AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

# COGNITIVE RADIO CLOUD NETWORKS: ASSURED ACCESS IN THE FUTURE ELECTROMAGNETIC OPERATING ENVIRONMENT

by

Lawrence O. Jones, Major, United States Marine Corps

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Mr. Allen Peck, Lieutenant General, USAF (retired)

4 April 2016

## DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

**Abstract**

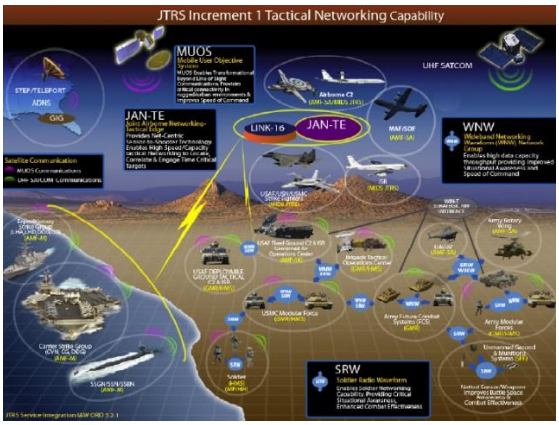
The electromagnetic spectrum is a finite resource that is critical to the United States military's ability to gain superiority in the other five warfighting domains. The Department of Defense's electromagnetic strategy is spectrum access when and where needed to achieve mission success. The future electromagnetic 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. 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: Cognitive Radio Cloud Networks.

# Contents

## 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 resulting system is known as the Joint Tactical Radio System (JTRS). After 19 years, upwards of $17 billion and three operational requirement document (ORD) revisions, the Multifunctional Information Distribution System (MIDS) JTRS and JTRS Handheld, Manpack & Small Form Fit (HMS) are the only full rate production radios to be produced. The JTRS Ground Mobile Radio (GMR) was cancelled in 2011 and although certified for use; it was never used due to poor performance and obsolete hardware.

JTRS was, at its time of conception in 1997, a truly radical idea. Software Defined Radios (SDRs) were mostly theoretical then. WiFi, 3G, and 4G networks did not exist. The DoD was, with a 10-year plan, being aggressive. What the DoD failed to consider however, was the exponential acceleration of computing technology articulated in Moore's Law. The commercial sector, embracing Moore's Law continued to develop cheaper, limited-function digital radios that were able to embrace the ever increasing processing power from smaller, faster microchips.[2] Soon the commercial sector's radios began to exceed the original capability requirements of JTRS, introducing requirements creep, and beginning 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 it is 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 has shared interest in a viable solution, since they share the same problem set. It will now be up to the DoD to help develop not only an innovative solution to the problem, but an innovative way to match the procurement and development cycle of the commercial sector.

## Thesis

Cognitive Radio Cloud Networks (CRCNs) will assure the Department of Defense (DOD) is capable of gaining and maintaining spectrum access and network connectivity in order to gain a decisive warfighting 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 cyberspace domain, all Department of Defense (DOD) joint functions are enabled by spectrum-dependent systems (SDSs) that are currently vulnerable. The challenge of conducting Joint Electromagnetic Spectrum Operations (JEMSO) and assuring access in the future operating environment is that the EMS will be simultaneously heavily congested from civilian use and heavily contested by adversarial action. This research paper will define the problems facing the DOD in the 2035 electromagnetic operating environment (EMOE), argue CRCNs are the most feasible option for the DOD to solve those challenges, and assess the future research and development collaboration potential of CRCNs.

## The Problem

Assured access to the EMS will be the most crucial and challenging endeavor the DOD will undertake in preparation for the battlefield of 2035. The EMS is a finite resource shared by all nations, but regulated individually to ensure their sovereign right to its unlimited use.[3] As a result it not only will be contested by the adversary, but will be congested by civilian and commercial usage. Add an ever-growing DOD bandwidth requirement, and the complexity of maneuvering through the Electromagnetic Operating Environment (EMOE) to accomplish the mission is daunting. Figure 1 is a visual depiction of EMS constraints.

