THE WRIGHT FLYER PAPERS

Cognitive Radio Cloud Networks

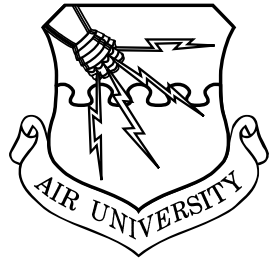
Assured Access in the Future Electromagnetic Operating Environment

Lawrence O. Jones
Major, USMC

Air Command and Staff College
Wright Flyer Paper No. 63

Please send inquiries or comments to
Editor
The Wright Flyer Papers
Department of Research and Publications (ACSC/DER)
Air Command and Staff College
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426
Tel: (334) 953-3558
Fax: (334) 953-2269
E-mail: acsc.der.researchorgmailbox@us.af.mil

AIR UNIVERSITY
AIR COMMAND AND STAFF COLLEGE



Cognitive Radio Cloud Networks

Assured Access in the Future Electromagnetic Operating Environment

Lawrence O. Jones
Major, USMC

Wright Flyer Paper No. 63

Air University Press
Curtis E. LeMay Center for Doctrine Development and Education
Maxwell Air Force Base, Alabama

Project Editors
Belinda Bazinet
Maranda Gilmore

Copy Editor
Carolyn B. Underwood

Cover Art, Book Design, and Illustrations
Daniel Armstrong

Composition and Prepress Production
Vivian D. O'Neal

Print Preparation and Distribution
Diane Clark

AIR UNIVERSITY PRESS

Director and Publisher
Dr. Ernest Allan Rockwell

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6026
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://www.facebook.com/AirUnivPress

and

Twitter: https://twitter.com/aupress

Accepted by Air University Press in October 2016, published in October 2018

Disclaimer

This Wright Flyer and others in the series are available electronically at the AU Press website: https://www.airuniversity.af.edu/AUPress.

Contents

Illustrations

Foreword

It is my great pleasure to present another issue of the Wright Flyer Papers. Through this series, Air Command and Staff College presents a sampling of exemplary research produced by our residence and distance-learning students. This series has long showcased the kind of visionary thinking that drove the aspirations and activities of the earliest aviation pioneers. This year's selection of essays admirably extends that tradition. As the series title indicates, these papers aim to present cutting-edge, actionable knowledge—research that addresses some of the most complex security and defense challenges facing us today.

Recently, the Wright Flyer Papers transitioned to an exclusively electronic publication format. It is our hope that our migration from print editions to an electronic-only format will fire even greater intellectual debate among Airmen and fellow members of the profession of arms as the series reaches a growing global audience. By publishing these papers via the Air University Press website, ACSC hopes not only to reach more readers, but also to support Air Force–wide efforts to conserve resources. In this spirit, we invite you to peruse past and current issues of the Wright Flyer Papers at https://www.airuniversity.af.edu/AUPress/Wright-Flyers/.

Thank you for supporting the Wright Flyer Papers and our efforts to disseminate outstanding ACSC student research for the benefit of our Air Force and war fighters everywhere. We trust that what follows will stimulate thinking, invite debate, and further encourage today's air, space, and cyber war fighters in their continuing search for innovative and improved ways to defend our nation and way of life.

BRIAN HASTINGS
Colonel, USAF
Commandant

About the Author

Maj Lawrence O. Jones is a native of Plano, Texas and enlisted in 1999 into the United States Marine Corps (USMC) Reserve as an M-198 artillery mechanic assigned to Ordnance Maintenance Company in Waco, Texas. Major Jones completed Officer Candidates School via the Platoon Leaders Class junior increment in the summer of 2001 and senior increment in the summer of 2002. He was commissioned in December 2003 after graduating from Texas A&M University with a degree in history. Upon completion of The Basic School in March 2004, Major Jones reported to Naval Air Station Pensacola, Florida, and Naval Air Station Corpus Christi, Texas, for flight training. Major Jones was designated a Naval Aviator in August 2006.

In September 2006, Major Jones reported to Marine Heavy Helicopter Training Squadron 302 at Marine Corps Air Station New River, North Carolina for training in the CH-53E. Upon completion in April 2007, Major Jones reported to Marine Aircraft Group 24, Marine Corps Base Hawaii for a series conversion to the CH-53D. Once complete Major Jones reported to Marine Heavy Helicopter Squadron (HMH) 463.

While assigned to HMH-463, Major Jones served as the ground safety officer, aviation safety officer, airframes officer, quality assurance officer, weapons and tactics instructor, and assistant operations officer. During this tour, Major Jones deployed twice with the HMH-463 in support of Operation Enduring Freedom and once on the unit deployment program.

In June 2012, Jones reported to Marine Aviation Weapons and Tactics Squadron One (MAWTS-1), Marine Corps Air Station Yuma, Arizona. During this tour, Major Jones was selected to the Aviation Development Test and Evaluation Department as the assault support specialist, rotary-wing aircraft survivability equipment and digital interoperability subject matter expert.

After completion of his MAWTS-1 tour in July 2015, Major Jones reported to the Air Force Command and Staff College (ACSC) in Montgomery, Alabama where he was the recipient of the 2016 Armed Forces Communications and Electronics Association research award.

Following ACSC Major Jones reported to HMH-465 where he would deploy on the 11th Marine Expeditionary Unit as the future operations officer. Major Jones has over 2,000 mishap-free flight hours and holds all qualifications and flight leadership designations in the CH-53E. His personal decorations include the Meritorious Service Medal, the Air Medal with "C" and Strike/Flight numeral "12," the Navy and Marine Corps Commendation Medal, the Navy and Marine Corps Achievement

Medal with gold star, and the Selective Marine Corps Reserve Medal. He was also awarded the 2011 USMC Exceptional Pilot Award by the Order of the Daedalians and the 2012 Aviator of the Year by 1st Marine Aircraft Wing.

Abstract

The electromagnetic spectrum (EMS) is a finite resource critical to the US military's ability to gain superiority in the five war-fighting domains. The Department of Defense's (DOD) electromagnetic strategy is spectrum access, when and where needed, to achieve mission success. However, the future electromagnetic operating environment will find gaining assured access increasingly difficult due not only to adversaries actively contesting it, but also to the congestion attributed to the exponential growth in commercial and civilian access. Despite these signs, the US federal government and the DOD continue to cling to a century-old model for managing the EMS. A revolution is in order.

