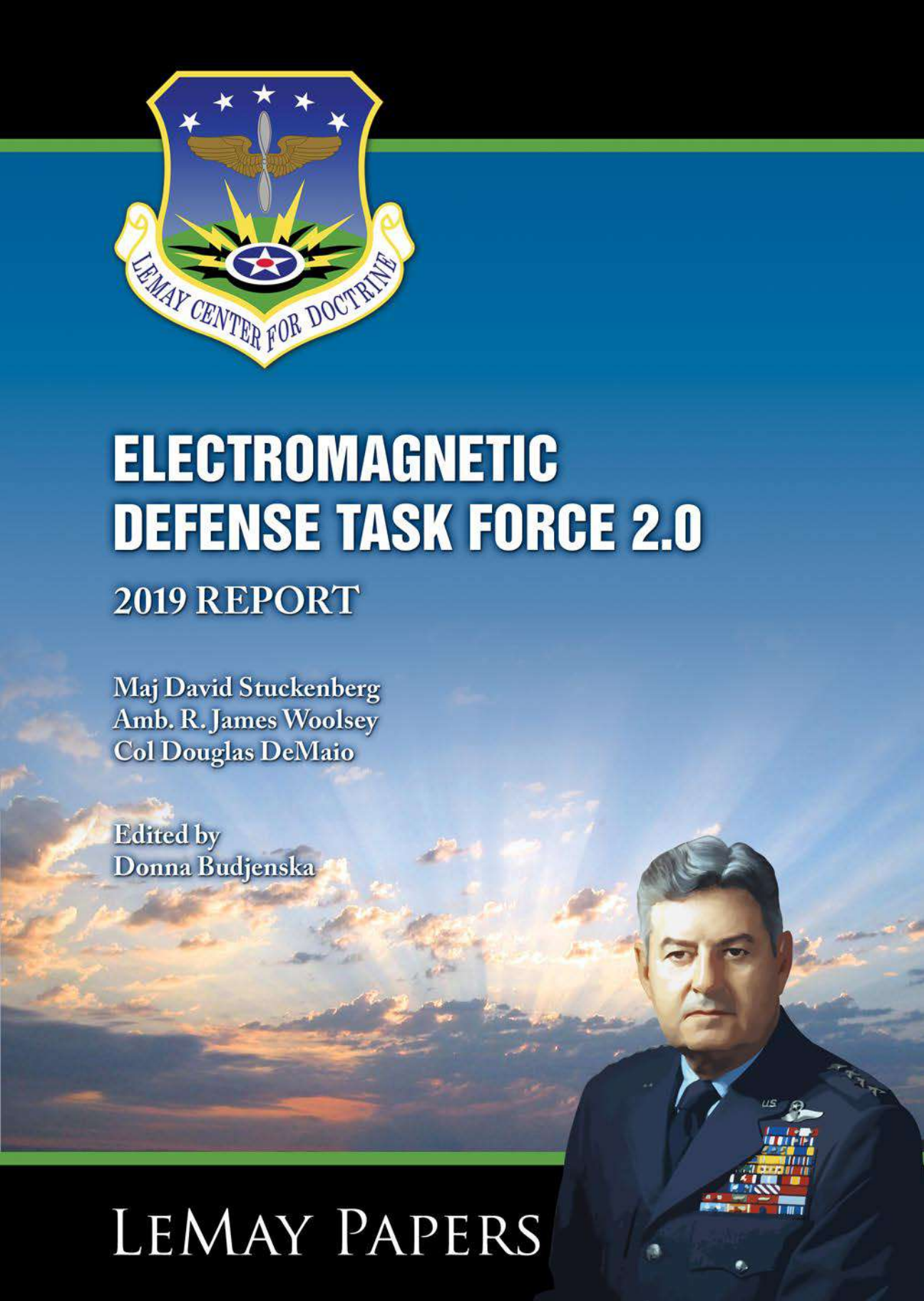
ELECTROMAGNETIC DEFENSE TASK FORCE 2.0

2019 REPORT

Maj David Stuckenberg
Amb. R. James Woolsey
Col Douglas DeMaio

Edited by
Donna Budjenska



LeMay Papers

Air University

Anthony J. Cotton, Lieutenant General, Commander and President

LeMay Center for Doctrine Development and Education

Brad M. Sullivan, Major General, Commander

AIR UNIVERSITY

LEMAY CENTER FOR DOCTRINE DEVELOPMENT AND EDUCATION

ELECTROMAGNETIC DEFENSE TASK FORCE (EDTF) 2.0

2019 REPORT

Maj David Stuckenberg
Amb. R. James Woolsey
Col Douglas DeMaio

Edited by
Donna Budjenska

LeMay Paper No. 4

Air University Press
Maxwell Air Force Base, Alabama

Commander, Curtis E. LeMay Center for Doctrine Development and Education
Maj Gen Brad M. Sullivan

Contributing Editors
Maj Jeremiah Gilmore
Mr. Dwayne Florenzie
Maj Stacy Rankin
Maj Rachel Ramirez

AIR UNIVERSITY PRESS

Director, Air University Press
Lt Col Darin Gregg

Managing Editor
Dr. Christopher Rein

Project Editor
Donna Budjenska

Cover Art, Book Design, and Illustrations
Leslie Susan Fair

Composition and Prepress Production
Nedra O. Looney

Print Preparation and Distribution
Diane Clark *Project Editor*

Air University Press

600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
https://www.airuniversity.af.edu/AUPress/

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

and

Twitter: https://twitter.com/aupress

Published by Air University Press in August 2019

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Department of Defense, the United States Air Force, the Air Education and Training Command, the Air University, or any other US government agency. Cleared for public release: distribution unlimited.

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

ELECTROMAGNETIC DEFENSE TASK FORCE (EDTF)

2019 REPORT

Approved for Public Release

This conference report is a product of the
USAF Air Education and Training Command,
Air University, and the
Curtis E. LeMay Center for Doctrine Development and Education

To obtain additional copies of this report or for additional information on the EDTF, contact Air Education Services at (800) 262-9140 or email au.education.support@us.af.mil.

Contents

Foreword

In every region of the globe, every day, the defense community works to ensure the health and security of the United States, our allies, and our interests.

The Electromagnetic Defense Task Force (EDTF), now in its second year, has provided great leadership and utility to the defense ecosystem by linking diverse experts and professionals together to make candid holistic assessments of threats emerging from within the electromagnetic spectrum. By forming a coalition of professionals without silos, the EDTF has discovered fresh insights that deserve deep consideration and perhaps bold action.

It is my hope you will continue to support and enhance this effort, and others like it, as we look over the horizon toward the threats ahead.

Lieutenant General Steven L. Kwast
Commander, Air Education and Training Command

Executive Summary

In 2018, the Electromagnetic Defense Task Force (EDTF) was created to undertake an audacious effort to holistically understand challenges and opportunities facing militaries and societies in an age increasingly dominated by the electromagnetic spectrum (EMS), a broad area of activity characterized by the visible and invisible movement of light and energy. The task force was a triage response to an enterprise-wide knowledge deficiency about the criticality of issues confronting the United States and its allies as every aspect of modern society becomes increasingly reliant on the EMS.

As the journey began, the principals assembled a coalition of experts ("fellows") like no other, including a broad and diverse range of representatives from every possible agency, including federal, military, industry, and academia. The effort also required a unique approach to addressing complex and even seemingly unsolvable challenges. To accomplish this, fellows took part in almost 5,000 hours of war-gaming and tabletop exercises (TTX) to develop a more comprehensive understanding of the central issues within the community.

The EDTF ecosystem now comprises more than 360 distinguished fellows, many of whom have invested the greater part of their careers solving and understanding the intricacies of the EMS. Covering EMS management and 5G to electromagnetic pulse (EMP) and space weather to quantum and lasers to directed energy and beyond, the task force's primary purpose is to digest and disseminate EMS knowledge of a critical nature to the defense community. Thus, in 2018, the EDTF published four key findings:

- **Finding 1:** EMP and geomagnetic disturbance (GMD) are significant and continuing threats to the military and civil society. Risks include but are not limited to nuclear power station resilience, military installation resilience, and exercise realism and training (education).
- **Finding 2:** Emerging 5G technologies and the design of regional and continental networks can present strategic threats.
- **Finding 3:** Directed energy (DE) and high-powered microwave systems can pose threats to human biology and hardware dependent on electronics.
- **Finding 4:** EMS management is struggling to maintain pace with rapid technical evolutions within the spectrum.

Furthermore, it was understood that the EMS had unique characteristics deserving priority consideration. EMS had become an essential part of every war-fighting domain (space, air, land, sea, and cyberspace)—yet was often poorly understood due to a lack of education—and it was maturing as form of

gray zone warfare (competition below the threshold of war) used by revisionist powers to challenge the "rules-based order."[1]

In short, the EMS was a powerful area of activity ready for tactical-, operational-, and strategic-level exploitation. Finally, as the task force evaluated the complexities of how modern societies function, it became apparent that along with cyber, the most unique and effective way to affect large segments of a modern nation without a retaliatory attack was to use the EMS to disrupt life-sustaining elements such as water, food, sanitation, communications, transportation, and—especially—the electric power infrastructure upon which all such systems depend. Based on extensive war gaming, the task force also found that certain EMS phenomena may potentially bypass traditional strategic deterrence schemes and present challenges to the health and economies of states, even up to the point of "stop[ping] a modern nation's broad civil and defense activities."[2]

To address these findings, the 2018 EDTF report made a series of national-, regional-, and local-level recommendations on how to increase the resilience of key military and civil critical infrastructure. The report remains one of the most accessed documents in the history of Air University and has been discussed by media around the world. In 2018, two of the task force's findings were addressed by presidential executive orders. The third finding supported Headquarters US Air Force actions. However, the work required to lend advantage to the United States and its allies, in what may prove to be one of the most technologically important areas in the history of competition, is far from complete.

In 2019, the Vice Chairman of the Joint Chiefs of Staff (VCJCS) met with EDTF leaders and noted the value of the task force to the international dis-

1. The rules-based order is often described as the international *status quo* (or way things are) while revisionist powers are those whose efforts seek to upset the international order. Chatham House, The Royal Institute of International Affairs. Chatham House, The Royal Institute of International Affairs, "The London Conference: Challenges to the Rules-Based International Order" (London: Chatham House, 2015), https://www.chathamhouse.org/london-conference-2015/background-papers/challenges-to-rules-based-international-order. The text reads: "The international order established by the victorious allies after the Second World War has been remarkably enduring. The framework of liberal political and economic rules, embodied in a network of international organizations and regulations, and shaped and enforced by the most powerful nations, both fixed the problems that had caused the war and proved resilient enough to guide the world into an entirely new era. But given its antique origins, it is not surprising that this order now seems increasingly under pressure. Challenges are coming from rising or revanchist states; from unhappy and distrustful electorates; from rapid and widespread technological change; and indeed from the economic and fiscal turmoil generated by the liberal international economic order itself."

