[H.A.S.C. No. 117–12]

DEPARTMENT OF DEFENSE ELECTROMAGNETIC SPECTRUM OPERATIONS: CHALLENGES AND OPPORTUNITIES IN THE INVISIBLE BATTLESPACE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
MARCH 19, 2021

U.S. GOVERNMENT PUBLISHING OFFICE
44–411 WASHINGTON : 2021

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
SETH MOULTON, Massachusetts
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania, *Vice Chair*
JASON CROW, Colorado
ELISSA SLOTKIN, Michigan
VERONICA ESCOBAR, Texas
JOSEPH D. MORELLE, New York

ELISE M. STEFANIK, New York
MO BROOKS, Alabama
MIKE GALLAGHER, Wisconsin
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
STEPHANIE I. BICE, Oklahoma
C. SCOTT FRANKLIN, Florida
BLAKE D. MOORE, Utah
PAT FALLON, Texas

TROY NIENBERG, *Professional Staff Member*
CHRIS VIESON, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

DEPARTMENT OF DEFENSE ELECTROMAGNETIC SPECTRUM OPERATIONS: CHALLENGES AND OPPORTUNITIES IN THE INVISIBLE BATTLESPACE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS,
Washington, DC, Friday, March 19, 2021.

The subcommittee met, pursuant to call, at 3:00 p.m., via Webex, Hon. James R. Langevin (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. LANGEVIN. Good afternoon, everyone. The Subcommittee on Cyber, Innovative Technologies, and Information Systems will come to order.

I want to thank our witnesses for being with us today. I am looking forward to their testimony.

I am going to give an opening statement in just a minute and then yield to the ranking member for her opening statement, but before we do, I just have to read some technical information for members, including myself, who are joining remotely by video.

So, with that, I would like to welcome the members who are joining today's remote hearing. Members who are joining must be visible on screen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting.

Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a member experiences technical difficulties, they should contact the committee staff for assistance.

Video of members' participation will be broadcast via the television internet feeds.

Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding.

Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave the video function on. If members will

be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and then rejoin if they return.

Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

So, with that, I am going to begin my opening statement, as I said, then yield to the ranking member.

But I want to welcome everyone to our hearing today on the Department of Defense's electromagnetic spectrum operations. I want to thank Ranking Member Stefanik for joining me in holding this hearing today.

And I would like to recognize also my good friend and colleague on the CITI [Cyber, Innovative Technologies, and Information Systems] Subcommittee, Representative Larsen, for his leadership on this issue as co-chair of the Electromagnetic Warfare Working Group, along with his fellow co-chairs, Representative Austin Scott and Don Bacon. And I am proud to be a co-chair with them as well.

I also want to thank our witnesses, of course, for appearing today. Today we welcome Mr. Bryan Clark, senior fellow and director of the Center for Defense Concepts and Technology at the Hudson Institute; also, Dr. William "Bill" Conley, former Director for Electronic Warfare in the Office of the Secretary of Defense; and Dr. Joseph "Joe" Kirschbaum, Director of the Government Accountability Office Defense Capabilities and Management Team.

Thank you all for appearing today.

The electromagnetic spectrum underpins nearly every aspect of the modern U.S. military, and, as co-chair of the Electromagnetic Warfare Working Group, I have long recognized its importance.

The Department uses the electromagnetic spectrum for situational awareness, communicating with friendly forces, identifying enemy capabilities, directing strikes, navigation, and countless other tasks. In fact, nearly every U.S. military capability, from airplanes to night vision goggles, satellites, ships, and radios, depend on the spectrum to function. And they depend on it today. This isn't just something in the future. This is something they depend on today.

While previous CITI hearings covered what lies ahead in defense, again, the military is facing unseen challenges in the electromagnetic spectrum right now. Many of the United States most important weapons systems, like the F–35 or *Ford*-class aircraft carrier, are at a disadvantage today without uncompromised access to the electromagnetic spectrum.

So this challenge and the importance of electromagnetic spectrum operations will only grow as emerging technologies like autonomous weapons, connected battle networks, artificial intelligence, and directed energy continue to fundamentally change warfare. Future combat will be less about the capability of individual weapons systems and more about how a networked system of systems communicate and work together through the use of the electromagnetic spectrum.

Seeing this trend, competitor nations like China and Russia are developing their own capabilities to dominate this domain and connect their forces. These governments believe the electromagnetic spectrum represents a potential critical vulnerability for the U.S. military which they can exploit to reduce our advantage and the efficacy of our high-end weapon systems.

Recent cases in the field speak to this. Russia has conducted electronic attacks against U.S. coalition forces in Syria. And, in 2018, then-U.S. Special Operations Command head General Raymond Thomas called it, and I quote, "the most aggressive electronic warfare environment on the planet from our adversaries," end quote.

So we saw similar activity in Ukraine when the Russians launched surprise artillery strikes using signals emanating from Ukrainian troops' cell phones. There are also alarming reports of directed-energy incidents targeting U.S. Government personnel, producing extremely concerning bio-effects, a phenomenon known as Havana syndrome.

So Congress and the Department have, therefore, undertaken significant efforts recently to position and equip the U.S. military for success. I want to recognize the progress the Department and the military services have made furthering these efforts. However, we have more work to do to ensure that the United States maintains its advantage and closes the gap where we have lost our edge.

As the Department modernizes its systems and capabilities, it must ensure that both new and existing platforms are networked together in a joint environment. To do so, we need to develop the right management structures, strategy, and resources at the Department of Defense. And I know our witnesses will have much insight into how to accomplish these objectives.

So, with that, I look forward to hearing from our expert panel, but first I will turn to the ranking member, Ranking Member Stefanik, for her remarks.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 31.]

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Ms. STEFANIK. Thank you, Chairman Langevin. And thank you to our witnesses today.

The electromagnetic spectrum is, quote, "the invisible battlefield," end quote, and a domain in which the U.S. military's success depends. However, our dominance in this domain is no longer secure. The Department of Defense's Electromagnetic Spectrum Superiority Strategy lays out a path to reassert our overmatch within the electromagnetic operating environment while also recognizing the important evolution of private-sector spectrum use.

As the Department's strategy points out, this new dynamic in the spectrum environment will present opportunities as well as challenges. However, the strategy is clear in its goal: "freedom of action in the electromagnetic spectrum at the time, place, and parameters

of our choosing." This is a requirement for the continuation of our operations in any domain.

It is difficult to understate the importance and range of spectrum operations undertaken by the Department. From critical command, control, and communications to electronic warfare and weapons guidance, the ability to operate in spectrum is an existential capability for our Armed Forces.

Yet spectrum is a finite resource that has become a congested, constrained, and contested environment. Actions by other countries and their militaries, the private sector and their operations, and various regulations all restrict our military's ability to operate within spectrum.

It is within this framework that Congress and the Department must take concentrated steps to stay ahead of our adversaries and innovate new technologies to achieve the goals of the strategy.

One of the most concerning threats is our adversaries' decades of studying our reliance on spectrum to conduct every aspect of military operations. China and Russia, specifically, are testing and developing offensive and defensive capabilities to be used against our systems. All the while, we have failed to transform our own capabilities to stay ahead of these near-peer competitors.

Russia's employment of spectrum operations in 2014 to disrupt their adversary's capabilities in Ukraine and rapidly capture Ukrainian territory should serve as a stark warning of our adversaries' evolving spectrum capabilities.

However, I am encouraged by the Department recognizing this problem, and Congress must be willing to support efforts to boost our competitive advantage as quickly as possible.

We must also find solutions to balance DOD's [Department of Defense's] need to access certain bands of spectrum with the private sector and rural communities' critical need to develop spectrum for modern communications and 5G capabilities.

Our Nation's private sector and civilian access to spectrum correlates directly with our economic competitiveness and, by extension, our national security as well. Our adversaries, especially China, recognize the inextricable link between spectrum development and national power.

Going forward, we will have to determine how to most efficiently and effectively allocate spectrum to ensure both economic prosperity and military superiority. The benefits of correctly balancing these priorities are profound, while the consequences of getting this balance wrong could be disastrous.

With that, Mr. Chairman, I look forward to hearing from our witnesses, and I yield back.

Chairman, I think you are muted.

Mr. LANGEVIN. I am. Thank you very much, Elise.

And I want to thank the ranking member for her remarks, and we will now receive testimony from Mr. Bryan Clark.

Mr. Clark is a senior fellow and director for the Center for Defense Concepts and Technology at the Hudson Institute. He was also the primary author of a review mandated by the 2019 NDAA [National Defense Authorization Act] entitled "Winning the Invisible War," which I am sure we will hear about today.

Mr. Clark, you are now recognized to summarize your testimony for 5 minutes, and we welcome you before the subcommittee today.

STATEMENT OF BRYAN CLARK, SENIOR FELLOW, HUDSON INSTITUTE

Mr. CLARK. Thank you very much, Chairman.

Chairman Langevin, Ranking Member Stefanik, and distinguished members of the committee, thank you for this opportunity to talk about the challenges and opportunities facing U.S. military operations in the electromagnetic spectrum.

As you have noted, the spectrum is arguably the most important environment to modern warfare. It connects nearly every one of our forces together across multiple domains. It is also the mechanism by which almost all of our sensing, navigation, and communication technologies work.

It is also, in a lot of ways, the most unheralded warfighting space, at least within the U.S. defense community. Although we experience the spectrum every day through our smartphones and our mobile computers and the vehicle collision avoidance systems in our cars, in a lot of ways it is a forgotten domain, because we can't feel it like the land or really experience it every time we get on the computer like cyberspace.

So, despite its invisibility, though, access to the electromagnetic spectrum is critical for U.S. forces, who without it wouldn't be able to do the combined arms warfare that they have perfected in a lot of ways over the last century of integrating forces from multiple domains.

America's adversaries, particularly Russia and China, recognize this importance of the spectrum, and, as you noted, they have been aggressively pursuing mechanisms to deny the spectrum to U.S. forces so they can take apart the ability of the battle networks the U.S. military uses to conduct operations, successful operations like we have done in Iraq and Afghanistan or even in Kosovo.

Unfortunately, during the two decades that followed the Cold War, the U.S. largely sat on its hands and let its rivals get a leg up on them in the electromagnetic spectrum. We didn't do a lot of advancements in technologies or operational concepts, and we let them get ahead of us in many ways. So multiple assessments have now argued that the U.S. military in a lot ways is behind its rivals in the electromagnetic spectrum and electromagnetic spectrum technologies, particularly China.

And, at this point, given the timeframe we are looking at—Admiral Davidson just recently talked about there being less than a decade for us to deter China—and our fiscal constraints, we are not going to be able to go and, system versus system, try to match the Russian and Chinese and rest of world's electromagnetic spectrum capabilities. We are going to have to, instead, mount some different kind of efforts to use different operational concepts and different technologies to get a spectrum advantage.

Keeping us back from that, unfortunately, is that, today, about 40 percent of the Pentagon's electromagnetic-warfare-related procurement and research development funding goes to about 10 platform-centric programs that largely perpetuate the Cold War operational approaches that we relied on from 30 years ago, such as

using manned jamming aircraft to confuse sensors that enemies use for air defenses so that we can get a manned bomber in to go attack a target. We still use those tactics even though 30 years ago that was the state of the art; now it may not be.

So we are going to need to have leap-ahead concepts and technologies that can move away from these old concepts and try to mount new approaches that allow us to get an advantage in the spectrum.

So Congress can help in this effort. According to GAO [Government Accountability Office], a series of recent governance changes that were directed by Congress haven't really yielded the benefits in electromagnetic spectrum superiority that we desired. And so, instead of maybe further governance and process changes, Congress should focus now on making sure that DOD pursues the operational concept and technology changes that are going to help it gain an advantage in the spectrum competition with adversaries like Russia and China.

The new Electromagnetic Spectrum Superiority Strategy is a very good part of that. It highlights technology such as adaptable systems, agile network, electromagnetic warfare, and then virtualized training and testing, as well as open architecture systems. All of those are going to be very important to the new operational concepts and technologies that we need to gain an advantage. Section 152 of last year's NDAA also highlighted some of these technologies.

Making those technologies come into fruition, though, is going to require detailed work on the part of Department of Defense, such as is reflected in the implementation plan for the new Electromagnetic Spectrum Superiority Strategy. That implementation plan, though, is going through the Pentagon staffing process and may eventually come out of it and be acted upon, but it needs to be managed by an organization that is able to really make direction and decisions regarding resourcing and operational concept development, such as the JROC [Joint Requirements Oversight Council], as opposed to being staffed out and turned into another Pentagon staffing exercise that doesn't result in real change.

And before I close, I just want to highlight a couple of technology areas that we are going need to focus on. Adaptability is going to be very important, and we can talk about that during the hearing. And then, also, technologies that allow us to be able to maneuver in the spectrum in real time and using AI [artificial intelligence] and cognitive systems to manage that maneuver are going to be very important, which involves electromagnetic battle management and involves the use of new decision support systems for operators.

So we are going have to make a shift in how we manage our operations within the spectrum and move away from traditional methods of controlling the spectrum towards new approaches. If we don't do that, we are going to have our capabilities erode, and we are going to face a situation where our adversaries are going to be able to control the destiny of their warfighting operations and we won't be able to protect our allies or our own interests.

Thank you for your time, and I look forward to your questions.

[The prepared statement of Mr. Clark can be found in the Appendix on page 34.]

Mr. LANGEVIN. Very good. Thank you, Mr. Clark. I appreciate your testimony and for being here today.

We will now hear from Dr. Bill Conley. Dr. Conley is appearing in his personal capacity today, though he was previously the Director of Electronic Warfare in the Office of the Secretary of Defense. He is now a senior vice president and chief technology officer of Mercury Systems.

Dr. Conley, thank you for being here. I appreciate your work in this area for many years, and, again, thank you for being here. You are now recognized for 5 minutes to summarize your testimony.

STATEMENT OF WILLIAM "BILL" CONLEY, FORMER DIRECTOR FOR ELECTRONIC WARFARE, OFFICE OF THE SECRETARY OF DEFENSE

Dr. CONLEY. Chairman Langevin, Ranking Member Stefanik, distinguished members of the committee, I thank you for the opportunity to appear today in a personal capacity. This is my first appearance as an individual expert, having departed the Pentagon in 2019. I request that my written statement be included in the record.

Two years ago, I performed an analysis between the Chinese state and the United States, particularly comparing the gross domestic products of the economy, of defense spending, and of research and development using a purchase-power ratio comparison. What I found in that is that the Chinese state economy, their gross domestic product, is already 10 percent larger than ours. Fortunately, their R&D [research and development] spending is only 80 percent that of the United States and their military spending is only 60 percent.

Unfortunately, as the size of their economy continues to grow, we should expect their R&D as well as their defense budgets will continue to increase. This is a very different strategic situation than we faced during the Cold War against the Soviet Union. The Soviet Union's economy never approached parity with that that we had in the United States.

I believe the strategic question we are faced with today is this: How do we want to compete?

The United States has largely leveraged our manufacturing capacity as a proxy for military strength. Globally, however, we have transitioned into the information age, in which global leadership is defined by innovation, technology development, and technology adoption as well as integration. Our strategy must reflect this transformation.

Back in 2015, China formed their Strategic Support Force, an equal mix of electronic warfare, cyberspace operations, and space operations. The Chinese Strategic Support Force reports directly to their central military commission as a peer of their Army, Navy, Air Force, as well as their Strategic Rocket Force headquarters. In comparison, the United States has maintained electromagnetic warfare as well as spectrum management as capabilities to achieve a tactical outcome.

Strategy: I would like to spend a couple minutes talking about strategy.

Electromagnetic battle management—the dynamic reconfiguration of our sensors, of our networks, as well as our electromagnetic attacks in real time—may become the preferred way to achieve power projection when compared to the defensive utilization of the electromagnetic spectrum.

As a nation, the United States strategy should be based in innovation and our technology development and our adoption of these innovations for national defense and in the full integration of these innovations into military tactics and operations. Just inventing it is not adequate today. This is a dramatic departure from our platform- and program-centric legacy investment strategy that we have pursued. Instead of viewing capability gaps and shortfalls, EMSO [electromagnetic spectrum operations] can actually create opportunities for us.

Innovation: Where does it come from, what does it mean, and how do we access it?

The National Science Foundation reports that across the United States Government, in totality, accounts for approximately a quarter of our economic investment into research and development. The other three-quarters comes from the private sector. The government should seek to maximum the value of this investment from the commercial sector.

For discussion today, I offer six major recommendations, the first of which is to incentivize R&D investment by commercial companies, particularly for defense applications.

Second, to develop a strategic framework for innovation by both traditional defense contractors as well as nontraditional commercial companies; one size does not fit all in this regard.

Third, to develop policies to share data broadly across our national innovation base, government-furnished information really needs to be available to the entirety of the supply chain to generate the maximum return.

Fourth, any insight, report, or deliverable generated on a government contract or by a government thought leader should be broadly available to those with the need to know to improve our national competitiveness.

Fifth, ensuring a realistic EMSO environment and threat capability—that is, in budgeting, in testing, as well as in training.

Sixth, to establish a strategic offensive EMSO service core function to create an enduring advantage in this space.

In closing, while organization and authority are important, the greatest risk I see today is continuing to apply a legacy strategy to the strategic realities of today.

I again thank you for the opportunity to testify and look forward to your questions.

[The prepared statement of Dr. Conley can be found in the Appendix on page 54.]

Mr. LANGEVIN. Very good, Dr. Conley. Thank you very much.

We will now receive testimony from Dr. Joe Kirschbaum. Dr. Kirschbaum is the Director of the Government Accountability Office Defense Capabilities and Management Team. He was the primary author of a review mandated by the 2020 NDAA entitled "Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority."