This paper explores how the collision between technological advances in software-defined radios, machine learning, and cloud computing offers a viable solution to this growing problem. That solution is cognitive radio cloud networks.

Introduction

In 1997 the Department of Defense (DOD) embarked on an ambitious goal to "provide the Warfighter with a software programmable and hardware configurable digital radio networking system to increase interoperability, flexibility, and adaptability in support of varied mission requirements."[1] The Joint Tactical Radio System (JTRS) resulted from this goal (fig. 1). The Multifunctional Information Distribution System JTRS and JTRS Handheld, Manpack and Small Form Fit are the only full-rate production radios to be produced after more than $17 billion and three operational requirement document revisions. The JTRS ground mobile radio was cancelled in 2011. Although certified for use, it was never used due to poor performance and obsolete hardware.

Figure 1. JTRS increment 1 tactical networking capability. (*Reprinted from* http://www.public.navy.mil/jtnc/PapersBriefsReports/MIL_2008_NetworkProgrammingOfJtrsRadios.pdf.

JTRS was, at its time of conception, a truly radical idea. Software-defined radios (SDR) were mostly theoretical then, and WiFi, 3G, and 4G networks did not exist. With a 10-year plan, the DOD was being aggressive. However, what the DOD failed to consider was the exponential acceleration of computing technology articulated in Moore's Law.[2] The commercial sector, embracing Moore's Law, continued to develop cheaper, limited-function digital radios that could embrace the ever increasing processing power from smaller, faster microchips.[3] Soon the commercial sector's radios began to exceed the original capability requirements of JTRS. This introduced requirements creep, and began the cycle of the JTRS program trying to keep up with technology.

The DOD is once again faced with a new challenge regarding radios and waveforms, but not about interoperability or overcoming single channel jamming. Rather, it's about the ability to maneuver and assure access in a heavily contested and congested electromagnetic operating environment (EMOE). Fortunately, the commercial sector is interested in a viable solution, since they share the same problem set. It will now be up to the DOD to help develop an innovative solution to the problem and an innovative way to match the procurement and development cycle of the commercial sector.

Thesis

Cognitive radio cloud networks (CRCN) will assure that the DOD is capable of gaining and maintaining spectrum access and network connectivity to gain a decisive war-fighting advantage in the information age. The future of network-enabled warfare will rely heavily on the ever-increasing digital exchange of information transported through the electromagnetic spectrum (EMS) to shape the battlespace and assure synergistic effects. Whether operating in the air, space, land, maritime, or cyber domain, all DOD joint functions are enabled by vulnerable spectrum-dependent systems (SDS). The challenge of conducting joint EMS operations and assuring access in the future operating environment is that the EMS will be simultaneously heavily congested from civilian use and by adversarial action. This research paper defines the problems facing the DOD in the 2035 EMOE, argues that CRCNs are the most feasible option for the DOD to solve those challenges, and assesses the future research and development collaboration potential of CRCNs.

The Problem

The most crucial and challenging endeavor the DOD will undertake in preparation for the battlefield of 2035 is assured access to the EMS. The EMS is a finite resource shared by all nations but regulated individually to ensure the nation's sovereign right to its unlimited use.[4] As a result it not only will be contested by the adversary but also congested by civilian and commercial usage. Add an ever-growing DOD bandwidth requirement, and the complexity of maneuvering through the EMOE to accomplish the mission is daunting. Figure 2 is a visual depiction of EMS constraints.

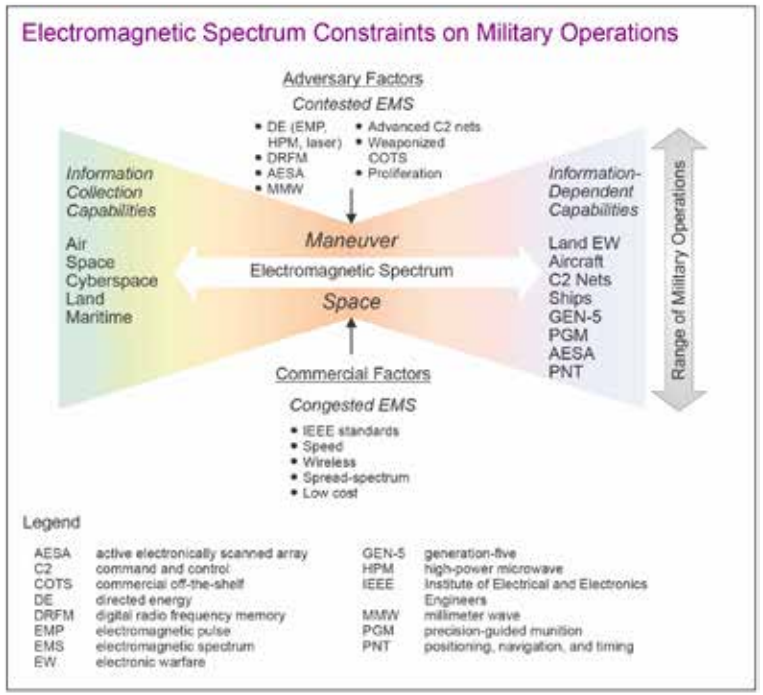


Figure 2. Constraint on the EMS. (*Reprinted from* Joint Publication [JP] 6-1, *Joint Electromagnetic Spectrum Management Operations*, 20 March 2012, I-2).

Operationally, the EMS is the physical medium in which military forces must have assured access to gain superiority in the physical domains. "Control of the EM environment must be achieved early to sup-

port freedom of action. This control is important for superiority across the physical domains and information environment," JP 3-0, *Joint Operations*, states.[5] This will remain true in the future. However, the current means of access and the method of EMS management—the static assignment of spectrum—will be insufficient in the future EMOE. The current doctrinal stance of "once the allotted EMS has been allocated to support specific capabilities or systems in a specific geographical area, it is no longer available for use" is an analog method that does not even take advantage of already decade-old commercial digital technology for sharing or reuse.[6]

Contested

The overwhelming success of Operation Desert Storm created the blueprint for how the DOD would posture and procure its systems to fight wars into the twenty-first century. The use of highly coordinated combined arms with unmatched positioning and reconnaissance capabilities created a decisive military advantage by placing Iraqi forces on the horns of a dilemma. As a result, Congress was quick to fund massive communication; space-based intelligence, surveillance, and reconnaissance (ISR); and command-and-control systems to digitally link the battlespace. Over the next few decades, the trend continued to produce more spectrum-dependent systems (SDS) and buzzwords like "network-centric warfare" came into vogue. Peer and near-peer adversaries such as China and Russia observed the DOD's continual overreliance on the EMS, identified the critical vulnerability, and developed comparatively low-cost systems to deny access. Both Russia and China developed EMS denial-and-disruption capabilities ranging from local active jamming to electromagnetic pulses that can range several hundred kilometers or high-altitude electromagnetic pulses that can affect a continent-sized area.[7]

However, by 2035 it will not be just the peer/near-peer nations that can contest the DOD's access to the EMS. Moore's Law has driven a global shift from analog to digital technologies, resulting in proliferation of high-power, low-cost commercial products. Small countries and insurgencies can now conduct EMS denial-and-disruption operations that formerly required a large nation-state's resources.

