MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 37
Issue 5 *Journal of the National Security Forum*

Article 6

2011

Responses to the Ten Questions

Eric Jensen

RESPONSES TO THE TEN QUESTIONS

Eric Jensen†

8. WHAT IS THE NEXT THING PRESIDENT OBAMA SHOULD DO TO PROTECT AMERICAN CYBER SECURITY?

PRESIDENT OBAMA AND THE CHANGING CYBER PARADIGM

Among the most important issues for American national security is the national response to the growing threat from cyber activities. This threat is both ubiquitous and potentially catastrophic. It will force the United States, and the entire world, to reevaluate the way in which nations think of both national security and the concept of armed conflict. To combat this threat, President Obama must refocus America's attention by both reallocating the primary governmental responsibility for cyber security from the Department of Homeland Security (DHS) to the Department of Defense (DOD) and overhauling the public-private partnership that he has made a key component of his cyber strategy.

I. PRESIDENT OBAMA'S CYBER EMPHASIS

Beginning with President Clinton in 1996 and continuing

† Visiting Assistant Professor, Fordham Law School. The author wishes to thank SueAnn Johnson for her exceptional research and editing skills.

through President George W. Bush to President Obama, the executive branch has taken the lead on securing the nation from cyber threats but has focused its efforts mainly on government computers and systems.[1] Shortly after entering office, President Obama embarked on a potentially new and expanded view when he called for a complete review of government cyber policies and practices. The report was published several months later.[2] In response to the findings and recommendations of the report, President Obama stated that,

> From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.[3]

President Obama's expanded vision of what the focus of Governmental concern should be is undoubtedly correct in that it reflects the reality of today's national security threats. But even this vision is mired in a parochial and anachronistic view of the changing world and its impact on national security.

II. A CHANGING THREAT

The nature of the changing cyber threat is clearly demonstrated by recent budget decisions in the United Kingdom. During a time of significantly reduced budgets, the UK government made some difficult decisions on the allocation of defense resources. In a move that would shock most other nations, the United Kingdom opted to forego the production of aircraft capable aircraft carriers and allocate those resources to expanding and

1. *See* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1555-63 (2010).

2. WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

3. President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009) (transcript available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure).

maintaining its cyber defenses.[4]

The significance of this decision cannot be overstated. There are few pieces of military hardware that reflect the force projection power of a nation more effectively than a fully capable aircraft carrier. In a world where nations view other nations as the primary threat to peace, fully capable aircraft carriers are among the top priorities. Parking such a weapon off the coast of some recalcitrant nation is a clear statement of military power. This is particularly true for a country with a history of ocean dominance, such as the UK.

But an aircraft carrier can do nothing to protect a nation from the evolving national security threat of cyberattacks. The United Kingdom's decision to forego the immense power provided by a fully operational aircraft carrier in exchange for increased cyber capability is an astounding statement of their view of future national security threats and the actors who present them. It is no longer states and full scale warfare that the United Kingdom views as its dominant threat, but rather cyberattacks from not only other nations but also from criminal business networks, transnational terrorist organizations, citizen activist groups, flash mobs of like-minded individuals across transnational borders, recreational hackers, and individuals. These same threats exist for all other nation-states, including the United States. For nations and their leaders, including President Obama, this worldwide transition from state-on-state armed conflict to state versus nonstate actors will have a profound effect on national security, the law that governs it, and processes that preserve it. Nowhere is this truer than in the area of

4. In an effort to maintain its force-projection capability, the UK found it necessary to sign a defense pact with France, basically merging their aircraft carrier capabilities where the UK and France would rely on each other's capabilities when their own ship was in refit. *See, e.g.*, Kim Sengupta, Jerome Taylor & Michael Savage, *Threat of Cyber Attack is the New Priority as Cuts Hit Major Projects*, THE INDEPENDENT, Oct. 19, 2010, http://www.independent.co.uk/news/uk/home-news/threat-of-cyber-attack-is-the-new-priority-as-cuts-hit-major-projects-2110273.html. As one commentator put it, "[t]his compromises our operational integrity completely. If we need to send a carrier to protect one of our territories, and ours is in refit, and the French say, 'Well, we don't agree – you're not using ours,' we're not going to be doing much protecting." Daily Mail Reporter, *Britain and France to Share Nuclear Secrets as Cameron and Sarkozy Sign Historic 50-Year Military Agreement*, DAILY MAIL (Nov. 2, 2010, 9:39 PM), http://www.dailymail.co.uk/news/article-1325863/Britain-France-sign-historic-50-year-military-agreement.html#ixzz1ABlMPaPS.

cyber operations.