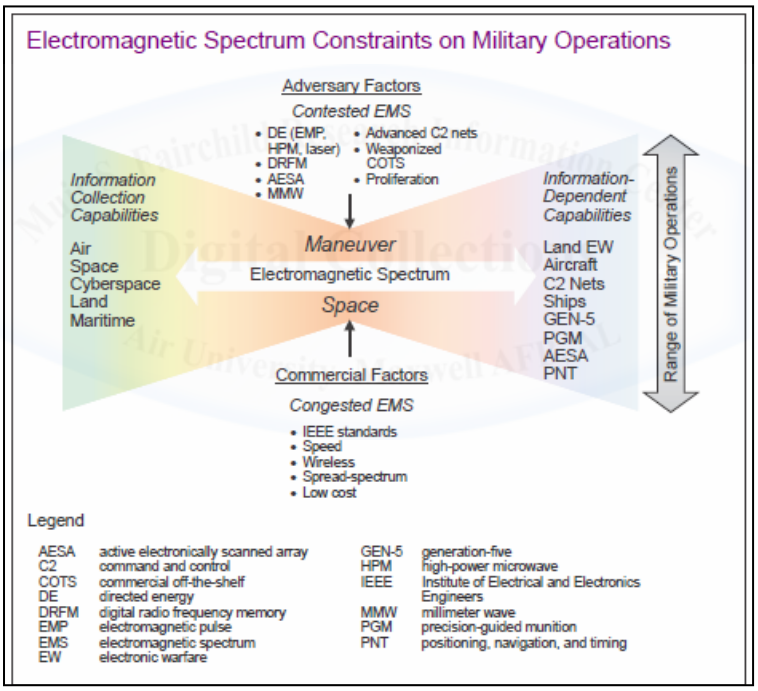



**Figure 1 Constraint on the EMS**[4]

Operationally, the EMS is the physical medium in which military forces must have assured access in order to gain superiority in the physical domains. Joint Publication 3-0 *Joint Operations* states, "Control of the EM environment must be achieved early to support freedom of action. This control is important for superiority across the physical domains and information

environment."[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"[6] is an analog method that does not even take advantage of already decade-old commercial digital technology for sharing or reuse.

**Contested**

It was the overwhelming success of Operation Desert Storm that created the blueprint for how the DOD would posture and procure its systems to fight wars into the 21st 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 ISR and command and control systems to digitally link the battle space. Over the next few decades, the trend continued to produce more spectrum-dependent systems (SDSs) and buzzwords like 'network centric warfare' became in 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 (EMPs) that can range several hundred kilometers or high-altitude electromagnetic pulses (HEMP) that can affect a continent-sized area. [7]

By 2035 however, it will not be just the peer/near-peer nations that can contest the DOD's access to the EMS. Moore's Law[8] has driven a global shift from analog to digital technologies resulting in proliferation of high-power, low-cost commercial products. Small countries and insurgencies are now able to 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 (ComDef) 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."[9] 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.

> The adversary will deliberately attempt to degrade friendly use of the electromagnetic spectrum, to include disruption of space and cyber systems. Due to heavy joint reliance on advanced communications systems, such an attack will be a central element of any enemy antiaccess/area-denial strategy, requiring a higher degree of protection for friendly command and control systems.
>
> - Joint Operational Access Concept 2012

Peer nations in 2035 may not attempt brute force denial as forecasted by the JOAC (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 in order 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. Therefore military power has, to an extent, been marginalized in favor of assuring growth in the economic sector. As stated in the *Department of Defense Electromagnetic Spectrum Strategy*, "In June 2010, President Obama directed the National Tele-communications and Information Administration (NTIA) to work with the FCC to 'make available a total of 500 MHz of federal and non-federal spectrum over the next 10 years, suitable for both mobile and fixed wireless broadband use.'"[10] As a result, in 2013, 645MHz (including 95MHz 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 alone, with every dollar having a $2.32 return. This accounted for 1% of the US GDP.[11] Other nations have followed the United States lead based on the economic growth potential.

Doctrinally, the Geographic Combatant Commanders (GCC) are responsible for coordination of spectrum access within all nations inside his Area of Responsibility (AOR). Confounding the task is that there are very few regional standards with spectrum allocation, as each host nation has allocated different spectrum inside of their borders. When each nation re-appropriates spectrum to meet internal demands, the ever-narrowing bands of spectrum available to the DOD no longer overlap. Noncompliance with the shrinking available spectrum may be

considered a violation of international treaties or laws resulting in the Joint Force Commander (JFC) being held criminally or financially liable.[12]

