CYBER WARFARE

BOOKS

HM743 .F33L47 2014 Lee, Newton. *Facebook Nation: Total Information Awareness*. New York: Springer, 2014.

HV6773.2 .B74 2011 Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: Penguin Press, 2011.

Summary: A former top level national Security Agency inside evaluates pressing threats in digital security, revealing how operatives from hostile nations have infiltrated power, banking, and military systems to steal information and sabotage defense mechanisms.

HV6773.2 .C57 2010 Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco, 2010.

Summary: Security expert Richard A Clarke goes beyond the "geek talk" to succinctly explain how cyber weapons work and how vulnerable America is to the new world of the nearly untraceable cyber criminals and spies. This sobering story of technology, government, and military strategy involving criminals, spies, soldiers, and hackers begins the much needed public policy debate about what America's doctrine and strategy should be, not just for waging, but for preventing the First Cyber War.

JF1525 .A8B427 2011 Betz, David. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon; New York: Routledge, for the International Institute for Strategic Studies, 2011.

PS3619 .I572455G48 2015 Singer, P.W. and Andrew Cole. *Ghost Fleet: A Fiction Novel of the Next World War*. Boston: Houghton Mifflin Harcourt, 2015.

Summary: The year is 2026. China has taken over as the world's largest economy, while the United States, mired in an oil shortage, struggles to adjust to its diminished role. Then, a surprise attack throws the U.S. into a chaos unseen since Pearl Harbor. As the enemy takes control, the survival of the nation will depend upon the most unlikely forces: the Navy's antiquated Ghost Fleet and a cadre of homegrown terrorists.

QA76.9 .A25 S562 2014 Singer, P.W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford; New York: Oxford University Press, 2014.

Summary: Our entire modern way of life fundamentally depends on the Internet. The resultant cybersecurity issues challenge literally everyone. Singer and Friedman provide an easy-to-read yet deeply informative book structured around the driving questions of cybersecurity: how it all works, why it all matters, and what we can do.

U163 .C936 2015 Green, James A. (ed.) *Cyber Warfare: A Multidisciplinary Analysis*. Abindgon, Oxon; New York: Routledge, 2015.

Summary: "This book is a multi-disciplinary analysis of cyber warfare, featuring contributions by leading experts from a mixture of academic and professional backgrounds. Cyber warfare, meaning inter-state cyber aggression, is an increasingly important emerging phenomenon in international relations, with state-orchestrated (or apparently state-orchestrated) computer network attacks occurring in Estonia (2007), Georgia (2008) and Iran (2010). This method of waging warfare - given its potential to, for example, make planes fall from the sky or cause nuclear power plants to melt down - has the capacity to be as devastating as any conventional means of conducting armed conflict. Every state in the world now has a cyber-defence programme and over 120 states also have a cyber-attack programme. While the amount of literature on cyber warfare is growing within disciplines, our understanding of the subject has been limited by a lack of cross-disciplinary approaches. In response, this book, drawn from the fields of computer science, military strategy, international law, political science and military ethics, provides a critical overview of cyber warfare for those approaching the topic from whatever angle. Chapters consider the emergence of the phenomena of cyber warfare in international affairs; what cyber-attacks are from a technological standpoint; the extent to which cyber-attacks can be attributed to state actors; the strategic value and danger posed by cyber conflict; the legal regulation of cyber-attacks as part of an on-going armed conflict and the ethical implications of cyber warfare. This book will be of great interest to students of cyber war**,** cyber security, military ethics, international law, security studies and IR in general"-- Provided by publisher.

U163 .H37 2014 Harris, Shane. *@War: The Rise of the Military-Internet Complex*. Boston: Houghton Mifflin Harcourt, 2014.

Summary: The United States military now views cyberspace as the "fifth domain" of warfare, alongside land, air, sea, and space. The Pentagon, the National Security Agency, and the CIA field teams of hackers who launch cyber strikes against enemy targets--and amass staggering quantities of personal information on all of us. These same virtual warriors, along with a growing band of private-sector counterparts, are charged with defending us against the vast array of criminals, terrorists, and foreign governments who attack us with ever-increasing frequency and effectiveness. Journalist Shane Harris infiltrates the frontlines of this fifth domain, explaining how and why government agencies are joining with tech giants like Google and Microsoft to collect huge amounts of information and launch private cyber wars. The military has also formed a new alliance with tech and finance companies to patrol cyberspace, and Harris offers a penetrating and unnerving view of this partnership. Finally, he details the welter of opportunities and threats that the mushrooming "military-Internet complex" poses for our personal freedoms, our economic security, and the future of our nation.--From publisher description.