Mr. Kirschbaum, thank you for being here. You are now recognized to summarize your testimony for 5 minutes.

STATEMENT OF JOSEPH KIRSCHBAUM, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT TEAM, GOVERNMENT ACCOUNTABILITY OFFICE

Dr. KIRSCHBAUM. Thank you, Mr. Chairman.

Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee, I am pleased to be here today to discuss the vital role the electromagnetic, or EM, spectrum plays in the Department of Defense's military operations.

My testimony today is based on that report that we issued in December 2020 on DOD electromagnetic spectrum operations. It provides information on the EM spectrum's importance to military operations, adversaries' advantages and advances in spectrum capabilities, and the extent to which the DOD is positioned to ensure spectrum superiority.

Now, as my colleagues have pointed out, the EM spectrum is the range of all electromagnetic radiation frequencies. And many technologies, in fact most, that are used on the battlefield use these frequency bands to operate. DOD is dependent on the EM spectrum across all warfighting domains: air, land, sea, space, and cyberspace.

Where warfare from ancient times through much of the industrial age involved strictly line-of-sight operations and weapons, warfare in the information age involves the use and the denial of use of the EM spectrum at all levels of operation. This includes communications, signals intelligence, information systems, command and control, identifying friendly and adversarial forces, targeting support, and implementing self-protection countermeasures.

It is not an exaggeration to say that the ability of our forces to successfully operate anywhere depends on success in the EM spectrum.

It is also important to appreciate that the EM spectrum operations take place in the broader context of the information environment. In this context, cyberspace EMS operations, information operations, and similar activities are all interconnected. This is true in actual war, and it is also true in activities that fall short of the threshold of armed conflict, which is where our primary adversaries seek to operate today.

While the United States focused on counterterrorism operations over the last 20-plus years, China and Russia were working to advance their peer-to-peer military capabilities, and that includes the EM spectrum operations.

Among the advances we have seen in either Russian or Chinese capabilities are the deployment of old and new systems—jammers, small UAVs [unmanned aerial vehicles], et cetera—at the company level; incorporation of other information-related capabilities, such as cyber, psychological warfare; and demonstration that EMS operations have been integrated into a combined arms doctrine and practice.

As part of our work, in addition to interviewing a wide range of defense officials and reviewing original source documents, we re-

viewed some 43 studies about defense electromagnetic spectrum issues.

There was remarkable agreement among those studies on the challenges to DOD's EM spectrum capabilities. These challenges included outdated capabilities themselves, lengthy and disjointed acquisition process, increased spectrum competition and congestion, and gaps in experienced staff and training, realistic training. Many of these studies also agreed with DOD officials that among the chief causes for lack of progress in many of these areas was governance.

DOD issued department-wide electromagnetic spectrum strategies in 2013 and 2017 and published a third strategy in October 2020. We found that DOD had not fully implemented either the 2013 or 2017 strategies. This was not because they were bad strategies—quite the opposite—but, rather, because of bureaucratic and organizational hindrances.

Specifically, DOD did not take action to develop detailed implementation plans, focus leadership on offices and individuals with authority to execute, or create processes to review progress and assess results to ensure that they achieved intended outcomes. Rather than do these things, DOD re-sought and remade each successive strategy. We think this pattern threatens potential success for the 2020 strategy.

In our December report, we made recommendations in each of these areas. DOD generally agreed with our recommendations and told us the Department planned to address many of them in the implementation plan for the 2020 strategy.

In just under 2 weeks, DOD will reach its own 180-day deadline for issuing that implementation plan. We have not yet seen it, but we do look forward to seeing the extent to which DOD takes the kind of actions we identified in December 2020.

In conclusion, DOD's response to our December report shows that officials are well aware of the challenges and opportunities affecting military use of the EM spectrum. Ultimately, by addressing the gaps and challenges noted in our report, DOD would improve its ability to innovate and expand in the way that Mr. Clark and Dr. Conley have mentioned and operate in the spectrum. This is important to achieve the Department's vision of spectrum superiority.

I look forward to continuing to work with you and the Department to help address spectrum challenges and to make the most of its opportunities.

Chairman Langevin, Ranking Member Stefanik, members of the subcommittee, this completes my prepared statement, and I am happy to address any questions you may have.

[The prepared statement of Mr. Kirschbaum can be found in the Appendix on page 64.]

Mr. LANGEVIN. Very good, Dr. Kirschbaum. Thank you very much for your testimony.

And to the panel, greatly appreciate your being here today. I am anxious to get to questions. I am going to defer and go last in the questions. We will get members in who are going to get flights.

And, with that, I am going to yield time first to Mr. Larsen for 5 minutes.

Mr. LARSEN. Yeah. Thank you, Mr. Chair. I appreciate that very much. I have to get out to Dulles Airport, so I appreciate that.

Dr. Kirschbaum, in 2006, 15 years ago, the Electronic Warfare Working Group, at the time it was named, issued a report on EW in the Pentagon that concluded that what needed to happen for focus was that we needed to have leadership, we needed to have a pipeline of training on EW, and we needed to have the research and development budgets that resulted in capabilities.

Can you explain to me how, if I came back, if I was here 15 years from now, that your report, which largely mirrors a report that we wrote 15 years ago, won't say the same thing?

Dr. KIRSCHBAUM. That is a great question. I am hopeful that it won't, for a number of reasons, the first of which is the amount of attention that is paid to this critical issue by you, Chairman Langevin, Ranking Member Stefanik, and people like us, whereas it was much more specialized in those days.

Now, what we see when we interview the people in the Pentagon that are responsible for putting the strategies together, they get it. They understand the critical issues. They understand the impact and the way the operational doctrine needs to change, the way that needs to flow into training, the way that needs to drive innovation.

What happens is, as I alluded to, once those strategies are put out and everyone signs off on them, they go into the normal process. And that normal process is governed by the services, who are responsible for training and equipping forces.

Mr. LARSEN. Right.

Dr. KIRSCHBAUM. They have their priorities. And even though you have broad agreement about that things like EM spectrum cut across all those efforts, when push comes to shove and the dollars get spent, they are not going to achieve——

Mr. LARSEN. Can I stop you there? Because this is a great segue for a question for Mr. Conley, who pointed out the PLA's [People's Liberation Army's] Strategic—or the—yeah, the Strategic Support Force, the SSF. It is actually organized so that cyber and space are on par with the other services, and points out that we don't have that when it comes to EMSO.

So, Mr. Conley, can you address how we can get there and if we can get there? Or do your recommendations even help us get there?

Dr. CONLEY. Right. So what I would offer is, in my opinion, the part that China, with their Strategic Support Force, did in a way that I think is really insightful and could be valuable for us is, first off, the blending of electronic warfare, cyberspace, and space operations as peers and, secondarily, that elevation to say, this is strategically important and we are going to use it to achieve a strategic outcome.

It is the combination of both of those things that I think are really important for operationally what they have been able to do. There is a governance conversation, there is a structure conversation, there is a resourcing conversation. But what they have achieved operationally, I think, is really pretty darn impressive.

Mr. LARSEN. Well, we should find out more about that.

And I want to ask Mr. Clark in my remaining time: I have NAS [Naval Air Station] Whidbey Island in my district. We have the Growlers; we have the jamming pods on those. These are the ex-

pensive platforms that you were talking about that maybe have a—well, they certainly do have a critical function in certain areas but not in other areas.

How should we think about balancing resources that we give to EMSO largely, you know, whether it is a platform like a plane or a platform like a motherboard?

Mr. CLARK. Right. So I think there are a lot of opportunities. There is a lot of great work that has been going on in terms of research and development over the last decade to develop small-form-factor electronic warfare/electromagnetic warfare systems that can go onto UAVs and also the networking to allow networked electronic warfare.

And so what I would see in the future is that the Growler, Prowler now—or Prowler, now Growler——

Mr. LARSEN. Right.

Mr. CLARK [continuing]. Is going to be the quarterback, right? It will be the quarterback for electromagnetic warfare operations.

So it may not be doing a mod [modified] escort jamming operation, where it is going to get in relatively close and jam an air defense radar so that a bomber can go hit a target. It may stand back and be coordinating the actions by both itself and then some expendable UAVs that will go in closer. And some of those are being developed by DOD right now.

But what that means is some of that investment is going to have to shift away from the platform to these other systems.

Mr. LARSEN. All right. Thank you.

Mr. Chairman, thank you very much for yielding me your time at the beginning so I can get to the airport. I very much appreciate that. And I don't yield back, because I have no time to yield back, so I won't be pretentious and say I am going to yield back anything. Thanks a lot.

Mr. LANGEVIN. Very good. And I appreciate your leadership in this area. I know that you take great pride in the work that you have done in working to try to solve this problem. So thank you for your leadership and your expertise that you bring to the table too.

Mr. LARSEN. Thank you.

Mr. LANGEVIN. So thank you. Thank you very much.

I would now recognize the ranking member for 5 minutes.

Ms. STEFANIK. Sir, I will yield to Mr. Moore, who looks like he is in an airport right now.

Blake, do you want to take my 5 minutes for questions?

Mr. MOORE. You know, I am good for another 40 minutes. I am not in any immediate rush. So I am actually okay, if you want to give your opening statements. Thank you, though. I appreciate that. But, yes, I am at the airport, but I am okay for the next 45 minutes.

Ms. STEFANIK. Okay. So I will take back that time if you will yield it back to me.

Mr. MOORE. Yield back.

Ms. STEFANIK. My question is: Mr. Clark, in your report, "The Invisible Battlefield," you and your colleagues provide extensive analysis of China's strategy, operational concepts, and their four stages to achieve electromagnetic spectrum superiority: number one, me-

ticulous planning; number two, multilevel integration; number three, precise release of energy; and, number four, demonstrating effects.

In which of those stages do you believe that China is most effective and which of those stages is the U.S. most vulnerable? And then what are your overall thoughts on China's ability to effectively execute these steps to superiority?

Mr. CLARK. Well, thank you for the question.

So they are very well-positioned to be able to execute these steps. I would say that the ones where they have the most efficacy are the meticulous planning—they have analyzed our battle networks to an exquisite degree of detail, both through clandestine means and because they just look and see what we have available on the open web, to figure out how we are going to put our pieces together to be able to create a set of forces that are going to conduct an operation.

And then they have also done very well at building the specific systems necessary to release the precise energy that is going to disconnect the parts of our battle network away from each other, so to jam our communications, to deceive our sensors. So they have identified what those key nodes are in the force packages that we are going to send downrange so that they can prevent them from being effective.

So they have done very well with those two steps, I would say, in particular, the planning and the release of energy.

The demonstrating of effects I see less from them. I mean, the goal there is to try to deter us by showing that they not only have planned this out but they have figured out how to release the energy in specific ways that can defeat our battle networks.

So they are working on that, and, obviously, we have seen indications of that in the intel world. But they have not done as much of that as I thought they might, given the gray-zone operations they have been pursuing.

Ms. STEFANIK. Thank you.

I will yield back the balance of my time.

Mr. LANGEVIN. Very good.

Next, Ms. Escobar, if you are still there, I will recognize you for 5 minutes.

Ms. ESCOBAR. I am. Thank you so much, Mr. Chairman, not just for this hearing but also for the accommodation that you are making on a Friday fly-home day, especially for those of us who live further away.

And to our panel, thank you so much for your work, your expertise, and your testimonies, which are really informative and helpful.

My questions are for Dr. Conley. And, actually, I really appreciate Dr. Clark's focus on the need to be adaptable and, Dr. Conley, your emphasis on innovation.

One of the many goals of the 2020 electromagnetic spectrum operations strategy under the Defense Department has been to develop new EMS capabilities.

In my home district of El Paso, Texas, the University of Texas at El Paso, or UTEP, has been a leading force in the worldwide revolution of 3D printing. In 2000, the Keck Center and UTEP's

College of Engineering made strategic investments in additive manufacturing technologies in order to assist manufacturers in prototyping parts before investing in costly manufacturing tools needed for production.

Most recently, in 2018, UTEP became the North American base of operations for one of the world's emerging technology leaders in the production of 3D printing equipment.

As you strategically evaluate opportunities to strengthen our EMS capabilities, to what extent would you say there are components and applications of EMS that can be potentially involved with additive manufacturing?

Dr. CONLEY. So I really appreciate that question. As an engineer myself, this is a fascinating and great time to be a practicing engineer in any way, shape, or form. And the reason for saying that is really based around what is happening with the digital transformation and the ability to do a digital design to rapidly prototype—additive manufacturing being exactly one of those capabilities—and the ability to actually not have to prototype and go and exhaustively test it, to then redesign, to then build the actual thing that you want, but to actually take that 3D piece and go and immediately start using it.

And so what I think is really exciting about additive manufacturing are all of the different places it allows us to more rapidly integrate a capability onto a platform and do really well there.

There is one part, though, that I think is really core to our electronic warfare, our electromagnetic warfare, and our EMSO capabilities, which is the microelectronics which underpin them. And for where we are today, additive manufacturing won't solve that part of the problem, but it will solve substantial parts of the problem that we have and, I think, will allow us to go faster more affordably and generate more value.

Ms. ESCOBAR. And, Dr. Conley, just in the time that I have left, just a couple minutes, how do we best utilize that talent, that skill set, that brain power in academia, in these young minds, and connect them to the work that we need to do to innovate and to lead and to demonstrate superiority?

Dr. CONLEY. So one of the things that I mentioned in my opening statement was that ability to broadly and democratically share information and insights that we have. And so I think, in many cases, we have challenges and problems that we actually can expose to the academic community, to students, prior to them joining the workforce, prior to worrying about things like security clearances, and we can actually get them working on problems that really matter.

When you look underneath the hood of our EMSO capabilities today, the vast majority of them are really defined by software-defined radio technology. And these are things that you actually can go ahead and, you know, play with on a college campus and work with the entirety of your time while you are in school and immediately bring that knowledge into being a technology developer in support of our EMSO capabilities and ultimately our national defense with strategic implications.

Ms. ESCOBAR. Thank you so much, Dr. Conley. This is, I think, an exciting area of opportunity for us, one that we definitely need to exploit.

Mr. Chairman, again, thank you so much for accommodating me before I run to the airport. I yield back.

Mr. LANGEVIN. You are very welcome. Glad you got your questions in, and have a safe flight home.

Ms. ESCOBAR. Thank you.

Mr. LANGEVIN. I don't have the list in front of me. I think we are going to go with Mr. Moore next. I am not sure. I don't have the seniority list. They have not sent me that list quite just yet, so I apologize to my colleagues if I am going out of order.

But, Mr. Moore, I will recognize you for 5 minutes.

No? He may be offline.

Ms. STEFANIK. Bice.

Mr. LANGEVIN. Okay. Mrs. Bice is recognized for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman.

And thank you to the witnesses for being here. As a freshman, I am still learning a lot about this particular issue, and so I appreciate you all kind of bringing some historical context to what you have done in the past.

My question is really a twofold question. Mr. Clark and Dr. Conley, you really talked about making a shift in how we manage the spectrum and then also research and development and investment in the future.

Can you talk a little bit or flesh a little bit more out, how do we incentivize young people to want to look at this particular issue? Because it is, in some ways, sort of abstract, right? You can't see it, feel it, touch it. How do you, sort of, explain and understand—or explain and incite someone that may be looking at this to get involved?

And then what do you see on the research front? What do we need? What is the long-term vision for us, trying to figure out what is next on the horizon past electromagnetic spectrum?

Mr. CLARK. Well, I can start, because I think Dr. Conley is going to have a lot more to say on this subject than I do.

But I will say, I think one of the most important things is to make an area, a technology area, exciting for people to want to go into. Today, electrical engineering in a lot of cases means computer engineering, and back when I was in college, it meant actually dealing with, you know, circuits and wires and stuff.

So I think that part of it is shifting people's focus to think of this as an exciting area of research. And one of the ways to do that is this focus on adaptable, cognitive systems that are AI-enabled—basically, taking advantage of the virtualization that is happening in machines to begin to use our electromagnetic spectrum systems more like virtualized computer-type systems, where they are able to adapt in real time to an adversary's emission, create new techniques and new waveforms in real time to be able to defeat those jamming effects or to create a new communications link with another platform.

So that kind of merging of the software and the hardware worlds, if you will, I think, could be very exciting for people to go into.

And it deals with the problem that I just talked with Member Stefanik about, which is the advent of the Chinese approach to warfare, where they plan meticulously, develop a way to defeat our forces. But then, if we present them something that is much less predictable, because we are using these cognitive and AI-enabled electromagnetic systems, it might defeat that attempt on their part to take apart our battle networks.

So I will turn it over to Dr. Conley.

Mrs. BICE. Thank you.

Dr. CONLEY. Thank you, Mr. Clark.

What I would add is, in my—my own story. I studied nanotechnology when I did my Ph.D. And so nanotechnology intrinsically is, well, nano, something small and therefore something invisible. And so, personally, it was a very easy journey for me into this EMSO community, because I was already used to studying and working on things that, candidly, I couldn't see without using specialized tools. The electromagnetic spectrum, in many ways, is no different.

And building on, you know, Mr. Clark's comments there on the AI side, that ability to expose someone to the most pressing national security challenges for them to understand the impact of what that meant—in my case, it was a radio-controlled improvised explosive device on a roadside in Iraq or Afghanistan and the ability to say, "If we figure out how to defeat this thing, we can save lives," that is motivation to get up and get to go to work in a way that nearly nothing else is.

And so I think there is a lot there that we actually can get, you know, young kids really excited about as soon as they finish college. And so I think there is a great opportunity there.

The second thing that I will offer and one of the really unique things about EMSO is that the rate of technology adoption and the critical nature of it is profound for the implications it has. Bryan and I previously have chatted about this exact topic.