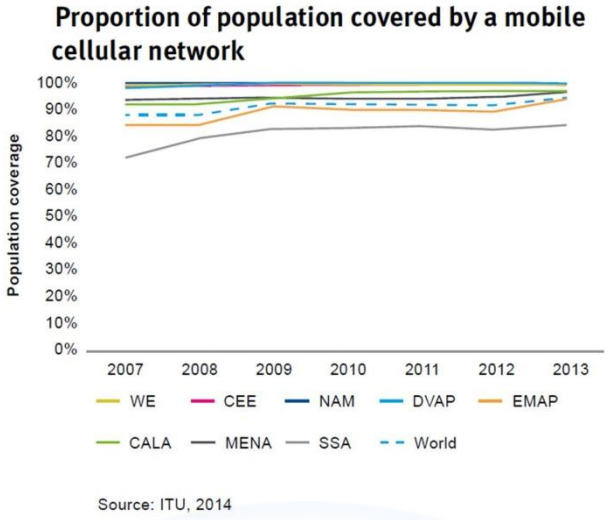


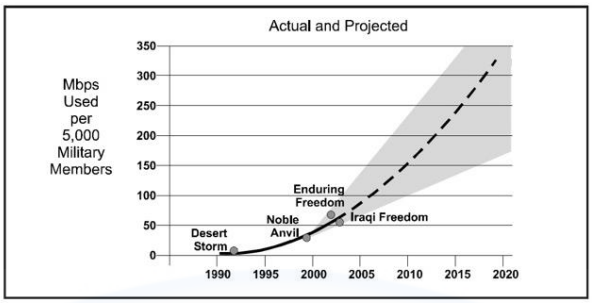

**Figure 2**[13]

The heart of the economic expansion of the EMS has been the mobile computing boom. In 2013, global mobile internet penetration[14] was 28%; by 2019 it is forecasted to be 71%. The Asia-Pacific region is already above 100% with North America, Western Europe, and Central and Latin America exceeding 100% by 2017.[15] With over 90% of the world's population already covered by a mobile cellular network (see figure 2) and companies like Google and Facebook[16] attempting to bring free internet access to under developed countries, it is fair to project by 2035 global mobile internet penetration will likely be exceeding 100%. Nations are likely to continue to meet the economical demands of spectrum at the expense of the military.

**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 (COP) or Common Tactical Picture (CTP). 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 (figure 3).




**DoD Spectrum Requirements are Changing and Increasing**

**Figure 3**[17]

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 (UAS), 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.[18]

**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, described intelligent, self and environmentally aware radios that autonomously made decisions through model-based reasoning.[19] 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 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.."[20] When compared to the DoD Strategy (figure 4), the objectives are the same.


**Figure 4 DoD Electromagnetic Spectrum Strategy[21]**

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 (figure 5). 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.

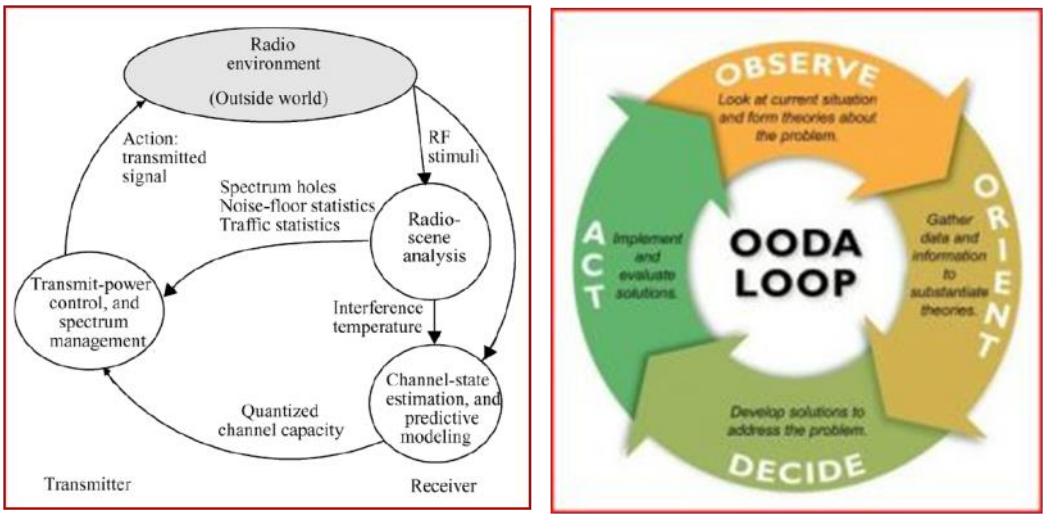



**Figure 5 Haykin's Cognitive Radio (left) and Boyd's OODA Loop (right)**

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." [22] In order to manage priority, DSA recognizes primary users and secondary users (also referred to as licensed and unlicensed). Primary users have priority inside their band, but if they are not using it, then secondary users may use the "white space" to transmit. In essence, think of DSA as a game of hopscotch (figure 6) through