U163 .S73 2010 Stiennon, Richard. *Surviving Cyberwar.* Lanham, MD: Government Institutes, 2010.

Summary: Military and intelligence leaders agree that the next major war is not likely to be fought on the battleground but in cyber space. The author argues the era of cyber warfare has already begun. Recent cyber attacks on the United States government departments and the Pentagon corroborate this claim. China has compromised e-mail servers at the German Chancellery, Whitehall, and the Pentagon. In August 2008, Russia launched a cyber attack against Georgia that was commensurate with their invasion of South Ossetia. This was the first time that modern cyber attacks were used in conjunction with a physical attack. Every day, thousands of attempts are made to hack into America’s critical infrastructure. These attacks, if successful, could have devastating consequences. IN this book, the author introduces cyberwar, outlines an effective defense against cyber threats, and explains how to prepare for future attacks. He also examines the cyber threats and where they come from, explains how defensive technologies can be used to counter cyber attacks and to secure American infrastructure, considers the major recent cyber attacks that have taken place around the world, discusses the

implications of such attacks, and offers solutions to the vulnerabilities that made these attacks possible. The book begins with Shawn Carpenter and his discovery that China had hacked into his work place, Sandia Labs. It follows the rise of cyber espionage on the part of the Chinese People's Liberation Army (PLA) as increasingly sophisticated and overt attacks are carried out against the government and military networks around the world. It moves from cyber espionage to cyberwar itself, revealing the rise of distributed denial of service (DDoS) as a means of attacking servers, websites, and countries. It provides a historical perspective on technology and warfare is provided, drawing on lessons learned from Sun Tsu to Lawrence of Arabia to Winston Churchill, and finishes by considering how major democracies are preparing for cyberwar and predicts ways that a new era of cyber conflict is going to impact the Internet, privacy, and the way the world works. This text is a stimulating and information look at one of the gravest threats to Homeland Security today, offering new insights to technologies on the front lines, helping policy makers understand the challenges they face, and providing guidance for every organization to help reduce exposure to cyber threats.

UA23 .J35 2014 Jarmon, Jack. *The New Era in U.S. National Security: An Introduction to Emerging Threats and Challenges*. Lanham, MD: Rowman & Littlefield, 2014.

Summary: Part I: the establishment and the national security environment -- The national security establishment -- Policies and processes in the new geopolitics -- Industrial age warfare and information age weapons -- The new arena of conflict and economic competition -- Part II: current, emerging, and impending threats and challenges -- The maritime supply chain: vast, diverse, and anarchic -- The gatekeeper's challenge -- The cyber war: new battlefronts, old and new enemies -- Cyber guerilla war -- Terrorism versus crime -- Building a global network -- Chemical biological radiological and nuclear: the chemical threat -- Chemical biological radiological and nuclear: the biological threat -- Chemical biological radiological and nuclear: the radiological nuclear threat -- Part III: policy implications and the public private partnership -- Industrial policy and defense policy.

UG450 .S45 2009 Singer, P.W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Press, 2009.

Summary: A military expert reveals how science fiction is fast becoming reality on the battlefield, changing not just how wars are fought, but also the politics, economic laws, and ethics that surround war itself.

UG593 .Z48 2014 Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Crown Publishers, 2014.