The rate of the innovation of new radar and radar warning receivers during World War II for the identification of German U-boats in the Bay of Biscay, it was a standard period of time of 4 months. And that was seven decades ago now. And it was 4 months from measure to countermeasure. Today, we should expect it to be even faster. You can't do that with a large aircraft, but you can with a software-defined radio capability and implementing EMSO holistically.

Mrs. BICE. And what about the research and development piece? What do you see as far as needs for DOD to invest in this? I think the need is there, but how do you sort of push that to the forefront? And what are we looking at?

Dr. CONLEY. Yep. What I would offer is, it is a mix of what is happening with microelectronics with the ability to use them in a defense application. It is very different when you put a chip in an air-conditioned, climate-controlled environment versus on a military aircraft that shakes when it flies. And so we have to get that part right. There is a lot about the thermal there that is really critical.

And then the other side is, it is really easy to get excited about the digital, but, in reality, there are a lot of really hard analog problems on the radio frequency side—filters, mixers, components

that have to go in—to really be able to get that performance at a level that we want. And every time you start talking about advanced technologies, price almost immediately shows up. And so how do we generate that at a value that we can do in low quantity for defense applications while we get that necessary value out of it?

And so, if I was to offer a couple suggestions for really important problems to work on, I think those would be my top couple.

Mrs. BICE. Great.

Thank you so much, Mr. Chairman. I yield back.

Mr. LANGEVIN. Very good. Thank you, Mrs. Bice.

I think that I am next, unless there is another member on the Democratic side who is on who hasn't been recognized.

But let me start with this. And I know we have touched on this a bit already, but let me just jump into it again and expand on it.

To Mr. Clark or Dr. Conley, I wanted to know, you know, again, further discuss, you know: Is DOD adequately leveraging spectrum to enable future concepts like Multi-Domain Operations, Distributed Maritime Operations, and Joint All-Domain Command and Control? And how will those concepts contribute to future U.S. military operations?

In addition, how do we ensure that both legacy and future capabilities and systems are networked and interoperable among military services?

We can start with Mr. Clark and then go to Dr. Conley.

Mr. CLARK. Thank you, Mr. Chairman.

So, on Joint All-Domain Command and Control, one of the things we are finding in the work that we are doing there is that, in the future, our communication networks are going to not be able to necessarily provide us the command and control relationships we always want. We want to have this very hierarchical command and control team, with somebody in a distant headquarters controlling forces way out in the field. Our networks aren't going to be able to do that against a capable adversary like China.

So, instead, we are going to have to think about adjusting our command and control relationships to accommodate our communications availability, which means we are going to have to be ready to shift the command node to different places at different times depending on what communications are available.

So that is going to reinforce this idea of, we need interoperable forces that are able to quickly mix and match their forces to be able to create force packages that can deliver the right effects at the time. So interoperability will be really important.

And, also, the network flexibility will be very important. So, to get that network flexibility, we need systems that are agile and can move across the spectrum to avoid enemy jamming and then can be able to communicate with one another where they are so they can reconnect their networks in a mesh sort of framework.

So that requires systems that are able to work across a wide range of frequencies and adjust their bandwidth and power levels to minimize their chances of being detected. So agility both in power and in beam width and beam direction and in frequency are going to be necessary.

And then we are going to need to be able to cause those forces to interoperate. So, inside of trying to use gateways to connect a force that uses a Link 16 to a guy who is using a MADL [multifunction advanced datalink] to a guy who using a SADL [situation awareness datalink]—three different communication protocols—we are going to have to use software-defined toolkits, like STITCHES [System-of-Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems], which is a program that DARPA [Defense Advanced Research Projects Agency] developed which builds an interoperable connection between those two networks on the fly. So, instead of having to build a hardware gateway between the two, it will write software in real time to accommodate that connection.

So those are——

Mr. LANGEVIN. Can I——

Mr. CLARK [continuing]. Some of the things they——

Mr. LANGEVIN. Is that something that is exquisite technology that will be DOD, or are there commercial off-the-shelf options that we can adopt and get into the field more quickly?

Mr. CLARK. So the STITCHES and similar programs are DOD systems today. There are some commercial versions of those. We talked about software-defined radios. There is a new version—the new radio that is part of the 5G infrastructure is a software-defined radio that can reprogram its waveforms in real time, if programmed correctly to do that. So there are commercial systems that allow you to reprogram a radio to use a different waveform in real time that could allow a radio to talk to another radio that maybe it wasn't originally designed to work with.

So there are commercial versions of——

Mr. LANGEVIN. Okay.

Mr. CLARK [continuing]. This, because, of course, interoperability is a thing in the commercial world as well.

Mr. LANGEVIN. Great. Thank you.

Dr. Conley.

Dr. CONLEY. Yeah. The one thing that I would add on top of what Mr. Clark said is, with electromagnetic battle management, the integration of that with the multidomain operation, Joint All-Domain Command and Control, the ability to maneuver in and through the electromagnetic spectrum is something that every time that you turn the dial on your radio you actually are doing. You are maneuvering in the electromagnetic spectrum when you do that in the same way that you can move to a different lane on the highway. Your cell phone does that automatically today with all of the different adjustments that are happening underneath the hood.

But for a military commander, the ability to go ahead and not only physically maneuver an aircraft, a ship, a ground unit, but also maneuver in the electromagnetic spectrum in a coordinated scheme is actually what I alluded to in my opening statement: It may be one of the best strategic offensive advantages that we can actually have that will be enduring in a way that I think is really powerful for us. And so that is an area that I personally am really excited about.

Mr. LANGEVIN. Very good. Thank you.

And, Dr. Conley, again, elaborating on this, because I think you touched on this earlier, but, you know, the perspective you can provide on the speed at which DOD adapts and moves to address challenges versus what you have seen in the private sector thus far. How do you think DOD can better incorporate private-sector innovation and talent at scale and speed up its ability to innovate to confront emerging threats and take advantage of opportunities?

Dr. CONLEY. So there are two dramatically different directions I could take the answer. And so, one of which that has been suggested many times is, how do we shorten the planning cycle and how do we allow a new program to start at a faster rate? I am not going to touch on that because I think that that has been discussed substantially by others, but it definitely is one viable option.

The other option is, how can you attract commercial capital into our Nation's defense problems, and how can you go ahead and generate a rate of return that will attract that capital to come into the ecosystem? And I think that we actually can plan that in a way that is much more familiar to those of us that are used to the Federal budgeting process, but we can actually go ahead and set up an ecosystem that allows that to occur.

And so that is what I touched on earlier with that making sure, for both traditional defense contractors as well as nontraditional commercial companies that want to service the defense ecosystem, how do we get the appropriate expectation for the income statement, for the balance sheet, for the cash-flow side to actually make our national security problems an area that they want to work in with a business model that closes.

Mr. LANGEVIN. Very good. I will hold there. Hopefully we will have time for a second round, but I will hold there for now. Thank you for those answers.

Mr. Moore is recognized for 5 minutes.

Mr. MOORE. Thank you, Chairman.

I would like to continue a little bit with what we were discussing a few questions ago. I was intrigued by the concept of how we encourage students and new professionals to get into this.

Workforce development has been something that I continually harp on, and am very frustrated that in my role in Congress I don't know how to fix it, but it is something that I definitely want to be involved with.

Could you speak to anything that can be specifically done to encourage, whether it be on the commercial side, whether it be potential, you know, jobs within the Federal Government, within the DOD, to—what changes will we need to make to our educational institutions to get them so they would be equipped in addressing some of this need and being able to, you know, prepare and produce enough talent that we can, you know, answer the call for the future on this particular issue?

I speak with the—my district is Hill Air Force Base in the First District of Utah, and, you know, they talk to me all the time about how they could hire as many electrical engineers or any type of engineers as would graduate in Utah and still have a need.

What specifics would you foresee—and this question, I will throw it to all of you; thank you for being here. What shift does education need to do to produce this? And is there anything we can do, even

as a committee, to encourage or incentivize potential employers for providing the necessary credentialing or certifications that would be needed?

I will pause there.

Dr. CONLEY. So the first part that I would offer—and there are a lot of facets of this. Unfortunately, it is a complex problem, as you pointed out.

The first part that I would go ahead and emphasize is making sure that we are attracting graduate students and undergraduate students to our universities who ultimately stand a decent chance of going on to work in defense.

When we look at, kind of, where is the biggest segmentation of the pipeline of the total available talent versus those that are interested, I think that is an area that we definitely should consider what would be required to help there. And so I offer that as a data point to you.

The secondary part of it that I would offer is making sure that we are bringing in people with the right skills, the right education, the right background for what type of problem it is that we need. As someone with a Doctor of Philosophy degree, not every problem in the electronic warfare community that I have been able to work on over the years requires a Ph.D., right?

And so, with that in mind, it is, how do we make sure that people are broadly aware of these problems but we get the right problem to the right person's desk for them to work on? And so I think there is a lot that we can do there. As we say, what is the role of industry? What is the role of government? And what type of skill sets do we want, in which different places, to make sure that we do the right thing?

The third part that I would offer—I had a peer in the Pentagon. He and his wife had three children, all of whom went on to work in, basically, the high-tech side of industry on advanced AI, advanced robotics. Despite the fact that he is a Naval Academy grad, none of his three kids are working on defense programs. He and his wife met in the Navy.

And so that is a little bit of a unique opportunity, I think, to say, what is there that culturally we want to do to make sure that we make these types of problems accessible, but what do we also want to do on the business side to attract that kind of talent?

A young graduate that is excited and passionate is looking for a company where they get equity today. If you look at Federal acquisition regulations and you say, "Hey, I would like to go ahead and give a 22-year-old engineer a share of this company," that is not a cost that you actually can go ahead and pass on.

And so I think the question is, how do we get the right business model to drive things to create a culture both in the private and the public sector that really attracts what we want to achieve?

Mr. CLARK. I——

Mr. MOORE. Let me—please, go ahead.

Mr. CLARK. I would add, one of the things we have looked at in the work we have been doing inside the Pentagon has been professionalizing the electromagnetic spectrum operations community, which is not just the military side—so, you know, trying to get the professional development for the military side such that folks in

that world feel like they are developing as technicians or as supervisors and leaders—but also on the civilian side.

And we have done not a great job in the DOD of professionalizing the folks that work in the electromagnetic spectrum operations community on the engineering and the program management side. They feel like they are just kind of a cog in the overall organization, they could be easily interchanged out with somebody else, when, in fact, that is not really true.

So by professionalizing the track, you know, for people coming in to work at the labs, people who come to work at the warfare centers, and they feel like they are entering a professional community that is going to have their back and is going to develop them over time—that is something that DOD has been trying to do and has failed to really pull together. But on the civilian side, if we could do that, it would make the DOD a much more attractive employer to young engineers coming out and looking, potentially, for a long-term—or at least a career for a while.

Mr. MOORE. Let me quickly add in there, this technology is going to change rapidly, in my opinion, almost exponentially. Are we equipped at the DOD level to be able to reskill and upskill our current workforce so they can continually meet the challenge? Or does this have to then—once they have been in the industry 5 years, do they have to go back, do they have to go dig deep into the education world and bring out the new pieces? Are we going to be able to adjust on the fly is my question.

Dr. CONLEY. Absolutely——

Mr. CLARK. I think we could rapidly reskill people. And I will let Bill answer.

Dr. CONLEY. I would offer, I think that we can definitely upskill. And there is a lot of the analog side of the problem, in particular, which is a little bit like art, and it is art meets a lot of science. But you need that artisan that understands the history of why we do things today. And so I think there is a lot that we can do with upskilling the current workforce.

Mr. MOORE. I appreciate it.

Thank you, Chairman. I apologize. I yield back.

Mr. LANGEVIN. No worries. Thank you, Mr. Moore.

Elise, I only had one or two more questions. Are you okay if we go for a second round?

Ms. STEFANIK. Uh-huh. Yes.

Mr. LANGEVIN. Okay. Great.

Dr. Kirschbaum, I know we have kind of talked about this as well, but DOD is now in its third electromagnetic spectrum strategy in 7 years. Based on what the GAO is seeing, is this strategy different from the prior two, and should we expect a different result? What steps can Congress take to ensure positive momentum and implementation?

I know we kind of talked on this at the end of Mr. Larsen's line of questions, but if you want to elaborate.

Dr. KIRSCHBAUM. Well, thank you, Mr. Chairman.

I think, you know, you hit on it rather well—and, first of all, as I said in my opening statement, we are concerned about the direction for the implementation of 2020, because, so far, we have seen a pattern before. So we are concerned about it.

The strategies themselves have definitely recognized a lot of the concepts that my colleagues and I have hit on: the idea that you need to innovate and not just catch up with technology, you need to think of bigger concepts. These strategies themselves have taken aboard some of those ideas. The idea of how we appreciate and understand electromagnetic spectrum and operations today is different than it was just a few years ago, and these strategies incorporate those ideas.

There is also a lot of consideration right now for ideas that are going to make some of the connections, hopefully, in the operational side—how you tie these things together into battle management, how you achieve some of those broader effects. Those kinds of things are going to be critical to glom on to for future. Whether it is the education and motivating people for education we just talked about or whether it is system development, those are all critical to do that.

In order to get there, we have to put the right Department emphasis on achieving those things and making sure that what we are doing, what we are testing, what we are breaking apart, what we are learning lessons from, what we are then going back into experiment with, that is the rhythm and that is the accepted rhythm and that is what we are doing. That is what really needs to be done, and that is what we are looking forward to.

Mr. LANGEVIN. Very good.

If I could, too, given the organizational challenges that you have highlighted today and how these issues impact so many issues across the information environment, including electromagnetic spectrum issues, cybersecurity, cyberspace operations, and information operations, what organizational change or changes would you recommend the subcommittee and/or DOD consider to address these broader issues?

Dr. KIRSCHBAUM. So I would say that, if you look at the balance of our recommendations that we made at the end of 2020 on this, we are very specific that it needs to be organizational responsibility to execute the strategy. So that needs to be offices and/or people who have the authority and responsibility to do so.

It is the next best thing to say, we don't care who that is except those conditions need to be achieved. It needs to be someone who has the authority to execute, backed up by a process to assess what actions are taken and assess whether or not those actions met the intent of the vision.

Those things are going to help the Department get over the hump, as it were, that we have seen in other areas. So, for example, you are well aware, sir, that we have worked with you and Ranking Member Stefanik on things like the DOD Cyber Strategy implementation, and we have seen the difference. In those cases where you have someone with authority and a process to back it up, you have seen some progress. And your committee, in particular, has been vital in ensuring that success.

We have seen it in other areas, like with the nuclear enterprise, nuclear deterrence reform efforts, where it has got the attention and that helps push things along in terms of where we need to go on innovation.

Mr. LANGEVIN. Thank you very much, Dr. Kirschbaum.

Ranking Member Stefanik, you are recognized.

Ms. STEFANIK. I have no further comments or questions, Jim, so I will yield back for the next Republican.

Mr. LANGEVIN. Okay. Thank you.

Mrs. Bice.

Mrs. BICE. I don't have any additional questions either, Mr. Chairman.

Mr. LANGEVIN. Okay. Thank you very much.

Then Mr. Moore.

Mr. MOORE. No additional. Well, if you could summarize—in fact, let me just be very, very brief.

If you could summarize, like, as we just kind of wrap this up, what would you say, compared to some of our key adversaries, where are we? Where is our biggest deficient area that we need to focus on?

And then, if we want to say Russia and China, that is great, or if you feel like there are other adversaries that could be targeting. But what areas are we most vulnerable? I would love to just get your candid thoughts. That is not scripted or anything like that. And I will pause there.

Mr. CLARK. So I would say our biggest vulnerability is our reliance on active sensors and wide-area high-power networks.

When we have to operate inside the near abroad of China or Russia, you know, we are on their turf. You know, they are the home team. They have their sensor networks out there; they are able to listen for any of our emissions. So the fact that our ships and our airplanes have to rely, to a great degree, on active radars to be able to do missile defense or active radars to find targets and then on these wide-area networks, like Link 16, to communicate makes us, you know, very detectable, and it makes it easy for them to figure out what we are doing and attack us.

That is our biggest vulnerability, I think, is this home-team advantage that the Chinese and Russians have and the fact that we need to develop new technologies and tactics to be able to still operate in those contested areas using passive sensors and multistatic sensors and LPI—Low Probability of Intercept/Low Probability of Detection sensors.

So it is a different approach that we need to mount, which is uncomfortable, in a lot of ways, for the military forces of today.

Dr. CONLEY. From my perspective, I would offer, we have to ensure that we train as we intend to fight. In many cases, I think we actually have an adequate understanding of adversary capabilities, but when you look at the operational level and we bring operational units together to train before a deployment, we want to make sure that we exercise our command and control network in a way that demonstrates that we have command and control over those forces and we are able to execute everything we want. That is exactly what either China or Russia would attempt to fight us in. And it is an area, when we prepare, we have to make sure we get right. At the operational level, I would offer that.

At the strategic level, the other thing I would offer is: I believe, from the three different testimonies that this subcommittee has received so far this year, for this session of Congress, this is the first one that does not have a former Deputy Secretary of Defense, ei-

ther acting or confirmed in the role, who is appearing. And so making sure that, at the strategic level, the investment that we are making is aligned with where we want the strategy to go and making sure there is that senior-leader buy-in from the budgeting side.

Dr. KIRSCHBAUM. I would say it is kind of a melding of those two—two things.

The first is, from that strategic level, the appreciation of where and how vital EM spectrum operations are to that entire information environment, as I mentioned—its importance to everything from strategic messaging, information operations, cyber. That incorporation and appreciation from the strategic, operational, and tactical level is crucial, and we are not quite there.

The other one is much more of, kind of, a pace, that technology, doctrine, learning pace.

