

Electromagnetic Spectrum: A Selected Bibliography



DTIC-TR- 2022-01

Distribution Statement A

Authorized for public release. Distribution is unlimited.

Introduction: New challenges have emerged as the competition across the electromagnetic continuum becomes increasingly congested, contested, and complex. The DoD uses the spectrum for a host of day-to-day military operations; consequently, assured access and understanding of the electromagnetic spectrum are critical because of its spectrum dependent technologies. Mission effectiveness and

spectrum efficiency requires an understanding of the spectrum and how it can use, manipulate, or develop technologies for current and emerging DoD operations.

How this selected bibliography is organized:

This selected bibliography was created using Distribution A technical reports that are currently stored in the Defense Technical Information Center's repository. The summaries are arranged in descending order by topic areas associated to the Department of Defense's usage of the electromagnetic spectrum.

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> <i>OMB No. 0704-0188</i>		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 02-01-2022		2. REPORT TYPE Technical Report		3. DATES COVERED (From - To) 2000-01-01 – 2021-06-01	
4. TITLE AND SUBTITLE Selected bibliography: Electromagnetic Spectrum			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Penn, Angela D.			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Technical Information Center, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6218			8. PERFORMING ORGANIZATION REPORT DTIC-TR- 2022-01		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6218			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION / AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This is a selected bibliography on the topic of electromagnetic spectrum. The abstracts included focus on the DOD spectrum strategies and policies, spectrum management, electromagnetic spectrum operations and electromagnetic spectrum domains.					
15. SUBJECT TERMS: Aviation, C5I (Command, Control, Communications, Computers, Cyber, & Intelligence), Environment & Waterways (EW), IT & Networks (ITNET), Surface					
16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT U2	18. NUMBER OF PAGES 27	19a. NAME OF RESPONSIBLE PERSON: Angela D. Penn
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (include area code) (571) 448-9674

Contents

Introduction	5
Background Information	6
Overview of Department of Defense Use of the Electromagnetic Spectrum.....	6
Electromagnetic Defense Task Force (EDTF) 2.0	6
21st Century Military Operations in a Complex Electromagnetic Environment.....	7
Joint Spectrum Vision 2010.....	8
Strategies and Policies	8
Department of Defense Electromagnetic Spectrum Superiority Strategy	8
Electromagnetic Spectrum Strategy	9
Policy and Procedures for Management and Use of the Electromagnetic Spectrum. DoD Instruction .	10
Department of Defense Net-Centric Spectrum Management Strategy	10
Electromagnetic Spectrum Management	11
DoD's Broad Vision for Electromagnetic Battle Management.....	11
Marine Corps Spectrum Management	11
Joint Electromagnetic Spectrum Management Operations	12
Filter Technology for Spectrum Management.....	12
Spectrum Management and Electromagnetic Environmental Effects (E3) Business Process	13
Optimal Spectrum Planning and Management with Coalition Joint Spectrum Management Planning Tool (CJSMPT)	13
Spectrum Management in the Acquisition of Equipment	14
Spectrum 101: An Introduction to Spectrum Management.....	14
Electromagnetic Spectrum Operations.....	15
Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority	15
Afloat Electromagnetic Spectrum Operations Program (AESOP) Spectrum Management Challenges for the 21st Century	16
A Determination of the Risk of Intentional and Unintentional Electromagnetic Radiation Emitters Degrading Installed Components in Closed Electromagnetic Environments	16
Communication	17
Electromagnetic Sensing with Low-Cost Software Defined Radio.....	17
Radio Frequency Photonics: Enabler of Electromagnetic Spectrum Dominance	17
Cognitive Radio Cloud Networks: Assured Access in The Future Electromagnetic Operating Environment.....	18

Testing of Policy-Based Dynamic Spectrum Access Radios	18
Electronic Warfare	19
Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack.....	19
Defense Primer: Electronic Warfare	19
Electronic Warfare and Signals Intelligence; South China Sea Military Capability Series: A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea.....	20
CHINA: EMP THREAT: The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack.....	20
Biologically Derived Magnetite Nanoparticles (mNPs) for Use in Electromagnetic Pulse Shielding	21
Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum	22
Simulation of Electromagnetic-Environment Susceptibility to Jamming Systems	22
Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight.....	23
Electronic Warfare in Operations	24
Cyberspace	24
Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance	24
EW and Cyber Convergence: Beyond Information Warfare	25
Warfare in the Electromagnetic Spectrum and Cyberspace: United States Air Force Cyber/Electromagnetic Warfare Command Construct.....	25
Cyber Electromagnetic Activities within the Mission Command Warfighting Function: Why is it Important and What is the Capability?	26
Index	27

Introduction

Military forces are organized around multiple domains; the Electromagnetic Spectrum (EMS) provides the critical connectivity that enables all other domains, but it can also be a serious vulnerability within military operations. To enable equipment and applications across the electromagnetic spectrum, military services must be able to continue to access the spectrum, identify spectrum sharing frequencies, and develop technologies that continue to support day to day and military operations.

How this selected bibliography is organized:

This selected bibliography was created by using Technical Reports in the Defense Technical Information Center's repository and Congressional Research Service Reports. The summaries are arranged by the subject within the electromagnetic spectrum operational environment field and are arranged in descending order by date.

Background Information

Overview of Department of Defense Use of the Electromagnetic Spectrum		
Accession Number:	Report Date:	Access Restrictions:
AD1115153	2020-10-08	A - Approved for Public Release. Public Release: 2245-04-24. Other requests shall be referred to: Congressional Research Service, Washington, DC, 20000
Author:	Hoehm, John R., Gallagher, Jill C., Saylor, Kelley M.	
Corporate Author:	Congressional Research Service	
Descriptors:	5G wireless, fighter aircraft, directed energy weapons, data links, military applications, wireless communications, warfare, electromagnetic radiation, national security, information systems, millimeter waves, United States government, congress, detection, unmanned aerial systems, unmanned aerial vehicles, bandwidth, frequency bands, mobile phones, radio frequency	
Identifiers:	Electromagnetic spectrum	
<p>Communication using the electromagnetic spectrum (the spectrum) enables a number of modern military capabilities. The Department of Defense (DOD) uses electromagnetic radiation to enable military communications, navigation, radar, nonintrusive inspection of aircraft, and other equipment. DOD also heavily relies on electromagnetic radiation for intelligence, surveillance, and reconnaissance (ISR) applications such as missile early warning and signals intelligence. Individual branches of the military (e.g., the Air Force, Army, Marine Corps, Navy and Space Force) currently are allotted significant ranges of frequency bands to enable various equipment and applications that support military operations.</p>		

Electromagnetic Defense Task Force (EDTF) 2.0		
Accession Number:	Report Date:	Access Restrictions:
AD1122475	2019-08-01	A - Approved for Public Release. Public Release: 2052-06-26. Other requests shall be referred to: Air University Press, Maxwell AFB, AL ,36112
Author:	Stuckenberg, David, Woolsey, R. J., DeMaio, Douglas	
Corporate Author:	Air University Press	
Descriptors:	warfare, 5g wireless networks, health services, medical personnel, national security, unmanned aerial vehicles, aircrafts, department of homeland security, employment, national politics, students, united states strategic command, data links, management personnel, public policy, business administration, information systems, personnel management, doctrine, military force levels	
Identifiers:	lemay papers, Joint Chiefs of Staff, edtf (Electromagnetic Defense Task Force), quantum communications, ecct (Enterprise Capability Collaboration Team), emp (Electromagnetic Pulses), EMS-degraded environments, ems (electromagnetic spectrum), ttx (tabletop exercises), gmd (geomagnetic disturbance), Joint Force	

