The Age of Digital Conflict: A Review Essay

José de Arimatéia da Cruz

Books Reviewed:

War Play: Video Games and the Future of Armed Conflict
By Corey Mead

The New Digital Age: Reshaping the Future of People, Nations and Business
By Eric Schmidt and Jared Cohen

Cybersecurity and Cyberwar: What Everyone Needs to Know
By P.W. Singer and Allan Friedman

According to Eric Schmidt, Executive Chairman of Google, and Jared Cohen, Director of Google Ideas and an Adjunct Senior Fellow at the Council on Foreign Relations, the Internet is among the few things humans have built that they do not truly understand. The Internet is a network of networks, a huge and decentralized web of computer systems designed to transmit information using specific standard protocols. Nations and individuals rely on the Internet on a daily basis to conduct business, connect with friends, and even find love. To state the Internet is an integral part of our way of life is not an overstatement. The Internet allows for friendships, alliances and enmities between states to be extended into the virtual world, adding a new and intriguing dimension to traditional statecraft. As the Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey stated, "the spread of digital technology has not been without consequence. It has also introduced new dangers to our security and our safety."[1]

Three books will be reviewed here which highlight the addition of the Internet to an already complex international system in which combat takes place not only in the physical domain but also now in the cyber domain. The Department of Defense designated cyberspace a new domain of warfare in 2011. This elevation in strategic importance makes cyberspace comparable to land, sea, air, or outer space as a new battle frontier. The US Government and its Armed Forces recognize the importance of cyberspace as a potential future battleground. Former Defense Secretary Leon Panetta stated "cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers."[2] The Chairman of the Joint Chiefs of Staff, General Dempsey, stated "the Department of Defense is adding a new mission: defending the nation, when asked, from attacks of significant consequence—those that threaten life, limb, and the country's core critical infrastructure."[3] For international jihadists the Internet has become the most cost-effective means of delivering its messages worldwide, and coordinating attacks. The Internet allows jihadist organizations to recruit without leaving the confines of their safe havens. Jihadist groups and terrorist organizations are using the Internet as a tool to carry-out their "cyberplanning" without fear of retaliation and in secret. Lieutenant Colonel Timothy L. Thomas, an analyst at the Foreign Military Studies Office in Fort

José de Arimatéia da Cruz Visiting Research Professor at the US Army War College and Professor of International Relations and Comparative Politics at Armstrong State University, Savannah, Georgia

1 Claudette Roulo, "DOD Must Stay Ahead of the Cyber Threat, Dempsey Says," *US Department of Defense*, http://www.defense.gov/news/newsartcle.aspx?id=120379.

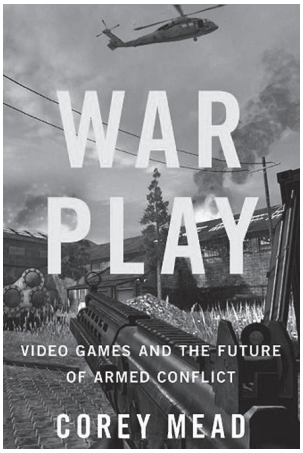
2 Leon Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," October 11, 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

3 Roulo, "DOD Must Stay Ahead of the Cyber Threat, Dempsey Says."

Leavenworth, Kansas, defines "cyberplanning" as "the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed."[4] An understanding of future armed conflict, combat and intervention in the new digital age will help US Army leaders to train its soldiers for new forms of armed conflict in the twenty-first cyberspace in light of sequestration and diminishing defense budget.

War Play: Video Games and the Future of Armed Conflict

How does the US military train its current and future soldiers for new forms of armed conflict in the twenty-first century in light of sequestration and a diminishing defense budget? Corey Mead's book *War Play* that the military is making use of more and more video games, that is, serious video games, as part of its arsenal of tools to fight the wars of the future. The military, according to the author, is turning to video games for scenarios involving new and unexpected roles for soldiers. For example, today's Generation Z soldiers, born in the age of cell phones and information, are using video games to learn skills such as cultural negotiations and cultural sensitive training. As a new generation of soldiers are recruited and deployed, in addition to learning combat skills, they may also have to negotiate with warlords or tribal leaders in remote villages. Also, virtual training sessions are helping the military ration training grounds, which are in especially short supply today as troops return from their overseas deployments (68). According to the author, video games allow for near-instantaneous user modifications, meaning soldiers in the field can, on a daily basis, input the enemy's latest fighting tactics, so that troops who are stateside can keep their training up to date (3).