III. A CHANGING ENEMY

Cyber threats have existed since almost the inception of the Internet. The first "attack" was the inadvertent Morris worm in 1988, written by a Cornell graduate student. Since that initial attack that shut down the embryonic Internet, the World Wide Web has become a rich source for cyber intrusions. U.S. Government computers and networks are constantly being probed.[5] In any twenty-four-hour period, DOD computers access the Internet "roughly seven million times"[6] and "known cyberattacks [against U.S. computers] rose to 37,258 [in 2008] from 4,095 in 2005."[7] Further, in a recent attack targeting "proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries," more than 75,000 computers at over 2,500 businesses in 196 countries were targeted.[8] The pervasive nature of the Internet and the increased capability it provides is accompanied by increased risks to nations and users.

One could argue that these attacks are not national security

5. A recent Center for Strategic and International Studies report stated "the Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities. The unclassified email of the secretary of defense was hacked, and DOD officials told us that the department's computers are probed hundreds of thousands of times each day. A senior official at the Department of State told us the department had lost "terabytes" of information. Homeland Security suffered break-ins in several of its divisions, including the Transportation Security Agency. The Department of Commerce was forced to take the Bureau of Industry and Security off-line for several months, and NASA has had to impose e-mail restrictions before shuttle launches and allegedly has seen designs for new launchers compromised." CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY: A REPORT OF THE CSIS COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY, 12–13 (Dec. 2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

6. Lieutenant Colonel Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DoD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 183 (2009).

7. Siobhan Gorman, *Bush Looks to Beef Up Protection Against Cyberattacks*, WALL ST. J., Jan. 28, 2008, at A8.

8. Ellen Nakashima, *More Than 75,000 Computer Systems Hacked in one of the Largest Cyber Attacks, Security Firm Says*, WASH POST., Feb. 18, 2010, at A03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816_pf.html.

threats involving the armed forces of a nation unless they come from a peer nation-state. Looking to current international law, one could further argue that these are criminal events that should be handled by international criminal law through cooperative investigation, extradition, and prosecution.[9] However, the fatal flaw in this argument was clearly demonstrated by the recent Stuxnet malware.

Though still shrouded in much mystery, the Stuxnet malware appears to be a highly sophisticated, precisely directed malware that has had a significant effect on the emerging Iranian nuclear capability. Because of its sophistication, many have concluded that it was sponsored by a nation that had a reason to try and stop Iran's nuclear program, most likely Israel. However, because of the inherent problems with attribution in the cyber realm, it is still unclear who is responsible for the malware. While many attribute the attack to a nation-state, computer security giant Symantec believes that such a cyber threat could be created by as few as five to ten highly trained computer technicians in as little as six months.[10]

The Stuxnet malware demonstrates the possibility of a debilitating cyberattack coming from any one of a broad range of actors and triggers a new era in cyber conflict. The possibility that six trained computer specialists, funded by some individual, corporation, or organization, might create malware that is highly lethal and capable of such discriminating effect further erodes the idea that only states can initiate armed conflict. It has become clear that national security threats requiring the full focus of the armed forces of a nation no longer come from only nation-states.

---

9. The European Cybercrime Convention establishes a cooperative regime for handling cybercrimes. *See* Convention on Cybercrime, opened for signature Nov. 23, 2001, S. Treaty Doc. No. 108-11, Europ., T.S. No. 185, *available at* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=07/04/2011&CL=ENG. The Convention was adopted at the 109th session of the European Council in November 2001. Though generated by the EU, the Convention is open to both EU and non-EU member states. There are currently twenty-nine EU member states and the US is the only non-EU member. However, there are seventeen other states that have signed but not ratified. *See* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

10. Josh Halliday, *STUXNET Worm is the 'Work of a National Government Agency*,' GUARDIAN, Sept. 24, 2010, http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency.

They now come from a full spectrum of sources, including cyber threats originated by anyone, from an organized transnational terrorist organization, to the highly trained individual hacker who has an axe to grind against some government. A new era of threats is emerging and will force the world to look at national security from a different and expanded perspective.