In 2018, the Electromagnetic Defense Task Force (EDTF) was created to undertake an audacious effort to holistically understand challenges and opportunities facing militaries and societies in an age increasingly dominated by the electromagnetic spectrum (EMS), a broad area of activity characterized by the visible and invisible movement of light and energy. The task force was a triage response to an enterprise-wide knowledge deficiency about the criticality of issues confronting the United States and its allies as every aspect of modern society becomes increasingly reliant on the EMS. As the journey began, the principals assembled a coalition of experts (fellows) like no other, including a broad and diverse range of representatives from every possible agency, including federal, military, industry, and academia. The effort also required a unique approach to addressing complex and even seemingly unsolvable challenges. To accomplish this, fellows took part in almost 5,000 hours of war-gaming and tabletop exercises (TTX) to develop a more comprehensive understanding of the central issues within the community. The EDTF ecosystem now comprises more than 360 distinguished fellows, many of whom have invested the greater part of their careers solving and understanding the intricacies of the EMS. Covering EMS management and 5G to electromagnetic pulse (EMP) and space weather to quantum and lasers to directed energy and beyond, the task force’s primary purpose is to digest and disseminate EMS knowledge of a critical nature to the defense community. Thus, in 2018, the EDTF published four key findings.

21st Century Military Operations in a Complex Electromagnetic Environment		
Accession Number:	Report Date:	Access Restrictions:
AD1001629	2015-07-01	A - Approved for Public Release.
Author:	Not Available	
Corporate Author:	Defense Science Board Washington	
Descriptors:	Electronic warfare, military operations, military forces (United States), military capabilities, risk, threats, countermeasures, Department of Defense	
Identifiers:	DOD (Department of Defense), United States Forces, DSB (defense science board)	
<p>High-end electronics technology that was once available only to defense system developers in a few large countries is today available worldwide and can be utilized by both large and small actors for electronic warfare (EW) capabilities. To address this situation, the Defense Science Board performed a year-long investigation of the ability to conduct U.S. military operations in a complex and congested electromagnetic environment. The study examined four operational support capabilities common to most military mission areas tactical communications; satellite communications; positioning, navigation and timing (PNT); and intelligence, surveillance and reconnaissance (ISR). Three representative mission areas were also examined tactical air combat, fleet defense, and ground warfare. Without exception, the ability to perform required functions and conduct required operations was seriously lacking in all seven areas in all but relatively benign EMS environments. Modern U.S. military operations base much of their success on the information dominance these abilities provide. Today, many countries, both near peers and regional powers, have the potential to limit the ability of U.S. systems to sense, communicate, network, and synchronize operations. The study recommends several actions intended to mitigate the most critical deficiencies and vulnerabilities within the seven specific areas investigated.</p>		

Joint Spectrum Vision 2010		
Accession Number:	Report Date:	Access Restrictions:
ADA373289	2000-01-01	Distribution Statement A. Approved for public release. Distribution is unlimited.
Author:	Not Available	
Corporate Author:	Assistant Secretary of Defense (Command Control Communications and Intelligence) Washington, DC	
Descriptors:	command control communications, electromagnetic spectra, information warfare, department of defense, military doctrine, interoperability, joint military activities, military applications, technology assessment	
Identifiers:	C4ISR (Command Control Communications Computers Intelligence Surveillance and Reconnaissance)	
<p>Joint Spectrum Vision 2010 (JSV 2010) outlines the conceptual framework for how the Department of Defense (DoD) will assure the availability of and access to sufficient electromagnetic spectrum for the United States (US) Armed Forces to achieve new levels of effectiveness in joint warfighting, as prescribed in Joint Vision 2010 (JV 2010). The implementation of JSV 2010 will involve the Office of the Secretary of Defense (OSD) staff, the Commanders in Chief (CINCs), Services, Defense Agencies, and Joint organizations, as well as the tactical frequency managers on the operational front; collectively, these compose the Joint Spectrum Management Team. JSV 2010 provides a coherent view of the mid-term and long-term spectrum implications of realizing JV 2010 and addresses how the Joint Spectrum Management Team is structured to carry out the actions necessary to provide assured, sufficient electromagnetic spectrum access to the US Armed Forces of the 21st century, enabling them to achieve Full Spectrum Dominance in warfighting. JV 2010 addresses the changes being implemented to bring US Armed Forces into the 21st century. It describes the improved command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities that must be available to US Armed Forces in the Information Age. JV 2010 presents four operational concepts for achieving Information Superiority: Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimensional Protection. Each of these operational concepts relies heavily on the leveraging of Information Age technological advances so that US Joint Forces may achieve the level of Information Superiority needed to ensure dominance over potential opponents across the full range of military operations. JV 2010 also illustrates that the continued, timely insertion of advanced technologies into weapons systems is a key enabler of Full Spectrum Dominance.</p>		

Strategies and Policies

Department of Defense Electromagnetic Spectrum Superiority Strategy		
Accession Number:	Report Date:	Access Restrictions:
AD1113597	2020-10-01	Distribution Statement A. Public Release: 2820-04-09. Other requests shall be referred to: Department of Defense, Washington, DC 20301
Author:	Not Available	
Corporate Author:	Department of Defense	

Descriptors:	National security, electromagnetic radiation, electronic warfare, warfare, artificial intelligence, Air Force, frequency bands, military operations, systems engineering, united states, department of defense, doctrine, electromagnetic interference, electromagnetic spectra, engineering, training, acquisition, agreements, battle management, commerce
Identifiers:	Not Available
<p>The purpose of the 2020 Department of Defense EMS Superiority Strategy is to align DoD EMS activities with the objectives of the 2017 National Security Strategy (NSS), the 2018 National Defense Strategy (NDS), and national economic and technology policy goals. This Strategy embraces the enterprise approach required to ensure EMS superiority by integrating efforts to enhance near-term and long-term EMS capabilities, activities, and operations. The Strategy informs the Department's domestic EMS access policies and reinforces the need to develop cooperative frameworks with other EMS stakeholders in order to advance shared national policy goals. The traditional functions of Electromagnetic Spectrum Management (EMSM) and Electromagnetic Warfare (EW)--integrated as Electromagnetic Spectrum Operations (EMSO)--are addressed within the document's strategic goals. This 2020 Strategy builds upon the successes of and supersedes both the DoDs 2013 EMS Strategy and 2017 EW Strategy.</p>	

Electromagnetic Spectrum Strategy		
Accession Number:	Report Date:	Access Restrictions:
AD1091174	2013-01-01	A - Approved for Public Release.
Author:	Not Available	
Corporate Author:	Deputy Secretary of Defense, Washington DC, United States	
Descriptors:	operational readiness, availability, combat readiness, technology, tactical intelligence, cybersecurity, digital information, warfare, management planning and control, crisis management, detection, communication systems, situational awareness, wireless networks, rapid deployment, Regulatory Reform	
Identifiers:	ems (Electromagnetic spectrum), efficient, flexible, adaptable, agile, commercial service capabilities	
<p>Electromagnetic spectrum (EMS) access is a prerequisite for modern military operations. DoDs growing requirements to gather, analyze, and share information rapidly; to control an increasing number of automated Intelligence, Surveillance, and Reconnaissance (ISR) assets; to command geographically dispersed and mobile forces to gain access into denied areas; and to train as we fight requires that DoD maintain sufficient spectrum access. Additionally, adversaries are aggressively developing and fielding electronic attack (EA) and cyberspace technologies that significantly reduce the ability of DoD to access the spectrum and conduct military operations. Concurrently, the global wireless broadband industry's demand for spectrum is driven by consumer demand for greater mobility and better data access. These competing requirements for finite spectrum resources have changed the spectrum landscape, nationally and internationally, for the foreseeable future. Going forward, our national leaders will be challenged to make decisions that balance national security with economic interests.</p>		

