science Board (DSB), *Defense Imperatives for the New Administration* (Washington, DC: DSB, August 2008), 3, available at <www.acq.osd.mil/dsb/reports.htm>.

[19] J. Michael McConnell, "Annual Threat Assessment," testimony before Senate Armed Services Committee, Washington, DC, February 27, 2008, 34, available at <www.dni.gov/testimonies/20080227_transcript.pdf>.

[20] Paul Kurtz, in Declan McCullagh and Anne Broache, "U.S. Cybersecurity Due for FEMA-like Calamity?" *CNET News*, October 10, 2005, available at <http://news.cnet.com/U.S.-cybersecurity-due-for-FEMA-like-calamity/2100-7348_3-5891219.html>.

[21] Bob Brewin, "Cost of Cybersecurity Initiative to Triple, Panel Says," *NextGov News*, May 19, 2008, available at <www.nextgov.com/nextgov/ng_20080519_1961.php>.

[22] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), Fifth Annual Report to the President and the Congress: *Forging America's New Normalcy* (Santa Monica, CA: RAND, December 15, 2003), L–8, available at <www.rand.org/nsrd/terrpanel/volume_v/volume_v.pdf>.

[23] Dan Lohremann, "Has the Next Generation of Cyber Problems Arrived?" *CSO Magazine*, August 17, 2008, available at <http://blogs.csoonline.com/has_the_next_generation_of_cyber_problems_arrived>.

[24] Langevin, 15.

[25] John Markoff, "Thieves Winning Online War, Maybe Even in Your Computer," *The New York Times*, December 6, 2008, A1, available at <www.nytimes.com/2008/12/06/technology/internet/06security.html?partner=rss>.

[26] Evgeny Morozov, "An Army of Ones and Zeroes—How I Became a Soldier in the Georgia-Russia Cyberwar," Slate.com, August 14, 2008, available at <www.slate.com/id/2197514>.

[27] Clay Shirky, *The Power of Organizing without Organizations* (New York: Penguin Press, 2008), 155.

[28] "EU Should Class Cyber Attacks as Terrorism: Estonia," *Brisbane Times*, June 8, 2007, available at <http://news.brisbanetimes.com.au/technology/eu-should-class-cyber-attacks-as-terrorism-estonia-20070608-h9r.html>.

[29] Ryan Naraine, "SSL Broken! Hackers Create Rogue CA Certificate Using MD5 Collisions," *ZDNet News*, December 30, 2008, available at <http://blogs.zdnet.com/security/?p=2339>.

[30] Eli Jellenc, in Iain Thomson, "Georgia Gets Allies in Russian Cyberwar," VNUNET Information Services, August 12, 2008, available at <www.vnunet.com/vnunet/news/2223776/georgia-gets-allies-russian-cyberwar>.

[31] James R. Langevin, in Shaun Waterman, "U.S. Urged to Go on Offense in Cyberwar," *Washington Times*, September 29, 2008, available at <www.washingtontimes.com/news/2008/sep/29/us-urged-to-go-on-offense-in-cyberwar>.

[32] *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, 2003), 28, available at <www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.>

[33] Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (Autumn 1996), 94, available at <www.carlisle.army.mil/usawc/parameters/96autumn/harknett.htm>.

[34] Gates, 1.

[35] Stewart Brand, "Wired Legend—Founding Father," *Wired Magazine*, March 2001, available at <www.wired.com/wired/archive/9.03/baran.html>.

[36] Harknett, 94.

[37] Peters, 1.

[38] Gilmore Commission, in "Looking Forward to a National Security Strategy," The Metropolitan Corporate Counsel, July 2004, available at <www.metrocorpcounsel.com/current.php?artType=view&artMonth=July&artYear=2004&EntryNo=1258>.

[39] See, for example, Jeffrey T.G. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," *Michigan Law Review* (2008), 1446–1447, available at <www.michiganlawreview.org/archive/106/7/kelsey.pdf>.