2. David Stuckenberg, R. James Woolsey, and Douglas DeMaio, "Significant Findings," in *Electromagnetic Defense Task Force 2018 Report* (Maxwell AFB, AL: Air University Press): 7–8, https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0002_DeMaio_Electromagnetic_Defense_Task_Force.pdf.

course on the EMS. Furthermore, the VCJCS evaluated and concurred with a war-gaming scenario for use as a backdrop to answering four questions during the second summit:

1. **Based on the [EMS] scenario, assess post-event Joint Force (military) capabilities: what assets/functions remain viable?**
2. **Based on what remains viable (preserved): what Joint Force strategies/regeneration options can be realistically put forward to national leaders for recovery and/or military response?**
3. **What are our strategic blind spots in regard to each track in a severe EMS-degraded environment, and how should we place near-term bets to counter/frustrate enemy efforts?**
4. **What happens when we lose positioning, navigation, and timing (PNT)?**[3]

During the second summit held 29 April–1 May 2019, more than 220 fellows participated in a series of TTXs (or war games) organized into four tracks: (1) electromagnetic spectrum operations (EMSO), (2) high-powered electronics and microwaves (HPEM)/DE/spectrum management, (3) EMP and GMD, and (4) quantum and 5G technologies. In total, 17 teams formed, including two special teams to address nuclear power station vulnerabilities and analyze commercial reports and data generated by the electric power industry.

This report makes no claim about the consensus of the more than 100 military, civilian, academic, and corporate employers represented or the task force's sponsors, Air University and Headquarters Air Force EMS Enterprise Capability Collaboration Team (EMS/ECCT). The narrative of this report should be considered the opinions of the primary authors based on an in-depth assessment of the totality of information covered and more than 4,800 hours of war gaming and study conducted by and with the task force's fellows. A classified briefing to this report is available on request to approved individuals and organizations.

EDTF 3.0 will be held in the National Capital Region in late 2019 or early 2020. The task force would like to recognize the efforts of more than 360 fellows who continue to contribute to this body of work. Thank you!

3. PNT is roughly equivalent to the functions provided by the modern US Global Positioning System (GPS) satellite constellation.

Introduction

We live in a time like no other in history. Things once thought impossible—such as the ability to travel by air and through space, the capability to sense or detect objects at great distances and see through dense materials, and the power to effortlessly communicate and move information across the universe—are now a part of the daily normal in much of the world. All of these advancements are underpinned by the electromagnetic spectrum (EMS), and each has become increasingly integral to the functionality and sustainment of modern civilizations.

However, it is also a time when the rules of the current global order are being called into question and rewritten. This transformation is driven in part by the reemergence of a great power struggle, the democratization of capability and knowledge, and a convergence of novel technologies.[1] Where these conditions intersect with the EMS, warfare, operations, the gray zone, and conventional defense elements, the United States and its allies have an opportunity to either rapidly seize the initiative or watch competitors exploit these conditions at our expense. Seizing the opportunity and preventing adversary exploitation will require a willingness to embrace thinking freed from past paradigms.

The United States and its allies have an opportunity to either rapidly seize the initiative or watch competitors exploit these conditions at our expense.

Primacy of learning, or how something is first learned, is a powerful influence on how humans think and behave.[2] In short, primacy establishes early cognitive patterns and habits of mind—the first wiring of our brain and how we tend to instinctively think and act.[3] When demonstrated in warfare, such thought patterns have led to unimaginable outcomes.

The largest defeat of a modern army by an indigenous force was suffered by the British at Isandlwana on 22 January 1879 (in the opening volley of the Anglo-Zulu war). Armed with short spears and cowhide shields, an army of 20,000 Zulu overtook 2,200 British regulars armed with breech-loading rifles and cannon. One day after this tragedy, 139 engineers at Rorke's Drift, a

1. David Stuckenberg, "Deterrence in the Gray Zone: Understanding NATO's Strategic Sufficiency" (unpublished PhD diss., King's College London, 2019), 7–10.

2. Vernon A. Stone, "A Primacy Effect in Decision-Making by Jurors," *Journal of Communication* 19, no. 3 (September 1969): 239–47, https://doi.org/10.1111/j.1460-2466.1969.tb00846.x.

3. Stuckenberg, "Deterrence in the Gray Zone," 53.

missionary outpost converted to field hospital, successfully fended off an attack by 4,000–7,000 Zulu. In this instance, British losses were limited to just 17 while the Zulu army suffered more than 2,000. The troop numbers and technologies used in both battles were proportionally equivalent. But the outcomes of these battles demonstrate that thinking—in contrast to technology—can be the differentiating element between life and death, victory and defeat.

At the Battle of Isandlwana, a seasoned commander, Lt Gen Frederick Augustus Thesiger, allegedly ignored information and intelligence about Zulu strategy, while the young officers at Rorke's Drift, Lt John Chard and Lt Gonville Bromhead, leveraged these insights to adapt their strategy and technology to the environment. Against the backdrop of this and similar clashes, it can be said that primacy of learning is possibly the most accidently dangerous cognitive phenomenon to manifest itself in the history of warfare.[4] Primacy compels action(s) based on yesterday's ideas even if there is an intuitive understanding that such actions are destined to fail. Ironically, primacy may often endanger the most educated while advantaging the agile and even ignorant as they innovate free of tradition and thought-confining inhibitions.[5] The latter example can be thought of as "thinking to win."[6]

Sound examples of thinking to win are demonstrated again and again throughout history. From the American Revolution that used often irregular tactics against predictable British columns to the Industrial Revolution that introduced technology that would change the lives of millions, thinking to win and the use of actual environmental conditions are often decisive factors in conflict and competition that can influence the fates of nations. Thus this

4. Stuckenberg, "Deterrence in the Gray Zone," 53. This assertion is based on the broader evaluation of battles lost and casualties caused by use of outmoded warfare in the face of better designed strategies and disregarded intelligence. Another historic example was well demonstrated in Germany's use of tanks and radios under air cover to bypass French fortifications known as the Maginot Line (situated on the eastern French border with Germany). In this situation, France believed the fortifications would buy time during a German invasion and even deter invasion. However, France failed to anticipate Belgium would declare itself neutral and that Hitler's Panzer divisions would punch through the Maginot in areas characterized by forested rolling terrain. Finally, France began to believe in its own propaganda—chiefly that the Maginot Line was impenetrable. Such a belief diverted French attention from strategies that would rapidly bring troop reinforcements to the front near the Maginot.

5. Stuckenberg, "Deterrence in the Gray Zone," 154-55.

6. Howard Wheeldon, "Thinking to Win—The RAF's New Leadership Strategy," Royal Aeronautical Society, accessed 1 June 2019, https://www.aerosociety.com/news/thinking-to-win-the-rafs-new-leadership-strategy/. "Thinking to win" is not a formal definition but a broad carrier idea that encapsulates mental agility, adaptivity, intelligence, innovation, determination, and a host of other cognitive habits that enable someone to outwit, outsmart, and win against the competition. This term has been used in literature in various forms. A recent use of the term was published by the Royal Aeronautical Society, as attributed to Air Chief Marshal Sir Andrew Pulford, at a lecture given at the Defence and Security Equipment International event, London, September 2015.

report is presented, first and foremost, with an understanding that technology in conflict and competition is important, but uninhibited and intellectually honest strategic thinking is paramount.

Irrespective of operation, whether on the ground, at sea, in the air, in space, or within cyberspace, communities of thinking warriors have always been dominant. Today is no different. As our nation prepares for what lies ahead, we must think to win!

Thinking to win makes unapologetic and unbiased appraisals of not only the environment but also competitor thinking and dispositions as well. This is done in order to develop a holistic understanding that enables those working within the environment to make rapid, informed, and intelligent judgments. Such thinking is not accidental but rather intentionally developed.

During a wider appraisal of the defense community, the presence of this kind of thinking with respect to the electromagnetic spectrum has been astonishingly absent. Primacy of learning for nearly all Americans—spanning civil servants and private citizens and including our most experienced war fighters—has a built-in assumption that many of these elements will be unchallenged.

However, in 2018 the White House, US Congress, the Enterprise Capability Collaboration Team (ECCT), and Electromagnetic Defense Task Force (EDTF) simultaneously converged on the reality that the preponderance of military forces is ill prepared for an environment characterized by a degraded electromagnetic spectrum. Thus, in 2019, the EDTF shifted its focus to Joint Force resilience rather than the wider US infrastructure. Notwithstanding, the Joint Force and civil society are codependent on the same infrastructure. Thus, the primary questions explored and exercised by the task force in 2019 kept this critical element in view.

Unlike other domains that connect but can be segregated, or that terminate at definitive boundaries such as a shoreline between land and the sea or at the skyline between air and land, the EMS crosscuts all domains.