Policy and Procedures for Management and Use of the Electromagnetic Spectrum. DoD Instruction		
Accession Number:	Report Date:	Access Restrictions:
ADA520441	2009-01-09	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Not Available	
Corporate Author:	Department of Defense, Washington DC	
Descriptors:	electromagnetic spectra, Department of Defense, policies, national security, management, combat readiness, efficiency, military capabilities, military research, allocations, international, military planning, spectrum analysis, negotiations, economic analysis, military operations, combat effectiveness	
Identifiers:	spectrum policy, spectrum management, economic security, sd (spectrum dependent)	
<p>POLICY. It is DoD policy that: a. The electromagnetic spectrum (hereafter referred to as "spectrum") is a critical resource, and access to the spectrum is vital to the support of military operations. Proper management and use of the spectrum available to the Department of Defense shall be an integral part of military planning, research, development, testing, and operations involving spectrum-dependent (S-D) systems. b. Spectrum policy and spectrum management functions shall be guided by the following core principles: (1) Ensure the U.S. warfighter has sufficient spectrum access to support military capabilities. (2) Support a U.S. spectrum policy that balances national and economic security, with national security as the first priority. (3) Use the spectrum as efficiently and effectively as practical to provide the greatest overall benefit to warfighting capability. (4) Pursue spectrum-efficient technologies to support the increasing warfighter demand for spectrum access and encourage development of S-D systems that can operate in diverse electromagnetic environments (EMEs). (5) Actively support U.S. policies and interests in international spectrum bodies and in international and bilateral negotiations for spectrum allocation and use.</p>		

Department of Defense Net-Centric Spectrum Management Strategy		
Accession Number:	Report Date:	Access Restrictions:
ADA454462	2006-08-03	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Grimes, John G.	
Corporate Author:	Assistant Secretary of Defense (Networks and Information Integration) Arlington VA	
Descriptors:	department of defense, resource management, radiofrequency, interoperability, electromagnetic spectra, bandwidth, computer networks, communications networks	
Identifiers:	spectrum management, net centric environment, connectivity, net centric warfare	
<p>The purpose of this document is to better manage the Department's Radio Frequency Spectrum, a finite resource, which is essential in accomplishing the Department's warfighting mission. Pursuant to the President's Management Initiative and the Department of Defense's Transformation, the Spectrum Management (SM) Strategy will improve the management of this vital resource now and in the future. The Department is taking an integrated approach to developing the transformation to net-centricity. This approach incorporates network and communications enhancements to provide</p>		

sufficient bandwidth and electromagnetic spectrum for the warfighter and the Department's operations. The net-centric environment is the framework of spectrum users' technical connectivity and interoperability for Department users and mission partners. Spectrum-dependent systems, such as radios, radars, satellites, unmanned aerial vehicles (UAVs), the Global Positioning System (GPS), and electronic warfare (EW), are required for all aspects of net-centric warfare. One of the goals of net-centric spectrum transformation-empowering users through access to trusted information shared in a trusted environment-has driven the development of this SM strategy.

Electromagnetic Spectrum Management

DoD's Broad Vision for Electromagnetic Battle Management		
Accession Number:	Report Date:	Access Restrictions:
AD1119479	2019-09-01	A - Approved for Public Release. Approved for public release 2052-07-27. Other requests shall be referred to: Office of the Under Secretary of Defense for Acquisition and Sustainment, Washington, DC, 20301
Author:	Conley, William G., Stine, John A., Landrum, Lance K., Miller, Adam	
Corporate Author:	The MITRE Corporation	
Descriptors:	situational awareness, warfare, department of defense, battle management, electronic warfare, military operations, radar, acquisition, computer network security, data links, electromagnetic environments, electromagnetic radiation, electromagnetic spectra, environment, maneuvers, national security, networks, radio communications, signal processing, spectra	
Identifiers:	EW ExCom (Electronic Warfare Executive Committee), embm (Electromagnetic Battle Management), emso (EMS Operations), ems (Electromagnetic Spectrum)	
<p>Through a two-year study funded by the Office of the Under Secretary of Defense for Acquisition and Sustainment and performed by MITRE in support of the EW EXCOM, we have identified visionary keys of how EMBM is a broader concept. DoD will build an EMBM tool to assist the Joint Force Commander in planning and understanding EMSO. To achieve the dynamic spectrum operations called out as an objective in the 2015 Defense Science Board study "21st Century Operations in a Complex Electromagnetic Environment" it must be designed to enable the overall concept. This article describes the vision that the DoD has for this broad concept of EMBM.</p>		

Marine Corps Spectrum Management		
Accession Number:	Report Date:	Access Restrictions:
ADA567237	2012-07-24	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	DeLeon, Arthur	
Corporate Author:	Command Control Communications and Computers (C4) Directorate, Headquarters Marine Corps Washington, DC	

Descriptors:	electromagnetic spectra, management, Marine Corps, efficiency, electromagnetism, guidance, Marine Corps personnel, organizations, policies, spectra, training
Identifiers:	Briefing charts
Spectrum Planning Section: Mission. Establish Marine Corps policy, provide oversight, guidance and procedures relating to the proper and efficient management of the electromagnetic spectrum. Provide Marine Corps representation (at the policy level) to various national, DoD, Joint, and DON organizations, working groups and forums. Provide administrative, technical and operational support to the Operating Forces (OPFOR) and Supporting Establishment (SE) in support of Marine Corps electromagnetic spectrum operational requirements.	

Joint Electromagnetic Spectrum Management Operations		
Accession Number:	Report Date:	Access Restrictions:
ADA565050	2012-03-20	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Not Available	
Corporate Author:	Joint Chiefs of Staff, Washington DC	
Descriptors:	electromagnetic spectra, military doctrine, agreements, electromagnetic environments, electromagnetic interference, electromagnetic radiation, electronic warfare, humanitarian assistance, intelligence, joint military activities, management, planning, policies	
Identifiers:	coordination, disaster relief, electromagnetic effects, electromagnetic spectrum, frequency management, JEMSMO (Joint Electromagnetic Spectrum Management Operations), JEMSO (Joint Electromagnetic Spectrum Operations), multinational operations, network operations, spectrum interference resolution, spectrum management	
<p>Military operations are complicated by increasingly complex demands on the electromagnetic spectrum (EMS). All modern forces depend on the EMS. The EMS is a physical medium through which joint forces conduct operations. The importance of the EMS and its relationship to the operational capabilities is the key focus of joint electromagnetic spectrum management operations (JEMSMO). The EMS is a highly regulated and saturated natural resource. The EMS includes the full range of all possible frequencies of electromagnetic radiation. Joint electromagnetic spectrum operations (JEMSO) include all activities in military operations to successfully plan and execute joint or multinational operations in order to control the electromagnetic operational environment (EMOE). JEMSO is comprised of electronic warfare (EW) and JEMSMO and aims to exploit, attack, protect, and manage resources within the EMOE and resolve electromagnetic interference (EMI) in order to achieve the commander's objectives. JEMSMO is planning, coordinating, and managing joint use of the EMS through operational, engineering, and administrative procedures. The primary goal of JEMSMO is to enable EMS-dependent capabilities and systems to perform their functions in the intended environment without causing or suffering unacceptable interference.</p>		

Filter Technology for Spectrum Management		
Accession Number:	Report Date:	Access Restrictions:

ADA532945	2010-07-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Jachowski, Douglas R., Guyette, Andrew C.	
Corporate Author:	Naval Research Lab, Washington DC, Electronics Science and Technology DIV	
Descriptors:	naval research laboratories, spectra, multiplexing, notch filters, tuning devices, bandstop filters, waveguide filters, symposia, bandpass filters	
Identifiers:	fixed frequency filters, multiplexers	
Some recent developments in filter technology at the Naval Research Laboratory will be described and the application of these technologies to spectrum management will be discussed.		