One of the dangers of inviting a historian to testify is you are going to get examples from a long time ago. So, in 1914, armies marched off to war with the appreciation that the machine gun was an awesome weapon. They had the machine gun set up in separate units that—you kind of used them where you needed them. Well, it didn't take long to figure out that that was the wrong way to use them. And the Army that figured out first that machine guns needed to be deployed in numbers throughout specific units to support actual operations, they had an advantage right away. And that was—the German Army did that.

Right now, we are kind of marching off in the 1914. We think of these kind of spectrum operations as enablers for existing operation, and in a lot of ways we still treat them that way. They are not as integrated as they need to be throughout the force. A lot of the work we saw characterized that. So that is the hump we need to get over.

Mr. MOORE. Thank you.

And I yield back. Appreciate the perspective there. Thank you, Chairman.

Mr. LANGEVIN. Very good. Thank you, Mr. Moore.

I guess I have one last one. I guess maybe this might be for Mr. Kirschbaum, but also Dr. Conley might want to weigh in.

Who or what entity within DOD is responsible for ensuring new and existing systems can connect to one another? You know, who is responsible for that plan and process? Especially systems owned by different services.

Dr. KIRSCHBAUM. So I would love Dr. Conley to help with this, because I know he is going to have some very good opinions on it.

Right now, the answer is: Everyone. Obviously, the CIO [Department of Defense Chief Information Officer] is responsible for that communications side and interoperability, but for systems development, the responsibility also lies in other places.

And that is actually one of the issues we have seen over time with this and other areas, where the responsibility to ensure that these systems are developed in an integrated fashion falls second, third, and fourth order of priority, versus individual service area development, so you don't get the connectivity.

Mr. LANGEVIN. Yeah. That is a bit troubling, obviously, to say the least.

So, Dr. Conley.

Dr. CONLEY. Yeah. So completely agree with CIO owning the strategy and the policy around that.

The other thing that I would add is, obviously, the services at the program officer level, the PEO [program executive office] level, obviously have a lot of responsibility, obviously, on the acquisition piece.

I think the only part that we didn't touch on yet is the JROC and the requirements process and ensuring, whenever we can, we articulate which links we want to make sure have to be able to talk with each other or how we set that expectation into a requirement that ultimately is testable so we can make sure that we are meeting that strategic objective that you mentioned.

Mr. LANGEVIN. Very good. Thank you.

I have no further questions. I would just ask the ranking member if you had anything?

Okay. Very good.

Well, this has been an excellent hearing. I want to thank you all for your time today, your incredibly valuable insights. You have given us a lot to think about and to work on. We look forward to staying in touch.

Members may have additional questions that they may want to submit for the record. If you could help in responding to those, we would appreciate that.

So, with that, again, excellent hearing. Thank you all for being here today and what you have had to say. It has been very, very helpful.

With that, this hearing stands adjourned.

[Whereupon, at 4:15 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 19, 2021

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 19, 2021

Opening Statement
Chairman James R. Langevin
Cyber, Innovative Technologies, and Information Systems Subcommittee
Department of Defense Electromagnetic Spectrum Operations: Challenges and Opportunities in the Invisible Battlespace
March 19, 2021

I would like to welcome the members who are joining today's remote hearing. Members who are joining must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those Members must continue to use the software platform's video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a Member experiences technical difficulties, they should contact the committee's staff for assistance.

Video of Members' participation will be broadcast via the television/internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If Members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member to, if necessary, mute unrecognized Members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

With that, I will give my opening statement. Welcome to our hearing today on the Department of Defense's electromagnetic spectrum operations. I want to thank Ranking Member Stefanik for joining me in holding this hearing today. And I would like to recognize my friend and CITI colleague Representative Larsen for his leadership on this issue as co-chair of the Electromagnetic Warfare Working Group along with his fellow co-chairs Representatives Austin Scott and Don Bacon.

I also want to thank our witnesses for appearing today.

Today we welcome:

- Mr. Bryan Clark—Senior Fellow and Director of the Center for Defense Concepts and Technology at the Hudson Institute.
- Dr. William (Bill) Conley—Former Director for Electronic Warfare in the Office of the Secretary of Defense.

- Dr. Joseph (Joe) Kirschbaum—Director of the Government Accountability Office Defense Capabilities and Management team.

I thank you all for appearing today.

The electromagnetic spectrum underpins nearly every aspect of the modern U.S. military and as a co-chair of the Electromagnetic Warfare Working Group, I have long recognized its importance. The Department uses the electromagnetic spectrum for situational awareness, communicating with friendly forces, identifying enemy capabilities, directing strikes, navigation, and countless other tasks. In fact, nearly every U.S. military capability—from airplanes, to night vision goggles, satellites, ships, and radios—depend on the spectrum to function, and they depend on it today.

While previous CITI hearings covered what lies ahead in defense, the military is facing unseen challenges in the electromagnetic spectrum right now. Many of the United States' most important weapon systems like the F-35 or Ford-class aircraft carrier are at a disadvantage today without uncompromised access to the electromagnetic spectrum.

This challenge and the importance of electromagnetic spectrum operations will only grow as emerging technologies like autonomous weapons, connected battle networks, artificial intelligence, and directed energy continue to fundamentally change warfare. Future combat will be less about the capability of individual weapons systems and more about how a networked "system of systems" communicate and work together through the effective use of the electromagnetic spectrum.

Seeing this trend, competitor nations like China and Russia are developing their own capabilities to dominate this domain and connect their forces. These governments believe the electromagnetic spectrum represents a potential critical vulnerability for the U.S. military, which they can exploit to reduce our advantage and the efficacy of our high-end weapons systems.

Recent cases in the field speak to this. Russia has conducted electronic attacks against U.S. coalition forces in Syria, and in 2018 then-US Special Operations Command head Gen. Raymond Thomas called it "the most aggressive electronic warfare environment on the planet from our adversaries." We saw similar activity in Ukraine, where Russians launched surprise artillery strikes using signals emanating from Ukrainian troops' cell phones. There are also alarming reports of directed energy incidents targeting U.S. government personnel producing extremely concerning bio-effects, a phenomenon known as "Havana syndrome."

Congress and the Department have therefore undertaken significant efforts recently to position and equip the U.S. military for success. I want to recognize the progress the Department and the military services have made furthering this effort. However, we have more work to do to ensure the United States maintains its advantage and closes the gap where we have lost our edge.

As the Department modernizes its systems and capabilities, it must ensure that both new and existing platforms are networked together in a joint environment. To do so, we need to develop the right management structure, strategy, and resources at the Department of Defense. And I know our witnesses will have much insight into how to accomplish these objectives.

And with that, I look forward to hearing from our expert panel.

I'll now turn to Ranking Member Stefanik for her remarks.

Hudson Institute

Prepared statement by:

Bryan Clark
Senior Fellow, Hudson Institute

Before the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems at a March 17, 2021 hearing titled "Department of Defense Electromagnetic Spectrum Operations: Challenges and Opportunities in the Invisible Battlespace."

March 17, 2021

Regaining EMS Superiority Through New Technologies

Chairman Langevin, Ranking Member Stefanik, and distinguished members of the committee, thank you for the opportunity to discuss the challenges and opportunities facing U.S. military operations in the electromagnetic spectrum (EMS). The EMS is arguably the most important environment in modern warfare, enabling nearly every sensing or navigation technology U.S. troops use and connecting forces from every domain through radio or laser communications. It is also the most unheralded warfighting space—at least in the U.S. defense community. Although we experience the EMS every day through our smart phones, mobile computers, or vehicle collision avoidance systems, the spectrum cannot be seen or felt like land and cyberspace, resulting in it sometimes being a forgotten domain.

Despite its invisibility, access to the EMS is critical for U.S. forces, who without it could lose the advantages they developed by integrating troops, platforms, and systems from multiple domains in combined-arms warfare over the last century. America's adversaries, from Iranian-based militias to People's Republic of China's (PRC) People's Liberation Army (PLA), understand the U.S. military's dependence on the EMS and have fielded a wide array of sensor and communications countermeasures to contest U.S. spectrum access. Unfortunately, the Department of Defense (DoD) allowed its rivals to catch up during the two decades following the Cold War by failing to invest in new technologies that would be more resilient against enemy jamming and deception or better able to degrade opponents' EMS operations.

Multiple assessments argue the U.S. military is now behind its adversaries in EMS capabilities.[1] With budgets tightening and the window for regaining an advantage now down to less than a decade against the PRC, it is unlikely the U.S. military will be able to restore EMS superiority by attempting to counter each adversary advancement with a new EMS system or countermeasure.[2] DoD will instead need to pursue new operational concepts and technologies that will allow it to "leap ahead" of its competitors and create enduring advantages in EMS operations.

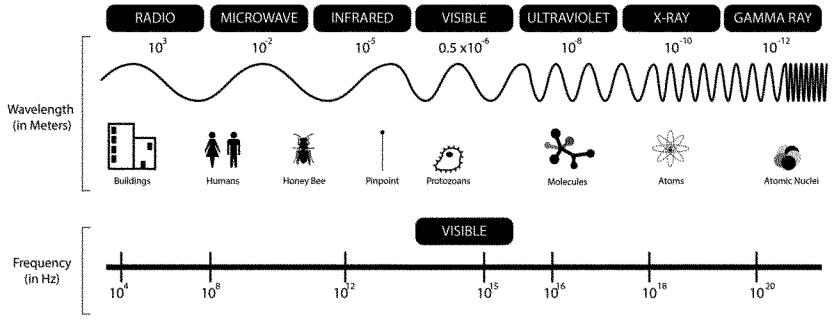
Hudson Institute

The U.S. Congress implemented several changes to DoD EMS governance during the last several years, which have not yielded substantial improvements in the U.S. military's ability to gain EMS superiority.[3] At the same time, the Federal Communications Commission has apportioned a more of the EMS to commercial users, constraining military EMS access. Rather than pursue further governance and process changes or resist commercial EMS innovation, the Congress should now focus its attention on ensuring DoD prioritizes the technologies that would enable it to better share the spectrum with civilian users and give the U.S. military an edge in the EMS competition with adversaries, as detailed below.

A congested, constrained, and contested environment

U.S. military doctrine organizes EMS activities into communications, sensing, and electromagnetic spectrum operations (EMSO). Communication and sensing systems such as radios and radar in the radiofrequency (RF) portion of the EMS are widely familiar to civilian and military users. EMS systems are now evolving to send signals using lasers in the higher-frequency infrared (IR) and ultraviolet (UV) ranges that can be detected by semiconductor-based focal plane arrays. Future capabilities are likely to incorporate X-ray and gamma ray emitters and sensors. Figure 1 illustrates the bands of the EMS.

Figure 1: The electromagnetic spectrum



Source: Wikimedia Commons

Similar to sea or air control operations, EMSO activities are intended to control the EMS by exploiting enemy emissions, attacking enemy and protecting friendly forces, and managing spectrum use by military forces. In addition to spectrum management to coordinate and deconflict civilian and military EMS activities, EMSO includes electromagnetic warfare (EW), which comprises three main categories of capabilities and activities:

- Electromagnetic attack (EA) involves the use of electromagnetic energy, directed energy like lasers or high-power microwave, or anti-radiation weapons to attack personnel, facilities, or equipment and is considered a form of fires.

- Electromagnetic protection (EP) refers to actions taken to protect personnel, facilities, and equipment from the effects of friendly, neutral, or enemy use of the EMS. EP is a very broad and important category that includes capabilities to avoid detection like stealth and passive or multistatic sensors as well as capabilities to defeat jamming such as frequency hopping or the use of spot beams by radars or radios.

- Electromagnetic support (ES) includes actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM energy. Although ES activities can support signals intelligence (SIGINT), ES is considered an operational activity to support commanders in controlling the EMS in real time, whereas SIGINT or electronic intelligence (ELINT) are intended to support future analysis and operations.[4]

Unlike objects physically moving through the air or along the ground or sea, electromagnetic energy travels at the speed of light and often does not stop at walls, boundaries, or exclusion zones. As a result, civilian, military, and environmental emissions cannot be separated like maritime or air traffic. To cope with the resulting congestion, U.S. forces rely on electromagnetic battle management (EMBM) processes and capabilities to coordinate military communications, sensing, and EMSO and deconflict them from civilian and non-combatant users. For example, EA operations must be coordinated with passive sensors to avoid the jammer being classified as a threat as well as with friendly and civilian radios and radars to prevent inadvertent interference. The congestion facing U.S. forces will likely increase as military EMS access is constrained by the need to allocate more spectrum to 5G mobile communications, expanded Wi-Fi coverage, and ubiquitous sensing and communications on vehicles and consumer products.

The EMS is also becoming more contested. Adversaries, most prominently the PRC and the Russian Federation, are countering U.S. military operations in the EMS using passive sensors and jammers to exploit the dependence of expeditionary U.S. forces on active radars for air defense and long-range RF communications for command and control (C2). As the "home team" in most likely military conflicts, U.S. adversaries can rely to a greater degree on wired communications, multistatic and passive sensing, and their understanding of local conditions to gain an advantage in a highly contested electromagnetic environment.[5]

The long-term EMS competition

The adoption of passive or multistatic sensors and less-detectable communications by PRC and Russian armed forces reflects the latest phase of a longstanding competition for EMS superiority that started with the creation of wireless radios and their employment in large-scale military operations during World War I. This early phase of the EMS competition was exemplified by the active use of radios to coordinate troop movements and direct fires and of passive direction-finding (DF) equipment to locate or listen to enemy radio transmissions.

While communications jamming emerged during this first phase of the EM warfare competition, it was not widely employed by military combatants. Operators of rudimentary radios realized that keying their systems could drown out with white noise the transmissions of other radios operating at the same frequencies. This tactic had limited operational value, since it also prevented the jamming force from using the same radio frequencies, and the jamming victim could use alternate means of communicating during the slow-moving operations of the early 20th Century. Moreover, commanders often gained more benefit from exploiting an enemy's radio transmissions for position information or intelligence rather than disrupting them.

The first phase of the EMS competition could be characterized as one of active networks and passive countermeasures in which radios and radars were used to find enemies and coordinate friendly operations, and DF systems were used to locate enemy transmissions or listen to their communications. The shift to the competition's second phase of active networks versus active countermeasures occurred during World War II when technological advances made airborne radars and jammers practical, and the increased tempo of warfare incentivized combatants to jam enemy transmissions as well as intercept and exploit them.

The air defense mission, in particular, helped spur the active network versus active countermeasures competition. Before the advent of air-delivered precision guided munitions during the Cold War, the effectiveness of bombing raids depended in large part on the accuracy of aircraft navigation systems. German air defenders exploited British bombers' use of radio beacons or radar navigation by deploying jammers and decoys to cause bombers to miss their targets. Allied forces responded with updated navigation systems and airborne jammers designed to obscure German air defense radars.[6]

The EMS competition entered is third phase during the late Cold War. As Soviet military sensors, surface-to-air missiles and anti-ship missiles grew in sophistication and number, DoD sought to leverage emerging stealth technologies as a means to break out of the active sensor and countermeasure competition. Since radars were the most capable contemporary systems for detecting aircraft and ships at long ranges, DoD initially emphasized stealth techniques and technologies to reduce the radar cross section of platforms. Stealth was complemented by passive sensors and sensors with waveforms and adjustable power levels to reduce the electromagnetic emissions of stealth platforms that could be detected by an enemy's passive sensors.[7]

DoD's shift toward stealth and low-power EMS capabilities was abruptly curtailed after the end of the Cold War. In the absence of significant competitors, DoD decided to sustain and improve its active networks based on systems such as the SPY-1 shipborne radar or E-3 airborne warning and control system (AWACS) and active countermeasures such as the EF-111 and EA-6B airborne electronic attack aircraft and SLQ-32 shipboard EW system. DoD halted B-2 stealth bomber production at 21 aircraft, and the Air Force was directed to procure only 187 operational F-22 aircraft.[8] Similarly, DoD capped procurement of DDG-1000 stealth destroyers at three ships and replaced its radar with a less capable one.[9]

Unfortunately, the shift to the third phase of EMS operations did not end just because DoD decided to truncate its procurement of stealth and less-detectable EMS capabilities. Adversaries such as the PRC and Russia developed their own low-observable platforms, advanced sensor and communication networks, and countermeasures designed to defeat America's Cold War-era active EMS systems, upgraded versions of which demand the majority of DoD EMS spending today.[10]

Addressing today's EMS challenges and opportunities

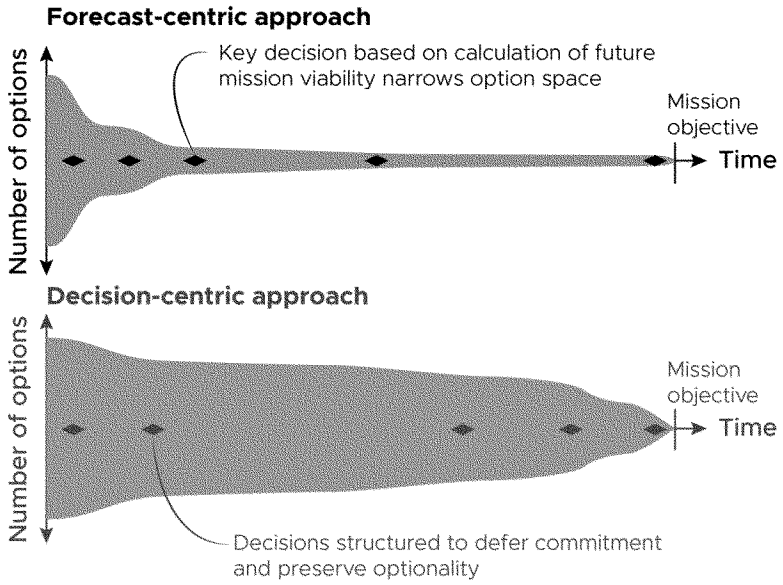
Restoring a U.S. advantage in the EMS will become more difficult as defense budgets come under pressure from costs to combat the ongoing COVID-19 pandemic, respond to economic recession, and service the growing national debt.[11] Given the increasing variety of adversary countermeasures and diverse demands for commercial spectrum, attempting to modify or replace U.S. military EMS systems in response to each new threat or civilian encroachment is likely to be unaffordable and continually late to need.