Corey Mead , *War Play: Video Games and the Future of Armed Conflict* (Eamon Dolan/ Houghton Mifflin Harcourt, 2013). 208 pages. $20.00

The proliferation of video games or computer-based war gaming programs as an integral part of the military's learning tools was recently re-energized by comments from Edward O. Wilson, emeritus professor of biology at Harvard University, and President Barack Obama. Wilson recently remarked, "games are the future of learning," while President Obama stated the creation of good education game software is one of the "grand challenges for American innovation" (5). True to his statement, President Obama created the Advanced Research Projects Agency for Education, which has as its major objective the creation of education software "as compelling as the best video game" (5). The Obama Administration is "pouring hundreds of millions of dollars into its Educate to Innovate campaign, a pro-STEM initiative that, in the president's words, is dedicated to reaffirming and strengthening America's role as the world's engine of scientific discovery and

4 Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of "Cyberplaning," *Parameters* 33, No. 1 (Spring 2003): 112-123.

technological innovation" (157). Two other events have led to the proliferation of video games or computer based war gaming as part of the military's arsenal. First, the end of the Cold War and the implosion of the Soviet Union have led to a reduction of the military's budget to a level commensurate with what Congress assumed was a greatly reduced geopolitical threat (22). Second, in the post-9/11 terrorist attacks against the homeland, former Secretary of Defense Donald Rumsfeld called for a "revolution in military affairs." According to Rumsfeld, the US military needed a "transformation." This transformation held that the US military's high technology combat systems and heavy reliance on air forces had dramatically reduced the need for large numbers of troops on the ground (50). Since wars of the future will shift from ground wars to cyberspace, the military needs a complete transformation, a "wholesale technological upgrade with the goal of changing the military into a lithe, agile, easily portable fighting force that could be instantly deployed to any of the world's future hot spots" (51). During times of across-the-board defense budget cuts and sequestration, cybersecurity is one of the few areas that will see an actual increase in its budget in the years ahead (167).

The use of video games or computer-based war gaming in today's Army as a training tool developed in conjunction with the US Army War College's introduction of the board game *Mech War* into its training curriculum in the 1970s (17). *Mech War* is part logistical, part strategic board game which also uses card drawing mechanics. *Mech War* allows students a chance to lead a team of mechs - enormous robot-like war machines. Using a wide variety of weapons, the goal is to secure a victory against other mechraider leaders. There are a number of other computer-based war games being used by the military today. But, perhaps the most successful computer-based war game is *America's Army*, the world's first video game developed by the military. The game is the idea of Colonel Case Wardynski, who for more than a decade ran the US Army's Office of Economic and Manpower Analysis.

The game was used not only as a basic recruitment tool but also as a public relations instrument. It has been as influential in the world of marketing as it has been in the military (77). The game recognized the Army as a professional organization soldiers would not only respect but want to join. The game emphasized the Army's "seven core values," namely: loyalty, duty, respect, selfless, service, honor, integrity, and personal courage (76). *America's Army* has more than 11 million registered users. The game was re-purposed several years ago for use as a government training tool and its platform is now used for dozens of training and simulation applications, including PackBot robots and nuclear, biological, and chemical reconnaissance vehicles (75). According to the game's official website, *America's Army* brings the best features of the previous versions to a new America's Army environment. *America's Army: Proving Grounds* stress small unit tactical maneuvers and training that echoes true-to-life Army scenarios. It reflects the current Army by focusing on these smaller self-contained, full spectrum units which can carry-out a variety of missions.