"We have lost the electromagnetic spectrum," said Alan Shaffer, the Pentagon's research and engineering chief, at the 2014 Common Defense conference. "People are able to create very agile, capable systems for very little money, and those agile, capable systems—if we don't develop counters—can impact the performance of some of our high-end platforms."[8] Specifically, platforms like the F-35 and the AN/TPS-80 ground/air task-

oriented radar (G/ATOR) are examples of advanced systems at risk since they depend heavily on access to the EMS in order to share and shape a picture of the battlespace.

Peer nations in 2035 may not attempt brute force denial as forecasted by the Joint Operational Access Concept—unless sovereignty is threatened—but rather force friendly movement into a portion of the spectrum that would be advantageous for exploitation for either cyber or electromagnetic deception operations. By allowing the DOD to maintain a portion of the EMS, any successful cyber intrusion or deception information could then be propagated throughout the DOD network. This more sophisticated technique would allow the adversarial forces use of the EMS for their own systems without inadvertent electronic fratricide.

Congested

In the international and national scope, the EMS is not a military resource but an economic one. Sovereign nations regulate and manage the EMS to meet the ever-growing needs of their civilian and commercial sectors by purposing bands for specific functions. Globalization combined with the proliferation of nuclear weapons has significantly reduced the likelihood of large nations going to war with each other. Military power has, to an extent, been marginalized in favor of assuring growth in the economic sector. "In June 2010, President [Barack] Obama directed the National Telecommunications and Information Administration to work with the FCC [Federal Communications Commission] to 'make available a total of 500 MHz [megahertz] of federal and non-federal spectrum over the next 10 years, suitable for both mobile and fixed wireless broadband use,'" the *Department of Defense Electromagnetic Spectrum Strategy* stated.[9] As a result, in 2013 645 MHz (including 95 MHz that was previously federally reserved) of licensed spectrum in the United States allocated for just the mobile wireless industry was valued at $500 billion, generating between $5 trillion and $10 trillion in consumer surplus. In that same year, consumers and businesses spent $172 billion on mobile wireless services, with every dollar having a $2.32 return. This accounted for 1 percent of the US gross national product.[10] Other nations have followed the US lead based on the economic growth potential.

Doctrinally, geographic combatant commanders are responsible for coordination of spectrum access within all nations inside his or her area of responsibility. Confounding the task is that there are very few regional standards with spectrum allocation, as each host nation allocates different spectrum inside their borders. When each nation reappropriates spectrum to meet internal demands, the ever-narrowing bands of spec-

trum available to the DOD no longer overlap. Noncompliance with the shrinking available spectrum may be considered a violation of international treaties or laws, and the joint force commander could be held criminally or financially liable.[11]

The heart of the economic expansion of the EMS has been the mobile computing boom. In 2013 global mobile Internet penetration was 28 percent; by 2019 it is forecasted to be 71 percent.[12] The Asia-Pacific region is already above 100 percent with North America, Western Europe, and Central and Latin America exceeding 100 percent by 2017.[13] With over 90 percent of the world's population already covered by a mobile cellular network (fig. 3) and companies like Google and Facebook attempting to bring free Internet access to underdeveloped countries, it is fair to project that global mobile Internet penetration will exceed 100 percent by 2035.[14] Nations are likely to continue to meet the economical demands of spectrum at the expense of the military.

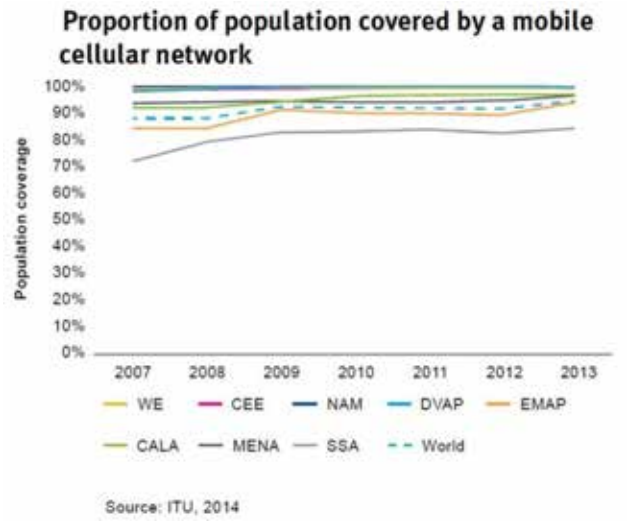


Figure 3. Proportion of population. (*Reprinted from* Michael Kende, *Global Internet Report 2015: Mobile Evolution and Development of the Internet* [Washington, DC: Internet Society, 2015]: 52). NAM=North America; CALA=Caribbean and Latin America; SSA=Sub-Saharan Africa; MENA=Middle East and North Africa; CEE=Central and Eastern Europe; WE=Western Europe; DVAP=Developed Asia Pacific; and EMAP=Emerging Asia Pacific.

DOD Growing Spectrum Requirements

At every echelon, the DOD is requiring larger portions of the EMS to conduct its mission. Every asset, while potentially not a consumer, is a contributor to what is commonly referred to as the common operating picture or common tactical picture. A large contributor to the accelerated requirements is the advancement in networked operations at the tactical level. Situational awareness tools providing video downlinks, blue force tracking, and real-time collaboration have provided the tactical user with previously unmatched kill-chain efficiencies. What used to take minutes, now takes seconds. The cost is an exponential growth in EMS access in order to support the increased data flow (fig. 4).