DoD's forecast-centric planning approach, embodied in the Joint Capabilities Integration and Development System (JCIDS), is ill-suited to identify capabilities that solve DoD's EMS challenges in a fiscally constrained and technologically dynamic environment.[12] Forecast-centric planning bases new requirements on the anticipated gaps between capabilities needed to execute desired concepts in future operations and a military force's current or projected capabilities. This analytic approach depends on assumptions regarding the scenarios in which conflict is likely to occur, the capabilities and tactics to be used by opponents, and the probable actions of U.S. allies and partners. The need to make multiple, interdependent assumptions reduces the accuracy of forecast-centric planning, and when assumptions prove incorrect, budget constraints could reduce the force's ability to adapt.

To regain enduring EMS superiority under today's conditions of technological and fiscal uncertainty, DoD will need to adopt a decision-centric planning approach in which adaptability is a more important metric than predicted performance against a particular threat in a specific scenario. In contrast with forecast-centric planning's mobilization of resources to efficiently develop a single solution, decision-centric planning would seek to preserve options for as long as possible within a mission or over a competition. Within operational timeframes, the optionality afforded by a more adaptable force could allow commanders to make faster and more effective decisions, while the complexity imposed on the enemy would degrade its decision-making process. Over strategic and industrial timescales, increasing the adaptability of military systems enables capability developers to leap ahead of an opponent's advancements and deconflict operations with civilian or commercial activities.

Hudson Institute

Figure 2: Forecast-centric versus decision-centric capability planning

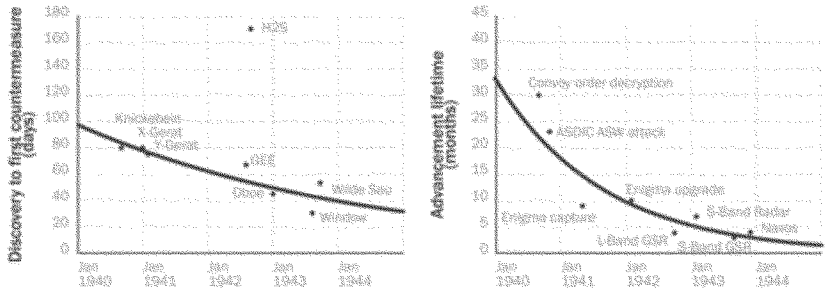


Source: Bryan Clark, Dan Patt, and Timothy A. Walton, *Implementing Decision-Centric Warfare: Elevating Command and Control to Gain and Sustain an Optionality Advantage in Military Conflict and Competition*, (Washington, DC: Hudson Institute, 2021), p. 11.

Adaptation is a proven path to sustaining EMS superiority in an extended conflict or confrontation. During World War II, for example, the anti-submarine warfare–submarine competition and bombing campaigns over Germany were won by the Allied powers in part because U.S. and British militaries were able to field a more rapidly evolving set of EMS capabilities on their ships and aircraft compared to the Axis powers. The accelerating move-countermove competition that resulted is depicted in Figure 3.[13]

Hudson Institute

Figure 3: EMS systems innovation during World War II



Source: John Stillion and Bryan Clark, *What It Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: CSBA, 2015), https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions.

Note: Left graph: Knickebein, X-Great, and Y-Great were German radio navigation aids used to direct bombers to targets in the UK; GEE and Oboe were radio navigation aids for British bombers attacking Germany; Wilde Sau was a German air defense fighter tactic; and Window was a British radar-obscuring chaff. Right graph: ASW = anti-submarine warfare; GSR = German Search Receiver; ASDIC = Allied Submarine Detection Investigation Committee. Enigma was a German code machine.

The U.S. military is unlikely to repeat the Allied success of World War II with today's generation of platforms and EMS systems. Modern U.S. ships and aircraft are monolithic and highly integrated. Incorporating a new sensor, communication system, or countermeasure in today's platforms can take years of software development, hull or airframe modification, electromagnetic deconfliction, and procedural evolution beyond the task of creating the new EMS system itself. Unfortunately, most of DoD's EW procurement and research and development (R&D) investment is tied up in these integrated, platform-based systems.

DoD will need to adopt new EMS technologies that allow it to gain a lead in the move-countermove cycle with military competitors and the growing spectrum needs of civilian users. To improve their ability to evolve between operations, EMS systems will need to be increasingly software-based and modular, allowing components or systems to be more easily upgraded or modified to incorporate new techniques and technologies.

DoD's recently released EMS Superiority Strategy supports the importance of adaptability in its central idea that U.S. forces need to maneuver in the EMS to avoid threats, exploit opportunities, and share spectrum with civilian users. The strategy is notable for its emphasis on creating a force that uses agility, battle management, open architecture, and virtual and constructive training systems to achieve freedom of action in the EMS. Each of the strategy's goals pursues this overall approach, as summarized below.

- **Goal 1: Develop superior EMS capabilities.** DoD should create open architecture multifunctional EMS systems that can sense, communicate, and maneuver in the spectrum as directed by EMBM capabilities while avoiding threats and counter-detection through their signal characteristics and maneuver. This method for gaining superiority is different from the attempt to dominate opponents in individual system-versus-system competitions, which was often the model of DoD's post–Cold War EMS capability development.

- **Goal 2: Evolve to an agile, fully integrated EMS infrastructure.** DoD should prioritize better integration and interoperability between intelligence and operational EMS activities to improve responsiveness; the department should also increase reliance on virtual and constructive training to raise proficiency in agile, networked EMS operations without risking adversary intelligence gathering during open-air exercises.

- **Goal 3: Pursue total force EMS readiness.** DoD should professionalize personnel in EMS-dependent fields to enable the career-long development needed for more sophisticated and dynamic EMS operations. To improve unity of effort between EMS specialists and other operators and technicians, the department should incorporate EMS doctrine into force-wide training.

- **Goal 4: Secure enduring partnerships for EMS advantage.** DoD should emphasize interoperability with allies and partners to help ensure that technical advances in DoD EMS operations will not be undermined by other friendly activities. To accelerate the technology improvement cycle, the Pentagon should also enhance its collaboration with industry and professional organizations.

- **Goal 5: Establish effective EMS governance.** DoD should adopt a sustainable governance structure for EMS capability development efforts to ensure the diverse array of EMS-dependent programs and activities is being coherently pursued in support of the strategy.[14]

The EMS Superiority Strategy's goals emphasize the importance of adaptable technologies, but adaptability alone will not yield an advantage if the underlying technologies do not mitigate challenges and exploit opportunities. For example, high-power broadcast radios or scanning search radars can be made highly adaptable using artificial intelligence (AI)-enabled controls, but their risk of counter-detection makes them a poor choice for operations against revisionist powers like the PRC that can deploy numerous distributed passive radiofrequency (RF) sensors in areas where they intend to initiate conflict.

Instead of merely pursuing adaptability, DoD should establish technology priorities that would help U.S. forces gain an advantage against their primary adversaries and which would essentially form the centerline of the decision-centric planning space shown in Figure 1. In the Hudson Institute's recent study, we used the technique of net assessment to identify EMS technologies

that leverage fundamental asymmetries between the DoD and its great power competitors to address the U.S. military's EMS challenges and opportunities.[15]

Asymmetries

DoD will need to focus its efforts on concepts and capabilities that provide U.S. forces enduring advantages against the PLA and Russian Armed Forces while mitigating U.S. disadvantages. The net assessment methodology identifies these opportunities based on asymmetries between competitors the U.S. and opposing militaries, such as those described below.[16]

Geography: The PRC and Russian militaries will likely be the home team in future military confrontations, given their ongoing gray-zone operations and stated interests in neighboring countries such as Taiwan for the PRC and the Baltic countries for Russia. As a result, the PLA and Russian Armed Forces can rely to a greater degree than the expeditionary U.S. military on wired communications and can employ passive and multistatic sensors that require multiple networked arrays and a sophisticated understanding of the local electromagnetic operating environment.[17]

Command, Control and Communications: The PLA can rely on redundant and resilient communications networks to support a relatively fixed C2 structure of unit commanders, theater commanders, and the Central Military Commission. Russian Armed Forces are more likely to build initial plans and rely on local commanders to execute them, or to improvise when conditions change, or communications are degraded.

The U.S. military exhibits elements of both the PRC and Russian approaches. DoD aspires to create the PRC's level of communications reliability so distant commanders at regional headquarters can manage operations across a theater. Under the concept of mission command, U.S. military doctrine directs local commanders to use their initiative and improvise when communications break down.

Technological innovation: The PLA's concept of system destruction warfare requires development of countermeasures that address specific nodes of U.S. systems of systems. The PLA can leverage the PRC's robust commercial electronics industrial base to develop new capabilities, enabling it to field a comprehensive and changing collection of EMS systems. Russia lacks the PRC's military budgets and fusion with civilian industry, leading the Russian Armed Forces to incrementally adapt existing EMS systems.

DoD largely pursues two tracks in new EMS technologies: new capabilities that are designed to support innovative operational concepts, and improvements to existing systems that counter new adversary capabilities. Because new concepts are not associated with existing major programs, the DoD approach results in the majority of U.S. EMS investment going toward incremental advancements of legacy systems that chase adversary initiatives rather than toward new innovations that create dilemmas for opponents.

Employment of AI: The PRC, Russian, and U.S. militaries are all aggressively pursuing AI as an element of their overall force development, but with different priorities for operational systems compared to management and support capabilities. Whereas DoD has prioritized AI incorporation into operational systems for tactical intelligence, platform control, and maintenance, the PLA and Russian Armed Forces have focused AI implementation on C2, management support systems, and intelligence, surveillance, and

reconnaissance (ISR).

EMS capability governance: Significant asymmetries exist between the DoD and its competitors regarding the organizations that govern EMS capabilities. The PLA developed a unified governance structure for EMS policy and capability requirements, which parallels the Russian Armed Forces' EW Commander and staff. The U.S. military, in contrast, divides responsibilities for doctrine and strategy between U.S. Strategic Command, the EW Executive Committee (EXCOM), and the EMSO Cross-Functional Team (CFT). Moreover, DoD does not give any of these bodies the authority to direct EMS-related spending or acquisition, reducing their ability to implement policy.

Deployment of EW capabilities: Although the PLA, Russian Armed Forces, and DoD all field operational- and tactical-level EW capabilities through their service branches, the scale and depth of deployment varies significantly. Because of the value they place on EW as an element of their respective military strategies and operational concepts, the PRC and Russian militaries equip units with offensive and defensive EW systems and personnel down to the ground force company, aviation squadron, and naval or paramilitary ship level. U.S. EW capabilities are deployed to varying echelons depending on the service, but generally are held at higher levels of command than in the PLA or Russian Armed Forces. Additionally, PLA and Russian Armed Forces units have employed broad area EW systems against adversaries and enemies with greater frequency than U.S. forces, suggesting EW authorities may be delegated to lower levels of command.

EMSO: The U.S. military introduced the EMSO concept to create a coherent framework for EW operations to control the EMS and EMBM to coordinate EMS activities such as EW, sensing, and communications. The PRC and Russian militaries do not have publicly released concepts for unified EMS operations, and largely treat EMS control through EW separately from communications, sensing, and spectrum management activities.

Technology Priorities

The asymmetries revealed by net assessment help identify significant U.S. advantages or vulnerabilities in EMS operations, including shortfalls that could be turned into advantages or are foundational and therefore unlikely to be overcome. EMS technology priorities should address U.S. strengths and weaknesses by supporting capabilities in four main categories: capabilities enabling DoD to obviate, rather than overcome, fundamental challenges; capabilities that undermine adversary advantages; capabilities that turn challenges into opportunities; and capabilities that exploit existing U.S. strengths.

The net assessment methodology accepts risk because it does not attempt to solve every potential future capability gap, which is an acceptable trade-off given DoD's time and fiscal constraints. The Hudson Institute study recommends that DoD prioritize the following areas to gain EMS superiority and address the growing diversity of civilian users. Some important technologies, such as attritable EW platforms, are mentioned but not specifically called for because they are already being pursued by DoD and therefore are not a new technology priority.

Capabilities to obviate, rather than overcome, fundamental challenges: The PLA's concept of system destruction warfare uses the PRC's fusion of military and civil sectors to create a comprehensive set of

EMS countermeasures designed to target key U.S. battle network nodes and platforms. Continuing to engage in an extended move-countermove competition with the PLA is costly and time-consuming. Therefore, U.S. EMS capability development should focus on adaptive capabilities that can reduce the predictability of U.S. battle network operations.

Capabilities that undermine adversary advantages: The PRC and Russian home team advantage could be countered in part by new technologies that improve the EP capabilities of U.S. forces and reduce their risk of counterdetection; specifically:

- **Passive and multistatic electromagnetic (EM) sensing:** U.S. forces, as the away team, will need to reduce their EM emissions and signatures across the RF, IR, and visual spectra to avoid counter-detection and targeting by PRC or Russian forces.
- **Passive and multistatic air and missile defense:** To reduce the vulnerability of air and missile defense systems, DoD will need to field passive and multistatic sensors that can detect and track subsonic, supersonic, and hypersonic aircraft and weapons.
- **Networked ES:** Passive receiving arrays need to securely communicate with one another or with multistatic emitters to enable more precise sensing.
- **Networked EA:** Systems that conduct high-risk EA operations inside contested areas will need to be expendable or inexpensive enough to be attritable. Small and cheap unmanned EA platforms can rely on proximity and coherently combined transmissions to make up for their lower power—an approach that places a premium on secure networking.
- **Low Probability of Intercept/Low Probability of Detection (LPI/LPD) active monostatic sensing:** As an expeditionary force, the U.S. military may have difficulty sustaining multiple passive sensor systems in position to support operations like air and missile defense, and therefore will need active radars to achieve the necessary precision for engagements. Radars, however, will need features that reduce their likelihood of revealing the defensive system's exact location.
- **Multifunction ES and EA capabilities:** The cost and complexity of using larger numbers of distributed ES and EA vehicles could be reduced in part by ensuring that DoD EW systems are able to perform either sensing or EA operations.

Capabilities that turn challenges into opportunities: As noted above, the PRC and Russian military's focus on potential vulnerabilities of U.S. battle networks could be turned into a disadvantage if U.S. force packages, configurations, and operational concepts are less predictable using technologies such as:

- **Cognitive wideband EMS systems:** The U.S. military could dramatically accelerate its EMS capability move-countermove cycle by fielding sensor, communication, and EW systems that can operate over multiple gigahertz of frequency spectrum and react to adversary operations in real time by developing and employing new courses of action using AI-enabled algorithms.
- **Automated EW system reprogramming:** Accelerating automated and AI-enabled reprogramming would improve the adaptability of systems that are not yet able to react in real time.
- **Decision support aids and communications management systems:** DoD could turn the challenge of contested communications environments into an advantage by giving junior commanders decision support systems that help them develop courses of action in the absence of connectivity with senior leaders and staffs.

Capabilities that exploit existing U.S. strengths: The U.S. military has adopted new approaches to EW and EMSO, supported by new training and capability integration approaches, that could substantially increase the adaptability and complexity of U.S. operations. These efforts should be accelerated by prioritizing relevant technologies:

- **Virtual and constructive EW/EMSO environments:** The U.S. military could exploit its investments in live, virtual, and constructive (LVC)-based EMSO experimentation and training by accelerating the introduction of virtual and constructive tools and environments at each organizational level, especially at home stations to support ongoing training and experimentation.
- **Electromagnetic battle management (EMBM) systems, including AI:** The U.S. military could capitalize on the PLA's and Russian Armed Forces' lack of EMSO doctrine and exploit the emerging generation of more adaptable EMS capabilities by accelerating the fielding of operationally useful EMBM systems.
- **Open architecture hardware standards:** Combined with a move away from monolithic, multi-mission EMS platforms, increased adoption of open architectures in U.S. military platforms and vehicles would allow use of more modular EMS systems that could be more easily exchanged and modified.
- **Open architecture software tools:** Another approach to open architecture is promoting interoperability between systems. DoD should accelerate the fielding of toolkits like the System-of-systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) that build software interfaces on demand to allow disparate networks to communicate.

Conclusion

DoD is at a crossroads in development of EMS-related technologies. The 2020 EMS Superiority Strategy and EMSO concept advance new approaches to regain an advantage and accommodate growing civilian uses by improving the adaptability of U.S. EMS capabilities. The resulting expansion of options could allow DoD to accelerate or break out of today's move-countermove EMS technology innovation cycle.

Making the shift to more dynamic, agile, and flexible EMS operations, however, will require accepting risk in traditional methods of controlling the spectrum. The U.S. military lacks the time and resources to gain EMS superiority against PRC and Russian forces using a symmetric system versus system approach. By the time DoD catches up, the PLA or Russian Armed Forces could exploit their EMS advantage to support aggression against their neighbors. DoD's choice is whether to accept continued erosion of its edge in the EMS or to make bold bets on the technologies most likely to circumvent or reverse the inherent advantages enjoyed by its great power competitors.

The technology priorities described above represent the U.S. military's best opportunity to establish enduring EMS superiority. They are all being pursued by DoD to varying degrees, but most are merely being sustained rather than accelerated in support of a new approach to EMSO. To reverse trends of the last three decades and give the PRC and Russia challenges to address, funding and attention will need to shift to these new priorities and away from legacy programs that helped win the Cold War.