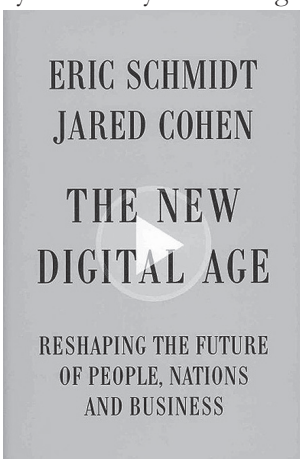
In addition to using video as a learning tool, the military is also extending the use of video games beyond the battlefield. It is using video

games to treat soldiers suffering from post-traumatic stress disorder as well as aiding veterans who are reintegrating into civil society after seeing the horrors of war. The military is not only using video games among its lowest ranks, but its leaders are also trained on video games. According to Mead, at the Army's School for Command Preparation and the Command and General Staff College at Fort Leavenworth, Kansas, lieutenant colonels and other leaders use *UrbanSim*, a game referred to by its creator as *SimCity Baghdad*. *SimCity* focuses on counterinsurgency. During exercises using *SimCity*, students are required to manage a complex mix of civil security and control, governance, and economic and infrastructure development (69).

Another video game being used by the military is *Virtual Battlespace 2*. This game is an army "program of record," meaning it will be maintained by the Army for as many years as possible before being replaced (105). It has been an important tool for due to its capacity to record sessions and follow up with "after-action reviews." This enables leaders to take the soldiers through the scenarios and identify what they did correctly and incorrectly (106). Another important function of this game is its content library, which features "more than four hundred military and civilian vehicles; hundred of characters representing at least five national militaries, press agents, and civilians; dozens of weapons; and countless varieties of animals, signs, buildings, natural objects, and paraphernalia such as alarm clocks and soda cans" (107).

The New Digital Age: Reshaping the Future of People, Nations and Business

Eric Schmidt and Jared Cohen are no strangers to the world of cybersecurity. In their groundbreaking text, the authors demonstrate "ways in which the virtual world can make the physical world better, worse or just different. Sometimes these worlds will constrain each other; sometimes they will clash; sometimes they will intensify, accelerate and exacerbate phenomena in the world so that a difference in degree will become a difference in kind" (6). This technological revolution of the twenty-first century will impact everyone but not equally. As the authors point out, "everyone will benefit from connectivity, but not equally, and how those differences manifest themselves in the daily lives of people" is the focus of their work. Although this technological revolution will not impact everyone equally, it will certainly provide a venue for those without a voice in the political process in many parts of the world.



Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (Knopf Publishing Group, 2013). 336 pages. $18.85

Schmidt and Cohen argue, "technology will empower people to police the police in a plethora of creative ways never before possible, including through real-time monitoring systems allowing citizens to publicly rate every police office in their hometown" (34). Governments as well will find it harder to ignore public protesters either in the physical

world or the online world as their citizens become more connected. Events that once took weeks if not months to be noticed by the world, now can be seen instantaneously as people become more connected and communication costs become more affordable. For example, farmers in Kenya now are able to determine the market price for their commodities and young people are able to organize online, and protest in the physical world. Indeed, it is a "brave new world."As technology becomes more affordable and available to the masses, governments around the world will find it harder to cover-up government malfeasance as corrupt politicians and human-rights abuses are exposed by the media. The Green Revolution, a political movement in Iran contesting the fraudulent election results of 2009 in which Mahmoud Ahmadinejad was reelected is a good example of political activism brought to light thanks to the advancement of technology. Young people armed with cell phones took to the streets to demand the removal of Ahmadinejad. When police and security forces attacked and arrested unarmed protesters, young Iranians armed with cell phones took pictures of police brutality including the killing of Neda Agha Soltan, who became a symbol of the Green Revolution. In countries where the media is not free, the advancement of the Internet represents a danger to corrupt officials, powerful criminals and other malevolent forces in a society. As Schmidt and Cohen point out, "one reason that corrupt officials, powerful criminals and other malevolent forces in a society can continue to operate without fear of prosecution is that they control local information through harassment, bribery, intimidation or violence" (52).

The result of authoritarian societies where the media is controlled by criminal elements in power, especially since the end of the Cold War when state-owned media was privatized, is "a lack of an independent press" reducing both "accountability and the risk that public knowledge of misdeeds will lead to pressure and the political will to prosecute" (52). As corrupt politicians and their cronies continue to manipulate and control the Internet to advance their own interests, we could see the proliferation of a "digital police state" (77).