Spectrum Management and Electromagnetic Environmental Effects (E3) Business Process		
Accession Number:	Report Date:	Access Restrictions:
ADA519549	2010-05-06	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Tabor, Chuck	
Corporate Author:	Fleet Electronic Warfare Center, Norfolk VA	
Descriptors:	radiation effects, management, spectra, electromagnetic environments, spectrum analysis, electronic equipment, communication equipment, policies, fuels	
Identifiers:	SPECTRUM MANAGEMENT, E3(ELECTROMAGNETIC ENVIRONMENTAL EFFECTS), BRIEFING CHARTS	
OPNAVINST 2400.20F: Electromagnetic Environmental Effects (E3) and Spectrum Supportability Policy and Procedures (Jul 2007). (1) PURPOSE: To establish Navy policy and procedures and assign responsibilities for Electromagnetic Environmental Effects (E3) and Spectrum Supportability (SS). (3) Scope and Applicability: (a) This instruction establishes Navy policy and assigns responsibilities for achieving SS and ensuring reliable, safe, and mission capable operations of all Electrical and Communications-Electronics (C-E) equipment, systems and subsystems, devices, ordnance, and fuels within their intended operational Electromagnetic Environment (EME), including effects on personnel.		

Optimal Spectrum Planning and Management with Coalition Joint Spectrum Management Planning Tool (CJSMPT)		
Accession Number:	Report Date:	Access Restrictions:
ADA501955	2008-11-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Poe, Randy, Shaw, Raymond, Zebrowitz, Harris, Kline, William, Heisey, William, Loso, Frank, Levy, Yoram	
Corporate Author:	Lockheed Martin Advanced Technology Labs Cherry Hill NJ	
Descriptors:	electromagnetic spectra, spectrum analysis, optimization, planning, information systems, software tools, interoperability, joint military activities, management, lessons learned, symposia, integrated systems, task forces	
Identifiers:	integrated spectrum operations	

The Coalition Joint Spectrum Management Planning Tool (CJSMPT) has been designated as Spiral I of the Global Electromagnetic Spectrum Information System (GEMSIS) program, which is intended to provide next-generation capabilities for integrated spectrum operations across the entire Department of Defense, in addition to interoperability with federal, state, and local government spectrum agencies and coalition forces. This paper describes the use of CJSMPT in automating key spectrum management planning processes including Joint Task Force (JTF) requirements generation and spectrum interference mitigation. This paper will also review additional CJSMPT capabilities, its architecture, and the current development effort.

Spectrum Management in the Acquisition of Equipment		
Accession Number:	Report Date:	Access Restrictions:
ADA463845	2005-06-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Lewingdon, A., Douglas, J., Howland, P.	
Corporate Author:	Defence Science and Technology Lab Malvern (United Kingdom)	
Descriptors:	military equipment, electromagnetic spectra, frequency allocation, military requirements, United Kingdom, cost benefit analysis, decision making, congestion, acquisition	
Identifiers:	spectrum management, foreign reports	
<p>Military spectrum management is becoming increasingly challenging as many civil and military users compete for scarce resources. This paper identifies and illustrates the problem by example. It then describes some novel methods in requirements and benefits analysis, to inform equipment acquisition decision-makers on the delivery of spectrally efficient solutions to provide a coherent approach to UK spectrum management. The application of the methods is reported and a proposed solution to raise awareness within the wider community is described.</p>		

Spectrum 101: An Introduction to Spectrum Management		
Accession Number:	Report Date:	Access Restrictions:
ADA458175	2004-03-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Stine, John A., Portugal, David L.	
Corporate Author:	MITRE Corp, McLean VA, Washington, C31 Div.	
Descriptors:	Department of Defense, management planning and control, access, bandwidth, wireless links, radiofrequency, allocations, military forces (United States), regulations, transformations, radio transmission, telecommunication, resource management, history, availability, competition	
Identifiers:	spectrum access, spectrum availability, spectrum management, NCW (Network Centric Warfare), radio communications, ITU (International Telecommunication Union), NTIA (National Telecommunications and Information Administration), FCC (Federal Communications Commission)	
<p>In the past, the availability of spectrum was a minor issue for the Department of Defense (DoD), as there was ample spectrum access to meet its needs. However, today, new technologies, the needs of other users, and the proliferation of wireless technologies worldwide have made maintaining even</p>		

current spectrum allocations difficult. New, exciting wireless communication products are creating a large demand for spectrum. Wireless subscriber services are growing rapidly worldwide. Emerging countries are choosing to deploy wireless infrastructure in lieu of wired infrastructure since it costs less. All of these factors make a more competitive environment for worldwide spectrum access. As the recent operations in Afghanistan and Iraq can attest, the DoD achieves much of its military capability from exploiting technology, especially information technology. Military capability is dependent on spectrum availability and the current military transformation will make it more dependent in the future. Unless the DoD manages spectrum smartly it will forfeit its potential capability. This paper has been written to provide an introduction to Spectrum Management with a DoD perspective. It assumes an audience that is unfamiliar with radio communications theory, with the current allocation and use of spectrum, and with the processes involved in managing spectrum. It begins by providing an introduction to basic concepts in radio communications theory to build the novice's intuition so that he/she might subsequently understand the rationale for the current allocations and the methods for managing spectrum. It attempts to give a historical record of how these processes and allocations came to be. It describes the current spectrum management process to include the major players and the procedures they use to make decisions. Finally, it gives a brief introduction to some new technologies that are being introduced and their ramifications on the spectrum management process.