[1] The most significant recent authoritative EW studies include the following: Defense Science Board (DSB), *21st Century Military Operations in a Complex Electromagnetic Environment* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2015), https://apps.dtic.mil/dtic/tr/fulltext/u2/1001629.pdf; Government Accountability Office, *Electromagnetic Spectrum Operations DoD Needs to Address Governance and Oversight Issues to Help Ensure Superiority* (Washington, DC: U.S. Library of Congress, 2020), https://www.gao.gov/assets/gao-21-64.pdf; Madison Creery, "The Russian Edge in Electronic Warfare," Georgetown Security Studies Review, June 26, 2019, https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronicwarfare/.

[2] Mallory Shelbourne, "Davidson: China Could Try to Take Control of Taiwan In 'Next Six Years'," USNI News, arch 9, 2021, https://news.usni.org/2021/03/09/davidson-china-could-try-to-take-control-of-taiwan-in-next-six-years.

[3] Government Accountability Office, *Electromagnetic Spectrum Operations DoD Needs to Address Governance and Oversight Issues to Help Ensure Superiority* (Washington, DC: U.S. Library of Congress, 2020), https://www.gao.gov/assets/gao-21-64.pdf;

[4] U.S. Joint Staff, "Joint Publication 3-85: Joint Electromagnetic Spectrum Operations," May 22, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

[5] Robert O. Work and Greg Grant, *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics* (Washington, DC: Center for a New American Security, 2019), especially p. 7, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Work-Offset-finalB.pdf?mtime=20190531090041.

[6] John Stillion and Bryan Clark, *What it Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: Center for Strategic and Budgetary Assessments, 2015), https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions.

[7] Alfred Price, *The History of Electronic Warfare, Volume III, Rolling Thunder Through Allied Force, 1964 to 2000* (Alexandria, VA: Association of Old Crows, 2000), p. 98.

[8] Rebecca Grant, "Return of the Bomber: The Future of Long-Range Strike," (Arlington, D.C.: Air Force Association, 2007), https://www.hsdl.org/?view&did=818115.

[9] Ronald O'Rourke, Navy DDG-51 and DDG-1000 Destroyer Programs: Background and Issues for Congress (Washington, DC: Congressional Research Service, June 25, 2014), p. 29.

[10] John Hoehn, "U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress," Congressional research Service, April 16, 2020, https://fas.org/sgp/crs/natsec/R45756.pdf.

[11] Congressional Budget Office, "An Update to the Budget Outlook: 2020 to 2030." September 2, 2020, https://www.cbo.gov/publication/56517.

[12] U.S. Joint Staff, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)."

[13] This analysis comes from John Stillion and Bryan Clark, *What It Takes to Win: Succeeding in 21st Century Battle Network Competitions* (Washington, DC: CSBA, 2015), https://csbaonline.org/research/publications/what-it-takes-to-win-succeeding-in-21st-century-battle-network-competitions.

[14] U.S. Department of Defense, "2020 Department of Defense Electromagnetic Spectrum Superiority Strategy."

[15] The discussion of asymmetries and technology priorities that follow are drawn from Bryan Clark, Timothy A. Walton, Melinda Tourangeau and Steve Tourangeau, "The Invisible Battlefield: A Technology Strategy for EMS Superiority," (Washington, DC: Hudson Institute, 2021), https://www.hudson.org/research/16738-the-invisible-battlefield-a-technology-strategy-for-us-electromagnetic-spectrum-superiority.

[16] Net assessment is not explained in detail here, but more detail can be found in James G. Roche and Thomas G. Mahnken, "What is Net Assessment?" in Thomas G. Mahnken, ed., *Net Assessment and Military Strategy: Retrospective and Prospective Essays* (Amherst, NY: Cambria Press, forthcoming in 2020); Eliot Cohen, "Net Assessment: An American Approach," JCSS Memorandum no. 29, April, 1990, available at https://www.inss.org.il/publication/net-assessment-an-american-approach/; George E. Pickett, James G. Roche, and Barry D. Watts, "Net Assessment: A Historical Review," and Stephen Peter Rosen, "Net Assessment as an Analytical Concept," in A.W. Marshall, J.J. Martin, and Henry S. Rowan, eds., *On Not Confusing Ourselves* (Boulder, CO: Westview Press, 1991); and Paul Bracken, "Net Assessment: A Practical Guide," Parameters, Spring 2006.

[17] US Department of Defense, "Military and Security Developments Involving the People's Republic of China 2020: Annual Report to Congress," 2020, p. 74, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-dod-china-

military-power-report-final.pdf; Glen E. Howard and Matthew Czekaj, eds., *Russia's Military Strategy and Doctrine* (Washington, DC: Jamestown Foundation, 2019), pp. 164–76, https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Doctrine-web-1.pdf?x30147.

Bryan Clark
Senior Fellow & Director, Center for Defense Concepts and Technology

Areas of Expertise

Defense Strategy
National Security
International Relations
Defense Spending
Military Procurement and Technology

Bryan Clark is a senior fellow and director of the Center for Defense Concepts and Technology at Hudson Institute. He is an expert in naval operations, electronic warfare, autonomous systems, military competitions, and wargaming.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: March 19, 2021

Hearing Subject:

Department of Defense Electromagnetic Spectrum Operations: Challenges and Opportunities in the Invisible Battlespace

Witness name: Bryan Clark

Position/Title: Senior Fellow

Capacity in which appearing: (check one)

○ Individual ◉ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Hudson Institute

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N00164-19-9-0001	Department of Defense	$85,278.00	Electromagnetic Warfare Strategy

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
N00164-19-9-0001	Department of Defense	$27,461.00	Electromagnetic Warfare Strategy

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Payment	BAE Systems	$55,480	Support for Center for Defense Concepts and Technology

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Payment	Lockheed Martin Corporation	$75,000	General Support

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Payment	Lockheed Martin Corporation	$85,000	General Support

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Payment	Lockheed Martin Corporation	$60,000	General Support

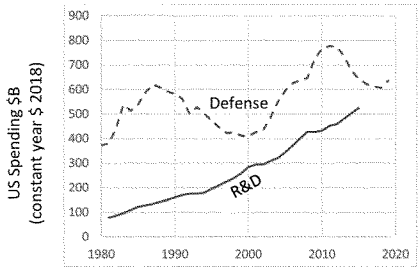
Prepared Statement by

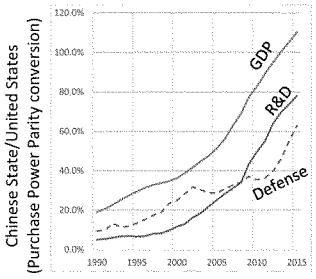
William Conley, Ph.D.

Before the House Armed Services Subcommittee on Cyber, Innovative Technologies, and Information Systems at a March 19, 2021 hearing titled "Department of Defense Electromagnetic Spectrum Operations: Challenges and Opportunities in the Invisible Battlespace."

Chairman Langevin, Ranking Member Stefanik, and distinguished members of the committee, I thank you for the opportunity to appear today. I am honored to personally testify today before the Cyber, Innovative Technologies, and Information Systems Subcommittee to the House Armed Services Committee. This is my first individual appearance as an expert having departed the Pentagon in 2019. After my tenure leading the electronic warfare portfolio in the Pentagon, you may wonder why I transitioned to the private sector and now partner with multiple non-profit organizations. The answer is quite simple, the innovation needed to support our electromagnetic spectrum operations capabilities occurs substantially in the private sector. I believe that our Nation must make it a priority to identify ways to make these commercial advances profoundly more accessible to the DoD.

A year ago, I performed an analysis between the Chinese State and the United States; particularly, comparing the size of the economy, of defense spending, and of R&D spending. I performed this comparison using Purchase Power Parity exchange ratios (not a simple exchange ratio). What I found is that the economy of the Chinese State is already 10% larger than that of the United States. Fortunately, the Chinese State invests only 80% as much into R&D and 60% as much into Defense as we do in the United States. Unfortunately, as the size of the Chinese State economy continues to grow, we should expect their R&D and defense budgets to continue to grow as well. This is a very different strategic situation than we faced during the Cold War – the Soviet Union's economy never approached parity with the United States.





I believe the strategic question we are faced with today is this, "how do we want to compete?" Since World War II, the US has largely leveraged manufacturing capacity as a proxy for military strength. However, globally we have transitioned into the Information Age, a landscape in which global leadership is defined by innovation, technology development, and technology adoption and integration. Formed in 2015, China's Strategic Support Force bundles electronic warfare, cyberspace operations, and space operations for a strategic advantage; all three functions are truly equals based on my research. China's Strategic Support Force reports directly to their Central Military Commission; based on their

organizational chart, they are a peer to the PLA Army, Navy, Air Force, and Rocket Force Headquarters. In comparison, the United States has maintained electromagnetic warfare and spectrum management as capabilities to achieve tactical outcomes. Our organizational charts reflect this tactical prioritization. Our competitive strategy must reflect that we are in the Information Age, and our strategy must also reflect our competitors' strategies.

At the operational and strategic level, successful warfighting depends upon the collection, aggregation, and analysis of information. This information allows commanders at all tiers to make timely, and well-informed decisions. As poor decisions made quickly have disastrous consequences, simply improving the speed of decision making is inadequate. Evolutionary improvements in weapon systems are expected to continue, the disruptive opportunity is manipulating the collection, aggregation, and/or analysis of information. While we disrupt an adversary, we must simultaneously protect and ensure that accurate data and information forms the basis for decision making by our commanders.

Military operations largely depend upon sensors that operate in the electromagnetic spectrum. Of military interest, the electromagnetic spectrum includes the optical, infrared, and radio spectrum. These portions of the spectrum allow electro-optics, infrared search and track, and radar sensors to detect, track, and target a threat. Electronic warfare, now called electromagnetic warfare, allows the innovative manipulation of this data.

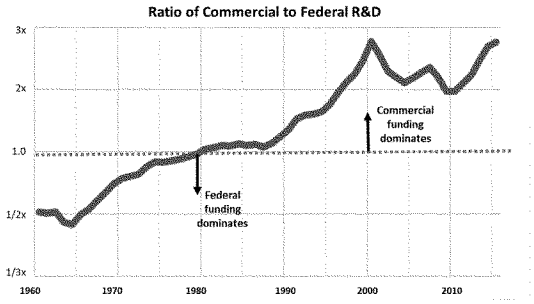
Electromagnetic attacks can deliberately interfere with the aggregation of data by an adversary. While commonly called jamming, this has occurred in all military operations since World War I. While the best artificial intelligence can analyze reams of data automatically, AI struggles to discriminate against bad & corrupted data. The adage "garbage in, garbage out" still applies today. Electromagnetic battle management, the dynamic reconfiguration of our sensors, our networks, and our electromagnetic attacks in realtime may be a preferred offensive strategy when compared to the defensive utilization of the electromagnetic spectrum in an integrated air and missile defense system, often called an IADS. Strategically, we may discover that EMSO offers a sustainable strategic advantage in our favor.

As a Nation, the United States should choose to pursue a strategy based on innovation: in our technology development, in our adoption of these innovations for our national defense, and in the full integration of these innovations into military tactics and operations. This is a dramatic departure from the platform and program-centric investment strategy we have pursued. Instead of viewing capability gaps and shortfalls, EMSO can generate opportunities and leverages the best of our private sector in support of our national defense. To remain a global power, the United States and our allied partners must pursue a strategy to leap ahead, not to merely close a gap.

Microelectronics underpin all the capabilities discussed today. Global market data published by the World Semiconductor Trade Statistics Organization estimates that less than 1% of microelectronics are used in military applications. As smart devices continue to improve lives, the defense market share will continue to shrink – this is true for both developers as well as fabrication of semiconductors. A deliberate strategy is required to ensure both innovation and access. The largest microelectronics designers and suppliers have market caps which are 2-5x greater than companies which deliver many weapon systems to the DoD each year. Addressing our national microelectronics challenges is a necessary, but not sufficient, step to addressing our EMSO challenges. Both of these priorities must be pursued simultaneously.

Largely due to privity of contract concerns, our nation has chosen not to fully utilize the innovative muscle that exists across the United States' Innovation Base. I am deliberately treating this Innovation Base as being separate from our Industrial Base. While the latter is focused on producing products, the former is focused on producing value. There is an extensive historical justification for the focus of the industrial base to maximize the return on invested capital for investors. While a full description is beyond the scope of discussion today, this legacy dates to the industrial might of the US in the first half of the 20th century. Over the past 50 years, we have seen a continued globalization as well a fundamental shift in where value is created in our innovation base. Incentives that reward growth and innovation can drive needed capital investment into EMSO capabilities. Growth-centric young innovators want to work at companies where all employees have equity; current acquisition regulations do not treat this as a reimbursable cost.

The National Science Foundation's annual Science & Engineering Indicators report shows that the United States Government today accounts for approximately a quarter of our economic investment in R&D. The government should seek to maximize the value of this investment. I expect this trend will continue into the future and must be leveraged in our strategic thinking.



Several recommendations could improve our EMSO ecosystem:

- Incentivizing R&D investment by commercial companies; and particularly ensure that the US tax code does not penalize R&D investment for future innovations. I endorse H.R. 1304, The American Innovation and R&D Competitiveness Act.
- Develop a strategic framework for innovation by traditional defense contractors as well as non-traditional commercial companies. One size does not fit all for these different business models. Innovative, rapidly growing commercial companies are likely to invest more in internal R&D; this is desirable for EMSO and government policies should not attempt to limit investment and growth. The DoD should study this concept, establish needed strategy and policy to grow innovative solutions, as well as innovative companies, for our national security challenges.
- Develop policies to share data broadly and democratically across our national innovation base. Government furnished information should be available to the entirety of the supply chain. Currently, privity of contract limits interaction and the sharing of taxpayer funded insights. Any insights, reports, and deliverables generated on government contracts, or by government

thought leaders, should be broadly available to those with a need-to-know. Non-profit associations and institutes could offer effective distribution of these insights.

- Ensure a realistic EMSO environment and threat capability. This is critical in all Live, Virtual, Constructive environments. Additionally, a realistic environment and threat capability must analytically support budget development. Certifications by USD(P&R), the Joint Staff J7, and the Director of Cost Assessment and Program Evaluation (D,CAPE) could be used to enforce compliance.
- Establish strategic offensive EMSO function, similar to what China has done with their Strategic Support Force. I advise assigning a single Service responsibility for this function and then prioritizing funding to man, train, and equip these forces.

While organization and authority are important, the greatest risk I see is continuing to apply legacy strategies to the realities of today. I again thank you for the opportunity to testify and look forward to your questions.

Dr. William Conley
Chief Technology Officer, Mercury

Bill Conley is Mercury's Chief Technology Officer and is responsible for the technical vision and implementation of strategic objectives. He is responsible for aligning technology investments across the company to meet customer needs. Bill has substantial experience in research, development, weapon system acquisition, technology road mapping, strategy development & implementation, and government.

Prior to joining Mercury, Dr. Conley was a member of the Federal Senior Executive Service, serving as the Director for Electronic Warfare in the Office of the Secretary of Defense. In that role, he led the $7B annual investment to develop and acquire electronic warfare weapon systems. Earlier in his civilian career, he was a program manager at the Defense Advanced Research Projects Agency, better known as DARPA, where he led a innovative investment portfolio focused on electronic warfare. He started his civilian career as an engineer for the Navy. While his individual contributions were recognized through multiple awards, he is most proud of the team awards from the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Association of Old Crows Capitol Chapter.

Dr. Conley earned a Bachelor of Arts from Whitman College and a Bachelor of Science and Doctor of Philosophy from Purdue University.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: March 19, 2021

Hearing Subject:

Department of Defense Electromagnetic Spectrum Operations: Challenges and Opportunities in the Invisible Battlespace

Witness name: William Conley

Position/Title: Dr.

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
Mercury Systems	Senior Vice President & Chief Technology Officer
Reginald Victor Jones Institute	Board of Directors - no fiscal relationship
National Defense Industrial Association Central Georgia Chapter	Board of Directors - no fiscal relationship
Hudson Institute Center for Defense Concepts and Technology	Board of Advisors - no fiscal relationship

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Employment	Mercury Systems	$104,456	Employee

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Employment	Mercury Systems	$480,702	Employee

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Employment	Mercury Systems	$62,096	Employee
Employment	Office of the Secretary of Defense	$155,046	Employee

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Employment	Office of the Secretary of Defense	$165,054	Employee

United States Government Accountability Office

Testimony

Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 3:00 p.m. ET
Friday, March 19, 2021

ELECTROMAGNETIC SPECTRUM OPERATIONS

DOD Needs to Take Action to Help Ensure Superiority

Statement of Joseph W. Kirschbaum, PhD, Director, Defense Capabilities and Management

GAO-21-440T

GAO@100

Highlights

Highlights of GAO-21-440T, a testimony before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representative

Why GAO Did This Study

The spectrum is essential for facilitating control in operational environments and affects operations in the air, land, sea, space, and cyberspace domains. Spectrum use is pervasive across warfighting domains and thus maintaining or achieving spectrum superiority against an adversary is critical to battlefield success.

This statement summarizes: (1) the importance of the spectrum; (2) challenges to DOD's superiority in the spectrum; and (3) the extent to which DOD has implemented spectrum-related strategies and is positioned to achieve future goals.

This statement is based on GAO's December 2020 report (GAO-21-64) and updates conducted in March 2021. For the report, GAO analyzed 43 studies identified through a literature review, reviewed DOD documentation, and interviewed DOD officials and subject matter experts. For the updates, GAO reviewed materials that DOD provided in March 2021.

What GAO Recommends

In its December 2020 report, GAO made five recommendations, including that DOD should identify processes and procedures, reform governance structures, assign leadership for strategy implementation, issue an implementation plan, and develop oversight processes. DOD generally concurred with the recommendations, and as of early March 2021 has an implementation plan being reviewed by senior leaders.