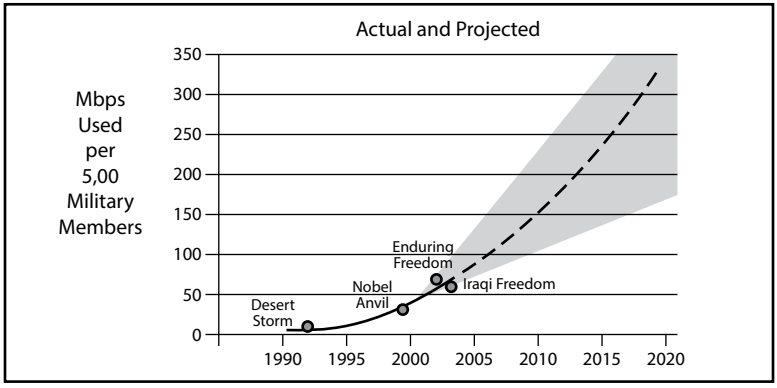


Figure 4. DOD spectrum requirements. (*Reprinted from* DOD, *Electromagnetic Spectrum Policy 2013* [Washington, DC: Deputy Secretary of Defense, September 2013]: 3).

The DOD finds itself in an environment, like the commercial sector, where a growing demand will require a new way to look at the EMS. The doctrinally static method as described in JP 6-1 simply will not be able to support the DOD information requirements in 2035. Unmanned aerial systems, ISR, robotics, space, and cyber technologies will place more stress on spectrum requirements as they develop and mature over the next 20 years. A dynamic approach, focusing on shared spectrum and reuse, must be aggressively pursued.

The Solution

Imagine you are sitting on your front porch and your friend, with whom you wish to speak, is at his house. Your two houses are separated by a forest, and to talk to your friend, you must pass through the forest. In order to accomplish this, there are three scenarios. In the first scenario you walk to the edge of the forest, but unable to see over the trees to the other side, you simply return to your porch. In the second scenario you build a path through the forest, cutting the trees down to give you a straight shot to his house. While this assures passage to and from your friend's house when you want, the path is rarely used and no trees will be able to utilize that space. Additionally, if an obstacle were to appear on the path, you would no longer be able to use it. In the final scenario, you simply walk into the forest and navigate through the empty spaces between the trees to make it to your friend's house. Your ability to recognize the environment and intelligence to apply logic and reason allows you to determine where you need to go and how to get there. If you make a wrong turn, you are able to remember what you did wrong and apply it to future trips. After several trips you have learned the optimal route.

These scenarios are simplified metaphors to illustrate how EMS management has evolved. In the beginning, the EMS was looked at as a two-dimensional concept with little regulation. The power of the signals in the environment was the size of the trees, while the frequency was the lateral placement of the trees along the tree line. If there was no open frequency for the signal to get through, then the power would have to be increased. Essentially if you are bigger than the trees you could walk over or through them. As licensing and regulation became prevalent with the Federal Radio Act of 1912, the EMS was allocated to different functional areas such as radio, television, public safety, etc. These paths assured band usage without interference, but left no flexibility if the path was blocked, and didn't allow for other users to share the band when it wasn't being used. Over a century later, this is still the current state of EMS management. The third scenario describes the concept the DOD needs to pursue, cognitive systems.

Cognitive radios are able to sense the EMOE, apply logic and learning (intelligence) to formulate an autonomous solution, learn from previous usage, and take advantage of the white and grey space available to assure access when and where it's needed. It answers the call for action spelled out in the *DoD Electromagnetic Spectrum Strategy* for "spectrally efficient, flexible, and adaptable systems." While this seems like an easy answer, cognitive radios by themselves do not have a practical usage due to size, weight, and power (SWaP) limitations. The processing power

alone for the radio to sense the environment; analyze it; implement the required artificial intelligence and machine learning; dynamically control the signals power, modulation, frequency, and quality of service; and, finally, assure signal receipt is substantial. In order to offload this burden, cloud computing enables the radio to push the heavy processing to less SWaP-restricted assets. Before fully explaining the merits of cloud computing and cognitive radio pairing, one must understand each individual technology.[15]

Cognitive Radios

The idea of the cognitive radio is credited to Dr. Joe Mitola in 1999, whom in a series of Institute of Electrical and Electronics Engineers (IEEE) articles about the future of mobile computing and software-defined radios (SDR), described intelligent, self- and environmentally aware radios that autonomously made decisions through model-based reasoning.[16] In 2005 Simon Haykin further refined the definition to include learning: "Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming radio frequency (RF) stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real time, with two primary objectives in mind: (1) highly reliable communications whenever and wherever needed; (2) efficient utilization of the radio spectrum."[17] When compared to the DOD strategy (fig. 5), the objectives are the same.

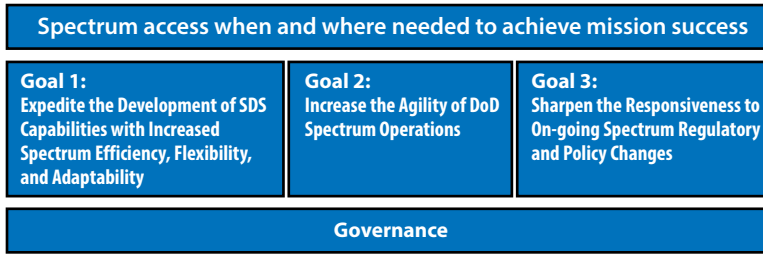


Figure 5. DOD electromagnetic spectrum. (*Reprinted from* DOD, *Electromagnetic Spectrum Policy 2013*, September 2013, 9).

Cognitive radios are the result of pairing SDRs, which can digitally reconfigure themselves, with a cognitive engine, which employs artificial

intelligence and machine learning. Cognitive radios' cognition models are similar to human cognition models. Compare Haykin's basic cognitive radio model to Boyd's OODA Loop (fig. 6). The radio senses the RF stimuli (observe), conducts radio-scene analysis (orients), estimates and predicts channel identification based on previous learning (decide), and then conducts transmit power control and dynamic spectrum access (act). The action (RF signal) is then in a feedback loop to the sensor.

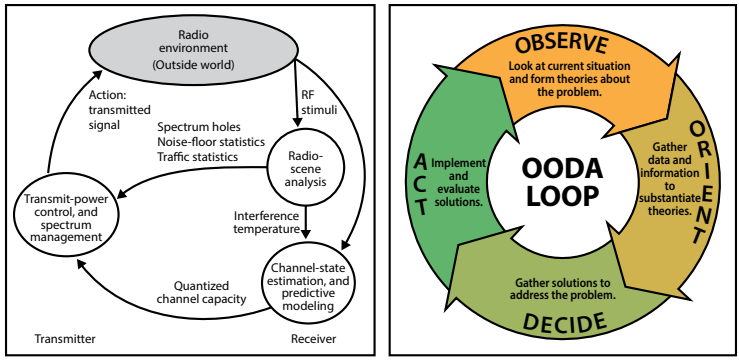


Figure 6. Haykin's cognitive radio (left) and Boyd's OODA Loop (right).