Electromagnetic Spectrum Operations

Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority		
Accession Number:	Report Date:	Access Restrictions:
AD1146306	2020-12-01	A - Approved for Public Release. Public Release: 2053-10-28. Other requests shall be referred to: Government Accountability Office, Washington, DC, 20548,
Author:	Kirschbaum, Joseph W., Baril, Tommy, Spence, Jennifer, Dunn, Haley, Jacobs, Matthew, Matuzsan, Gabrielle	
Corporate Author:	Government Accountability Office	
Descriptors:	CIO (chief information officer), EMSO CFT (electromagnetic spectrum operations cross-functional team), DOD (Department of Defense), ems (electromagnetic spectrum), EMSO (Electromagnetic Spectrum Operations), EW (electromagnetic warfare)	
Identifiers:	Not Available	
<p>According to DOD, the EMS is essential for facilitating control in operational environments and impacts operations in the air, land, sea, space, and cyber domains. The pervasiveness of the EMS across warfighting domains means that maintaining or achieving EMS superiority against an adversary is critical to battlefield success. House Report 116-120 that accompanied a bill for the National Defense Authorization Act for Fiscal Year 2020 included a provision that GAO assess DOD's EMS strategy. This report (1) describes reported threats from peer adversaries; (2) outlines challenges to DOD's superiority in the EMS; and (3) evaluates the extent to which DOD has implemented EMS-related strategies and is positioned to achieve future goals. GAO analyzed 43 EMS studies identified through a literature review, reviewed DOD documentation, and interviewed DOD officials and subject matter experts.</p>		

Afloat Electromagnetic Spectrum Operations Program (AESOP) Spectrum Management Challenges for the 21st Century		
Accession Number:	Report Date:	Access Restrictions:
ADA519589	2010-03-03	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Neel, Margaret	
Corporate Author:	Naval Surface Warfare Center Dahlgren Div.	
Descriptors:	electromagnetic environments, electromagnetic spectra, management, spectrum analysis, policies, military doctrine, interoperability, communication equipment, planning, radar equipment, strike warfare, symposia, military requirements, software tools, frequency, emission	
Identifiers:	AESOP (Afloat Electromagnetic Spectrum Operations Program), EME (electromagnetic environment), briefing charts	
<p>AESOP is the US Navy tool for Strike Group Radar and Communications Planning for coordinating spectrum interoperability in afloat operations worldwide. AESOP uses previously allocated frequencies to generate optimal Radar Plans and OPTASK COMMs that adhere to laws and numbered fleets' emission policies. AESOP integrates and de-conflicts the spectrum requirements of all acquired systems in the global operational electromagnetic environment (EME).</p>		

A Determination of the Risk of Intentional and Unintentional Electromagnetic Radiation Emitters Degrading Installed Components in Closed Electromagnetic Environments		
Accession Number:	Report Date:	Access Restrictions:
ADA632391	2015-06-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Johnson, Jared A.	
Corporate Author:	Naval Postgraduate School, Monterey CA	
Descriptors:	electromagnetic interference, emitters, wireless communications, communication and radio systems, degradation, determination, electromagnetic environments, electromagnetic spectra, probability distribution functions, radiotelephones, risk analysis, sensitivity, systems engineering, theses	
Identifiers:	Not Available	
<p>This report proposes a method of risk determination that incorporates a loss function and a probability function in order to better enable decision makers in determining the risk of implementing wireless technologies in reverberant enclosed spaces that contain sensitive installed components. There is a constant desire to include new technology into the systems being designed to operate onboard U.S. Naval vessels. One of these technologies is wireless communications. This technology relies on the use of the electromagnetic spectrum in order to transfer information from one point to another. This type of information transfer can be advantageous in various applications. Exposing sensitive electronic components to a time-varying electromagnetic field increases the risk of an electronic upset in those components that will degrade the functionality of installed systems. This risk determination should provide a way to weigh the risk of introducing wireless technologies in enclosed spaces. This risk determination relies on the assumption that at some point there will be enough data</p>		

collected to properly determine the overall risk to at-risk equipment. Until that occurs, incorporating new methods of shielding and low power technologies is recommended.

Communication

Electromagnetic Sensing with Low-Cost Software Defined Radio		
Accession Number:	Report Date:	Access Restrictions:
AD1151052	2021-06-01	A - Approved for Public Release.
Author:	Liles, Kenneth H.	
Corporate Author:	Naval Postgraduate School	
Descriptors:	computer programming, mobile phones, detectors, operating systems, sensor networks, computer programs, information science, computers, digital signal processing, signal processing, software defined radio, united states, radio equipment, shell scripts, electromagnetic spectra, cost benefit analysis, cost effectiveness	
Identifiers:	Not Available	
<p>Sensing electromagnetic emissions for offensive and defensive purposes is becoming increasingly important, and software defined radios (SDRs) provide a wide range of electromagnetic spectrum (EMS) sensing capability. This thesis examines the applicability and effectiveness of commercial-off-the-shelf (COTS) technology for electromagnetic sensing and analysis by producing an SDR sensor network prototype. A high-level cost-effectiveness model is developed to produce insights for decision makers regarding the employment of this type of technology. Testing and experimentation suggest that SDRs may be employed as accurate EM sensors with continued research and prototype refinement.</p>		

Radio Frequency Photonics: Enabler of Electromagnetic Spectrum Dominance		
Accession Number:	Report Date:	Access Restrictions:
AD1107501	2020-04-16	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Salvador, John A	
Corporate Author:	Air Command and Staff Coll Maxwell AFB, AL	
Descriptors:	electronic warfare, frequency bands, bandwidth, photonic integrated circuits, electromagnetic spectra, department of defense, phased arrays, microwave photonics, electronic components	
Identifiers:	Not Available	
<p>The world operates in a continuum of electromagnetic radiation energy of alternating electric and magnetic fields of various wavelengths traveling at 3×10^8 m/s. This continuum of light is referred to as the electromagnetic spectrum (EMS). For the military, the EMS is one of the most critical operational domains in modern warfare.⁴ Many parts of the spectrum remain underutilized or entirely unused due to physical limitations in electronic circuits.⁵ Expanding the use of EMS is not a new idea. The Department of Defense (DoD) identified in its 2013 Electromagnetic Spectrum Strategy, all joint functions including movement and maneuver, weapon engagements (fires), command and control, intelligence, protection, sustainment, and information are enabled by spectrum-dependent</p>		

system (SDS) capabilities.⁶ The path of SDS capabilities is growing exponentially and subsequently compounds the pace of EMS technological advancement. It is imperative for the US and its national security to remain the leader in EMS superiority.

Cognitive Radio Cloud Networks: Assured Access in The Future Electromagnetic Operating Environment

Accession Number:	Report Date:	Access Restrictions:
AD1031392	2017-04-04	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Jones, Lawrence O.	
Corporate Author:	Air Command and Staff College, Air University Maxwell Air	
Descriptors:	denial of service attack, cognitive radio, mobile devices, wireless networks, cloud computing, electromagnetic spectra, wireless communications, command and control systems, load monitoring, broadband, communication networks, internet, information assurance	
Identifiers:	cognitive radio cloud networks	

The electromagnetic spectrum is a finite resource that is critical to the United States military's ability to gain superiority in the other five warfighting domains. The Department of Defense's electromagnetic strategy is spectrum access when and where needed to achieve mission success. The future electromagnetic operating environment, however, will find gaining assured access increasingly difficult due not only to adversaries actively contesting it, but due to the congestion attributed to the exponential growth in commercial and civilian access. Despite these signs, the United States Federal Government and the Department of Defense continue to cling to a century old model for managing the electromagnetic spectrum a revolution is in order.