The new digital age is also transforming the field of international relations. As Schmidt and Cohen argue "friendships, alliances, and enmities between states will extend into the virtual world, adding a new and intriguing dimension to traditional statecraft" (83). As powerful nations around the world, in order to protect their territorial integrity, filter and restrict what can and cannot be seen by their citizens, we are witnessing the "balkanization" of the Internet. This balkanization will have a tremendous impact on the future of nation-states. Again, Schmidt and Cohen argue, "the Internet could ultimately be seen as the realization of the classic international-relations theory of an anarchic, leaderless world" (83).

As the world becomes more connected and relations move from the physical world to the cyber world, this "leaderless world" will also become more dangerous. While the Cold War may have ended with the implosion of the former Soviet Union, a new "Code War" is just beginning. In this new interconnected world of the twenty-first century, "embedded moles, dead letter drops and other tradecraft will be replaced by worms, key-logging software, location-based tracking and other

digital spyware tools" (113). Although some observers argue war in the digital age is not really war from a Clausewitzian's perspective, that is, "a continuation of policy by other means," others argue to the contrary. For example, Craig Mundie, Microsoft's chief research and strategy officer and leading thinker in Internet security, calls cyber-espionage tactics "weapons of mass disruption" (105). Schmidt and Cohen go on to argue,

> "states will do things to each other online that should be too provocative to do off-line, allowing conflicts to play out in the virtual battleground while all else remains calm. The promise of near-airtight anonymity will make cyber attacks an attractive option for countries that don't want to appear overtly aggressive but remain committed to undermining their enemies" (105).

The evolution of the digital age is also changing the traditional definition of war. While guns and bullets are still an integral part of combat, so are bits and bytes. Warfare is not a new concept in strategic analysis. What is different today is nations will use "cyber war primarily to meet intelligence objectives, even if the methods employed are similar to those used by independent actors looking to cause troubles. Stealing trade secrets, accessing classified information, infiltrating government systems, disseminating misinformation—all traditional activities of intelligence agencies—will make up the bulk of cyber attacks between states in the future" (103). As nations around the world recognized the utility of cyber attacks as a form of strategic offense, cyber attacks will occur with greater frequency and more precision with each passing year (104). With the establishment in 2009 of the United States Cyber Command (USCYBERCOM) and former secretary of defense Robert Gates declaring cyberspace to be the "fifth domain" of military operations, alongside land, sea, air and space, there has been a proliferation of a "cyber-industrial complex" (110). The cyber-industry is estimated to be worth somewhere between $80 billion and $150 billion annually (110).

Another important concept with the advancement of the digital age is cyber terrorism. In his remarks to the Business Executives for National Security, New York City, Secretary Panetta warned business leaders, "A cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorist attacks on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation."[5] Panetta also goes on to state, "the collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability." While a "cyber Pearl Harbor" has not yet occurred, rogue nations are either creating or improving their cyber capabilities. For example, as Schmidt and Cohen point out, "most terrorist organizations have already dipped a toe into the media marketing business, and what once seemed farcical—al Qaeda's website heavy with special effects, Somalia's al-Shabaab insurgent group on Twitter—has given way to a strange new reality (157).

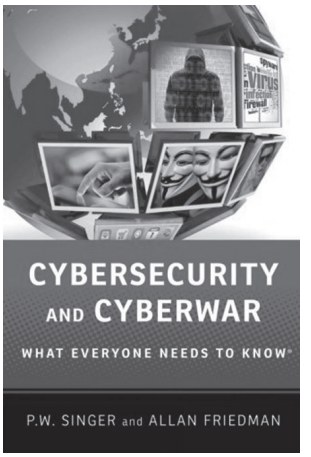
This new reality of the twenty-first century under the digital age calls for nations to practice two foreign policies and two domestic policies—one for the virtual world and one for the physical world—and these policies may appear contradictory (255). In their final analysis,

5 Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City."

Schmidt and Cohen argue, "anyone passionate about economic prosperity, human rights, social justice, education or self-determination should consider how connectivity can help us reach these goals and even move beyond them" (257).