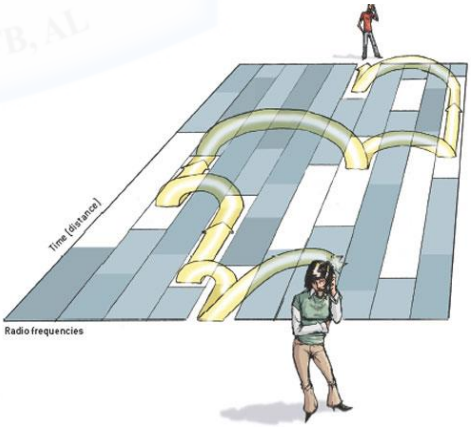



**Figure 6 Dynamic Spectrum Access**

the radio traffic in the ESM. The objective is to reach the other side and you must avoid the space where your beanbags (primary users) are.

In a contested environment, cognitive radios have the potential to bring to the battlefield the ability to communicate through active jamming 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 it uses. As an example, a strobe light that is turning off and on at 120 times a second would, to the human eye, appear to simply be a normal lightbulb that is turned on. The truth of the matter is that 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 first determine at what hertz the light bulb was operating by sensing the environment. 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 off time of the light while actively assuring QoS through its feedback loop.

**Cloud Computing**

The National Institute of Standardization and Technology (NIST) 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."[23] Companies like Google and Apple use cloud computing to off-

board tasks that require more processing power than the standard handheld device internally has. Services like Voice-to-Text, Google Maps, and Gmail are all processed in the cloud. Your device only has to upload and download the data. This reduces storage, processing power, and energy requirements to your 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). With SaaS, the user is able to use the provider's software on a cloud infrastructure. There is no need to download the application onto the user's machine, only a portal application like email. 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 United States Army deployed the first DoD tactical cloud computing node in 2011. The Distributed Common Ground System-Army (DCGS-A) Version 3 (figure 7) was deployed to Afghanistan in response to Army Maj. Gen. Michael Flynn's joint urgent operational need statement.[24] The capability need was for the compilation of vast amounts of historical data on improvised explosive devices (IED) locations to create a predictive tool for protecting logistics routs. DCGS-A had to tie in ISR assets with an exploitation tool directed at the end user. This was possible due to the permissive and uncongested environment in Afghanistan along with the massive communication network assuring access to the cloud.

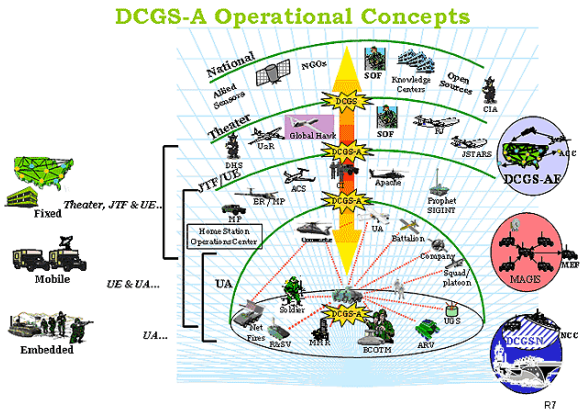
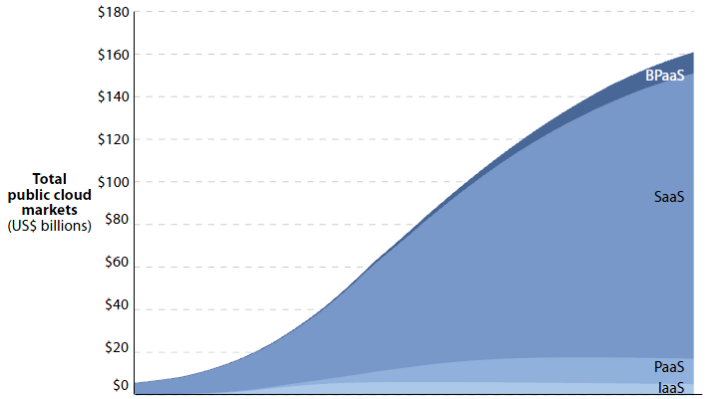