While there is little consensus on when or where an EMS degradation might occur, or even the extent of damage that may occur, there is consensus on the technical and scientific feasibility (whether natural or man-made) of the threats and risks. Natural EMS events may be produced by a coronal mass ejection (CME) from the sun interacting with Earth's magnetic field (in what is known as a geomagnetic disturbance [GMD]) or by intentional acts generating electromagnetic pulse (EMP), laser energy, microwaves, or even use of 5G systems to access and/or disrupt information networks. The potentially catastrophic effects of these types of natural

or man-made EMS events are not science fiction but science fact and have been well studied and documented for nearly six decades. These risks must continue to be addressed in accordance with responsive US laws which state, for example, "It is the policy of the United States to prepare for the effects of EMP through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement."[7]

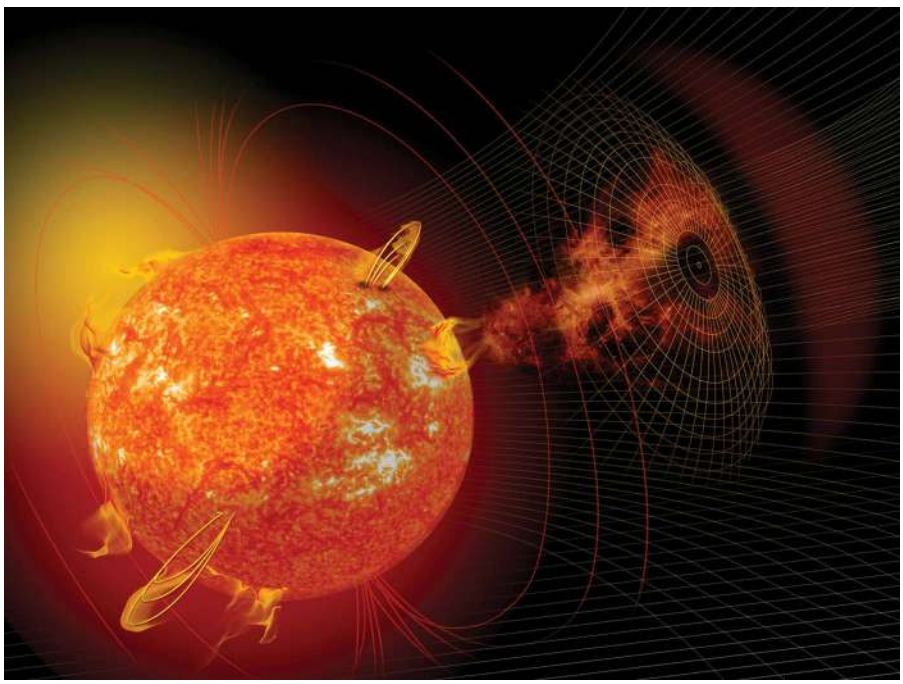


Figure 1. **Artist's depiction of a coronal mass ejection (CME)**. CMEs are magnetically generated solar phenomena that can send billions of tons of solar particles, or plasma, into space that can reach Earth one to three days later and affect electronic systems in satellites and on the ground. (Reproduced by permission from NASA.)

7. Executive Order (EO) 13865, Coordinating National Resilience to Electromagnetic Pulses, 26 March 2019, 3 C.F.R. 1, https://www.federalregister.gov/documents/2019/03/29/2019-06325/coordinating-national-resilience-to-electromagnetic-pulses. It is the policy of the United States to prepare for the effects of EMP though targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement.

Given the life-sustaining umbilical between the Joint Force and civil society, it is reasonable to expect that negative impacts to one side will bring negative impacts to the other. EMS effects may be evident regardless of whether shocks impact civil society, the military, or both and may, at times, be astonishing in scope.[8] In light of this, the EDTF advises that the strongest consideration be given to training the Joint Force in the foundational elements of how to operate and win in an EMS-degraded environment. This effort is already under way within the US Air Force and must be a national imperative not only within all military services but also within civil government. If education and training in this area are not made a priority, risk of total mission failure and loss of civil order cannot be dismissed. This is in part due to the exceptional and unique attributes of the EMS.

Unlike other domains that connect but can be segregated, or that terminate at definitive boundaries such as a shoreline between land and the sea or at the skyline between air and land, the EMS crosscuts all domains. In other words, degradation to an EMS environment can degrade operations in and permeate all other environments at the same time.

In this region of unbounded risk, current and future adversaries may attempt to achieve strategic offsets that simultaneously undermine operations in all domains. At the writing of this paper, quantum physics is advancing experimentation that allows for the instantaneous manipulation of physical properties across space and time. To date, the US and China have advanced quantum communications techniques that raise the specter of broadcast-free (with no antenna) global communications. As technologies advance, a significant EMS degradation may be potentially more devastating and ubiquitous than even large-scale and simultaneous cyberattacks.

The US faces almost impossible odds of winning future competitions if the EMS domain is insufficiently dominated by Western interests.

In understanding how to posture people and assets to counter EMS threats at all levels, it is well understood the United States has always oriented forces with respect to domains.[9] Notwithstanding, it bears consideration that the

8. John S. Foster Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood Jr., and Joan B. Woodard, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, Cong. Rept. 1-208, April 2008, https://apps.dtic.mil/dtic/tr/fulltext/u2/a484672.pdf.

9. Presently the accepted US Department of Defense war-fighting domains include air, land, sea, space, and cyberspace.

true power and potential of EMS was overlooked because our understanding of the broader environment developed piecemeal over time. Consequently, the Department of Defense (DOD) and other exponents tended to undertake disjointed and uncoordinated activities that failed to holistically address the totality of issues inherent to an exceptional, demanding, and complex environment. Thus, while in 2018 EDTF addressed the potential value in naming EMS a war-fighting domain, this 2019 report makes the strongest and most robust recommendation that EMS be declared a joint war-fighting domain.

While the concept of EMS as a domain may seem unnecessary and even adventurous, there remains virtually no other way to advantage the United States and its allies in this increasingly contested area of rapidly expanding operations. The US faces almost impossible odds of winning future competitions if the EMS domain is insufficiently dominated by Western interests. This exceptional domain cannot be isolated, is the most connected, and undergirds the very survival of electronics-dependent civilizations.

This report does not suggest creating a service component to organize, train, and equip for this environment, as these responsibilities can be, with the right emphasis, shared equally as new interservice training, operations, and standards pave the way for enhanced future operations within an existing service framework. However, it is feasible that better management of the electromagnetic domain can be later incorporated into a functional Cyber-EMS Combatant Command or an existing combatant command, such as Space Command, whose purpose would ultimately develop to exploit opportunities and mitigate risk at the nexus of space, cyberspace, and the EMS.

Finally, the future of the electromagnetic domain in competition and warfare will continue to blur, blend, fade, and set aside boundaries, which is why competitor efforts within the gray zone are strongly trending toward combined cyber-EMS activities. Thus, the use of EMS attack strategies within the gray zone may invariably change the very context of competition—yet again. From a comparison standpoint, imagine an army standing rank and file on a battlefield when, for the first time, war elephants emerge from the opposing side. This early "shock and awe" strategy not only caused battle-hardened soldiers to break formation but also caused psychological terror.

Similarly, the average person has become unconsciously dependent on the EMS to such a degree that the interruption of the EMS or EMS-dependent services will have both physical and psychological impacts. Thus, as part of broad education efforts, the public and government should be sensitized to the realistic prospect of both short- and long-term EMS outages and effects. By addressing these kinds of issues, the EDTF will continue thinking to win in the electromagnetic domain.

Joint Chiefs of Staff Questions with Task Force Findings

Within the context of the electromagnetic spectrum, the following questions were paramount to the Joint Chiefs of Staff. EDTF endeavored to provide in-depth answers to these questions against the backdrop of an intensive and technically feasible war game. The foundational premise of the war game was a significant electromagnetic attack on the 48 contiguous states.

The scenario encompassed elements of the Joint Force and large segments of US civil society and critical infrastructure. From the outset, it was apparent issues within the EMS cause many unanticipated second- and third-order effects. EMS issues that are limited in scope may rapidly translate into national issues with far-reaching effects, including the failure of transportation, food distribution systems, bulk-fuel and logistics systems, water purification and treatment, and communications and data-transmission systems. These failures were in part due to the ability of the EMS to be used as a tool to disrupt sensitive electronics that operate, run, mechanize, or govern modernized computer-based systems. Where such disruptions impacted the Joint Force, the effects often led to mission failure.

QUESTION 1: What are our strategic blind spots in regard to each track in a severe EMS-degraded environment,10 and how should we place near-term bets to counter/frustrate enemy efforts?

Over the past 20 years, the strong migration from sturdy but cumbersome legacy systems toward efficient but delicate systems has increased—by an astonishing margin—US and allied vulnerabilities to various forms of electromagnetic disruption. Additionally, a number of novel systems such as 5G, the internet of things (IoT), artificial intelligence (AI)-controlled robotics, and space-based networks are introducing variables not yet well understood. As these elements are added to key system touch-points, complexities and blind spots are being introduced at a shocking pace. Coupled with the electromagnetic domain, hypernetworked modern systems-of-systems enable actors to take powerful advantage of opportunities to disrupt and destroy critical systems in all domains—simultaneously. In this way, modern adversaries are developing robust capabilities toward leveraging the EMS domain as powerfully as the first navy that harnessed steam power to move fleets. Even now, the true power of the electromagnetic domain is only tacitly understood. Once fully leveraged, this domain will enable total communications and information control in the twenty-first century. Such may lead to a state where the dominant feature of future warfare becomes electromagnetic warfare (EW).

Once fully leveraged, this domain will enable total communications and information control in the twenty-first century. Such may lead to a state where the dominant feature of future warfare becomes electromagnetic warfare (EW).

The utility of the EMS is such that competitor military writings speak of the EMS as a secret weapon confounding all aspects of a nation, including its diplomatic, informational, military, and economic (DIME) power.[11] For example, in 1999, the Central Intelligence Agency translated the writing of two influential Chinese colonels, Qiao Liang and Wang Xiangsui, who predicted:

> The new concept of weapons will cause ordinary people and military men alike to be greatly astonished at the fact that commonplace things that are close to them can also

10. The tracks were as follows: (1) electromagnetic spectrum operations (EMSO), (2) high-powered electronics and microwaves (HPEM)/directed energy (DE)/spectrum management, (3) electromagnetic pulse (EMP) and geomagnetic disturbances (GMD); and (4) quantum and 5G technologies. In total, 17 teams were formed, including two special teams to address nuclear power station vulnerabilities and analysis of commercial reports and data sources associated with the electric power industry.

11. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 54, https://www.c4i.org/unrestricted.pdf.

> become weapons with which to engage in war. We believe that some morning people will awake to discover with surprise that quite a few gentle and kind things have begun to have offensive and lethal characteristics.[12]

It is compelling that the future utility of EMS was understood as far back as 1999 when this insight was penned. While there is little consensus as to whether or not the US and its allies are behind competitors in technology, there is little argument about the reality that US competitors are demonstrating a more complete understanding of the promise and potential of the EMS as a domain of warfare. Like the tortoise and the hare, the US as the hare has rested too long due to confidence in its initial sprint to the leading edge of capability. What follows is a brief review of how EMS is being applied to the instruments of DIME power from within the gray zone (activities below the threshold of war).