The action component in the application of cognitive radios is the concept of dynamic spectrum access (DSA), sometimes referred to as dynamic spectrum management. IEEE defines dynamic spectrum access as "the real-time adjustment of spectrum utilization in response to changing circumstances and objectives. . . .Changing circumstances and objectives include (and are not limited to) energy-conservation, changes of the radio's state (operational mode, battery life, location, etc.), interference-avoidance (either suffered or inflicted), changes in environmental/external constraints (spectrum, propagation, operational policies, etc.), spectrum-usage efficiency targets, quality of service (QoS), graceful degradation guidelines, and maximization of radio lifetime."[18] DSA recognizes primary and secondary users (also referred to as licensed and unlicensed) to manage priority. Primary users have priority inside their band but if not using it, secondary users may use the "white space" to transmit. In essence, think of DSA as a game of hopscotch (fig. 7) through the radio traffic in the EMS. The objective is to reach the other side, avoiding the space where your beanbags (primary users) are.

Figure 7. Dynamic spectrum access. (*Reprinted from* Roger Bacchus, Tanim Taher, Kenneth Zdunek, and Dennis Roberson, "Spectrum Utilization Study in Support of Dynamic Spectrum Access for Public Safety," in *Proceedings of New Frontiers in Dynamic Spectrum (DySPAN)*, 2010 Institute of Electrical and Electronics Engineers (IEEE) Symposium [Singapore: IEEE, 6–9 April 2010).

In a contested environment, cognitive radios have the potential to bring the ability to communicate through active jamming to the battlefield rather than just move around it. Jamming focused on denying communication is typically pulsed, whether intentionally to reduce power requirements or unintentionally by the type of electricity used. For example, to the human eye a strobe light turning off and on at 120 times a second would appear to simply be a normal lightbulb that is turned on. For every second the strobe light is on, half of the time the room is dark despite our eyes perceiving it to be continuously lit. If a cognitive radio wanted to get information through the room with the strobe light on, but the information had to be passed in the dark, the cognitive radio would sense the environment to first determine the light bulb's hertz. The analysis from the pattern detected would help formulate predictive tools as to how to send the signal and what interference it would expect. Using DSA, the radio would pulse its signal to broadcast only during the light's off time while actively assuring QoS through its feedback loop.

Cloud Computing

The National Institute of Standardization and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[19] Companies like Google and Apple use cloud computing to off-board tasks that require more processing power than the standard handheld device has internally. Services like Voice-to-Text, Google Maps, and Gmail are all processed in the cloud. The device only has to upload and download the data, which reduces storage, processing power, and energy requirements to the device. This technology is quickly becoming the backbone of the modern commercial industry.

Cloud computing offers three services: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The user can use the provider's software on a cloud infrastructure with Saas. There is no need to download the application onto the user's machine. PaaS allows the user to run his or her own applications on the cloud infrastructure as long as the user's applications are supported by the provider's infrastructure. The user does not have control over any of the base systems or storage. IaaS allows the user to run base programs like operating systems and storage, but the user does not have control over the cloud infrastructure. Cloud computing can further be deployed into four different models: private (single organization), community (multiple organizations), public (general public), or hybrid clouds (any combination).

The US Army deployed the first DOD tactical cloud computing node in 2011. The Distributed Common Ground System-Army (DCGS-A) Version 3 (fig. 8) was deployed to Afghanistan in response to Maj Gen Michael Flynn's joint urgent operational need statement.[20] The compilation of vast amounts of historical data on improvised explosive devices locations to create a predictive tool for protecting logistics routes was the capability need. DCGS-A had to tie in ISR assets with an exploitation tool directed at the end user. The permissive and uncongested environment in Afghanistan along with the massive communication network assuring access to the cloud allowed the tie-in.

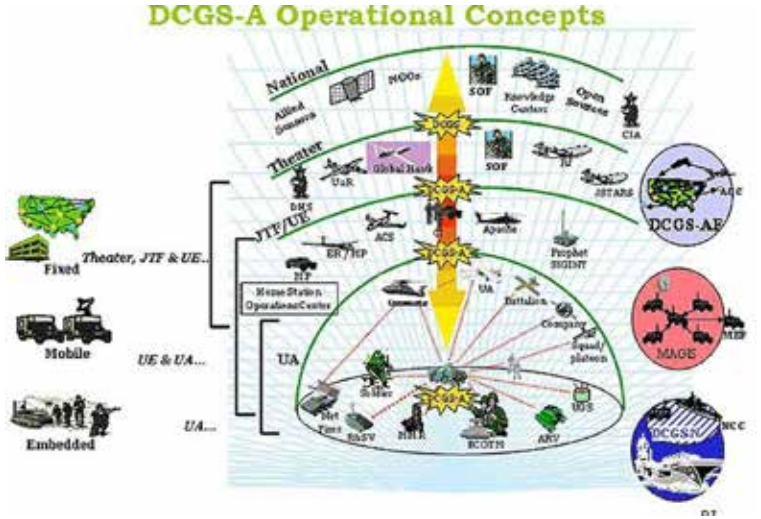


Figure 8. Distributed Common Ground System-Army. (*Reprinted from* Distributed Common Ground System-Army).

Over the next 20 years, cloud computing will become the backbone of the commercial market. The market of the public cloud alone is expected to reach $160 billion by 2020 (fig. 9). While the DOD certainly can benefit from the growth of the cloud computing market, so will our potential adversaries. Transnational criminal organizations and violent extremist organizations will have access to massive computing power, which only large nations previously enjoyed. Additionally, with more services moving to the cloud, the congestion of the EMS will become more exacerbated.

Figure 9. Global public cloud market size forecast, 2011–2020. (*Reprinted from* Global Public Cloud Market Size Forecast, 2011–2020). The global cloud computing market will grow from a $40.7 billion in 2011 to $241 billion in 2020, according to Forrester Research, 22 April 2011.