**Figure 7 Distributed Common Ground System - Army**

Over the next 20 years, cloud computing will become the backbone of the commercial market. As depicted in figure 8, the market of the public cloud alone is expected to reach $160 billion by 2020. 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 (VEO) will have access to massive computing power to which only large nations previously enjoyed. Additionally, with more services moving to the cloud, the congestion of the EMS will only become more exacerbated.




| | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BPaaS ($) | 0.15 | 0.23 | 0.35 | 0.53 | 0.80 | 1.26 | 1.95 | 2.93 | 4.28 | 6.00 | 7.66 | 9.08 | 10.02 |
| SaaS ($) | 5.56 | 8.09 | 13.40 | 21.21 | 33.09 | 47.22 | 63.19 | 78.43 | 92.75 | 105.49 | 116.39 | 125.52 | 132.57 |
| PaaS ($) | 0.05 | 0.12 | 0.31 | 0.82 | 2.08 | 4.38 | 7.39 | 9.80 | 11.26 | 11.94 | 12.15 | 12.10 | 11.91 |
| IaaS ($) | 0.06 | 0.24 | 1.02 | 2.94 | 4.99 | 5.75 | 5.89 | 5.82 | 5.65 | 5.45 | 5.23 | 5.01 | 4.78 |

58161 Source: Forrester Research, Inc.

**Figure 8 Global Public Cloud Market Size Forecast, 2011-2020[25]**

**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 it would need to conduct its cognitive function. That however, is not realistic. Cognitive radios, especially battery powered, man-portable versions, need to off load the processing requirements of the cognitive functions in order 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 in the event 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. Cloud computing 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 are able to manage QoS and enforce rules for the sharing of high bandwidth requests like full motion video (FMV). 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 (DoS) and distributed denial of service (DDoS) attacks. Losing the cloud, or the cloud providing erroneous information to the cognitive radios, could cause them to operate poorly. Distributing the clouds as previously discussed 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[26], Sybil attacks[27] or beacon flood attacks[28]. While many of these security challenges are theoretical due to cognitive radios currently being in their infancy, it serves to highlight they are still potentially susceptible.[29]

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 June 28, 2010, President Obama released a presidential memorandum titled *Unleashing the Wireless Broadband Revolution*. In this document 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.[30] Two years later, the President's Council of Advisors on Science and Technology (PCAST) 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."[31] In 2013, President Obama released a presidential memorandum titled *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), who had done some early work with cognitive radios and DSA with neXt Generation (XG) project, began a series of new projects. In 2012 DARPA began Advanced RF Mapping (RadioMap), and in 2013 it followed with Shared Spectrum Access for Radar and Communications (SSPARC). In 2014, DARPA offered the Spectrum Challenge offering a $150,000 reward to the winner. More impressively, in 2015 the DoD created the National Spectrum Consortium[32] entering into a five-year, $1.25 billion deal to exploit emerging capabilities and prototypes that assist in improved electromagnetic spectrum awareness, sharing, and use.



**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."[33] 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.[34] However, due to budget cuts and issues with acquisition strategies (contract vehicles) the procurement is slowing down.[35] In 2014, the DoD CIO rescinded the memorandum naming DISA as the manager of the Cloud and instead moved it to the services.[36] 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 while not helpful, 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 United States 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 they will continue to develop innovative solutions to similar problem sets, the DoD acquisitions process will need to evolve in order to work with the rapidly growing commercial sector. Low-level insurgents already have more networking capability with their smart phones than American forces deploy with. 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's 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 new processes to interact. To quote Douhet, "Victory smiles upon those who anticipate the changes in the character of war, not upon those that adapt themselves after the changes occur."[37] The DoD cannot afford another JTRS program.