Summary: "Top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran's nuclear efforts and shows how its existence has ushered in a new age of warfare-- one in which a digital attack can have the same destructive capability as a megaton bomb. In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at an Iranian uranium enrichment plant were failing at an unprecedented rate. The cause was a complete mystery-- apparently as much to the technicians replacing the centrifuges as to the inspectors observing them. Then, five months later, a seemingly unrelated event occurred; a computer security firm in Belarus was called in to troubleshoot some computers in Iran that were crashing and rebooting repeatedly. At first, the firm's programmers believed the malicious code on the machines was a simple, routine piece of malware. But as they and other experts around the world investigated, they discovered a mysterious virus of unparalleled complexity. They had, they soon learned, stumbled upon the world's first digital weapon. For Stuxnet, as

it came to be known, was unlike any other virus or worm built before; rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak actual, physical destruction on a nuclear facility. In these pages, Wired journalist Kim Zetter draws on her extensive sources and expertise to tell the story behind Stuxnet's planning, execution, and discovery, covering its genesis in the corridors of Bush's White House and its unleashing on systems in Iran--and telling the spectacular, unlikely tale of the security geeks who managed to unravel a sabotage campaign years in the making. But Countdown to Zero Day ranges far beyond Stuxnet itself. Here, Zetter shows us how digital warfare developed in the US. She takes us inside today's flourishing zero-day "grey markets," in which intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks. She reveals just how vulnerable many of our own critical systems are to Stuxnet-like strikes, from nation-state adversaries and anonymous hackers alike-- and shows us just what might happen should our infrastructure be targeted by such an attack. Propelled by Zetter's unique knowledge and access, and filled with eye-opening explanations of the technologies involved, Countdown to Zero Day is a comprehensive and prescient portrait of a world at the edge of a new kind of war. "-- Provided by publisher.

AUDIOBOOKS/EBOOKS

Andress, Jason and Steve Winterfield. *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*. Waltham, MA: Syngress, an imprint of Elsevier, 2014. Donovan E-Collections.

Summary: This book explores the battlefields, participants, and tools and techniques used during today's digital conflicts. The concepts discussed provide those involved in information security at all levels a better idea of how cyber conflicts are carried out now, how they will change in the future and how to detect and defend against espionage, hacktivism, insider threats and non-state actors like organized criminals and terrorists.

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to do About It*. HarperCollins e-Books, 2014. Donovan E-Collections.

Summary: Richard A. Clarke warned America once before about the havoc terrorism would wreak on our national security, and he was right. Now he warms us of another threat, silent but equally dangerous. Cyber War is a powerful book about technology, government, and military strategy; about criminals, spies, soldiers, and hackers. It explains clearly and convincingly what cyber war is, how cyber weapons work, and how vulnerable we are as a nation and as individuals to the vast and looming web of cyber criminals. This is the first book about the war of the future ‘cyber war’ and a convincing argument that we may already be in peril of losing it.

Leonhard, Robert. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 2013. Donovan E-Collections.

Summary: One of the most cogent and respected strategic theorists **in** today's military sounds the alarm: We have no viable doctrine for tomorrow's war. The advent of the information age renders the hallowed Principles of War useless. Forged in agrarian times and honed by the more modern conflicts **of** the industrial age**,** the principles that have guided generations of America's military leaders have become dangerously outmoded. In this, his latest book, Lt. Col. Robert R. Leonhard, author of the influential Art of Maneuver and Fighting by Minutes, proposes a new set **of** principles, indeed a new approach to armed conflict.

Singer, P.W. *Ghost Fleet: A Fiction Novel of the Next World War*. Boston: Houghton Mifflin Harcourt, 2015. Available in both E-book and Audiobook. For summary, see listing in the "Books" section.

Winterfield, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Lanham, MD: Rowman & Littlefield, 2014. Donovan E-Collections.

Summary: Part I: the establishment and the national security environment -- The national security establishment -- Policies and processes in the new geopolitics -- Industrial age warfare and information age weapons -- The new arena of conflict and economic competition -- Part II: current, emerging, and impending threats and challenges -- The maritime supply chain: vast, diverse, and anarchic -- The gatekeeper's challenge -- The cyber war: new battlefronts, old and new enemies -- Cyber guerilla war -- Terrorism versus crime -- Building a global network -- Chemical biological radiological and nuclear: the chemical threat -- Chemical biological radiological and nuclear: the biological threat -- Chemical biological radiological and nuclear: the radiological nuclear threat -- Part III: policy implications and the public private partnership -- Industrial policy and defense policy.