Cognitive Radio Cloud Networks—the Best of Both Worlds

Cognitive radios need cloud computing to be effective. Ideally, the base radio unit would have all the internal power and processing needed to conduct its cognitive function. That, however, is not realistic. Cognitive radios—especially battery-powered, man-portable versions—need to offload the processing requirements of the cognitive functions to preserve battery life. As the radios move upward in power, from man-portable to vehicle-borne to communication centers, more functionality could remain internally within them. This would create smaller, distributed clouds that could provide critical functionality if the primary cloud connection was lost. As long as two cognitive radios could sense each other, they could share tasks to reduce the burden by not duplicating process and services. The cloud also provides the cognitive radios with a greater library of learned events. In this sense, the entire network becomes cognitive as each radio shares what it has learned about the environment and can access a greater database for spectrum analysis and identification.

Cloud computing needs cognitive radios to be effective. It relies on assured access from the user to the cloud, but communication on the tactical edge can be disruptive and unreliable. Cognitive radios provide the ability to find white space through the contested and congested EMOE and reduce the chances of being spectrally denied through DSA. Additionally, cognitive radios can manage QoS and enforce rules for the sharing of high bandwidth requests like full-motion video. This reduces the chances of users exceeding the capacity of any particular node.

There are also several security challenges that must be addressed before the CRCN could be optimized. First, the cloud infrastructure is most susceptible to side-channel, denial-of-service, and distributed denial-of-service attacks. Losing the cloud, or the cloud providing erroneous information to the cognitive radios, could cause poor operation. Distributing the clouds will provide some reconciliation, but the network will still be suboptimal. Secondly, the cognitive radios themselves may be able to be "fooled" into operating poorly by confusing or misleading the cognitive functions through techniques like playback, Sybil attacks, or beacon flood attacks.[21] While many of these security challenges are theoretical, it serves to highlight cognitive radios are still potentially susceptible.[22]

Despite the challenges moving towards a CRCN, it is the most viable and likely approach to be successful operating on the battlefield of 2035. Investment strategies, and research and development should be directed into the convergence of cloud computing and cognitive radios.

Getting to the Finish Line

On 28 June 2010 President Obama released a presidential memorandum titled *Unleashing the Wireless Broadband Revolution*. The president called for the FCC to make available a total of 500 MHz of federal and nonfederal spectrum over the next 10 years, suitable for both mobile and fixed wireless broadband use.[23] Two years later, the president's Council of Advisors on Science and Technology released *Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth*. A key finding was that the selling off of licensed spectrum would not be a sustainable model for economic growth. The council recommended a new model of advanced spectrum sharing promising to turn "scarcity into abundance."[24] In 2013 President Obama released *Expanding America's Leadership in Wireless Innovation* calling for innovation in spectrum sharing technologies.

Moving Forward with Cognitive Radios

The DOD has responded with several initiatives. In 2014 the DOD released its *Electromagnetic Spectrum Strategy: A Call to Action*. The Defense Advanced Research Projects Agency (DARPA), which had done some early work with cognitive radios and DSA with the neXt Generation (XG) project, began a series of new projects. In 2012 DARPA began Advanced RF mapping (RadioMap); in 2013 it followed with shared spectrum access for radar and communications. The next year DARPA offered a $150,000 reward to the Spectrum Challenge winner. More impressively, in 2015 the DOD created the National Spectrum Consortium entering into a five-year, $1.25 billion deal to exploit emerging capabilities and prototypes that assist in improved EMS awareness, sharing, and use.[25]

Slowing Down in Cloud Computing

In 2012 the DOD chief information officer (CIO) released the *Cloud Computing Strategy* with the stated goal to "implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the department's mission, anywhere, anytime, on any authorized device."[26] The strategy ranged in service from the larger enterprise to the tactical edge, which it listed as a primary challenge due to disconnected, intermittent, and low-bandwidth (DIL) users.[27] However, due to budget cuts and issues with acquisition strategies (contract vehicles) the procurement is slowing down.[28] In 2014 the DOD CIO rescinded the memorandum naming the Defense Information Systems Agency as the manager of the cloud and instead moved it to the services.[29] Currently the Army, Navy, and Marines have active cloud pilot programs, but the gap between the commercial and military acquisitions process is stifling progress.

Always Leaning Forward

The slowing down in DOD cloud computing advancement is not relatively damaging to progress. The commercial sector will continue to advance the research and development of cloud computing with or without the government's assistance. Apple, Google, Samsung, and Amazon will invest more money into research and development in one year than the DOD could invest in 10. Cognitive radios, however, do not have a large commercial market and therefore require the continued assistance from the DOD and the federal government to continue advancement. The National Spectrum Consortium is a tremendous step to this end.

Recommendation

Control of the EMS will be a key to the US military's continued dominance on the global scene. The only way to assure access and to protect our SDS is to heavily invest in capabilities that are agile enough to operate in a heavily contested and congested environment. The commercial sector is no longer developing systems; rather, they are developing services. While continuing to develop innovative solutions to similar problem sets, the DOD acquisitions process will need to evolve to work with the rapidly growing commercial sector. Low-level insurgents already have more networking capability with their smartphones than deployed American forces deploy. The DOD should continue to use the presidential guidance to invest heavily in cognitive radios and cloud computing pairing.

Conclusion

CRCNs are the most viable solution to assure access to the EMS when and where it is needed to accomplish the mission. In order to get there, the DOD will need to be an equal partner with the commercial sector, innovating not only new technologies but also new processes to interact.

"Victory smiles upon those who anticipate the changes in the character of war, not upon those that adapt themselves after the changes occur," Guilio Douhet said.[30] The DOD cannot afford another JTRS program.

Notes

Notes will appear in full form only in their first iteration. Thereafter, they will appear in shortened form. For full details, see the appropriate entry in the bibliography.

1. "Joint Tactical Radio System," US Army, http://www.army.mil/aps/06/maindocument/infopapers/J-28.html.
2. Moore's law is the observation that the number of transistors in a dense integrated circuit doubles approximately every two years. The period is often quoted as 18 months because of Intel executive David House, who predicted that processing power would double every 18 months.
3. Sean Gallagher, "How to Blow $6 Billion on a Tech Project: Military's 15-Year Quest for the Perfect Radio is a Blueprint for Failing Big," *ARS Technica*, 18 June 2012, http://arstechnica.com/information-technology/2012/06/how-to-blow-6-billion-on-a-tech-project/1/.
4. Joint Publication (JP) 6-1, *Joint Electromagnetic Spectrum Management Operations*, 20 March 2012, II-1.
5. JP 3-0, *Joint Operations*, 11 August 2011, V-48.
6. JP 6-1, *Joint Electromagnetic Spectrum*, I-10.
7. Ibid., I-9.