## NOTES

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] Definition pulled from US Army informational portal http://www.army.mil/aps/06/maindocument/infopapers/J-28.html.
[2] Gallagher, *How to blow $6 billion on a tech project*.
[3] JP 6-1, II-1.
[4] JP 6-1, I-2.
[5] JP3-0, V-48.
[6] JP 6-1, I-10.
[7] JP 6-1, I-9.
[8] 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.
[9] Freedberg Jr, *US has Lost Dominance in Electromagnetic Spectrum*.
[10] DOD Electromagnetic Spectrum Strategy, 3.
[11] Bazelon, *Mobile Broadband Spectrum,* 2.
[12] JP 6-1, I-7.
[13] Kende, *Global Internet Report,* 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; EMAP=Emerging Asia Pacific
[14] Mobile Internet penetration is the number of mobile devices connecting to the internet divided by the population.
[15] Kende, *Global Internet Report,* 44.
[16] Google and Facebook have both publically stated an intent to bring global free internet access. Google has invested $billions in satellite and balloon technology alone.
[17] DOD Electromagnetic Spectrum Strategy, 3.
[18] Follow the hyperlink for video explaining cognitive radio capabilities from the Nokia Research Center. https://www.youtube.com/watch?v=20wqZZaXG9o
[19] Mitola, *Cognitive Radio,* 13.
[20] Haykin, Cognitive Radio, 202.
[21] DOD Electromagnetic Spectrum Strategy, 9.
[22] 1900.1a-2012 - 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.
[23] Mell, *The NIST Definition of Cloud Computing*.
[24] Jackson, *Army Deploys First DoD Tactical Cloud Computing Node*.
[25] The global cloud computing market will grow from a $40.7 billion in 2011 to $241 billion in 2020, according to Forrester Research. 22 Apr 2011.
[26] 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 reciever. 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.
[27] 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.
[28] A beacon flood attack is when the attacker generates thousands of counterfeit beacons to make it hard for stations to find legitimate access points.

[29] Click on the following link for a video on the potential vulnerabilities of cognitive radios: https://www.youtube.com/watch?v=L-LghSR57Bo
[30] Obama, *Presidential Memorandum: Unleashing the Wireless Broadband Revolution*.
[31] PCAST, *Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth* VI
[32] http://www.nationalspectrumconsortium.org/
[33] Department of Defense Chief Information Officer Cloud Computing Strategy, 2.
[34] Department of Defense Chief Information Officer Cloud Computing Strategy, E-2.
[35] Maucione*, DoD's cloud strategy hung up by budget*.
[36] Corrin, *Cloud providers wonder what DoD's strategy shift holds for them*.
[37] Douhet, 30.

## 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*. IEEE DySPAN, 2010.

Bazelon, Coleman and Giulia McHenry. *Mobile Broadband Spectrum: A Vital Resource for the U.S. Economy*. Prepared for CITA by The Battle Group, 2015.

*Capstone Concept for Joint Operations* (CCJO) 2020, 10 Sep 2012.

Clancy, T. Charles and Nathan Goergen. *Security in Cognitive Radio Networks:Threats and Mitigation.* Study Prepared for Laboratory for Telecommunication Sciences, US Department of Defense, 2009.

Clarke R.A. and Knake R. *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins, 2010.

Corrin, Amber. "Cloud providers wonder what DoD's strategy shift holds for them." *Federal Times*. 16 Dec 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 Chief Information Officer Cloud Computing Strategy*, July 2012.

*Department of Defense Electromagnetic Spectrum Policy 2013*, September 2013.

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

Feickert, Andrew. *The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS):Issues for Congress*. November 17, 2005.

Freedberg Jr, Sydney J. "US Has Lost 'Dominance In Electromagnetic Spectrum': Shaffer" *Breaking Defense*. 03 Sep 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, NY: 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 Jun 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*. The 2010 Military Communications Conference, 2010.

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

Haddadin, Osama S., Ph.D. (Senior Technical Fellow, L-3 Communication Systems-West), interview by the author, 27 January 2016.

Harada1, 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*, IEEE GLOBECOM, 2007.

Haykin, Simon. *Cognitive Radio: Brain-Empowered Wireless Communications*. IEEE Journal on Selected Areas in Communication, VOL. 23, NO. 2, Feb 2005.

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

*Joint Concept for Entry Operations (JCEO)*, 7 Apr 2014.

*Joint Operational Access Concept (JOAC)*, 17 Jan 2012.

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

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

Kende, Michael. *Global Internet Report 2015: Mobile Evolution and Development of the Internet*. 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*. IEEE INFOCOM, 2011.

Koerner, Brendan I. "Inside the New Arms Race to Control Bandwidth on the Battlefield." *Wired*. 18 Feb 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 Oct 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*. NIST Special Publication 800-145, September 2011.

Mitola III, J. and G. Q. Maguire, Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications Magazine*, vol. 6, nr. 4, pp. 13–18, Aug. 1999

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

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

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

Rizvi, Syed , Nathan Showan, and John Mitchell. *Analyzing the Integration of Cognitive Radio and Cloud Computing for Secure Networking*. Complex Adaptive Systems, Publication 5, The Authors, 2015.

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