One of the most obvious changes to our perception of national security threats is the idea of who poses a threat. International law is built on the foundation of state monopolization of violence that emerged in the wake of the Treaty of Westphalia, where states hired armies, navies, and police forces to not only control violence within their borders, but to also carry out violence on behalf of the sovereign without their borders. Under this paradigm, international law granted privileges and duties to the state's sovereign forces who served as agents for the state in conducting and controlling violence.[11] In the modern era of cyber warfare (and other potential threats such as nuclear terrorism), this paradigm's utility is severely diminished.

There is no doubt that cyber threats will continue to come from individuals who meet the formal definition of "combatants" under the law of war. Many nations have already participated in cyber activities that were viewed as a national security threat, and many others nations are trying to develop the capability to do so.[12] However, cyber actions just as threatening have come from non-state groups, either in conjunction with armed conflict or outside of it. Recent large-scale attacks in both Estonia in 2007[13] and

11. Combatants were granted prisoner-of-war status that resulted in treatment guarantees that included immunity for warlike acts that complied with the law of war. *See* Geneva Convention Relative to the Treatment of Prisoners of War, art. 99, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

12. "In 2007, McAfee's annual Virtual Criminology Report concluded that 120 countries had, or were developing, cyber espionage or cyber war capabilities." STEWART BAKER, SHAUN WATERMAN & GEORGE IVANOV, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 5 (2010), *available at* http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war (requires registration). *See also* Ray Walser, *State Sponsors of Terrorism: Time to Add Venezuela to List*, THE HERITAGE FOUNDATION, Jan. 20, 2010, *available at* http://www.heritage.org/research/reports/2010/01/state-sponsors-of-terrorism-time-to-add-venezuela-to-the-list.

13. Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES, May 29, 2007, at 1, *available at* http://www.nytimes.com/2007/05/29/technology/29estonia.html; Anne Applebaum, *For Estonia and NATO, A New Kind of War*, WASH. POST, May 22, 2007,

Georgia in 2008[14] illustrate the effectiveness of private groups with a political agenda.

Clearly, President Obama cannot afford to view national security threats as coming only from those who meet the legal definition of combatants under current international law. Rather, he must expand his view to a more holistic approach and be prepared to respond with national power to threats that come from any source.

IV. A CHANGING TARGET

In addition to expanding views of who may be a national security threat, new considerations as to who or what may be targeted in a cyber attack are also challenging traditional notions of national security. Under the current UN paradigm, any "use of force" is prohibited unless by consent of the target state, under authorization of the UN Security Council, or in self-defense against an armed attack or imminent armed attack. As the Stuxnet malware demonstrates, these aggression-limiting ideals that were created in the age of mechanized warfare have lost their ability to govern activities in the modern cyber era.

When the UN Charter was under discussion, Brazil and others argued that certain economic measures ought also to be proscribed under illegal uses of force. This suggestion was not accepted and "use of force" was narrowly understood as involving armed force. Yet in today's world, surely a cyber operation that destroys confidence in the stock markets of a nation should be seen as a national security threat. In 1998, the United States recognized stock markets and banking systems as critical infrastructure, along

---

at 15, *available at http://www.washingtonpost.com/wp-dyn/content /article/2007/05/21/AR2007052101436.html*; *Estonia: President Ilves's Speech on the Occasion of International Cyber Conflict Legal and Policy Conference in Tallinn*, US STATE NEWS, Sept. 9, 2009, http://www.eesti.ca/?op=article&articleid=25139. The attacks on Estonia prompted NATO to fund and create a new research center designed to boost their cooperative defenses against cyberattacks.

14. Siobhan Gorman, *Georgia States Computers Hit by Cyberattack*, WALL ST. J., Aug. 12, 2008, at 9; James R Asker, *Cyber Zap*, AVIATION WEEK & SPACE TECHNOLOGY, Sept. 7, 2009; Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN (Aug. 18, 2008, 11:47 AM), http://www.cnn.com/2008/TECH /08/18/cyber.warfare/index.html; Lieutenant Commander Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty To Prevent*, 201 MIL L. REV. 1, 4-5 (2009).