Testing of Policy-Based Dynamic Spectrum Access Radios

Accession Number:	Report Date:	Access Restrictions:
ADA535691	2010-01-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Boksiner, Jeffrey, Chang, Kauteng, Costello, Paul, Huck, Richard, Leising, Tim, Zankel, Michael, Posherstnik, Yuriy, Totaro, Mike, Mai, Trang, Molnar, Joseph	
Corporate Author:	Army Communications Electronic Research and Development ENG Ctr Fort Monmouth NJ Intelligence And Information Warfare Directorate	
Descriptors:	policies, spectrum analysis, radio equipment, networks, electromagnetic environments, test methods, interference, electromagnetic spectra, symposia, department of defense, simulation, fragmentation	
Identifiers:	cognitive radio, dsa (dynamic spectrum access), pbr (policy-based radio), test plan, framework	

Policy-driven Dynamic Spectrum Access (DSA) systems are emerging as one of the key technologies to enable the Department of Defense (DoD) to meet its increasing requirements for access to the electromagnetic spectrum. A key open issue surrounding deployment and continuing development of DSA systems concerns (1) the need to test and evaluate the performance of DSA in avoiding interference to itself and assigned incumbent users and (2) the performance of DSA network in the presence of various types of potential interference. In this paper we describe test framework and

concepts to characterize performance of DSA-enabled policy-based radios. Our test framework includes tests to characterize the inherent interference-avoidance characteristics of DSA, such as the time to abandon a channel, as well as tests that address performance implications of a particular DSA policy. The test framework also provides for the ability to inject a relevant electromagnetic environment (EME). The proposed framework is flexible allowing for customization of the relevant test conditions, such as the EME and facilitates simulation of typical communications events such as network formation and fragmentation.

Electronic Warfare

Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack

Accession Number:	Report Date:	Access Restrictions:
AD1124730	2021-01-28	A - Approved for Public Release.
Author:	Pry, Peter V	
Corporate Author:	DHS	
Descriptors:	nuclear weapons, cyberattacks, directed energy weapons, warfare, air force, civil defense, employment, military organizations, aircrafts, command and control systems, cyberwarfare, national security, nuclear warheads, ballistic missiles, cyber threats, electronic warfare, military exercises, cybersecurity, electromagnetic pulses, radio frequency	
Identifiers:	hEMP (high-altitude electromagnetic pulse)	

The United States and NATO allies regularly experience from Russia major cyber-attacks penetrating government agencies and critical infrastructures for electric power, telecommunications, transportation, and other sectors vital to electronic civilization. These events practice a new way of warfare, including EMP attacks, that could blackout North America and NATO Europe, and win World War III at the speed of light. Any nuclear weapon detonated in outer space, 30 kilometers or higher, will generate a high-altitude electromagnetic pulse (HEMP) damaging all kinds of electronics, blacking-out electric grids and collapsing other life-sustaining critical infrastructures. No blast, thermal, fallout or effects other than HEMP are experienced in the atmosphere and on the ground. Russian military doctrine, because HEMP attacks electronics, categorizes nuclear HEMP attack as a dimension of Information Warfare, Electronic Warfare and Cyber Warfare, which are modes of warfare operating within the electromagnetic spectrum.

Defense Primer: Electronic Warfare

Accession Number:	Report Date:	Access Restrictions:
AD1114210	2020-10-29	A - Approved for Public Release. Public Release: 2820-04-09. Other requests shall be referred to: Library of Congress, Congressional Research Service, Washington, DC,20540,
Author:	Hoehn, John R.	
Corporate Author:	Library of Congress, Congressional Research Service	

Descriptors:	congress, electronic warfare, military operations, department of defense, warfare, electromagnetic radiation, electromagnetic spectra, radar, air force, reconnaissance satellites, united states government, artificial satellites, improvised explosive devices, national security, marine corps, space based, spectra, united states, airborne, aircrafts
Identifiers:	Not Available
<p>Electronic warfare (EW), as defined by the Department of Defense (DOD), are military activities that use electromagnetic energy to control the electromagnetic spectrum (the spectrum) and attack an enemy. The spectrum is a range of frequencies for electromagnetic energy. EW supports command and control (C2) by allowing military commanders access to the spectrum to communicate with forces, while preventing potential adversaries from accessing the spectrum to develop an operational picture and communicate with their forces. Some have argued that EW is a component of anti-access/area denial (A2/AD) campaigns.</p>	

<p>Electronic Warfare and Signals Intelligence; South China Sea Military Capability Series: A Survey of Technologies and Capabilities on China's Military Outposts in the South China Sea</p>		
Accession Number:	Report Date:	Access Restrictions:
AD1128255	2020-08-06	A - Approved for Public Release. Public release: 2190-05-21. Other requests shall be referred to: Department of the Navy, Office of Naval Intelligence, Washington, DC, 20395
Author:	Dahm, J. M.	
Corporate Author:	Johns Hopkins University - Applied Physics	
Descriptors:	aircrafts, unmanned aerial vehicles, signals intelligence, military training, satellite imaging, artificial satellites, jamming, training, warfare, electromagnetic spectra, electronic countermeasures, electronic warfare, unmanned systems, vehicles, guidance, satellite communications, south china sea, spectra, direction finding, intelligence collection	
Identifiers:	PLA (Peoples Liberation Army), milcap (military capability), ew (electronic warfare), SCS (South China Sea), Spratly, islands	
<p>This military capability (MILCAP) study focuses on electronic warfare (EW) and signals intelligence capabilities on seven Chinese island-reef outposts in the South China Sea (SCS). These SCS MILCAP studies provide a survey of military technologies and systems on Chinese claimed island-reefs in the Spratly Islands, approximately 1,300 kilometers (700 nautical miles) south of Hong Kong (see Figure 1). These Chinese outposts have become significant Peoples Liberation Army (PLA) bases that will enhance future Chinese military operations in the SCS, an area where Beijing has disputed territorial claims (see Appendix B). The SCS MILCAP series highlights a PLA informational zed warfare strategy to gain and maintain information control in a military conflict.</p>		

<p>CHINA: EMP THREAT: The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack</p>		
Accession Number:	Report Date:	Access Restrictions:

AD1102202	2020-06-10	A - Approved for Public Release. Public Release: 2200-09-26. Other requests shall be referred to: Homeland Security, Washington, DC, 20016
Author:	Pry, Peter V.	
Corporate Author:	EMP Task Force on National and Homeland Security	
Descriptors:	national security, artificial satellites, hypersonic glide vehicles, warning systems, second world war, hypersonic cruise missiles, nuclear bombs, warfare, explosives, hypersonic weapons, early warning systems, information systems, information warfare, nuclear weapons, aircraft carriers, ballistic missiles, electronic equipment, high altitude, military doctrine, treaties	
Identifiers:	Emp (Electromagnetic Pulse), hemp (high-altitude electromagnetic pulse), hgvs (Hypersonic Glide Vehicles), hcms (Hypersonic Cruise Missiles)	
<p>China has long known about nuclear high-altitude electromagnetic pulse (HEMP) and invested in protecting military forces and critical infrastructures from HEMP and other nuclear weapon effects during the Cold War and continuing today. China has HEMP simulators and defensive and offensive programs that are almost certainly more robust than any in the United States. China's military doctrine regards nuclear HEMP attack as an extension of information or cyber warfare and deserving highest priority as the most likely kind of future warfare. Chinese military writings are replete with references to making HEMP attacks against the United States as a means of prevailing in war. The foremost People's Liberation Army textbook on information warfare, Shen Weiguang's World War, the Third World War Total Information Warfare, explicitly calls upon China to be prepared to exploit HEMP offensively and to defend against it.</p>		