Diplomatic

In 2018, the EDTF examined EMS events and technologies that affected US embassy staffs in Cuba and China starting sometime in 2016. During a series of events unfolding over many months, diplomatic staff members were diagnosed with traumatic brain injuries (TBI), injuries typically associated with some sort of shock or blow to the skull.[13] Analysis and testing demonstrated that the internal temperature of the victims' brains had been raised by an external electromagnetic source, triggering a response similar to concussive injuries.[14] While there is no doubt the capabilities and technologies needed to conduct this kind of operation exist, these were the first instances of use against nonmilitary diplomatic staff. In keeping with activities falling

If the US continues to pursue the creation of 5G networks, planners should give full consideration to the fact they will be providing a less resilient telecommunications system. Use of this knowledge can afford planners the ability to build in resilience and mitigate vulnerabilities, up front.

12. Liang and Xiangsui, *Unrestricted Warfare*, 26.

13. Maggie Fox, "Cuban Embassy Staff Had Concussion-Like Injuries, Doctors Say," NBC News, 15 February 2018, https://www.nbcnews.com/health/health-news/cuban-embassy-staff-had-concussion-injuries-doctors-say-n848291; and Emily Rauhala and Carol Morello, "State Department Warns US Citizens in China after Employee Suffers Possible Sonic Attack," *Washington Post*, 23 May 2018, https://www.washingtonpost.com/world/asia_pacific/state-department-warns-us-citizens-in-china-after-employee-suffers-possible-sonic-attack/2018/05/23/db7bbd44-5e68-11e8-8c93-8cf33c21da8d_story.html?utm_term=.3c2618446f25.

14. William J. Broad, "Microwave Weapons Are Prime Suspect in Ills of U.S. Embassy Workers," *New York Times*, 1 September 2018, https://www.nytimes.com/2018/09/01/science/sonic-attack-cuba-microwave.html.

below the threshold of war, these unknown actors demonstrated an ability to shape environments in a nonattributable way, a case study that will likely inspire other able actors to use similar means to influence targets.

China has demonstrated a willingness to use its diplomatic ties to create economic codependencies that will further widen EMS vulnerabilities. By providing 5G subsidies to nations at rates up to 10 times higher than Western companies, China has used liberal government funding to propel its Belt and Road Initiative. There is wide consensus that the 5G network is a major strategic play to create an infrastructure within the US and allied nations that will provide ultra-high-value services. But it will also allow competitive access to the private and secure information on those same networks. This knowledge is why the US government recently blocked the sale of Chinese-manufactured 5G technologies within the United States. During EDTF, 5G technology was assessed to create unique vulnerabilities on two fronts: (1) resilience and (2) dual uses (the military use of civil technologies). Only the first vulnerability will be discussed in this report.

For all the advertised benefits of new technologies, there tend to be second- and third-order effects or unintended consequences once implementation occurs. Most of the time, these latent issues are not evaluated prior to implementation. But for perhaps the first time in the history of infrastructure development, the US and the world have an opportunity to understand the potential consequences up front. In particular, the 5G network can be thought of as handfuls of small pebbles being thrown into a pond, creating dozens of small ripples, while the 4G network can be thought of as throwing one or two large stones in a pond, creating a couple of big waves. From a broadcasting standpoint, 5G cell sites can have a signal range of only about 2,000 meters. This limited area of signal propagation requires a higher number (or higher density) of sites to achieve network coverage. On the other hand, 4G tends to be deployed at lower frequencies and enjoys much greater coverage. This allows ample network coverage with fewer towers. However, to achieve 5G coverage over an area the size of the United States will require tens of millions of 5G sites as opposed to several million 4G sites.

The sheer number of 5G sites needed to achieve broad coverage makes any 5G network difficult to protect from EMS interruption. For example, larger 4G towers are often supplied with a generator and battery backup systems to ensure reliability. Retroactively providing the same resilience to tens of millions of small 5G sites is not practical. Thus, if the US continues to pursue the creation of 5G networks, planners should give full consideration to the fact they will be providing a less resilient telecommunications system. Use of this knowledge can afford planners the ability to build in resilience and mitigate

vulnerabilities, up front. It must be understood that if this is not accomplished, the 4G infrastructure that underpins the 5G may be increasingly critical. It might be the case that the 4G network should be kept in place longer in order to provide this level of resiliency.

An example of this hindsight can be seen with GPS. This context is provided with the understanding that with 5G, as with GPS, underlying older and more resilient legacy systems will eventually be dismantled. As the US transportation system became more dependent on reliable GPS, many of the analog navigational aids that formed the original navigation system for aircraft began to be defunded and dismantled. Today, however, as our understanding of natural and man-made GPS vulnerabilities evolves, there is an understanding that analog navigation aids may actually serve well as resilient and GMD-hardened backup systems. Similar consideration should be given to both landlines and 4G systems. However, as the next section will discuss, the security of the US 4G network may already be compromised.

Informational

There is no denying the US and its allies have been the prime targets of intentional and persistent influence operations that leverage information and even white noise (i.e., fake news) to manipulate perceptions and distract the public. However, where the electromagnetic domain is concerned, this condition may be more dangerous than previously understood. Currently there is an overarching belief in wider society that, despite efforts to disrupt the US and allied aspects of DIME, these activities will not cause long-term harm. This narrative is often based on the premise that competitors like China would not harm a close trading partner or can be persuaded to act always in accordance with international law. In some respects, there is a dangerous naiveté about the degree to which the US is in a competition with powers that seek to usurp the Westphalian system[15] as a whole. Of late, EDTF members have been asked by high-level officials within government, "how can China be per-

15. Richard Coggins, "Westphalian State System," abstract, *The Concise Oxford Dictionary of Politics*, 3rd ed., 2018. Author's note: "[A] term used in international relations, supposedly arising from the Treaties of Westphalia in 1648 which ended the Thirty Years War. It is generally held to mean a system of states or international society comprising sovereign state entities possessing the monopoly of force within their mutually recognized territories. Relations between states are conducted by means of formal diplomatic ties between heads of state and governments, and international law consists of treaties made (and broken) by those sovereign entities. The term implies a separation of the domestic and international spheres, such that states may not legitimately intervene in the domestic affairs of another, whether in the pursuit of self-interest or by appeal to a higher notion of sovereignty, be it religion, ideology, or other supranational ideal. In this sense the term differentiates the 'modern' state system from earlier models, such as the Holy Roman Empire or the Ottoman Empire."

suaded to use AI in a responsible way that does not violate human rights?" While such ideas may be well intended, such thinking is based in primacy of learning and serves the purposes of disciplined competitors by working against realities. The willingness of China and other actors to set aside the current order to achieve tactical, operational, and strategic objectives is well demonstrated. However, as finite assets, manpower, and time are expended on ineffectual efforts, the objectives of competitors are well served—even if unwittingly. In short, it will always serve a competitor's interest when US or NATO efforts are inert.

Whether it is China illegally expanding territories into the commercial and territorial commons of other provinces in the South China Sea or using lasers to force allied military aircraft to land[16] or Russia using state-controlled poisons to assassinate dissidents and gray zone warfare to illegally annex territories, the brilliant use of controlled narratives has become exceedingly serious. This behavior may be catalytic as other actors increasingly see the benefits and utility demonstrated with increasing success: "In particular, since gray zone actors may be unaware of or ignore [US and] NATO dispositions with respect to the gray zone, actors may perceive this area as abandoned. Such may then reinforce the idea of unimpeded access, which in turn may inspire the pursuit of even greater ambitions."[17]

Economic

Within the United States, there is a significant risk that insurgent economic campaigns have matured to the extent that influence operations can, in some cases, prevent corrective actions. It is a well-known fact that China holds ownership of nearly 70 percent of rural America's telecommunications networks. While this is a strategic risk in and of itself, the EDTF asserts that if China has the foresight to invest in critical communications infrastructure, other infrastructure, including the electric power grid, may also manifest like vulnerabilities. In light of this, it is not unrealistic to consider that if federal action becomes a requirement to enhance the protection and resilience of the wider US bulk power grid, which is

In this way, the United States and its allies must guard against patient Trojan horse strategies designed to compromise security and stability over decades. The detection of such strategies is especially important when any critical infrastructure is concerned.

16. "Australian Navy Pilots Struck by Lasers in South China Sea," Associated Press, 28 May 2019, https://www.apnews.com/e7a2592d30d743ddaecf4bf20324d55e.

17. Stuckenberg, "Deterrence in the Gray Zone," 149–50.

composed of nearly 3,000 private companies, China's influences could, through strong financial and leadership positions in owned companies, compromise or impede federal efforts.

Richard Danzig et al. note:

> China and Russia have been faster than the United States to grasp that they are engaged in a multifaceted strategic competition. Their more comprehensive approach is evident in their use of intelligence campaigns against technological and economic targets, government orchestration of their commercial sectors, pressure on foreign companies to share data and technologies as a prerequisite to access their domestic markets, and, in China's case, long-term funding of critical technologies and the use of trade, aid, and loans as a means of building relationships.[18]

In this regard, China's strategy has often been compared to the tarantula hawk wasp.[19] While the wasp is small, it possesses one of the most painful stings in the animal kingdom. When it stings its prey, the tarantula is incapacitated. The wasp then lays eggs inside the tarantula, which later hatch–killing the host. However, this illustration does not accurately portray the strategic reality. This is in part because once the tarantula is stung by the wasp, it is aware of it. If the United States is akin to the tarantula, most do not recognize that we have been stung. Rather than a wasp, China's strategy resembles instead a microfungus called cordyceps.[20] Cordyceps reproduces via spores that migrate into the central nervous system of the host. Once it takes over the host, it will direct the host to the point of perfect sunlight, temperature, and humidity and then kill the nutrient-rich host in the ideal place to nurture further growth and reproduction; such may also be accomplished with states.[21] In this way, the United States and its allies must guard against patient Trojan horse strategies designed to compromise security and stability over decades. The detection of such strategies is especially important where critical infrastructure is concerned.

Military

As the Joint Force becomes increasingly sophisticated, it also becomes more reliant on technologies. For instance, in an effort to ensure information relevance at the speed of decision-making and to alleviate certain risks, there

18. Richard Danzig, John Allen, Phil DePoy, Lisa Disbrow, James Gosler, Avril Haines, Samuel Locklear, James Miller, James Stavridis, Paul Stockton, and Robert Work, *A Preface to Strategy: The Foundations of American National Security* (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2018), 31, https://www.jhuapl.edu/Content/documents/PrefaceToStrategy.pdf.