View GAO-21-440T. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

March 2021

ELECTROMAGNETIC SPECTRUM OPERATIONS

DOD Needs to Take Action to Help Ensure Superiority

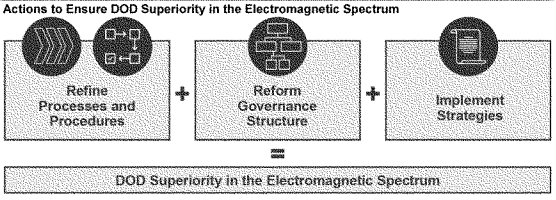
What GAO Found

The electromagnetic spectrum (the spectrum) consists of frequencies worldwide that support many civilian and military uses, from mobile phone networks and radios to navigation and weapons. This invisible battlespace is essential to Department of Defense (DOD) operations in all domains—air, land, sea, space, and cyberspace. The interruption of U.S. forces' access to the spectrum can result in a military disadvantage, preventing U.S. forces from operating as planned and desired.

According to the studies by DOD and others that GAO reviewed for its December 2020 report on military operations in the spectrum, adversaries, such as China and Russia, are also aware of the importance of the spectrum and have taken significant steps to improve their own capabilities that challenge DOD and its operations. For example, studies described how China has formed new military units and fielded new unmanned aerial vehicles with spectrum warfare capabilities, and Russian electromagnetic warfare forces have demonstrated their effectiveness through successful real-world applications against U.S. and foreign militaries. These developments are particularly concerning in the context of challenges to DOD's spectrum superiority. GAO's analysis of the studies highlighted DOD management challenges such as dispersed governance, limited full-time senior-level leadership, outdated capabilities, a lengthy acquisition process, increased spectrum competition and congestion, and a gap in experienced staff and realistic training.

GAO found that DOD had issued strategies in 2013 and 2017 to address spectrum-related challenges, but did not fully implement either strategy because DOD did not assign senior leaders with appropriate authorities and resources or establish oversight processes for implementation. DOD published a new strategy in October 2020, but GAO found in December 2020 the department risks not achieving the new strategy's goals because it had not taken key actions—such as identifying processes and procedures to integrate spectrum operations across the department, reforming governance structures, and clearly assigning leadership for strategy implementation. Also, it had not developed oversight processes, such as an implementation plan, that would help ensure accountability and implementation of the 2020 strategy goals (see figure).

Actions to Ensure DOD Superiority in the Electromagnetic Spectrum



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-440T

Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee:

I am pleased to be here today to discuss the vital role of the electromagnetic spectrum (the spectrum) in the Department of Defense's (DOD) military operations. The spectrum is the range of all frequencies of electromagnetic radiation that are subdivided into frequency bands. A wide variety of technologies use these frequency bands to operate. From using GPS and listening to streaming, satellite, FM, or AM radio stations in our cars to the military's infrared goggles illuminating soldiers' views of the battlefield, we depend on the spectrum. For this reason, control of this invisible battlespace is essential in ensuring our national security.

We are not the only global power to recognize the importance of spectrum superiority. Potential adversaries, including Russia and China, have made great strides in improving their electromagnetic warfare capabilities and use of the spectrum in general. While DOD has recognized this problem and has taken some steps that may help address this issue, the United States can no longer be assured of superiority in the spectrum.

DOD has published several strategies related to the spectrum, but the department has faced challenges in fully implementing them.[1] For example, DOD Chief Information Officer officials stated that officials involved in implementing the 2013 strategy could not compel action from other DOD organizations and received only temporary resources. DOD released the 2020 Electromagnetic Spectrum Superiority Strategy in October 2020 to try to unify the department's approach to ensuring control of the spectrum.[2] It is important for DOD to be well positioned to implement its 2020 strategy so that the United States will be able to effectively counter our potential adversaries' increasing capabilities in electromagnetic warfare. DOD's efforts are critical to ensuring the national security for our country and for our allies.

My testimony today provides information on (1) the criticality of the spectrum to military operations, (2) adversarial advances in spectrum

[1]Department of Defense, *Department of Defense Electromagnetic Spectrum Strategy 2013: A Call to Action*; Department of Defense, *The DOD Electronic Warfare Strategy* (2017) (FOUO).

[2]Department of Defense, *Department of Defense Electromagnetic Spectrum Superiority Strategy* (October 2020).

capabilities compared to previously identified DOD spectrum challenges; and (3) the extent to which DOD is positioned to ensure spectrum superiority.

This statement is based on the report we issued in December 2020.[3] To conduct that work, we performed a literature search and identified 43 unclassified, independent studies.[4] We also assessed DOD strategies, policies, and other documents, and interviewed DOD officials. In addition, we obtained updates in March 2021. Specifically, we reviewed written information from DOD about relevant actions it had taken and planned to take. Our December 2020 report provides more details on the scope and methodologies we used to carry out our work.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DOD Uses the Spectrum for Military Applications in All Domains

DOD is dependent upon the electromagnetic spectrum across all warfighting domains—air, land, sea, space and cyberspace (see figure 1). Gaining and maintaining control within the spectrum allows DOD freedom of maneuver and action and the ability to achieve tactical, operational, and strategic advantage. However, U.S. forces compete with adversaries as well as neutral parties for access and control. The interruption of U.S. forces' access to the spectrum can result in a military disadvantage, preventing U.S. forces from operating as planned and desired.

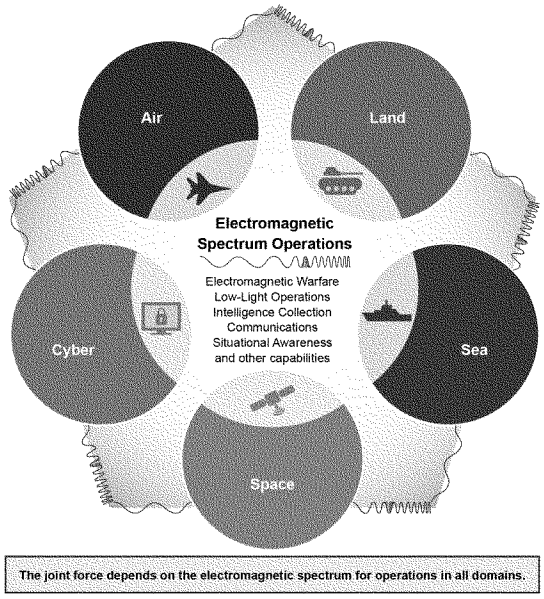
The U.S. military's use of the spectrum can identify threats and provide joint forces with information in real time. For example, signals intelligence, information operations, and command and control functions that link

[3]GAO, *Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64 (Washington, D.C.: Dec. 10, 2020).

[4]These 43 assessments, reviews, and studies were published from January 2010 through April 2020 and issued by DOD, performed on behalf of DOD by organizations such as RAND and the Institute for Defense Analyses, and independent organizations including our prior reports and Congressional Research Service reports. We did not analyze classified information because of the effects on government operations related to the coronavirus disease 2019 (COVID-19). We interviewed DOD subject matter experts to verify that classified information would not change our findings and conclusions.

communications between U.S. military forces rely on the electromagnetic spectrum. Access to the spectrum also allows troops to identify friendly and adversarial forces, access targeting support, and implement self-protection countermeasures.

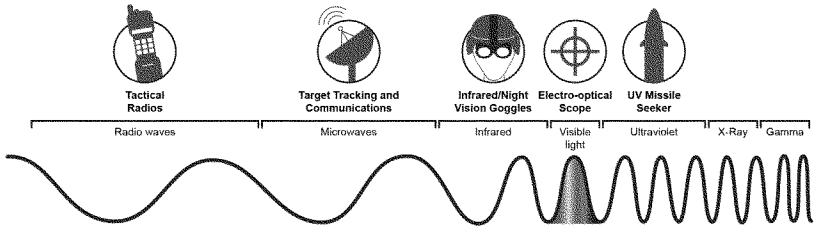
Figure 1: DOD's Use of the Electromagnetic Spectrum across Warfighting Domains



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-440T

At a more tactical level, DOD uses the spectrum to support a range of applications such as tactical radios, target tracking, and night-vision goggles, among other uses (see figure 2).

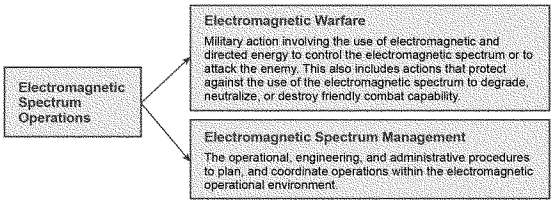
Figure 2: The Electromagnetic Spectrum and Department of Defense Applications



Source: GAO analysis based on Department of Defense information. | GAO-21-440T

DOD defines electromagnetic spectrum operations as coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment.[5] As shown in figure 3, these operations include electromagnetic warfare (i.e., the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack adversaries) and electromagnetic spectrum management.

Figure 3: Electromagnetic Spectrum Operations Are Composed of Two Coordinated Efforts



Source: GAO analysis of Department of Defense information. | GAO-21-440T

[5]Chairman of the Joint Chiefs of Staff, *Joint Publication 3-85. Joint Electromagnetic Spectrum Operations* (May 22, 2020).

Threats and Challenges to Spectrum Superiority Jeopardize DOD Operations

Adversaries Have Incorporated Spectrum Dominance as a Key Enabler against the United States

The summary of 2018 National Defense Strategy identified the reemergence of long-term, strategic competition and described the ways in which China and Russia seek to shape the world.[6] DOD reported in 2019 that while the United States focused on counter-terrorism, China and Russia were working to advance their spectrum-related capabilities.[7]

- **China** has formed new military units to achieve dominance in the spectrum and centralized space, cyber, electromagnetic warfare capabilities, and potentially psychological warfare, according to studies we reviewed for our December 2020 report.[8] A 2019 DOD report to Congress also stated that China has fielded several types of unmanned aerial vehicles with electromagnetic warfare systems.[9] China has also begun to practice, evaluate, and improve the use of spectrum-related capabilities in training events where units jam or confuse communications, sensors, and satellite navigation systems.[10]

[6]Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Jan. 19, 2018).

[7]Department of Defense, *Report on FY 2019 NDAA Section 1053, Guidance on the Electronic Warfare Mission Area and Joint Electromagnetic Spectrum Operations,* (Sept. 30, 2019).

[8]RAND Corporation, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: 2018). Costello, John and Joe McReynolds. Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, National Defense University. *China's Strategic Support Force: A Force for a New Era.* (Washington, D.C.: 2018).

[9]Department of Defense, Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (May 2, 2019).

[10]Clark, Bryan, Whitney Morgan McNamara, and Timothy A. Walton. Center for Strategic and Budgetary Assessments. *Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum.* (Washington, D.C.: 2019).

- **Russia** has been working to realize its spectrum goals. The Defense Intelligence Agency in 2019 described Russia's electromagnetic warfare forces as "world-class," and stated that Russia was capable of destroying others' command, control, communications, and intelligence capabilities.[11] Russia's electromagnetic warfare systems are highly mobile, making it more difficult for others to combat. Since 2014, Russia has also taken advantage of military operations in Ukraine and Syria to gain practical experience in electromagnetic warfare and has developed counter-space warfare capabilities.[12] For example, 2019 research suggests that Russia may be developing next generation nuclear reactors that could interfere with electronic signals in space.

In February 2021, we reported on the possibility of China and Russia using spectrum capabilities to disrupt communication and navigation systems on ships that DOD relies on to rapidly move equipment and personnel.[13] Specifically, we reported that the aging ships DOD uses for sealift do not have the defensive capabilities that might be needed in environments where China or Russia are also operating. For example, these ships could be susceptible to GPS spoofing, where manipulated signals deceive a GPS receiver.

Studies by DOD and Other Organizations Have Identified Multiple Challenges to Ensuring DOD's Spectrum Superiority

Our adversaries' developments are particularly concerning in the context of challenges within the department that many studies have identified about DOD's spectrum superiority. We found in December 2020 that nearly three-quarters of the 43 studies we analyzed described challenges, such as outdated capabilities, a lengthy acquisition process, increased spectrum competition and congestion, and gaps in experienced staff and realistic training.[14] Some spectrum technologies that DOD employs are

[11]Department of Defense, Defense Intelligence Agency, Russian Military Power: Building a Military to Support Great Power Aspirations, DIA-11-1704-161 (2017).

[12]Center for Strategic and Budgetary Assessments, *Recognizing the Electromagnetic Spectrum as an Operational Domain* (Dec. 22, 2017). Center for Strategic and International Studies, The Aerospace Security Project, *Space Threat Assessment 2020* (Washington, D.C.: March 2020).

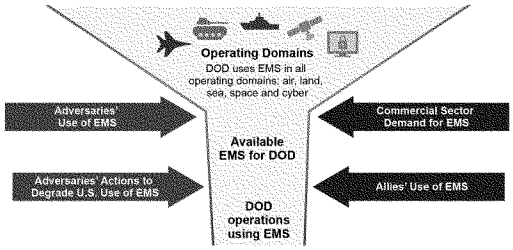
[13]GAO, *Defense Transportation: DOD Can Better Leverage Existing Contested Mobility Studies and Improve Training*, GAO-21-125 (Washington, D.C.: Feb. 26, 2021).

[14]See GAO-21-64 for a complete list of studies reviewed, including the studies that identify spectrum-related challenges, and the recommendations within those studies to address ongoing spectrum-related challenges.

outdated and have not functionally changed in design since they were fielded decades ago. Studies stated that, combined with DOD's slow and disjointed acquisition process, these dated technologies make it more difficult for DOD to field new and innovative technology, while our adversaries are developing satellite communication jammers and space-based lasers.

Another challenge that studies identified relates to spectrum competition and congestion. As more users use the spectrum—such as commercial entities, allies, and adversaries—military operations in the spectrum have become increasingly congested and contested (see figure 4). This crowding of the spectrum can lead to unintentional interference.[15] DOD officials have expressed concern that spectrum auctions and reallocations have limited the amount of spectrum available for military operations.

Figure 4: Increased Competition for Electromagnetic Spectrum (EMS) Decreases Availability for DOD Use



Source: GAO analysis of Department of Defense (DOD) information and non-DOD information. | GAO-21-440T

According to DOD officials, DOD had not prioritized spectrum operations over the past few decades. The result is that institutional knowledge of electromagnetic warfare and associated needs has deteriorated in the department. Compounding this issue, DOD has experienced challenges in training troops to operate in the kind of degraded electromagnetic

[15]Department of Defense, Office of the Chief Information Officer, *Information Paper: Expanded Office of the Secretary of Defense Level Responsibilities Necessary for the Full Range of Electromagnetic Spectrum (EMS) Activities within the Department of Defense.* (Jan. 20, 2020).

environment that it might face in real-world operations. DOD has made some improvements, but troops generally are not training in realistic conditions.

DOD Has Not Fully Implemented Prior Strategies for the Spectrum and Is at Risk of Not Achieving Long-Term Goals

DOD Did Not Fully Implement Its 2013 and 2017 Strategies

DOD issued two department-wide spectrum-related strategies in 2013 and 2017,[16] and published a third strategy in October 2020.[17] DOD's stated intention for its 2020 strategy is to bring together and expand the 2013 and 2017 strategies. The previous strategies presented several courses of action for DOD to adapt to the changing, congested, and contested spectrum environment, and to develop capabilities in this area. The 2020 strategy seeks to build on its predecessors as well as position the department to look at the spectrum holistically, lay the foundation for a robust spectrum enterprise, prepare professionals to leverage new technologies, and focus on strengthening alliances.

Our December 2020 report found that DOD had not fully implemented the 2013 and 2017 strategies, which we determined to be associated with bureaucratic and organizational hindrances within DOD. Specifically, DOD had not taken key actions to revise governance and oversight. For example, DOD officials told us they thought the 2013 strategy was successful at driving culture change and the way the department thought about the spectrum, but not all components called upon to implement the strategy's tasks did so. Specifically, as of January 2019 (i.e., more than 5 years after the 2013 strategy was issued), three of 23 recommendations based on the strategy had been completed. For example, DOD assessed

[16]DOD refers to the two strategies as the 2013 DOD Electromagnetic Spectrum Strategy and the 2017 Electronic Warfare Strategy.

[17]Department of Defense, *Department of Defense Electromagnetic Spectrum Superiority Strategy* (October 2020).

that it had made limited progress in writing new policy for spectrum sharing (due in 2016), and had not completed evaluating mission impacts related to spectrum access (due in 2017).

DOD also had limited success implementing the 2017 strategy. This strategy aimed to organize, train, and equip forces to be offensively focused, ready to gain and ensure spectrum superiority, and unified in effort. For example, in response to the strategy calling for an electromagnetic warfare workforce, each service established officer and enlisted communities that include such expertise. But these efforts generally placed these groups within broader communities or with cyber communities, and did not result in the intended emphasis on electromagnetic warfare. DOD officials agreed that this represented limited progress in implementing the 2017 strategy.

DOD Must Take Key Action to Ensure That the 2020 Strategy Is Implemented and Goals Are Achieved

Our December 2020 report also found that DOD had not completed congressionally mandated actions, nor had it addressed factors that contributed to the previous strategies' stalled implementation, and that this threatened the potential success of the 2020 strategy. Specifically, we found that the department had not issued processes and procedures, proposed and implemented governance reforms, assigned a senior official to oversee implementation of the strategy, and identified oversight activities. We made five recommendations to address these issues and DOD generally concurred with these recommendations. Each issue is discussed in more detail below.

Issue processes and procedures to integrate spectrum operations across DOD. In the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Congress required the Secretary of Defense to take specific actions related to processes and procedures for the spectrum.[18] Our analysis found that DOD had taken some steps, such as issuing guidance, but these did not cover all process and procedure elements required by the statute.