Biologically Derived Magnetite Nanoparticles (mNPs) for Use in Electromagnetic Pulse Shielding		
Accession Number:	Report Date:	Access Restrictions:
AD1098074	2020-05-01	A - Approved for Public Release.
Author:	Calm, Alena M., Kim, Michael, Kragl, Joe F., Savage, Alice, Beyer, Frederick L., Walck, Scott, Betts, Kelley	
Corporate Author:	Combat Capabilities Development Command Chemical Biological Center Abingdon United States	
Descriptors:	nanoparticles, electromagnetic pulses, electronic warfare, electromagnetic radiation, countermeasures, radiation shielding, bacteria	
Identifiers:	np(Nanoparticle), Magnetospirillum gryphiswaldense, mnp(Magnetite nanoparticle), emp(Electromagnetic pulse), Cubo octahedral, Magnetosome	
<p>Modern electronic warfare illustrates the need for innovative yet flexible electromagnetic pulse (EMP) protective capabilities for field-forward electronic equipment and components. The iron ore magnetite is a naturally occurring magnetic rock that can absorb radiation energy. Traditional magnetite nanoparticles (mNPs) produced using physical or chemical means have superparamagnetic properties and are an effective material for radiation shielding. New interest in mNPs from living organisms has arisen after it was discovered that biologically derived mNPs have qualities superior to abiotically produced mNPs, such as high chemical purity, low toxicity, good biocompatibility, and environmentally friendly production. Here, the bacterial mNP producer Magnetospirillum gryphiswaldense was used in large-scale microbially derived mNP production, delivering a new</p>		

material production and functionalization capability to the U.S. Army Edgewood Chemical Biological Center (now the U.S. Army Combat Capabilities Development Command Chemical Biological Center [CCDC CBC]; Aberdeen Proving Ground, MD). These milled and characterized mNPs could eventually be incorporated into an environmentally friendly, soy-based foam to make a customizable and sprayable EMP protective material. In the future, CCDC CBCs investments in synthetic biology, protein engineering, additive manufacturing, and materials science may leverage these mNPs to develop new materials and manufacturing capabilities across the CCDC CBC enterprise.

Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum

Accession Number:	Report Date:	Access Restrictions:
AD1083530	2019-05-23	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	King, Kenneth T.	
Corporate Author:	US Army School for Advanced Military Studies Fort Leavenworth United States	
Descriptors:	electronic warfare, military capabilities, military intelligence, military doctrine, encopresis, military organizations, military forces (united states), army, security	
Identifiers:	Electronics in military engineering Intelligence Branch Warfighting Military Technologies United States Army Security Agency, signals intelligence	
<p>This monograph focuses on stunted development of the US Army's modern electronic warfare (EW) capability. It compares the technological change that occurred in the US Army, Air Force, and Marines as it relates to the electromagnetic spectrum. It explores how the Army's Intelligence Branch, which was the proponent of the EW discipline from 1955 to 2005, mismanaged the discipline. Additionally, this monograph evaluates the Army's different operational concepts and the degree to which they advanced or retarded EW capacities. The US Army and Intelligence Branch involuntarily and intentionally neglected EW at different times throughout the history of the capability. A situation, from which the psychological disorder of encopresis is a metaphor. The US Army is still neglecting the EW discipline as of the writing of this monograph even as its competitors continue to advance its EW technology and tactics.</p>		

Simulation of Electromagnetic-Environment Susceptibility to Jamming Systems

Accession Number:	Report Date:	Access Restrictions:
ADA614775	2015-01-01	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Verdin, Berenice, Debroux, Patrick	
Corporate Author:	Army Research Lab White Sands Missile Range NM	
Descriptors:	electromagnetic susceptibility, jamming, radiation patterns, algorithms, communication and radio systems, communication equipment, computations, computer programs, control, electromagnetic spectra, far field, frequency, high frequency, limitations, radiofrequency, simulation, simulators	

Identifiers:	Not Available
<p>The US military relies on communication devices to manage and control operations. It is important to find the susceptibility of friendly-force assets to insure command and communication in an often-uncontrolled electromagnetic spectrum. Likewise, it is crucial to explore the enemy's susceptibility. Simulation of electromagnetic devices is often performed in a high-frequency structural simulator (HFSS). However, the complete susceptibility analysis cannot be performed in HFSS due to computational limitations including multiple devices. For this reason, this research project proposes to investigate the characterization of the susceptibility of radio frequency (RF) systems to jamming systems using HFSS (to obtain the far-field radiation patterns) and MATLAB software (to perform the susceptibility characterization). Thus, an algorithm that uses both reciprocity and superposition principles was developed. As a proof of concept, a simulation was performed in HFSS where the RF systems and the jammers far-field radiation patterns were simulated. The characterization of the susceptibility of RF systems was performed by obtaining 2-dimensional (2D) and 3-dimensional (3D) susceptibility areas.</p>	

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight		
Accession Number:	Report Date:	Access Restrictions:
ADA562373	2012-07-01	Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Lepore, Brian J., D'Agostino, Davi M., Pross, Mark A., Cavanaugh,Carolynn, D'Amore, Ryan, Helt, Brent, Powelson, Richard	
Corporate Author:	Government Accountability Office	
Descriptors:	defense planning, defense systems, department of defense, electronic warfare, policies, strategy, systems management, cyberwarfare, investments, joint military activities, leadership, military capabilities, research management, risk management	
Identifiers:	electronic warfare management, joint electronic warfare, electronic warfare oversight, cyberspace operations, joint electromagnetic spectrum control center, performance measures, organizational roles, organizational responsibilities, organizational coordination, governance framework, updated guidance	
<p>The Department of Defense (DoD) has committed billions of dollars to developing, maintaining, and employing warfighting capabilities that rely on access to the electromagnetic spectrum. According to DoD, electronic warfare capabilities play a critical and potentially growing role in ensuring the U.S. military's access to and use of the electromagnetic spectrum. GAO was asked to assess the extent to which DoD did the following: (1) developed a strategy to manage electronic warfare; and (2) planned, organized, and implemented an effective governance structure to oversee its electronic warfare policy and programs and their relationship to cyberspace operations. GAO analyzed policies, plans, and studies related to electronic warfare and cyberspace operations and interviewed cognizant DoD officials. GAO recommends that DoD should do the following: (1) include in its future electronic warfare strategy reports to Congress certain key characteristics, including performance measures, key investments and resources, and organizational roles and responsibilities; (2) define objectives and issue an implementation plan for the Joint Electromagnetic Spectrum Control Center; and (3) update key departmental guidance to clearly define oversight roles, responsibilities, and coordination for electronic warfare management, and the relationship between electronic warfare and cyberspace</p>		

operations. DoD generally concurred with these recommendations, except that the strategy should include performance measures. GAO continues to believe this recommendation has merit.