19. Danzig et al., *A Preface to Strategy*.

20. Stuckenberg, "Deterrence in the Gray Zone," 131.

21. Stuckenberg, "Deterrence in the Gray Zone," 131.

has been a movement to upload most unclassified DOD data to the cloud. However, because cloud networks rely on normal network hardware, where the EMS is concerned, such networks still carry risks. Although a secure server warehouse may be well protected from a variety of challenges both cyber and physical, the ability to access or destroy data—even when air gapped (an absence of a direct or indirect connection between a computer and the internet, effected for security reasons) to provide a measure of protection—means the value of such measures is being set aside through electromagnetic developments. An analogy can be drawn between this electronic evolution and the use of wood palisades (defensive walls used for protection). From early history, such barriers were raised by militaries and communities as a response to threats. However, once actors determined wooden walls could be set fire, the next generation in protective wall technology developed–the stone wall. To overcome stone walls, actors began digging under the foundations to cause collapse. As a countermeasure to mining, moats were dug and filled with water. Similar developments have been present with almost all technologies. However, there has scarcely been a time, when, despite gaps and moats, the attacker could not eventually succeed. But such conditions are rapidly changing. In this way, military network security measures may one day require robust signal hardening[22] or counterelectromagnetic fields to prevent adversary signal penetration and information network compromise. While new vulnerabilities are emerging, it is critically important to note that most systems remain unprotected even from well-known EMS threats such as EMP.

While EMP is often thought of as a short burst of energy arising from a nuclear detonation at altitude, such a pulse can also be generated by portable units such as those envisioned in the movie *Ocean's Eleven*.[23] Portable EMP systems have long been available to the public in the form of briefcases used to test signal-hardened buildings and facilities. It is conceivable that, in the future, EMP missiles may be designed and/or

In this way, military network security measures may one day require robust signal hardening or counterelectromagnetic fields to prevent adversary signal penetration and information network compromise.

22. Signal hardening is presently done on US Nuclear Command and Control systems to prevent EMP disruption; for instance, minimum performance requirements for low-risk protection from mission-aborting damage or upset due to high-altitude electromagnetic pulse (HEMP) threat environments are defined in MIL-STD-2169.

23. "EMP (Electromagnetic Pulse)," *Ocean's Eleven*, directed by Steven Soderbergh (Burbank, CA: Warner Brothers, 2001), https://www.youtube.com/watch?v=jrA-1cG_wq4.

employed to disrupt sensitive equipment aboard military aircraft. In the case of commercial aircraft, disruptions may be caused with less sophisticated means such as employing portable electromagnetic devices to disrupt navigation and fly-by-wire systems.

The opportunities for potential use of EMS for aggravated disruptions to modern systems are extensive and, in every way, on par with or even more potentially deadly than many of today's cyber and kinetic vulnerabilities. It should be noted that China has indicated it intends to develop substantial EMS capabilities in space. Such capabilities include both military and civilian applications, including space-based solar power, directed energy weapons, and lasers. While such ambitions might be dismissed, it should be noted that China has not missed a major space development benchmark since the 1980s. If such capabilities are developed for dual use, it is foreseeable that space-based assets could, in the future, serve to enforce access and denial operations. For instance, the ability to harvest solar energy without interruption can feasibly power weapons used to deny human access to communities and cities. Such can be thought of as geo-fencing but with directed or microwave energy. The same possibilities exist for space-based lasers, which could harass both commercial and nonmilitary ground-based or space-based assets.

Information Isolation

There was broad consensus among EDTF Fellows that a systemic lack of information sharing between the DOD and industry partners has led to gross misunderstandings regarding the scope and severity of EMS vulnerabilities. In some instances, there is a complete absence of knowledge. Such is especially true with respect to EMP. For example, participants noted that there is no common understanding of immediate, intermediate, and residual EMP effects on national, defense, and state systems and capabilities. While irrefutable EMP research exists (both at classified and unclassified levels), rapid changes in technology and the misinterpretation of research, potentially arising from adversary influence operations, have led to dangerous and lingering misconceptions about EMS. These misconceptions are a contributing factor in the long-standing absence of needed action. Blind spots arising from information isolation and misinformation may be addressed through the exercise of accountable leadership and information sharing and through rigorous peer review by authoritative experts.

Another point raised during deliberations relates to sharing novel technical solutions. Several companies and partners offered that there can be a reluctance to distribute proprietary data out of concern for protecting intellectual

property from adversary compromise. One proposed solution was to develop a streamlined patent process for national security–related technologies to allow IP protection and faster integration of new ideas into discussions, planning, and technologies that enhance electromagnetic resilience.

It was also noted that there is no clearinghouse or repository listing or linking EMS projects across DOD, industry, or government. The absence of a focal point leads to redundancy, reduces the opportunity for collaboration, and inhibits benchmarking. Additionally, fellows noted that institutional knowledge from previous EMP testing is rapidly disappearing—including data from nuclear testing during the 1950s, which cannot be digitized. This information should be captured and preserved in a secure repository to aid ongoing research and development. This repository should not only include historical data but also results from recent tests or simulations with modern electronics.

Finally, with respect to information isolation, the development of cross-organization information-sharing programs and a common language (definitions) are of paramount importance. Given the moratorium on above-ground nuclear weapons testing, information sharing and common definitions are necessary to build models and simulations to validate theories and claims. Furthermore, the DOD should reexamine classification controls and, where possible, downgrade and declassify in order to share findings and theories with industry and academia. Such a need became particularly evident when one of the leading technology companies in the United States acknowledged it had no idea about EMS risks associated with 5G or EMP. It was acknowledged that a flash bulletin system such as the Federal Bureau of Investigation's "Most Wanted" list could provide value by ensuring industry and academic entities possessing a national security role can stay timely informed. Along with this bulletin would be the provision of appropriate level clearances to decision-level staff.

Public Support

Another recurring theme during the conference was the acknowledgment that during the Cold War, the threat of attack on the contiguous United States was taken seriously and that the public, civic leaders, military leadership, academia, and industry actively requested information regarding threats and mitigating steps (i.e., bomb shelters, drills, etc.). Participants argued that "user pull" (public requests for action) will not happen until the nation realizes how EMS events may impact society. This idea returns to primacy of learning. In the most recent case, most Americans dismiss the possibility of a strategic attack on the homeland. Such views have been reinforced by false information

and sensational media, all of which have hindered efforts to ensure the wider US is prepared for an electromagnetic event, whether through EMP or GMD.

A recommendation for how to address this climate would be to launch a public service information campaign. These "Smokey Bear" campaigns could inform the nation of the need to become more resilient,[24] which could then extend to local community exercises. Additionally, participant discussions indicated that the military must continue to lead the way by developing a broad EMS-aware culture.

Strategy and Recovery Plan

The lack of an existing national and military plan to recover and retaliate from an EMP attack was an additional strategic blind spot. A nationwide plan, collaboratively led by both the Department of Homeland Security (DHS) and US Northern Command (USNORTHCOM), should be developed and exercised on a regular schedule. This plan should be integrated into local community exercise programs and used as means of educating the wider public on risks. Local emergency operations centers need to understand and prioritize recovery efforts and resources. It is likely nuclear power stations, airports, and hospitals will be the priority for the restoration of electricity during EMS disruptions to avoid long-term impacts to society and the nation's ecology.

Societal Psychology

Depending on the effects of an EMS attack, it is possible to see the breakdown of societal norms in as little as 72 hours. An example provided was the looting that occurred after Hurricane Katrina. Before beginning any official planning, planners must holistically understand the operating environment. Researching the psychology of human desperation, starvation, and living without the rule of law is vital to every emergency planner, especially when planning for a long-term blackout scenario. Any plan of action must provide a relatively safe environment for the people whom the plan depends on, including immediate families, for the plan to succeed. Additionally, a long-term plan to provide food, medical care, and housing, and so forth is necessary (an outline for this kind of plan may be found in the 2018 EDTF report, appendix 6: "Bullet Background Paper on Black Start Teams").

24. Author's Note: Smokey Bear is a national advertising campaign initiated by the US Forest Service in 1944; widely recognizable from television commercials and billboards, the bear mascot wears a forest service cap and says, "Only YOU can prevent forest fires." US Forest Service, 4 August 2014, https://www.fs.fed.us/features/story-smokey-bear.

EDTF recommends planners not only focus on a blackout emergency plan for the first two weeks but also plan for situations that last longer. This topic is further discussed in appendix 7: "EMS Resilience and Preparedness for Government and Society."

QUESTION 2: How can industry, academia, and military work together to counter our strategic blind spots and improve the nation's resilience?

Build a Community of Experts

To counter our strategic blind spots and improve the nation's resilience, we must include industry, energy companies, and data analysis personnel in the research and development of capability. We should invest in science, technology, engineering, and mathematics (STEM) as a public education baseline, as it will be required to support defense against EMP. In particular, few universities in the United States have specific training or education programs that encompass the cross-disciplinary aspects needed to deeply understand the physics, engineering, and mechanics of EMS hardening. Such programs should be developed with speed and intention. Parties interested in this topic should contact EDTF as the task force continues to expand its ecosystem. In particular, EDTF is interested in civilian and military fellows and subject matter experts from the following organizations: Air Force Institute of Technology (AFIT); Air Force Studies, Analysis, and Assessments (AF/A9); Air Force Office of Scientific Research; nongovernmental organizations (NGO) focused on EMS; and similar agencies.[25]

In the realm of academia, military elements may reinvigorate potential options such as Palace Acquire, which sets a career path for recruited STEM graduates. Additionally, programs should also engage younger teens (not just college graduates and not just for recruiting in the military, but also for the DOD civilian and contractor force).

The EDTF summits have created a variety of opportunities for military, industry, academia, scientific, and government leaders to discuss and collaborate on ways to mitigate EMS-related threats facing the US and NATO. What is more, it has spawned efforts to address them throughout the country. One example is an effort taking place in San Antonio, Texas.

Under the direction of the commander of the US Air Force Air Education and Training Command (AETC), a team formed using activated Air National Guard personnel to research and collaborate with military and community partners to locally implement EDTF recommendations. This innovative approach itself was the result of recommendations from EDTF 1.0 to utilize a

25. The EDTF has established a virtual working group at All Partners Access Network (APAN) Community (https://community.apan.org) to establish contact and share information across an expanding network. Anyone may request access to the group "EDTF" once they have received an APAN account.

"test city" to implement an action plan based on collaboration between the DOD and the local community to harden a base and surrounding community. In this case, the test city is San Antonio, and the DOD component is composed of the 11 installations that make up the Joint Base San Antonio (JBSA) complex.