with telecommunications, energy, transportation, water systems, and emergency services.[15] These critical national infrastructures are all potentially vulnerable to cyberattacks. Despite this designation, nothing has been done to ensure meaningful security for these critical infrastructures. And the costs of such attacks continue to rise. According to Ty Sagalow, chairman of the Internet Security Alliance board of directors, "[a]n estimated $1 trillion was lost in the United States in 2008 through cyber attacks."[16] This is more than the annual Gross Domestic Product of all but the top sixteen countries in the world.[17] The cost of downtime alone from major attacks to critical national infrastructure "exceeds . . . $6 million per day."[18]

It is untenable to continue to reject the idea that this is a national security threat. The loss of that much wealth each year has profound implications for a nation with a national debt of over $14 trillion. The entire international community, but certainly the United States, must adjust how it views an illegal "use of force," recognize that cyber attacks on economic and other similar targets are a potentially debilitating use of force, and commit itself to protection of these assets.

V. PUBLIC-PRIVATE PARTNERSHIP

One of the key findings and recommendations of the report concerned cooperation between the private and public sector. The report argued:

> The Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources. The common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core

15. WHITE HOUSE, PRESIDENTIAL DECISION DIRECTIVE NSC-63: CRITICAL INFRASTRUCTURE PROTECTION pt. I (1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

16. William Matthews, *Cyber War's 'Front Lines' May Be in Private Hands*, THE AMERICAS, Dec. 7, 2009, at 38.

17. *See* CIA, The World Factbook, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html (based on 2010 estimates) (last visited Mar. 13, 2011).

18. BAKER, WATERMAN & IVANOV, *supra* note 12, at 3.

responsibility of the Federal government.[19]

Identifying the protection of critical infrastructures, including banking and financial systems, from armed attack as a core responsibility of the federal government is a significant realization and should cause some reevaluation of the current approach to cybersecurity. However, in connection with the public-private partnership issue, President Obama stated,

> Let me also be clear about what we will not do. Our pursuit of cybersecurity will not—I repeat, will not include—monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free.[20]

This statement by President Obama seems to assume that "open and free" also means unsecure. That need not be the case; indeed, it cannot be the case. In fact, keeping the Internet "open" is going to be more and more reliant on increased security measures to maintain the functioning of the World Wide Web.

The government's current approach to public-private partnership is very hands off. In fact, even amongst key defense industries, "there are no regulatory requirements for conducting formal risk assessments"[21] and executives of U.S. critical infrastructure reported the "lowest levels" of government regulation across fourteen countries surveyed.[22] It appears that the current public-private partnership means that the private sector does what it wants and the government encourages and suggests security measures but provides no regulation or oversight. Such a system does not currently and will not continue to provide sufficient security in this age of cyber threats.

It may not be necessary for President Obama to go as far as Estonia and organize a Total Defense League of civilian specialists who work in the private sector and come to the aid of the

19. CYBERSPACE POLICY REVIEW, *supra* note 2, at 28.

20. President Barack Obama, *supra* note 3.

21. U.S. DEP'T OF HOMELAND SECURITY & DEP'T OF DEF., DEFENSE INDUSTRIAL BASE: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLANE 14 (May 2007), *available at* http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.

22. BAKER, WATERMAN & IVANOV, *supra* note 12, at 1.

government in times of cyber threat,[23] but certain steps must be taken to strengthen the national security. Since ninety-eight percent of all government communications traverse over civilian networks and systems,[24] the civilian sector is bound up in national security to a degree that cannot be ignored.

President Obama needs to give serious consideration to the current public-private partnership and begin to assert more regulation over security requirements in the private sector, particularly those which support government operability and critical national infrastructure. To accomplish this, the President should ask Congress to legislate standards of cybersecurity common to all of these private sectors with government oversight to ensure the standards are met. Companies willing to abide by the new standards should be free to do so, but for those companies who cannot or do not, the government should have the authority to step in and ensure the security of the networks from cyber threat.

Once the standards are in place, the government should create "red teams" to exercise the security measures of the private sector as they do now to the public sector in order to ensure security is sufficient. The results of these exercises should be made public in a "name-and-shame" effort to help the market drive increased security if government regulation proves less than fully adequate. Such steps are necessary to transform the current public-private partnership from a failed attempt at cooperation into an aggressive pillar of national cybersecurity.

VI. ALLOCATION OF RESPONSIBILITY

One of the other hallmarks of the U.S. Government's current approach to national cyber security is the designation of the DHS as the lead agency to combat cyber threats, with the DOD playing a supporting role. Ignoring obvious problems with DHS's ability to fulfill its responsibilities during the previous administration, President Obama has continued to utilize this approach.