ELECTRONIC SOURCES

Bonner III, E. Lincoln. "Cyber Power in 21st-Century Joint Warfare." JFQ: Joint Force Quarterly, Issue 74, 3rd Quarter 2014. *National Defense University Press*.
http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577536/jfq-74-cyber-power-in-21st-century-joint-warfare.aspx

Abstract: Incorporating cyber power into conventional military operations is relatively unexplored, with most attention going to cyberspace's espionage and coercive potential, yet it is critical to joint warfare. In particular, military cyberspace operations should aim to achieve and hold cyberspace dominance including the ability to cyber interdict to assist with kinetic actions, with an emphasis on air operations. Another focus should be to defeat adversary cyber-attacks and surveillance and then to suppress enemy cyber defense measures. Interdiction should concentrate on tactical data links and on data fusion centers, which are described here as the cyber version of a railroad marshaling yard. Cyberspace dominance and cyber interdiction will push enemies to make mistakes and give our joint warriors a decision-making advantage.

Case Western. "Talking Foreign Policy: A Discussion on Cyber Warfare." Case Western Reserve Journal of International Law, Vol. 47, pp. 319-342, Spring 2015. *Ebscohost*.

Abstract: Talking Foreign Policy is a production of Case Western Reserve University and is produced in partnership with 90.3 FM WCPN ideastream, Cleveland's NPR affiliate. Produced quarterly, the program is hosted by Case Western Reserve University School of Law Interim Dean Michael Scharf, and focuses on the most relevant foreign policy issues of the day.1 2 The January 30, 2014 broadcast covered the constantly evolving field of cyber warfare, and featured the following guests: ·Peter Singer, Director of the Center for 21st Century Security and Intelligence, Brookings Institution; · Michael Newton, Professor of Law, Vanderbilt University; · Milena Sterio, Associate Professor of Law, Cleveland-Marshall College of Law; and ·Shannon French, Professor of Philosophy and Director of the Inamori Center for Ethics and Excellence, Case Western Reserve University ·Archived broadcasts of Talking Foreign Policy in both audio and video format are available at http:// law.case.edu/ Talkin Foreign Policy.

Dev, Priyanka R. "'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response." Texas International Law Journal, Vol. 50, Issue 2, pp. 379-399, 2015. *Ebscohost*. q

Abstract: The article reports on the challenges faced by the international law over cyber warfare and discusses the role of technological innovation in increasing the dangers of cyber actions. Topics discussed include efficiency of application of existing laws of war in context to the information security, the Iranian hackers of distributed denial of service (DDoS) attacks, and need of reform in traditional law of armed conflict (LOAC) principles in context to cyber actions.

Eidman, Christopher R. and Gregory Scott Green. "Unconventional Cyber Warfare: Cyber Opportunities in Unconventional Wafare." Student Masters Thesis. Monterey, CA: Naval Postgraduate School, June 2014.
http://calhoun.nps.edu/bitstream/handle/10945/42615/14Jun_Eidman_Green.pdf?sequence=1&isAllowed=y

Grohe, Edwin. "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict." The Johns Hopkins University Applied Physics Laboratory: National Security Perspective, 15 April 2015. *Defense Technical Information Center*. http://www.dtic.mil/docs/citations/ADA620195

Abstract: This Perspective describes cyber operations known to have been used during the Syrian civil war from January 2011 until December 2013. The cyber operations of pro-regime forces, anti-regime forces, and nations providing support, as well as US involvement and its effects on these cyber operations, are discussed as a basis for drawing observations and implications for future conflicts.

Kovačević, Božo. "Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World." Politicka Misao: Croatian Political Science Review, Vol. 51 Issue 3, pp. 169-175, 2014. *Ebscohost.*
AN: 99629567

Libicki, Martin C. "Crisis and Escalation in Cyberspace." Prepared for the US Air Force by Rand Project Air Force. Santa Monica, CA: RAND, 2012. http://www.rand.org/pubs/monographs/MG1215.html

Summary: "The chances are growing that the United States will find itself in a crisis in cyberspace, with the escalation of tensions associated with a major cyber attack, suspicions that one has taken place, or fears that it might do so soon. The genesis for this work was the broader issue of how the Air Force should integrate kinetic and nonkinetic operations. Central to this process was careful consideration of how escalation options and risks should be treated, which, in turn, demanded a broader consideration across the entire crisis-management spectrum. Such crises can be managed by taking steps to reduce the incentives for other states to step into crisis, by controlling the narrative, understanding the

stability parameters of the crises, and trying to manage escalation if conflicts arise from crises."--P. [4] of cover.