8. Sydney J. Freedberg Jr., "US Has Lost Dominance in Electromagnetic Spectrum': Shaffer," *Breaking Defense*, 3 September 2014.

9. DOD, *DOD Electromagnetic Spectrum Policy 2013*, Washington, DC: Deputy Secretary of Defense, September 2013, 3.

10. Coleman Bazelon and Giulia McHenry, *Mobile Broadband Spectrum: A Vital Resource for the U.S. Economy*, report for the CTIA-The Wireless Association (Cambridge, MA: the Battle Group, 11 May 2015), 2.

11. JP 6-1, *Joint Electromagnetic Spectrum*, I-7.

12. Mobile Internet penetration is the number of mobile devices connecting to the Internet divided by the population.

13. Michael Kende, *Global Internet Report 2015: Mobile Evolution and Development of the Internet* (Washington, DC: Internet Society, 2015), 44.

14. Google and Facebook have both publicly stated an intent to bring global free Internet access. Google has invested billions in satellite and balloon technology alone.

15. A video explaining cognitive radio capabilities from the Nokia Research Center, https://www.youtube.com/watch?v=20wqZZaXG9o.

16. Joseph Mitola III and Gerald Q. Maguire, Jr., "Cognitive Radio: Making Software Radios More Personal," *IEEE Personal Communications Magazine* 6, no. 4 (August 1999): 13.

17. Simon Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE Journal on Selected Areas in Communication* 23, no. 2 (February 2005): 202.

18. DYSPAN P19001 Working Group, "IEEE Standard Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management," Amendment 1: Addition of New Terms and Associated Definitions, technical report, IEEE, Piscataway, NJ, 2008.

19. Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, Gaithersburg, MD: NIST, September 2011.

20. Kevin L. Jackson, "Army Deploys First DoD Tactical Cloud Computing Node," *Forbes*, 4 April 2011, http://www.forbes.com/sites/kevinjackson/2011/04/04/army-deploys-first-dod-tactical-cloud-computing-node/#1bc226c8679e.

21. A playback attack, also known as a replay attack or man-in-the-middle attack, is a network attack in which a previous transmission is recorded and then played back at a later time to trick a receiver. Even though the message may be encrypted and the attacker doesn't know the keys or passwords, retransmission of valid logon messages may be enough to allow the attacker network access. A Sybil attack, also known as psuedospoofing, is an attack on a reputations system based peer-to-peer networks in which a node creates many false identities to gain a disproportionally large amount of influence over the network. A beacon flood attack is when the attacker generates thousands of counterfeit beacons to make it hard for stations to find legitimate access points.

22. Hunter Scott, "Hacking Wireless Networks of the Future: Security in Cognitive Radio Networks," Defcon 21, 3 August 2003, https://www.youtube.com/watch?v=L-LghSR57Bo.

23. Barack Obama, *Presidential Memorandum: Unleashing the Wireless Broadband Revolution*, Washington, DC: Office of the Press Secretary, White House, 28 June 2010.

24. President's Council of Advisors on Science and Technology (PCAST), *Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth*, Report to the president, Washington, DC: PCAST, 20 July 2012, VI.

25. National Spectrum Consortium, http://www.nationalspectrumconsortium.org/.

26. DOD, *Cloud Computing Strategy*, Washington, DC: Chief Information Officer, July 2012, 2.

27. Ibid., E-2.

28. Scott Maucione, "DoD's Cloud Strategy Hung Up by Budget," *Federal News Radio*, 19 October 2015, http://federalnewsradio.com/defense/2015/10/dod-lays-cloud-adoption-challenges-new-report/.

29. Amber Corrin, "Cloud Providers Wonder what DOD's Strategy Shift Holds for Them," *Federal Times*, 16 December 2014, http://www.federaltimes.com/story/government/omr/dod-cloud/2014/12/02/cloud-providers-wonder-what-dods-strategy-shift-holds-for-them/19800831/.

30. Giulio Douhet, *Command of the Air*, translated by Dino Ferrari, 1998, Air Force History and Museums Program, Washington, DC, accessed 1 November 2015, http://permanent.access.gpo.gov/airforcehistory/www.airforcehistory.hq.af.mil/Publications/fulltext/command_of_the_air.pdf, 30.

Abbreviations

CALA	Caribbean and Latin America
CEE	Central and Eastern Europe
CIO	chief information officer
CRCN	cognitive radio cloud networks
DARPA	Defense Advanced Research Projects Agency
DCGS-A	Distributed Common Ground System-Army
DIL	disconnected, intermittent, and low-bandwidth
DOD	Department of Defense
DSA	dynamic spectrum access
DVAP	Developed Asia Pacific
EMAP	Emerging Asia Pacific
EMOE	electromagnetic operating environment
EMS	electromagnetic spectrum
G/ATOR	ground/air task oriented radar
IaaS	infrastructure as a service
IEEE	Institute of Electrical and Electronics Engineers
ISR	intelligence, surveillance, and reconnaissance
JP	Joint Publication
JRTS	Joint Tactical Radio System
MENA	Middle East and North Africa
MHz	megahertz
NAM	North America
PaaS	platform as a service
OODA	observe, orient, decide, and act
QoS	quality of service
RadioMap	RF mapping
RF	radio frequency
SaaS	software as a service
SDR	software-defined radios
SDS	spectrum-dependent systems
SDS	spectrum-dependent systems

SSA	Sub-Saharan Africa
SSPARC	shared spectrum access for radar and communications
SWaP	size, weight, and power
WE	Western Europe
XG	neXt Generation

Bibliography

Agre, Jonathan R., and Karen D. Gordon. *A Summary of Recent Federal Government Activities to Promote Spectrum Sharing*. Alexandria, VA: Institute for Defense Analyses, 2015.

Bacchus, Roger, Tanim Taher, Kenneth Zdunek, and Dennis Roberson. "Spectrum Utilization Study in Support of Dynamic Spectrum Access for Public Safety." In *Proceedings of New Frontiers in Dynamic Spectrum (DySPAN)*, 2010 Institute of Electrical and Electronics Engineers (IEEE) Symposium. Singapore: IEEE, 6–9 April 2010.

Bazelon, Coleman, and Giulia McHenry. *Mobile Broadband Spectrum: A Vital Resource for the U.S. Economy*. Report for the CTIA-The Wireless Association. Cambridge, MA: the Brattle Group, 11 May 2015.