23. Tom Gjelten, *Volunteer Cyber Army Emerges In Estonia*, NATIONAL PUBLIC RADIO (Jan. 4, 2011), *available at* http://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation.

24. Michael McConnell, Former Director on National Intelligence, currently Executive Vice President of Booz Allen Hamilton, Keynote Address at the Conference on Law at the Intersection of National Security, Privacy and Technology (Feb. 4, 2010).

In March of 2009, the Government Accountability Office (GAO) released a report on National Cybersecurity Strategy. The report found that "DHS has yet to fully satisfy its cybersecurity responsibilities designated by the [2003 National Strategy to Secure Cyberspace]."[25] DHS's inability to adequately respond to known vital national security requirements during the past six years demonstrates its similar incapacity to keep pace with the rapidly changing nature of cyber threats. A recent memorandum of agreement was signed between the DHS and the DOD to try and increase coordination and cooperation between the two agencies,[26] but it is simply insufficient. President Obama rightly acknowledged that cybersecurity is a key national security issue, but he has yet to respond appropriately to this acknowledgement by assigning responsibility to the agency with the current capability to handle threats to cybersecurity, the DOD.

As has been previously discussed, the cyber threat is truly a national security issue and though it threatens the homeland, it can originate from anywhere in the world and defies national borders. Assigning the overall responsibility for cybersecurity to DHS is parochial and ineffective. Furthermore, it bifurcates activities and responsibilities in a way that compromises the chance of success. Instead, the DOD ought to be given the lead and allowed to use its current assets such as the National Security Agency, Cyber Command, and other agencies that are already heavily engaged in cyber operations overseas to ensure that the cybersecurity umbrella adequately protects all U.S. assets throughout the world. A recent report from the Quadrennial Defense Review Independent Panel agrees. The report states:

> In addition, more than 80 percent of the Department's logistics are transported by private companies; mission-critical systems are designed, built, and often maintained by our defense industrial base. The majority of our military's requirements are not neatly bounded by the.mil

25. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-432T, NATIONAL CYBERSECURITY STRATEGY: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE 4 (2009), *available at* http://www.gao.gov/new.items/d09432t.pdf.

26. U.S. DEP'T OF HOMELAND SECURITY & DEP'T OF DEF., MEMORANDUM OF AGREEMENT BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY (Sept. 2010), *available at* http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

> (dot mil) domain; they rely on private sector networks and capabilities. *That is why the Panel believes it is vital that the Department of Defense ensure the networks of our private sector partners are secured.*[27]

Additionally, President Obama must ensure that the cyber activities of the DOD and other government agencies are adequately funded, that research is appropriately encouraged, and that the government has aggressive recruiting and pay structures to attract the very best minds in the area of national cyber security. Some of these measures are in their embryonic stages, but more must be done and done more quickly. U.S. Deputy Secretary of Defense William Lynn recently wrote in Foreign Affairs:

> The United States will lose its advantage in cyberspace if that advantage is predicated on simply amassing trained cyber professionals. The U.S. government, therefore, must confront the cyber defense challenge as it confronts other military challenges: with focus not on numbers but on superior technology and productivity.[28]

Assigning the DOD as the single agency responsible for this work and then adequately funding both personnel and research is a vital step in the right direction.

VII. CONCLUSION

The threat from cyberattacks is certainly among the most important issues for American national security. The changing nature of the threat, the enemy, and the targets make this an issue of urgent and enduring importance. President Obama must focus the full attention and powers of the government on this issue to ensure the safety of the nation. Two important steps that will do much to accomplish this task are the overhaul of the current public-private partnership that he has made a key building block of his cyber strategy and the reallocation of the primary governmental responsibility for cyber security from the Department of Homeland Security to the Department of Defense. The United States can

27. QUADRENNIAL DEF. REVIEW INDEP. PANEL, THE QDR IN PERSPECTIVE: MEETING AMERICA'S NATIONAL SECURITY NEEDS IN THE 21ST CENTURY 62 (2010) (emphasis added), *available at* http://www.usip.org/files/qdr/qdrreport.pdf.

28. William J. Lynn, III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF. (Sept./Oct. 2010), *available at* http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

either act now with commitment and foresight, or wait to do so in the aftermath of a potentially catastrophic cyberattack.