Magee, Clifford S. “Awaiting Cyber 9/11.” JFQ: Joint Force Quarterly, Issue 70, pp. 76-82, 2013. *EbscoHost: Military & Government Collection*.
AN: 92600954

Abstract: The article discusses the emergence of the cyber warfare which targets the national security, economy, and infrastructure in the U.S. It highlights the efforts of the Department of Defense in detecting, preventing and recovering from cyber attacks. It emphasizes the need for the U.S. to undergo a paradigm shift towards monitoring cyber domain and cites the importance of developing an organization with the capabilities or authorities to monitor cyber

Mahon, Tim. “Cyber – The 21st Century Threat.” Military Technology: Vol. 39, Issue 5, pp. 202-3, 2015. *Ebscohost*.
AN: 102963135

Abstract: The article discusses the issue of cyber threats or cyber-crime faced by governments and military forces. Topics include attack on the Canadian government websites in 2011 which forced Canadian economic agencies to disconnect from the Internet for a period; several **cyber** defence policies by the intergovernmental military alliance North Atlantic Treaty Organization (NATO); and several training facilities of NATO which support the evolution of a robust defence against cyber-warfare.

Martinsen, Thor. And Phillip E. Pace and Edward L. Fisher. “Maneuver Warfare in the Electromagnetic Battlefield.” Journal of Electronic Defense, Vol. 37, Issue 10, pp. 30-44, October 2014. *Ebscohost: Academic Search Elite*.
AN: 98885136

Abstract: Information about the Association of Old Crows 50th Annual International Symposium and Convention that was held in Washington (D.C.) in October 2014 is presented. Topics include the use of electromagnetic spectrum (EMS) in the U.S. Navy as well as the importance of EMS and cyber warfare. The symposium featured Jonathan Greenert, Chief of the Naval Operations (CNO) of the U.S. Navy.

Mulford, Laurie A. “Let Slip the Dogs of (Cyber) War: Progressing Towards A Warfighting US Cyber Command.” Norfolk, VA: Joint Advanced Warfighting School: Joint Staff Forces College – NDU, January 4 2013. *Defense Technical Information Center*. https://apps.dtic.mil/sti/citations/ADA587698

Abstract: Since late 2009, most offensive cyber capabilities have been unavailable to the Joint Force Commander. Outside of the boundaries of a theater of war, offensive cyber activities are limited to those in response to Presidential direction only. This limitation is a result of competing interests within the U.S. Government for control of cyberspace as an operational domain. The competition is currently being played out through an artificial legal debate over authorities and terminology.

To remove some of the subjectivity associated with the debate over cyberspace control, the author first engages in a plain language review of Congressional oversight pertaining to covert actions versus military special operations. Given the current attempts to apply this construct to cyberspace, what follows is analysis and explanation of why this approach is inappropriate for cyberspace as a domain of war. Finally, the author provides recommendations to enable a fully functional U.S. Cyber Command through executive policy, legislation, and extensive education and training for the Department of Defense

workforce on cyberspace. In doing so, offensive cyber capabilities will once again be available for incorporation within campaign and contingency plans in support of the assigned mission.

Osman, Nazan. "What are the Rules in Cyber Warfare?" SC Magazine: For IT Security Professionals, pp 14-17, Sept/Oct 2014. *Ebscohost: Academic Search Elite*.
AN: 97912729

Abstract: The article offers information on the Cooperative Cyber Defence Centre of Excellence (CCDCOE) which was established by the North Atlantic Treaty Organization (NATO) as a result of the cyber attack on Estonia, and the Tallinn Manual which ascertains international law on cyber warfare. Topics discussed include the moral issues of the acceptability of cyber war, the two main categories of the use of force in international law, and the Principle of Proportionality.