Clancy, T. Charles, and Nathan Goergen. *Security in Cognitive Radio Networks: Threats and Mitigation*. Study prepared for Laboratory for Telecommunication Sciences (LTS). College Park, MD: US Department of Defense, LTS, 2009.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010.

Corrin, Amber. "Cloud Providers Wonder what DoD's Strategy Shift Holds for Them." *Federal Times*, 16 December 2014. http://www.federaltimes.com/story/government/omr/dod-cloud/2014/12/02/cloud-providers-wonder-what-dods-strategy-shift-holds-for-them/19800831/.

Department of Defense. *Cloud Computing Strategy*. Washington, DC: Chief Information Officer, July 2012.

———. *Electromagnetic Spectrum Policy 2013*. Washington, DC: Deputy Secretary of Defense, September 2013.

Douhet, Giulio. *The Command of the Air*. Translated by Dino Ferrari. Washington, DC: Air Force History and Museums Program, 1998. Accessed 1 November 2015. http://permanent.access.gpo.gov/airforcehistory/www.airforcehistory.hq.af.mil/Publications/fulltext/command_of_the_air.pdf.

DySPAN P19001 Working Group. "IEEE Standard Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management." Amendment 1: Addition of New Terms and Associated Definitions. Technical report, IEEE, Piscataway, NJ, 2008.

Feickert, Andrew. "The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress." Congres-

sional Research Report (CRS) RL 33161. Washington, DC: CRS, 17 November 2005.

Freedberg, Sydney J. Jr., "US Has Lost 'Dominance in Electromagnetic Spectrum': Shaffer" *Breaking Defense*, 3 September 2014. http://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/.

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty First Century Release 3.0*. New York: Picador, 2007.

Gallagher, Sean. "How to Blow $6 Billion on a Tech Project: Military's 15-Year Quest for the Perfect Radio is a Blueprint for Failing Big." *ARS Technica*, 18 June 2012. http://arstechnica.com/information-technology/2012/06/how-to-blow-6-billion-on-a-tech-project/1/.

Ge, Feng, Heshan Lin, Amin Khajeh, C. Jason Chiang, Ahmed M. Eltawil, Charles W. Bostian, Wu-chun Feng, and Ritu Chadha. "Cognitive Radio Rides on the Cloud." In *Proceedings of the IEEE Military Communications Conference*, October–November 2010.

Gordon, John IV, and John Matsumura. *The Army's Role in Overcoming Anti-Access and Area Denial Challenges*. Santa Monica, CA: RAND, 2013.

Haddadin, Osama S., PhD, Senior Technical Fellow, L-3 Communication Systems-West. Interview by the author, 27 January 2016.

Harada, Hiroshi, Ha Nguyen Tran, Homare Murakami, Goh Miyamoto, Kentaro Ishizu, Mikio Hasegawa, Yoshitoshi Murata, Shuzo Kato, Stanislav Filin, Yoshia Saito. "A Software Defined Cognitive Radio System: Cognitive Wireless Cloud." In *IEEE GLOBECOM–IEEE Global Telecommunication Conference*, 2007.

Haykin, Simon. "Cognitive Radio: Brain-Empowered Wireless Communications." *IEEE Journal on Selected Areas in Communication* 23, no. 2 (February 2005): 201–20.

Jackson, Kevin L. "Army Deploys First DoD Tactical Cloud Computing Node." *Forbes*, 4 April 2011. http://www.forbes.com/sites/kevinjackson/2011/04/04/army-deploys-first-dod-tactical-cloud-computing-node/#1bc226c8679e.

Joint Publication 3-0. *Joint Operations*, 11 August 2011.

Joint Publication 6-01. *Joint Electromagnetic Spectrum Management Operations*, 20 March 2012.

Kende, Michael. *Global Internet Report 2015: Mobile Evolution and Development of the Internet*. Washington, DC: Internet Society, 2015.

Ko, Chun-Hsien, Din Hwa Huang, and Sau-Hsuan Wu. "Cooperative Spectrum Sensing in TV White Spaces: When Cognitive Radio Meets Cloud." In *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference*, 10–15 April 2011.

Koerner, Brendan I. "Inside the New Arms Race to Control Bandwidth on the Battlefield." *Wired*, 18 February 2014. http://www.wired.com/2014/02/spectrum-warfare/.

Maucione, Scott. "DoD's Cloud Strategy Hung Up by Budget, Contract Limitations." *Federal News Radio*, 19 October 2015. http://federalnewsradio.com/defense/2015/10/dod-lays-cloud-adoption-challenges-new-report/.

Mell, Peter, and Timothy Grance. *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology (NIST) Special Publication 800-145. Gaithersburg, MD: NIST, September 2011.

Mitola, Joseph III, and Gerald Q. Maguire, Jr., "Cognitive Radio: Making software radios more personal," *IEEE Personal Communications Magazine* 6, no. 4 (August 1999): 13–18.

Obama, Barack. *Presidential Memorandum: Expanding America's Leadership in Wireless Innovation*. Washington, DC: Office of the Press Secretary, The White House, 14 June 2013.

———. *Presidential Memorandum: Unleashing the Wireless Broadband Revolution*. Washington, DC: Office of the Press Secretary, The White House, 28 June 2010.

President's Council of Advisors on Science and Technology (PCAST). "Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth." Report to the President. Washington, DC: PCAST, 20 July 2012.

Rizvi, Syed, Nathan Showan, and John Mitchell. "Analyzing the Integration of Cognitive Radio and Cloud Computing for Secure Networking." Publication 5. San Jose, CA: Complex Adaptive Systems, November 2015.

Scott, Hunter. "Hacking Wireless Networks of the Future: Security in Cognitive Radio Networks." Defcon 21. 3 August 2003. https://www.youtube.com/watch?v=9zTaIEHU7pU.

Tangredi, Sam J. *Anti-Access Warfare: Countering A2/AD Strategies*. Annapolis, MD: Naval Institute Press, 2013.

US Joint Chiefs of Staff (JCS). *Capstone Concept for Joint Operations: Joint Force 2020*. Washington, DC: JCS, 10 September 2012.

———. *Joint Concept for Entry Operations (JCEO)*. Washington, DC: JCS, 7 April 2014.

———. *Joint Operational Access Concept (JOAC)*. Washington, DC: JCS, 17 January 2012.

AIR UNIVERSITY PRESS

https://www.airuniversity.af.edu/AUPress/