The team is called the JBSA-Electromagnetic Defense Initiative (JBSA-EDI), and its mission statement is to "educate, collaborate, and facilitate electromagnetic spectrum operations (EMSO) of mutual interest to the JBSA civilian and military communities." To that end, JBSA-EDI has developed a strategy and collaborative partnerships with the following lines of effort:

- Infrastructure resiliency against effects from man-made or natural EMP
- 5G network implementation risk awareness and mitigation
- Electromagnetic spectrum operations policy, doctrine and education development
- Local and state strategic planning for long-term regional power grid-down scenarios

Each line of effort is based on lessons learned or recommendations from both the 2018 and 2019 EDTF summits. Collaborative partnerships between JBSA; its mission partners; local power, gas, and water utilities; local and national research institutes; academic institutions; and state agencies formed quickly. One important lesson learned is that concerns highlighted by EDTF are known throughout military, government, and civilian communities. There is widespread desire to confront and mitigate the risk from EMS threats, but without leadership to provide a catalyst for action, most organizations and institutions are unsure of their roles and responsibilities. In the San Antonio example, the JBSA-EDI is providing the catalyst and coordination that military, industry, and local government partners have quickly rallied around. While still in the research and exploratory stage, JBSA-EDI has already made an impact organizing a workshop with 50+ participants representing more than 30 military and civilian organizations. Working groups have formed around the four lines of effort, and quarterly meetings are planned to report progress and facilitate additional collaborations. The progress of this test city will be briefed at future EDTF summits.

Other lines of effort have formed in Alabama, South Carolina, and Wyoming and are now starting to integrate across similar projects due to the efforts of the EDTF. One desired and necessary outcome of the EDTF is that other "Electromagnetic Defense Initiative" style efforts form throughout the

country, each focusing on the risks and opportunities relevant to their particular location and circumstance.

Understand Dissuasion[26]

During EDTF 2.0, there was consensus that reliance on traditional deterrence constructs such as the nuclear umbrella may be woefully insufficient to prevent strategic EMS attacks. One of the reasons deterrence may be insufficient is that it relies upon attribution (knowing who attacked). Without knowledge of who attacked, the ability to retaliate is limited or nonexistent. At the fundamental level of deterrence theory, if an actor has no ability to retaliate, there is no credibility. Hence, attackers may be emboldened to act if they are convinced there may be no penalty. Consequently,

A close cousin of deterrence, the art of dissuasion is a required study in response to the limitations of deterrence when limited attribution is a realistic prospect.

> In the wake of the Cold War, tensions relaxed and many of the technological capabilities once exclusive to states were diffused to state and non-state actors alike. In place of the bipolar system, a complex and chaotic system of geopolitical and military interactions has emerged.
>
> In this emerging space, no few strategic threats may be presented by way of artful military strategy and technological creativity. Moreover, certain perplexing strategic activities can be difficult or impossible to attribute and, thus, increasingly difficult to deter. This contemporary conflict space is often called the "gray zone." The inability to deter strategic attacks within the gray zone is a potentially severe limitation of deterrence within the contemporary defense context.
>
> One potential method of preventing strategic enemy actions from within the gray zone is to ensure resilience is built into the national infrastructure of all alliance members. In this way, a state will not need to maintain the status quo through fear of retaliation or pain (which may be hard to levy when you don't know who will carry out an act), but rather diminish risk of action through a very non-specific form of general deterrence. Where more assurance is needed, however, dissuasion is the only strategy with application in the gray zone where an actor uses opacity to conceal strategic actions.

26. This section is adapted from comments presented by David Stuckenberg at King's College London, 18 January 2019: "Re-orienting NATO Deterrence: The Reality of Strategic Gray Zone Threats." Paper presented at SAS-141 Research Symposium on Deterrence & Assurance within an Alliance Framework, King's College London, UK, 17–18 January 2019, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-141/MP-SAS-141-16.pdf.

> A close cousin of deterrence, the art of dissuasion is a required study in response to the limitations of deterrence when limited attribution is a realistic prospect. Dissuasion may altogether remove the incentive for an adversary to act when deterrence cannot apply due to an inability to hold an actor at risk. Rather than keeping the status quo through a prolonged and often progressive contest of pain (hard power), dissuasion is a soft-power strategy that gets to the heart of an actor's motivation calculus. By analogy, if deterrence prevents action by threatening punishment for taking a cookie out of a container, dissuasion reinforces the idea that there is no cookie in the container to begin with, therefore an actor may never be tempted to take a cookie.
>
> Therefore, dissuasion works to prevent action by removing the enticement to act in the first place. In other words, if actors cannot achieve their desired ends—why would such act at all? In the case of a power grid, if such were hardened against [high-altitude electromagnetic pulse (HEMP)], an actor may never consider the strategic use of a HEMP as it would not have catastrophic consequences. Thus, dissuasion is a contest that seeks to remove an actor's motivation to act rather than, as with deterrence, create a fear or hold at risk to those who may have the desire or occasion to act. As a form of strategic influence, dissuasion has profound utility in the gray zone where deterrence is often misapplied or overrelied upon to prevent able actors from acting.[27]

Develop a Strategic Plan

A strategic-level plan, from deterrence to recovery, will require participation from all elements of government and industry. Cohesiveness and agreement may be difficult to obtain, as responsibilities often shift depending on the source of the EMS interference. DOD, industry, and academia must determine which organization will take charge in which situation. Organizations must have integrated exercises and testing for various plans. Furthermore, strategic planners must work with local planners to ensure the nation's resilience at the community level.

When developing a national strategy, standardized terms and definitions are important when determining responsibilities. "EMP" insinuates a nuclear detonation, "GMD" insinuates a natural occurrence, and "electromagnetic attack" describes the use of a localized weapon conducting intentional electromagnetic interference (IEMI). It is recommended that the Federal Emergency Management Agency (FEMA) classify GMD and EMP as natural disasters and that FEMA be included in future EDTF summits and EMP research events. It is also recommended that FEMA be tasked to respond to wide regional events if the power grid were destroyed.

It is also recommended that the DOD institute readiness reporting for critical assets to provide a good understanding of what will be available and function-

27. Stuckenberg, "Re-orienting NATO Deterrance."

ing after an EMS attack. To do this, DOD installation commanders will need to have an understanding of not just organic assets but all critical infrastructure functions supporting an installation's essential operations and the EMS vulnerabilities created by those dependencies. Since DOD maintains the nation's most proven EMP hardening standards, it must not only define hardening requirements for organic mission sets and provide readiness standards for reporting but must also engage local civilian critical infrastructure owners, operators, and/or partners with this information to help them determine how to harden their assets as well. In some cases, federal funding to support local critical infrastructure improvement may be required.

An additional recommendation to consider is a policy that would establish critical electrical power generation networks that can be federalized during a threat by GMD or EMP. The precedent for such actions exists in the commercial airline industry program called the Civil Reserve Air Fleet (CRAF). During a national crisis, US air carriers may have a percentage of their aircraft federalized to provide surge airlift and logistics capabilities to the DOD. Establishing an equivalent program for US power utility companies could not only buy down risk for power companies during crisis, it could also help fund additional technologies needed to protect the key infrastructure surrounding major US cities and manufacturing centers (by providing additional funding to power utility companies).

Numerous EDTF personnel working on pilot projects at the local level with electric utilities have witnessed a trend where industry partners cite industry-funded EMS or EMP research as a basis for planning and strategy. Such research includes sometimes questionable research associated with the Electric Power Research Institute (EPRI). These observations became more compelling as EDTF 2.0 convened, as EPRI released a report on EMP on the second day of the summit. Since the task force had a working group consisting of the world's foremost EMP experts digesting reports and data, the task force was able to review the EPRI report in detail. *The EDTF has determined* that *reliance on the EPRI report could result in a lack of critical infrastructure protection, particularly extra high voltage (EHV) transformers and long-lead-time replacement items required for the power grid to function.*

It is important to note that telecom service providers have established procedures for catastrophic events such as hurricanes, earthquakes, volcanoes, and power outages; the next step would be to test and include EMP resilience. Such testing should be well considered in light of the previous discussion of 4G and 5G network vulnerabilities. Planners should determine which equipment has been tested for EMP and work together on solutions to address the most vulnerable parts of the network first. An agile infrastructure

can include portable, geographically dispersed systems (like mobile base stations called "cells-on-wheels") or additional deployable nodes in the form of drones or balloons. To help facilitate the rollout of EMS resilient requirements, federal statutes should also require that requests for information/proposals associated with these types of infrastructure consider EMS hardening standards and requirements.

Finally, there is a need to continue advocacy for Black Start programs and capabilities. These teams can assist civilian companies in restarting certain power facilities powering critical government functions. In addition, teams should have a post-event plan to move to and survey predetermined high-voltage transformers in critical locations. Such inspections are vital information to gather within 24–48 hours to determine the extent of damage and generate an estimate of service outage duration. Such information is vital to ensuring that the correct national contingency plan is implemented.

Incentivize Industry

EMS resilience demands innovative service providers willing to invest in enhancing their network security. Beside cybersecurity concerns, mobile service providers place a high priority on service continuity, as they continually face issues of network restoration after power outages and disruptions. The military community must better engage industry regarding system redundancy and resilience and industry's plans to ensure both with the advent of 5G.

One recommendation was to develop an EMS-Star rating that scores companies based on how well they conform to certain EMS hardening standards. Inspired by the Energy Star program run by the US Environmental Protection Agency to promote energy efficiency and awareness, the EMS-Star would incentivize companies to increase their EMS resilience in order to increase their score. These scores can be used in the acquisition process for DOD or "military-grade" EMS shielding. Such programs could also be expanded to reward cities for completion of EMS resilience programs.

Figure 2. The Energy Star logo

In summary, the DOD needs to lead the way by setting the requirements for military-grade EMP hardening. These standards must ensure normal operations during an EMP event and allow the military to support local emergency operations trans- and post-event and retaliate if necessary.

Finally, academia must develop and revitalize EMS programs, incentivize engineering disciplines, and ensure security protocols are in place so that proprietary and national security–oriented research at universities and labs remains within the US and is available only to US citizens and vetted allied personnel.

QUESTION 3: Are quantum and 5G communications resilient to threats within the EMS?

5G is not just an extension of 4G cellular networks but rather a convergence of 5G mobility, the IoT, and AI. Additionally, 5G can enable very low latency, meaning almost no delay in receiving signals. This will enable real-time, mission-critical operation and control. We have never before experienced these extreme capabilities simultaneously. Together, these elements will promote new applications and businesses previously impossible to imagine. While the discussion focused mainly on 5G, quantum communications are just as vulnerable to EMS attack because they do not circumvent the transmitter and receiver vulnerabilities of more traditional communications capabilities unless effectively EMS hardened. The translation of information using quantum entanglement, however, is not currently, from a theoretical standpoint, subject to EMS interference.