Cybersecurity and Cyberwar: What Everyone Needs to Know®[6]

Written by P.W. Singer, Senior Fellow and the Director of the 21st Century Defense Initiative, and Allan Friedman, Fellow in Governance Studies and Research Director of the Center for Technology Innovation both at the Brookings Institute, *Cybersecurity and Cyberwar: What Everyone Needs to Know®* is an easy-to-read yet deeply informative book on the nature of cybersecurity and cyberwar. Unlike Schmidt and Cohen, Singer and Friedman argue cyberspace may be global but it is not "stateless" or a "global commons" (14). According to Singer and Friedman, cyberspace "is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared" (13). Singer and Friedman also argue cyberspace is not purely virtual as it is commonly sensationalized by media reports. Cyberspace, according to Singer and Friedman, comprises computers storing data plus the systems and infrastructure allowing it to flow. Included in this total package is the Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, and space-based communications (13-14). Regardless of one's operational definition of the Internet and cyberspace, one thing is for certain: cyberspace, as *Wired* magazine editor Ben Hemmersley points out, is "the dominant platform for life in the 21st century" (16).



P.W. Singer, *Cybersecurity and Cyberwar* (Oxford University Press, 2014). 320 pages. $63.36

This book is divided into three parts. Part I answers the important question to latecomers that is, "How It All Works;" Part II answers the question, "Why It Matters;" and finally, Part III "What Can We Do?" In Part I "How It All Works," several important themes are discussed including, but not limited to, what do we mean by security when it comes to the Internet; how do we trust in cyberspace; how do we keep the bad guys out of our critical infrastructure; and who is the weakest link when it comes to cyberspace. Cyberattacks against financial institutions, governmental agencies, individuals, and corporations are on the rise as other nations begin to develop their own cyber soldiers. According to Singer and Friedman, quoting a study prepared by the National Research Council in 2009, a cyberattack occurs when an individual or nation-state take "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (68). Cyberattacks usually take place against a nation's critical infrastructure as well as against Supervisory Control and Data Acquisition (SCADA). A nation's

6 See the review by Major Nathan K. Finney elsewhere in this issue.

critical infrastructure is "the underlying sectors that run our modern-day civilizations, ranging from agriculture and food distribution to banking, health-care, transportation, water, and power" (15). The Supervisory Control and Data Acquisition is "the computers systems that monitor, adjust switching, and control other processes of critical infrastructure" (15). A concern regarding SCADA (besides its vulnerability to cyberattacks) is the fact that between 85 percent and 90 percent of US critical infrastructure is controlled by the private sector. While there have been major improvements in the private sector when it comes to cybersecurity; the default still remains the federal government. Therefore, when a cyberattack occurs, the blame game between the private sector and the federal government begins without anyone taking responsibility and stepping up to protect the US's critical infrastructure.

Singer and Friedman also discuss how criminal elements and organizations are taking advantage of advances in computer capability and capacity to commit crimes that not too long ago were commonly practiced by street thugs. Cybercrime, "the use of digital tools by criminals to steal or otherwise carry out illegal activities," has become a major concern to law enforcement officers worldwide (85). General Keith Alexander, head of the US National Security Agency (NSA) and US Cyber Command, has called cyber economic espionage one of the many nefarious forms of cybercrime being committed today against American corporations and the "biggest transfer of wealth in history," which is estimated to cost US corporations $250 billion in stolen information and another $114 billion in related expenses.[7] Several culprits top the US list of countries actively engaged in cybercrime. According to the *New York Times*, cybertheft has become the "No. 1 problem" between the US and China, especially as the later proclaims its peaceful rise (95). The Cold War may have ended with the collapse of the Soviet Union, but a new Code War is just beginning. In this new Code War, bytes become the "twenty-first century nuclear weapons equivalent," in the words of Secretary of State John Kerry during this confirmation hearing.[8]

Advances in computer technology have also created a new venue for rogue states, transnational organized criminals, and terrorist organizations as they rely on the web to conduct their nefarious activities and cyberterrorism. Lieutenant Colonel Thomas, argues terrorist organizations are using the Internet not only to recruit new foot soldiers but also for cyberplanning. Thomas defines "cyberplanning" as "the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed."[9] In their "cyberplanning," terrorist organizations are also spreading a peculiar type of knowledge called "TTPs," an acronym for "tactics, techniques, and procedures" (1001). Singer and Friedman have also argued, "for terror groups, Internet communication does more than just create new connections and spread viral ideas; it also maintains old ones much in the same way that the rest of us use social networks to keep in touch with high school friends" (1001).