Parker, Kevin L. "The Utility of Cyberpower." Military Review: Vol. 92, Issue 3, pp. 26-33, May/Jun 2014. *Ebscohost: Academic Search Elite*.
AN: 95901062

Abstract: The article looks at U.S. national security and military policy as of 2014, focusing on the domain of cyberspace. It discusses aspects of the Internet that distinguish cyber warfare from other forms of warfare, looking at both offensive and defensive strategies. Topics include the lag in policy development regarding technological innovations such as cyberspace and the anonymity and nonlethal character of offensive cyber attacks.

Poirier, William J. and James Lotspeich. "Air Force Cyber Warfare." Air & Space Power Journal, Vol. 27, Issue 5, pp. 73-97, Sept/Oct 2013. *Ebscohost*.
AN: 90333740

Abstract: The article discusses the cyber warfare in the U.S. Air Force which can be used as a national instrument for military power. It states that the capability of Air Force in the cyberspace exists on a continuum which ranges from nascent to responsive support of combatant commanders. It mentions that warfare in cyberspace remains underdeveloped for a combat environment. It adds that commanders will understand how to best utilize the cyber forces through effective development of weapon systems.

Roeder, D. Bruce. "CyberSecurity." Military Review: Vol. 92, Issue 3, pp. 38-42, May/Jun 2014. *Ebscohost*.
AN: 95901064

Abstract: The article looks at cybersecurity as an element of U.S. national security as of 2014. The author emphasizes that given the nature and seriousness of cyber-crime and cyber warfare, Internet security must be viewed as a core responsibility of the U.S. government and the U.S. military, not a marginal one to be delegated to technology personnel. Topics include the U.S. Cyber Command (USCYBERCOM), cooperation between businesses and government on cybersecurity, and common characteristics of hackers.

Schmitt, Michael N. "The Law of Cyber Targeting." Naval War College Review: Vol. 68, Issue 2, Spring 2015. *Ebscohost*.
AN: 101161512

Abstract: The article discusses the laws of cyber targeting. Information on the use of cyber warfare in the war between Georgia and Russia in 2008, the technological abilities of the United States

Army, and the development of wars is presented. Also included is information on the NATO Cooperative Cyber Defense Centre of Excellence.

Williamson, Mark L. LTC, USAF, "The Cyber Military Revolution and the Need for a New Framework of War." Student Master's Thesis. Norfolk, VA: Joint Advanced Warfighting School: Joint Forces Staff College, April 16, 2012. *Defense Technical Information Center*.
https://apps.dtic.mil/sti/citations/ADA562392

Abstract: Because of the cyber military revolution, warfare is no longer adequately defined as violent campaigns and battles sought among armed fighting forces occurring between periods of peace. War is now a continuous battle between diverse multi-faceted actors waged primarily in the virtual cyber domain, occasionally accompanied by violent clashes in the physical domain. When changes to warfare are this fundamental, it requires a new framework of war to guide strategy, doctrine development, and military operations at all levels of warfare. This thesis uses case studies and analysis to demonstrate why the current framework of war, based upon a theory of warfare described in Carl Von Clausewitz' classical work On War, leaves a conceptual gap that does not fully address the challenges of warfare in the cyber age. To address this conceptual gap, the thesis recommends a revised framework of war that uses Colonel John Boyd's philosophy of war and his Observe-Orient-Decide-Act loop as the foundational core elements.

Wilson, J.R. "Cyber Warfare Ushers in 5th Dimension of Human Conflict." Military & Aerospace Electronics, Vol. 25, Issue 12, pp. 8-15, December 2014. *Ebscohost: Military & Government Collection*.
AN: 100040050

Abstract: The article reports on the formation of the U.S. **Cyber** Command (CYBERCOM) of the U.S. Air Force in May 2010. Topics discussed include the significant role of CYBERCOM in ensuring the computer security for military systems, the challenges on mitigating cyberintrusion and hacking in the U.S., and the proposed regulations related to cybersecurity in the U.S. Congress.

VERTICAL FILE
For additional printed sources, check the vertical file at MCoE HQ Donovan Research Library. Ask circulation desk for assistance.

Contact Virtual Reference Desk for assistance at:
usarmy.benning.mcoe.mbx.donovan-ref-desk@army.mil