The exceptional attributes of quantum entanglement should drive further research to discover how communications can advance uninterruptible secure communications and information transfer in a contested electromagnetic domain. In this respect, it is clear the properties of quantum entanglement will have widespread implications. Presently, China and Germany have both pioneered in development of drones that use quantum entanglement to operate and relay communications and information. The rapid maturation of quantum communications technologies presents the realistic prospect of transmission or "broadcast-free" control networks in as little as five to 10 years. The advantages arising of proliferated quantum technologies to future battlefields are sobering and may afford friendly and adversary nations with an ability to operate drones and precision-guided weapons and to send and receive communications even in a EMS-denied environment.

Developments in quantum communications networks and 5G networks will begin deployment in 2019 and continue expansion throughout the next decade. As 5G becomes an intrinsic part of the nation's infrastructure, there must be continued evaluation of how to take effective action to protect ourselves from hostile entities that would want to exploit, control, or undermine these capabilities.

Ultimately, if the 5G network deployed in the United States is not designed and constructed to be inherently resilient to EMS threats, and the electric power assets sustaining this network are not resilient to EMS threats, our nation will face an even more profound vulnerability than the status quo.

Although EDTF 5G working groups included leading government and industry participants, a necessary next step is validating the review with technical experts in the field to better understand what has already been done and then collaborate on steps to raise awareness and enhance all aspects of prevention, mitigation, and network recovery. This needs to be a focused effort that includes all mobile service providers, applications developers, equipment vendors, military planners, and those involved in disaster preparedness.

The Potential Impact Caused by an Electromagnetic Attack

A large-scale electromagnetic attack that knocks out a region's power would significantly degrade the existing mobile communications network, as all portions of the network are dependent on external power. This will be especially true for 5G, which relies on large quantities of small cells that are connected to lampposts, utility poles, and rooftops and do not have backup power systems. However, 4G is vulnerable to external power fluctuations as well. Although the larger towers and base stations may have backup power systems, if some of these locations cease to operate, neighboring locations pick up some of their load, which can overwhelm surviving cells, taking them offline as well. Another concern from an electromagnetic attack is the optical transmission that could be disabled if an associated base station or link is impacted. Again, power would continue to be a critical dependency.

In a 5G network, more of the processing will take place closer to the base stations or even in the cloud. With a traditional design, these base stations will not operate if they are not connected in some way to the core, which is necessary for the control of the network. Ultimately, if the 5G network that deploys in the United States is not designed and constructed to be inherently resilient to EMS threats, and the electric power assets sustaining this network are not resilient to EMS threats, our nation will face an even more profound vulnerability than the status quo.

Industry representatives at the conference postulated that adding resiliency after the initial infrastructure build would likely be 10 times more expensive than designing resilience in from the start. Because there is an understanding of the vulnerabilities on the front side of the network deployment, there is a unique opportunity to "design-in" EMS resilience at the beginning. EDTF suggests this should be done immediately with the deployment of the FirstNet 5G infrastructure as a proof of concept for the rest of the 5G infrastructure.

FirstNet is a Department of Commerce initiative authorized by Congress in 2012 to develop, build, and operate a nationwide broadband network for

first responders. Since the current 5G network associated with the FirstNet emergency communications system is not EMP hardened, this vulnerability should be immediately remedied. Moreover, because 5G will eventually impact all aspects of society, the 5G network should be considered an integral part of a national response after an EMS attack or impact. The framework would bring local and state governments together with time- or event-phased plans that do not rely on outside inputs or robust communications among nodes. NATO partners should be made part of this plan. The plan should focus on rebuilding networks from the outside in with close coordination with the electric and telecom industries.

The Potential Impact Caused by an Attack from Within the Network

Present-day communications networks face daily cyberattacks and back doors to either capture information or disable capabilities. In the future, 5G will be connected to billions rather than millions of people and things—this will include access to a nation's vital infrastructure and information. Therefore, it is essential to establish a trusted network free of possible attack points. An attack on a network from within could have debilitating effects similar to an electromagnetic attack. Even more alarming is how access from within the network could enable an adversary to collect or manipulate information on the network without detection or fingerprints. This has been a concern with 4G, but with 5G, there will be more equipment and entry points on the network. These entry points will be difficult to monitor due to the massive volume of data and the dramatic increase of nodes.

Prevention and Mitigation

Given the forecasted scale of 5G network deployment and its capabilities, interconnectivity, and unlimited potential as an information and communications corridor for the economy, protecting 5G is paramount. EDTF teams discussed multiple prospective actions to maximize 5G's potential and settled on the following overarching recommendations:

1. Ensure uninterrupted access
2. Assure financial viability
3. Increase consumer and industry understanding
4. Secure network resilience
5. Conduct R&D in quantum and applications in next-next generation networks such as 6G

Also, while not specific to 5G, a few interrelated points such as EMS domain recognition and DOD accessions will help underpin 5G's success and are therefore also addressed below.

First, to ensure unfettered access and in accordance with presidential and other senior US governmental guidance, the 5G network must be free of state-controlled equipment. Even under strict supervision, no service provider or government can ensure a mobile vendor is not manipulating or controlling information being transported over their networks. These mobile vendors have the systemic capability to allow, willing or unwilling, backdoor access into the network through design and servicing. This is especially a concern with equipment produced by Chinese companies since the Chinese government has the ability to force Chinese companies to comply with broad and sweeping intelligence collection directives. Therefore, the US government (USG) requires everything it buys to be free of state-controlled equipment, such as equipment provided by China's telecommunications vendors Huawei and ZTE. The USG is highlighting these vulnerabilities to other countries and encouraging them to adopt policies that restrict the proliferation of Chinese 5G technologies.

Similarly, and equally important, supply chain integrity is vital. It will take a concerted effort to assess the security and vulnerability of each product and component integral to the end-to-end supply chain. Even non-state-controlled mobility equipment vendors like Ericsson and Nokia manufacture equipment in China. Consequently, the USG must work with each of these companies to require supply chain integrity and procedures. Another critical action is to work with the standards bodies, equipment vendors, service providers, and security corporations to improve network-level data security and encryption. A form of deterrence is to institute significant trade tariffs on any country or company found to introduce backdoors or other serious security vulnerabilities.

Since none of these precautions will be foolproof, Western states must establish a "zero-trust model" to mitigate vulnerabilities. The DOD should also plan to move to quantum-resistant key exchange mechanisms to deal with the eventual fall of public key exchange algorithms, particularly given China's investments in quantum computing. All of industry must work together to develop innovative processes enhancing security encryption capabilities. It is essential to continue to work with other nations, encouraging them to adopt similar policies so as to limit the detrimental impact on our global connected societies.

The advent of quantum communications makes the concept of quantum-based malware very interesting. In this regard, a nonsecure supplier could potentially add entangled bits to a computer or hardware and disable or

interfere with it even in an EMS-hardened facility. It is conceivable that, in time, such could present the capability of penetrating cloud-based databases and other architectures thought to be secure.

Next, it is crucial the United States move forward with a financially viable and competitive 5G plan. The current US plan for 5G, that of using millimeter wave (mm Wave) technology in the high-band 5G spectrum, needs to be re-evaluated due to its disproportionately high costs. China and the rest of the world are currently planning to use the mid-band 5G spectrum, especially sub 6Ghz, because of the significantly lower infrastructure requirements and attenuation problems that are associated with using the high-band spectrum. While it seems like a simple solution, the United States faces the challenge that both DOD and other USG entities are already utilizing the mid-band spectrum. Yet, to remain financially viable, both from a world standardization perspective and from an infrastructure deployment perspective, USG, DOD, companies, and academia must join together to either reallocate this mid-band spectrum or develop a way to share it.

One way to create this internal partnership is through incentives such as tax breaks, indemnification, or other measures. Another potential option is for these organizations to develop cheaper solutions using high-band, but as has been noted, this will create a disparity with the rest of the world. The Defense Innovation Board released a report in April 2019, "The 5G Ecosystem: Risks and Opportunities for DOD,"[28] which provides a more detailed assessment and recommendations. We will need USG and DOD to quickly and carefully review its ownership of mid-band spectrum to determine what should be kept, freed, and/or shared to maximize the effective use of the spectrum.

Education is the next key area requiring attention so 5G can be effectively and securely incorporated into society. As described previously, 5G is more than "just faster 4G." We need to overcome misunderstandings about 5G and help our nation understand 5G's benefits and vulnerabilities. Furthermore, as military base design and operations incorporate 5G, it will be important to plan for contingencies. Along with educating key military installation and operations planners, a broader DOD training plan should be implemented. Next, academia would benefit from instructing students on 5G's capabilities and then inviting students to explore the 5G trade space and technical opportunities in ways that could bring prestige and potential financial benefits to the institution. Likewise, corporations have a similar urgency to educate em-

28. USA. Department of Defense, Office of the Secretary of Defense. Defense Innovation Board. The 5G Ecosystem: Risks & Opportunities for DoD. By Milo Medin and Gilman Louie. Washington, DC: DOD, 2019. Available at https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY _04.04.19.PDF.

ployees on 5G's capabilities to highlight the potential unique, exclusive, and leading-edge uses of 5G. The USG could also partner to develop ad campaigns or videos to inculcate the public.

Such training should incorporate teaching about the potential threats to and from 5G. Also, informing the public of the interdependencies and risks associated with losing 5G would help raise this narrative to the forefront and drive action from policy makers. Finally, we would be wise to look at lessons learned from clubs, forums, and other parts of the country that engage in nongovernmental emergency preparations and then include these applicable lessons learned in the educational process throughout the whole of society.

The future is bright, and potential applications using the capabilities of 5G are bounded only by our own creativity. However, we must evaluate and act on the recommendations and actions provided to ensure uninterrupted access, financial viability, understanding, and resiliency across the 5G universe, which, as 4G did for 5G, lays the foundation for the 6G networks to follow.

QUESTION 4: What sustainable, efficient, and cost-effective approaches do we need to invest in/develop right now to keep Joint Force capability operational (viable) in a severe EMS-degraded environment?