---

7 John D. Negroponte and Samuel J. Palmisano, *Defending an Open, Global, Secure, and Resilient Internet*, Independent Task Force Report No. 70 (New York: Council on Foreign Relations, June 2013), 17.

8 Ibid., 23.

9 Thomas, "Al Qaeda and the Internet: The Danger of "Cyberplaning," 112-123.

The US Armed Forces have also recognized the dual utility of Internet technologies in the new post-Cold War international system and its usefulness as a force multiplier in combat. The US Air Force has developed and implemented a plan for cyberwarfare known as the "Five D's plus One" (128). According to this cyberwarfare strategy, a nation's cyberwarfare capabilities should be able to "destroy, deny, degrade, disrupt, and deceive" while at the same time "defending" against the enemy's use of cyberspace for the very same purpose (128). The US military has also developed Plan X, a $110 million program designed to "help war-planners assemble and launch online strikes in a hurry and make cyber attacks a more routine part of US military operations" (128). Perhaps the greatest recognition that Internet "connection needs to be treated as a potential source of serious danger" came about with the establishment of the US Cyber Command.[10] On June 23, 2009, the Secretary of Defense directed the Commander of US Strategic Command to establish a sub-unified command, United States Cyber Command (USCYBERCOM). Full Operational Capability (FOC) was achieved Oct. 31, 2010. The command is located at Fort Meade, Maryland.[11] The US Cyber Command brings under one umbrella all agencies or organizations of the US military that work on cyber issues such as the Army's Ninth Signal Command to the Navy's Tenth Fleet (133). The US is not the only superpower paying attention to the dual utility of the Internet in the post-Cold War international milieu. Russia and China have also developed their own equivalents of the US Cyber Command in order to match American cyberwarfare capabilities in the eventuality of a cyber conflict. China's Beijing North Computer Center, otherwise also known as the General Staff Department 418 Research Institute or the PLA's 61539 Unit, has at least ten subdivisions involved in "the design and development of computer network defense, attack, and exploitation systems" (141).

According to Ambassador John D. Negroponte and Samuel J. Palmisano, "cyberspace is now an arena for strategic competition among states, and a growing number of actors—state and nonstate—use the Internet for conflict, espionage, and crime."[12] Recent incidents involving Russia and the Republic of Georgia in which Georgia's government websites were bombarded with a Distributed Denial of Service (DDoS) eventually were brought to a stand still show the awesome power of cyberwarfare. Cyberwarfare is indeed a power multiplier. It also shows that, as Colin S. Gray points out, "cyber can only be an enabler of physical effort. Stand-alone (popularly misnamed as "strategic") cyber action is inherently grossly limited by its immateriality."[13] Cyberterrrorists and rogue nation-states have realized the dual utility of the Internet. As Martin C. Libicki points out, "cyberattacks have neither fingerprints nor the smell of gunpowder, and hackers can make an intrusion appear legitimate or as if it came from somewhere else."[14] Given the attribution

10 Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: US Army War College, Strategic Studies Institute, 2013), 49, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1147.

11 "US Cyber Command," *US Strategic Command*, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

12 Negroponte and Palmisano, *Defending an Open, Global, Secure, and Resilient Internet*, 66.

13 Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*, 44.

14 Martin C. Libicki, "Don't Buy the Cyberhype," *Foreign Affairs*, August 14, 2014, http://www.foreignaffairs.com/print/136836.

problem, we could very well see a proliferation of attacks coming from such states as North Korea, Venezuela, Iran, China, and Russia and yet be unable to attribute any of them to those countries. In conclusion, I concur with Colin S. Gray that while the "sky is not falling," military leaders and students are highly recommended to comprehend the nature and utility of this powerful new tool of war.