Electronic Warfare in Operations		
Accession Number:	Report Date:	Access Restrictions:
ADA496144	2009-02-25	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Not Available	
Corporate Author:	Department of The Army Washington, DC	
Descriptors:	electronic warfare, military doctrine, army operations, manuals, electromagnetic spectra, electromagnetic environments, military capabilities, joint military activities	
Identifiers:	Not Available	
<p>FM 3-36 provides Army commanders and their staff guidance on how the electromagnetic spectrum can impact their operations and how friendly EW operations can be used to gain an advantage. This manual describes the application of EW in support of full spectrum operations and provides a baseline for ensuring a common understanding and operational consistency. Although new equipment, tactics, techniques, and procedures continue to be developed, the physics of electromagnetic energy remains constant. So, as new strategies and tactics are devised to meet the cyberspace environment of the 21st century, electronic warfare remains a critical component of our national defense.</p>		

Cyberspace

Cyber and Electromagnetic Activities (CEMA) Operations Impacts on Human Performance		
Accession Number:	Report Date:	Access Restrictions:
AD1089733	2020-01-01	A - Approved for Public Release. Public Release: 2052-11-27. Other requests shall be referred to: U.S. Army CCDC Data and Analysis Center, Aberdeen Proving Ground, MD, 21005,
Author:	Plott, Christopher, Keller, John	
Corporate Author:	Alion Science and Technology	
Descriptors:	Not Available	
Identifiers:	CEMA attacks, cyber security, human performance, stress and decision making, cyber defense analyst, cyber threat scenarios	
<p>In this report we review the cyber and electromagnetic activities (CEMA) threats and attacks that can impact human performance. We then use the available data to translate these impacts, as best we can, into algorithms that can be used in human performance models. Since many of the threats, attacks, and impacts are dependent on the context of their use and what or who is targeted, we provide a framework for the development of scenarios for building and exercising human performance models that incorporate the CEMA threats, attacks, and impacts, with a focus on cyber defense operations and the cyber defense analyst.</p>		

EW and Cyber Convergence: Beyond Information Warfare		
Accession Number:	Report Date:	Access Restrictions:
AD1112357	2020-04-01	A - Approved for Public Release. Public Release: 2053-02-26. Other requests shall be referred to: Air University, Maxwell AFB, AL, 36112
Author:	Worrell, Ryan J.	
Corporate Author:	Air Force Fellows Program, Maxwell AFB, AL	
Descriptors:	air force, computer networks, electronic warfare, military applications, information warfare, air defense, cyberspace operations, network protocols, warfare, weapon systems, aircrafts, electromagnetic spectra, information operations, wireless networks, application software, cross domain, cyberattacks, cyberspace, cyberwarfare, defense systems	
Identifiers:	EMSO (Electromagnetic Spectrum Operations), CO (Cyberspace Operations), C2 (Command and Control), CAN (Computer Network Attack), OCO (Offensive Cyber Operations), SEAD (Suppression of Enemy Air Defenses), EP (Electromagnetic Protection), ES (Electromagnetic Support)	
<p>Electromagnetic Spectrum Operations (EMSO) and Cyberspace Operations (CO) are on divergent organizational paths driven by historical mission applications. Although both operate in and through the electromagnetic spectrum (EMS), each organization views its use differently. EMSO focuses on exploiting, attacking, protecting, and managing the physical EMS, while CO is focused on the data driven human use of digital applications and the data contained within cyberspace and the EMS. Each community has a specialty developed over many years, but entrenched thought has created a divide between the two. Over time, doctrinal rhetoric or relabeling of terms may close the divide, but these efforts are cumbersome and often unsustainable. A more successful approach would be the assignment of common focus areas to unify applicable portions of each community. One such focus area should be building a coherent process within the Air Force to develop, test, and field relevant technology for embedded cyber applications in a timely manner. This focus areas mission would be fighting system to system with an initial Suppression of Enemy Air Defense (SEAD) type approach of a blue aircraft system versus a re-integrated Air Defense System (IADS). This approach could be further scoped to air centric with a focus on the blue aircraft network versus the red aircraft network. To do this many classification boundaries will need to be lowered to enable EWOs, COs, engineers, and pilots to work together to field a sustainable system approach within the Air Force.</p>		

Warfare in the Electromagnetic Spectrum and Cyberspace: United States Air Force Cyber/Electromagnetic Warfare Command Construct		
Accession Number:	Report Date:	Access Restrictions:
AD1055497	2014-02-13	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Cole, Harold T	
Corporate Author:	Air War College, Air University Maxwell AFB United States	
Descriptors:	electromagnetic spectra, cyberspace, cyberwarfare, electronic warfare, military forces (united states), air force	

Identifiers:	Military commands, ems (electromagnetic spectrum) ew (electronic warfare), Cyberspace Operations, a2ad (anti access area denial)
<p>The information revolution brought significant change to the world over the past thirty years. Similarly, that same revolution continues to play a significant role in shaping military organizational structures worldwide. The primary contributors to this revolution were the exploitation of the electromagnetic spectrum (EMS) and the rapid growth of information availability made possible by rapid advances in affordable digital computing power. This paper seeks to examine current United States Air Force organizational constructs for electronic warfare (EW) and cyberspace operations to determine their effectiveness in preparing the Air Force for conflict over the next thirty years. A brief background of the EMS and cyberspace is provided to frame the discussion to follow. The relationship between cyberspace and the EMS is explained, with perceived and actual positions of the Army, Navy and Air Force discussed to show alternative thinking within the Department of Defense. The evolution of Air Force Electronic Warfare and Cyberspace Operations are both examined to provide context and frame discussion regarding why the Air Force chose to organize in its current manner. Future threats in cyberspace and the EMS are presented to show why these two environments will continue to grow in importance over the next three decades. Finally, recommendations offered focus on improving the state of EW in the Air Force and strengthening the organizational relationship between cyberspace and EMS operations.</p>	

Cyber Electromagnetic Activities within the Mission Command Warfighting Function: Why is it Important and What is the Capability?		
Accession Number:	Report Date:	Access Restrictions:
ADA599661	2013-12-13	A - Approved for Public Release. Approved for public release; distribution is unlimited.
Author:	Coonfield, III, James D.	
Corporate Author:	Army Command and General Staff College, Fort Leavenworth KS	
Descriptors:	cyberwarfare, electromagnetism, defense systems, emplacement, military operations, protection	
Identifiers:	Not Available	
<p>Over the past 20 years, the increased incorporation of cyber capabilities into military command and control functions has necessitated an intensive defensive cyber posture for protection, but little effort was put into offensive cyber capabilities. The recent uses of cyber as a means of achieving national goals has changed not only how cyberspace is viewed by military leaders but has also changed the potential for offensive cyber as a military weapon. This thesis argues for the placement of cyber electromagnetic activities within the Mission Command warfighting function by identifying the capability that cyber electromagnetic activities provides to military operations.</p>		

Index

A

Air Force Electronic Warfare, 26

C

CEMA, 24

Coalition Joint Spectrum Management, 14

cognitive radio, 18

cyber capabilities, 26

cyberwarfare, 19, 23, 25, 26

D

dynamic spectrum access, 18

E

Electromagnetic Battle Management, 11

Electromagnetic Defense Task Force, 6

electromagnetic environment, 7, 16, 19

Electromagnetic Environmental Effects, 13

electromagnetic interference, 9, 12, 16

electromagnetic radiation, 21

electromagnetic spectra, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 20, 22, 24, 25

electromagnetism, 12, 26

Electronic warfare, 7, 20

Electronic Warfare Executive Committee, 11

G

Global Electromagnetic Spectrum Information System (GEMSIS), 14

H

high-altitude electromagnetic pulse, 19, 21

I

integrated Air Defense System (IADS), 25

ISR, 6, 7, 9

J

jamming, 20, 22, 23

joint electromagnetic spectrum management operations, 12

Joint Spectrum Management Team, 8

N

National Defense Strategy, 9

Navy policy, 13

Network Centric Warfare, 14

networks, 6, 9, 10, 11, 17, 18, 25

O

Offensive Cyber Operations, 25

Overview, 6

S

signals intelligence, 6, 20, 22

software defined radios, 17

spectrum analysis, 10, 13, 16, 18

spectrum landscape, 9

Spectrum Management, 8, 9, 10, 11, 12, 13, 14, 15, 16

Spectrum Planning, 12, 13

Suppression of Enemy Air Defense, 25