DOD has been submitting reports to Congress on its progress in meeting the statutory requirements, but we found that the reports did not address

[18]The specific statutory requirements were to 1) establish processes and procedures to develop, integrate, and enhance the electromagnetic warfare mission area and the conduct of joint spectrum operations in all domains across the department; and 2) ensure that such processes and procedures provide for integrated defense-wide strategy, planning, and budgeting with respect to the conduct of such operations, including activities conducted to counter and deter such operations by malign actors. See Pub. L. No. 115-232, § 1053(a)(1-2) (2018).

the required processes and procedures. DOD agreed with our recommendation that the department should issue the required processes and procedures, and stated that it would take action via an implementation plan for the 2020 strategy. As of early March 2021, DOD officials told us that senior DOD officials were reviewing the draft implementation plan but said they did not have a timeframe for when the department would publish the plan.

Propose and implement governance reforms. Multiple studies that we reviewed identified governance as a major challenge for DOD spectrum operations, including dispersed governance across the department and full-time responsibilities being located at lower organizational levels. For example, DOD officials said there is no central coordinating authority for the multiple offices with spectrum duties. The Institute for Defense Analyses reported that having so many offices with spectrum duties means in practice, nobody is accountable for addressing the spectrum as a whole and the Secretary has nowhere to turn for decisive action.[19]

Congress similarly shared this concern about governance and mandated that the Secretary of Defense designate a senior official to help address this problem by proposing governance and management reforms.[20] The Secretary established a cross-functional team consistent with this statutory requirement and another section of the act.[21] However, DOD's progress reports from 2019 through 2020 acknowledged that governance issues persisted and continued to put DOD's spectrum operations at risk. Our work found DOD did not address reforms needed to resolve this problem. For example, the 2020 status report to Congress stated that the DOD Chief Information Officer has sufficient authorities to serve as DOD's lead for spectrum issues. However, the same report stated that the cross-functional team believed the current Chief Information Officer structure limits its influence to advance spectrum issues within the department.[22]

[19]Institute for Defense Analyses, *Independent Assessment of EMS Enterprise Organizational Alternatives,* (Alexandria, VA.: 2019), 4.

[20]Pub. L. No. 115-232, § 1053(b)(2)(C) (2018).

[21]Pub. L. No. 115-232, §§ 918 and 1053(c) (2018).

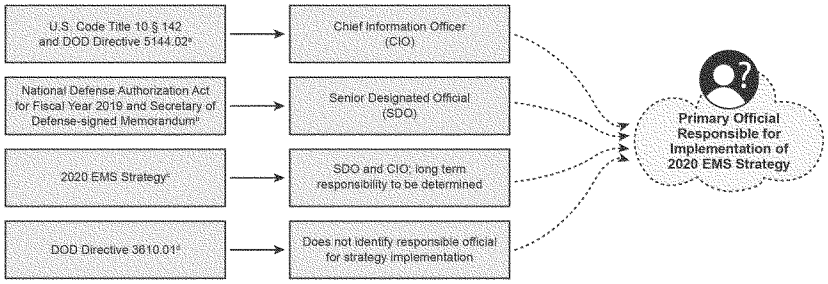
[22]Department of Defense, *Second Report on Section 1053(d)(4) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Guidance on the Electronic Warfare Mission Area and Joint Electromagnetic Spectrum Operations.* (July 2020).

A cross-functional team official told us during our review these governance reforms will come about as part of the new 2020 strategy. While the 2020 strategy identifies effective spectrum governance as a goal, a strategic goal is not the same as specific proposals for reform. DOD agreed with our December 2020 recommendation that the Vice Chairman of the Joint Chiefs of Staff, as the Senior Designated Official of the cross-functional team, should propose these reforms. In mid-March 2021, DOD stated that the implementation plan for the 2020 strategy would address this recommendation by including spectrum governance reforms.

Assign a senior official with appropriate authority to oversee long-term strategy implementation. We found that DOD had not taken another key governance action—assigning a senior official with appropriate authority and resources to ensure that the new 2020 strategy is implemented long-term. According to DOD, the lack of an official with appropriate authority likely limited the success of the previous 2013 and 2017 strategies. Implementation of the 2020 strategy is due to begin April 1, 2021, 180 days after the 2020 strategy was issued. As shown in figure 5 below, we found that the lack of clarity across DOD guidance and federal law about which official is primarily responsible for long-term implementation contrasts with the 2020 strategy's long-term vision for superiority in the spectrum.[23] In particular, four different DOD documents assign responsibilities related to the spectrum. They are not consistent about which official has the authority and resources to organize efforts across DOD components and to ensure they implement the department's strategy and goals.

[23]The long-term vision in the 2020 strategy aims for forces in 2030 and beyond to be ready to fight and win through the deliberate, institutional pursuit of spectrum superiority. *Department of Defense Electromagnetic Spectrum Superiority Strategy*.

Figure 5: Federal Laws and Department of Defense Documents Related to Electromagnetic Spectrum (EMS) Strategy Implementation



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-440T

[a]CIO officials told us that they believe their statutory and department-assigned responsibilities will make the CIO responsible for overseeing strategy implementation.

[b]These documents assign responsibility to the SDO (Vice Chairman of the Joint Chiefs of Staff).

[c]The foreword of the strategy states that the SDO, in partnership with the CIO, will oversee strategy implementation. However, the strategy later states the SDO will oversee strategy implementation only until this responsibility transitions to a permanent governing entity, but does not identify who this permanent governing entity will be.

[d]DOD Directive 3610.01, Electromagnetic Spectrum Enterprise Policy (Sept. 4, 2020) assigns responsibilities for enabling spectrum superiority. However, this directive does not identify an official responsible for strategy implementation.

Similar governance issues limited DOD's progress on previous efforts. For example, the Chief Information Officer staff said officials involved with implementing the 2013 strategy did not have the seniority to compel other components to act, and DOD provided only temporary resources. Similarly, the Electronic Warfare Executive Committee that was responsible for implementing the 2017 strategy had portfolio constraints that limited their ability to do so. We also found that the Chief Information Officer does not have the ability to influence the services' budgets or compel them to take action for electromagnetic warfare or other acquisition programs.

This challenge is not unique to the spectrum, especially within DOD's information environment, but we have an example of when DOD has successfully taken a different approach to leadership. For example, when

it issued the 2018 DOD Cyber Strategy, DOD clearly assigned long-term leadership responsibilities and associated authority. According to officials from the Office of the Principal Cyber Advisor, DOD made the Principal Cyber Advisor responsible for and accountable to the Secretary of Defense for ensuring the strategy's implementation. Also, the Principal Cyber Advisor was established as an enduring position, so the official and their office were in a position to oversee implementation and transitions across cyber strategies. The officials said this consistency enabled DOD to more effectively achieve the goals identified in the cyber strategy. Congress took similar action in the National Defense Authorization Act for Fiscal Year 2020, mandating that the Secretary of Defense designate a Principal Information Operations Advisor.[24]

As a result, we recommended the assignment of clear responsibility with the necessary authority and resources for implementing the 2020 strategy. DOD agreed with the intent of our recommendation, and in early March 2021 a DOD official told us that the department planned to address this issue in the strategy's implementation plan.

Issue an implementation plan and create associated oversight activities. We found that gaps in DOD's oversight processes for the previous strategies meant that it was at risk of not implementing the 2020 strategy. Oversight processes include elements such as descriptions of how objectives are to be achieved and by when (e.g., in an implementation plan), performance metrics, and regular process reviews.

Specifically, we found that DOD did not issue implementation plans in a timely manner for the previous spectrum-related strategies. Further, we found that as of December 2020, DOD had not taken actions that would be needed to fulfill an implementation plan and support meeting the strategy's objectives. In particular, DOD had not decided which senior officials would be accountable for taking action and providing progress reports.

These gaps are similar to our findings in previous work on DOD information operations. In 2019, we reported that DOD made limited progress implementing its 2016 strategy for operations in the information environment in part because it lacked oversight processes.[25] In that

[24]Pub. L. No. 116-92, § 1631(a)(1) (2019).

[25]GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU, (Washington, D.C.: Oct. 18, 2019).

report, we recommended that DOD establish a process to facilitate implementation for a revised strategy. We made similar recommendations in our recent spectrum review that DOD ensure it issues an implementation plan and also create an oversight process to facilitate the implementation. DOD agreed with the intent of the recommendations, but stated that it also needed to decide who would be responsible for long-term implementation. In early March 2021, an official told us this would be part of the finalization of the implementation plan. As previously discussed, senior DOD officials were reviewing the draft implementation plan at that time and DOD did not have a timeframe for when the department would publish the plan.

On April 1, 2021, DOD will reach the 180-day timeframe established in the strategy for issuing an implementation plan. We believe that DOD will continue to encounter similar challenges as with the previous strategies unless it takes specific actions, as we recommended in December 2020, to overcome the bureaucratic and structural roadblocks that exist within such a large and complex department. For example, an implementation plan will help ensure that DOD facilitates action related to the strategy. Further, developing oversight processes to facilitate strategy implementation would better position DOD to make measurable progress, fully implement the 2020 strategy, and achieve the department's future spectrum superiority goals.

In conclusion, DOD's response to our December report shows that officials are aware of the challenges and opportunities affecting military use of the spectrum. Ultimately, by addressing the gaps and challenges noted in our report, DOD would improve its ability to manage the use of the spectrum in military operations, and influence and interrupt the ability of our adversaries to use the spectrum when we need to. DOD has opportunities for further improvements to protect all of our systems—weapon systems, communication systems, computer systems, networks, and all other capabilities that are vital to military operations in the Information Age. This is especially critical as the department pursues spectrum superiority given that our adversaries have made great strides during the last two decades and will likely continue to do so. I look forward to continuing to work with you and the department to help it address spectrum challenges and to make the most of its opportunities.

Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions about this testimony, please contact Joseph W. Kirschbaum, Director, Defense Capabilities and Management, at (202) 512-9971 or Kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Tommy Baril (Assistant Director), Jennifer Spence (Analyst-in-Charge), Haley Dunn, Matthew Jacobs, and Gabrielle Matuzsan. Other contributors to the testimony include Nicolaas Cornelisse (Assistant Director), Kasea Hamar (Assistant Director), Usman Ahmad, Tracy Barnes, Yecenia Camarillo, Adrianne Cline, Carolyn Demaree, David Jones, Richard Powelson, Terry Richardson, Pamela Snedden, Jordan Tibbetts, Hai Tran, and Yee Wong.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/fraudnet/fraudnet.htm Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

Joseph W. Kirschbaum, PhD

Joe Kirschbaum is a Director in the Defense Capabilities and Management Team of the U.S. Government Accountability Office (GAO). He assists congressional committees by overseeing evaluations of U.S. Government programs in the Strategic Warfare and Intelligence area, focusing mostly on the Department of Defense.

Over his 27-year career with GAO, Mr. Kirschbaum conducted and led audits throughout the range of defense and national security programs. Among the topics he has covered are U.S. strategic nuclear forces; military cyberspace doctrine and operations; information operations; intelligence, surveillance, and reconnaissance; counterproliferation of weapons of mass destruction; chemical, biological, radiological, nuclear, and high-yield explosive preparedness and consequence management; homeland defense; Army and Navy force structure; and development of the Navy's littoral combat ship. In 2013 Mr. Kirschbaum served as an acting director in GAO's Homeland Security and Justice Team, overseeing evaluations of federal emergency preparedness and homeland security programs.

Mr. Kirschbaum comes from a Navy family and upon graduating High School served briefly on active duty in the U.S. Navy's nuclear propulsion program. Mr. Kirschbaum has a Bachelors degree in History and Political Science, a Masters degree in National Security Studies (both from California State University, San Bernardino) and a Ph.D in military history from George Washington University.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 19, 2021

QUESTIONS SUBMITTED BY MR. MOULTON

Mr. MOULTON. Mr. Clark, in addition to defending our spectrum use against adversaries, we must also share spectrum overseas with allies. In your view, how can we best ensure that we successfully work with our allies in this "domain"? Should we focus on improving international standards of spectrum use? Should we focus on building interoperable systems that leverage complementary parts of the spectrum? Are there other courses of action we can pursue?

Mr. CLARK. Interoperability is one of the most significant challenges facing U.S. and allied forces in countering the threats posed by adversaries such as China and Russia. Although other opponents like Iran and transnational insurgents will contest allies' use of the spectrum, China and Russia can comprehensively attack multiple allied sensor and communication systems while also presenting challenges in other domains that increase the allies' reliance on a contested electromagnetic spectrum (EMS).

To counter Chinese and Russian EMS threats, the U.S. military is pursuing more sophisticated electromagnetic warfare (EW), radar, and communication systems that incorporate artificial intelligence-enabled controls, adaptive algorithms, and wideband apertures. In addition to circumventing enemy countermeasures or detection, these systems would enable U.S. forces to dynamically share spectrum with other users such as 5G mobile communications. However, more agile U.S. EMS capabilities could be less interoperable with legacy systems employed by allies.

One approach to sustain EMS interoperability among U.S. allies would be for DOD to share its EMS technologies and tactics, which may present security risks outside of the Five Eyes countries or fail to succeed if allies are unable to implement equivalent capabilities in their own forces. A more feasible approach would be to share new spectrum control and management technologies that improve systems already shared among allies, such as new algorithms for protecting Link-16 from jamming and interception.

For systems that are not already shared, such as ALQ–249 Next Generation Jammer or F–15 Eagle Passive Active Warning Survivability System (EPAWSS), U.S. and allied forces could focus on deconflicting operations with allies procedurally. Allied forces could geographically or spectrally separate their EMS activities by assigning zones where different allied force would conduct sensing or jamming operations. This approach may work in geographically dispersed regions like the Western Pacific, where U.S. forces may be operating forward with allied forces protecting mid and rear areas. In Eastern Europe, procedural deconfliction may be infeasible due to the constrained geography and fast operational tempo. Another approach would be near real-time deconfliction. Allied forces could use electromagnetic battle management (EMBM) systems such as the Army electronic warfare planning and management tool (EWPMT) or Navy Real-Time Spectrum Operations (RTSO) systems to plan EMS operations and communicate those plans to other allied forces shortly before they are executed. Allied units could coordinate their plans electronically using EMBM tools or use them to prevent interfering with one another's operations. This approach may the most promising because EMBM tools are already being employed in the U.S. military and could be adopted by U.S. allies with minimal disruption to their current EMS systems.

Whether done by sharing technology and tactics, procedure, or using communications, the DOD and its allied counterparts need to begin developing processes and systems that promote EMS interoperability. Otherwise, the U.S. military risks leaving behind allies that are not yet able to field the highly-adaptive and cognitive EMS capabilities being pursued by U.S. forces.

Mr. MOULTON. Dr. Kirschbaum, China has consistently and aggressively engaged with international bodies like the ITU to shape global spectrum operations in a way that benefits Chinese companies and government. What can we do to counter these efforts and ensure that our interests and values are better represented in global spectrum standards?

Dr. KIRSCHBAUM. In short, in order to be more effective in international bodies, we need to do a better job of collaborating between the federal government and the private sector and between military and civilian interests on all spectrum-related

matters. We've talked during this hearing about the level of civil-military fusion the Chinese enjoy in comparison to our own approach. This allows the Chinese to think about and operationalize broader strategic approaches to EM spectrum operations—both in the normal military operational construct and in the "gray zone" below the level of armed conflict. It also allows them to combine efforts in international bodies. Whereas Western public and private concerns tend to approach matters according to their own interests and vote separately, Chinese members tend to vote as a bloc. We have long recommended that the federal government better coordinate its own efforts in spectrum management. This involves much more than sharing separate points of view. It involves serious policy discussion to avoid conflicts and ensure progress. It also involves collaboration on technical and technological matters and opportunities for innovation that may help us better arrive at and communicate spectrum sharing practices and influence international standards. The recent National Strategy to Secure 5G provides a good example of vision and direction to collaborate and coordinate within the federal government, between public and private sectors, and for coordinated effort in international standard setting bodies. DOD's own recent strategies recognize the need to be more involved with its government and civil partners along these lines.

Mr. MOULTON. Dr. Kirschbaum, can you speak a little more about the future of secure spectrum use? We know that the Department of Defense is already investing in capabilities like millimeter wave spectrum use to mitigate communications interception. In your view, is that the appropriate use of Department resources to fight spectrum interference or interception? What, if any, alternative methods exist to help our warfighters operate on the EM spectrum without interference or interception?

Dr. KIRSCHBAUM. With respect to use of the EM spectrum, obviously, the military has different interests from other civil government bodies and from the private sector. In many cases, these interests have been in direct opposition. The military would prefer to secure unfettered access to portions of the spectrum that the civil sector deem vital for new technologies. That constriction of the spectrum is a common theme in the many studies we reviewed for our work and in discussions with defense officials. 5G is a good recent example. The military views the millimeter wavelength bands as crucial for operations. But these are among the very frequencies required for commercial success of 5G. So some sort of collaboration and accommodation will need to be achieved. One of the encouraging things we found in our work that is reflected more and more in DOD's strategies and thinking is the appreciation of the need for DOD to be a much fuller partner with federal government and commercial stakeholders on all spectrum related issues. This includes the traditional policy and governance considerations of spectrum use. It also includes a deeper commitment to exploring and collaborating on innovation and ways to use and adapt new technologies to the problem. For example, DOD's emerging Joint Operating Environment anticipates the central role artificial intelligence and quantum computing will play in managing spectrum use in general and in the future success of offensive and defensive EM spectrum capabilities. The concept of Dynamic Spectrum Sharing is one such idea DOD is committed to in order to ease sharing of the spectrum rather than attempting to wall off portions solely for military use when that might not be practical, especially in an overseas operational environment.

○