Doctrine

The electromagnetic spectrum is a war-fighting domain. As US defense has increasingly relied on technology and as defense platforms and weapon systems increasingly rely upon the EMS, so have our adversaries and competitors increasingly challenged it. Consensus on this reality provides a common understanding and lexicon among the US government, military, allies, and civilian population. This consensus should also instill a culture of EMS awareness and unity across the nation, therefore setting the bedrock for future resource investment and doctrinal development that incorporates an appreciation for the EMS as a domain.

The development of a new EMS war-fighting doctrine cannot occur without broad awareness of EMS threats and opportunities. Unfortunately, many examples point to the USG's current lack of awareness of threats and opportunities in these areas.

Two recent examples were examined by EDTF. The first is a DOD request for information (RFI) for a small nuclear reactor to be used for forward operating bases,[29] and the second is a DHS request for proposal (RFP) for priority telecommunications services associated with the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD). Assets developed by the private sector for these two governmental requests will be critical to future expeditionary and domestic DOD operations and future DHS emergency management services, yet neither request incorporated resilience to EMS threats.

Interestingly, such examples provide proof the US government is aware infrastructure resilience is needed but often lacks a complete understanding of how to develop or enhance it when seeking solutions. Consequently, the EDTF recommends that the originator of such RFIs amend them to include an additional objective: "Resilience to all natural and man-made hazards, including physical, cyber, and electromagnetic spectrum threats; tested to

29. RFI for Small Mobile Nuclear Reactor, Solicitation no. RFI-01182019-RD-WHS019, https://www.fbo.gov/index.php?s=opportunity&mode=form&tab=core&id=5f70e466e904a1b12748d6e04fcbaad4&_cview=0.

applicable military standards for IEMI and EMP survivability associated with nuclear weapons and command and control systems."

The DHS solicitation is for information technology and telecommunication services associated with the DHS's CISA ECD, which "collaborates with the public and private sectors to ensure the national security and emergency preparedness communications community has access to priority telecommunications and restoration services to ensure communication under ALL circumstances."[30] EDTF believes these circumstances include those associated with an EMS-degraded environment, specifically in the aftermath of a EMP attack. However, EDTF personnel were unable to find where this RFP requires EMS resilience.[31]

These examples illustrate the need for a targeted education program designed to alert civil servants and contracting officers at all levels (from federal to local) of the need for EMS resilience. Furthermore, EMS standards for new acquisitions should be made a requirement.

During discussions about doctrine, it was noted that during the Cold War the USAF would translate Soviet military doctrine and make such available to the military and universities. It is therefore also recommended this approach be reinstated to allow the United States and its allies to better understand the militarization of EMS. It was suggested that these be translated and made available at Air University's Curtis E. LeMay Center for Doctrine and Education. Members commented that they believe doctrine and policy are lacking in the area of EMP defense and that a doctrinal-level statement is likely the most critical starting point to normalize and unify EMP resiliency discussions.

Some efforts in the area of Air Force EMS doctrine have already begun. Recently the LeMay Center hosted an electromagnetic spectrum operations summit to update EW/EMS doctrine and draft an Air Force Annex 3-51 *Electromagnetic Warfare and Electromagnetic Spectrum Operations*. Annex 3-51 was in final coordination and published as this report was being prepared. The LeMay Center is working to coordinate between AETC and the other major commands to develop standardized EMS academics for all Airmen. See appendix 2 for more information on the Enterprise Capability Collaboration Team (ECCT).

Additionally, research into the "golden hour" that is used in the medical community may be helpful in establishing doctrine or strategy for recovery

30. Department of Homeland, Security Cybersecurity and Infrastructure Security Agency, Emergency Division, https://www.dhs.gov/oec-planning-and-preparedness-support.

31. RFP for Cybersecurity and Infrastructure ECD Priority Telecommunication Services, Solicitation no. 70RNPP19R00000004, https://www.fbo.gov/index.php?s=opportunity&mode=form&id=539562678ceb5c59b46d67a38ebaf53b&tab =core&_cview=0.

operations. What is our golden hour after an EMP or GMD event? What does hour-one look like? There are critical systems that must be brought back on immediately after an event to enhance the chance of survival.

Contingency Planning, Training, Education, and Exercises

Beginning with the military-first approach discussed under 5G, we recommend all military members have EMS operations training and education. EMS vulnerabilities are present in every career field, and mitigation must be as understood as cyber hygiene. In addition to education and training, EMS objectives should be incorporated into all US exercises, war gaming, and primary, alternate, contingency, and emergency communications plans. Doing so will ensure a properly tested joint combined military and civilian strategy during catastrophic EMS degradation.

It is the strongest possible recommendation of the task force that mission-type orders and contingency plans be developed by US Northern Command (USNORTHCOM) to ensure the capabilities and assets at more than 300 military installations and defense properties in the CONUS can achieve coordination if communications are lost or disrupted for extended period.

One tenet of airpower that has not been stressed is centralized control and decentralized execution. The task force observes that over the last 25 years the US military has benefited from an overwhelming supremacy and has not had to exercise centralized control and decentralized execution. This is because the Joint Force has been operating in a permissive environment where real-time information and battlespace awareness are readily available. In an EMS-degraded environment, however, where communications are nonexistent or in short supply, decentralized control and decentralized execution will be a necessity so commanders can ensure decision continuity at the lowest level necessary for mission execution. Without standing mission-type orders from more than 300 military installations and countless other essential federal functions, there is a realistic prospect that a nationwide disruption to the power grid or telecommunications networks could degrade the ability of organizations and agencies to assist with recovery. Such conditions warrant EMS degradation be widely incorporated into exercises and war gaming.

However, before this is accomplished, it is the strongest possible recommendation of the task force that mission-type orders and contingency plans be developed by USNORTHCOM to ensure the capabilities and assets at

more than 300 military installations and defense properties in the CONUS can achieve coordination if communications are lost or disrupted for extended periods. Without standing orders or instructions, commanders will be left guessing how to prioritize and position the disposition of available resources and assets. This must be remedied immediately and may be done at little to no cost.

Integration between USNORTHCOM, United States Strategic Command, and the DHS is necessary for sharing resources and knowledge to aid in the defense of the nation and to prepare for an EMS impact that could have widespread effects on the civilian population. As outlined previously, leadership may come from different agencies depending on the type of event, but prior design and coordination are essential.

Finally, to increase the effectiveness of education and training programs, creating an EMS "red team" is a prudent next step. Red teams would use adversary capabilities, doctrine, and thinking to train the force, conduct traveling DOD exercises, and participate in DOD and civic emergency response exercises. Participation in community exercises is a low-cost method for public outreach that is within the DOD's control and ensures continuing public education in EMS vulnerability mitigation. Similar programs exist across the DOD. For example, the USAF has an outreach program that develops briefings and seminars to ensure the safe integration of civilian and military air traffic.

Materiel

Today, many viable and creative options exist to solve anticipated communication disruptions, but the planning must start *now* and required equipment must be protected. During an EMS outage, alternative means for communications would be necessary until mobile networks can be restored. Recently, AETC tested a mesh network that allowed for drones to propagate signals over more than 5,000 square miles. Concepts such as this should be developed and deployed to high-density population centers and key strategic sites around the country as part of USNORTHCOM crisis and contingency planning efforts.

Meshed networks are a new technology that uses individual handsets as nodes to distribute data, which may allow for communication in remote areas and after an EMP attack or EMS degradation. More research is needed into software-defined/reconfigurable radios and laser-based communications, which may allow access in a contested environment. Other innovative ideas include the ability to quickly launch micro-sat systems that would temporarily serve as a communication network, functioning as a UHF/VHF repeater.

Other solutions discussed involved the use of cognitive electronic warfare and AI to instantaneously detect threats and protect networks and send mass alerts, similar to an Amber alert, so people have critical information upon which to base their decisions. Even a one- or two-minute warning will allow decision makers to react quicker and speed recovery. Because damage to the infrastructure can come from various sources, including terrestrial and space weather, it is essential to quickly recognize the source of a threat.

Communication assets may also be prepositioned in EMP-hardened facilities or containers as a means of potentially increasing survivability. As an example, at the mayoral level, a city in Wyoming built Faraday cages to store critical equipment such as generators and communications hardware. These storage facilities could be expanded for the military, to include allied and coalition countries.

A streamlined acquisition process is needed to quickly purchase and test new and innovative shielding designs and solutions. There are methods to make the solutions to this problem happen more quickly. This could be similar to the Air Force, Special Ops, and NATO acquisition-lite programs, AFWERx, SOFWERx, and the NATO Innovation Hub. Start-up companies might already have what is needed to meet military requirements—but may not have the wherewithal to navigate the military acquisitions construct. An acquisition-lite team could consist of a few members who can quickly test and certify small companies.

In addition, the government can require future critical assets be developed with EMP protection capabilities. The best way to accomplish this is to provide tax and other monetary incentives for building in resilience or backfitting equipment with EMS shielding according to standards set by the USG and scaled according to the vulnerability and criticality of the asset.

Micro-power grid systems are also recommended to ensure military installations are made less vulnerable by reducing reliance on the commercial power grid. These may be implemented according to a prioritized list for critical military installations and should be hardened for EMP and cyber. An example of an effective micro-grid design is being implemented by the Puerto Rico Electric Power Authority in the wake of Hurricane Maria.[32] The design will re-establish the electric grid by moving toward interconnected, decentralized regions able to independently generate electricity with an emphasis on solar energy, natural gas, and battery storage.

32. For more information, see Megan Kerins, "The Puerto Rico Renewable Micrgrid Toolkit: A Data-Driven Approach to Resilience," Rocky Mountain Institute, 21 December 2018, https://rmi.org/the-puerto-rico-renewable-microgrid-toolkit-a-data-driven-approach-to-resilience/.

In terms of alternative forms of communications that might be available in an EMS-degraded environment, the task force examined several, including fiber optics, high-frequency (HF) radios, and laser communications. Unlike the wider electric power grid, fiber optic lines are not vulnerable to EMP. However, the fiber nodes that power fiber optic lines are vulnerable. Fiber lines with hardened nodes can ensure fast and reliable communication. But, without prior attention to design and resilience, these lines of communications will also be unreliable. On the other hand, HF experts believe that HF radio would likely be more reliable after an EMP, for example, due to the ionization of the atmosphere.

Amateur radio has been a cornerstone of redundant and emergency communications for decades. Many member-owned radio stations are built with EMP and power grid–down considerations in mind. ARRL volunteer members have experience and awareness of space weather effects and emergency communications. Additionally, the military has a long-standing relationship with the HAM radio community through the Military Auxiliary Radio System (MARS, https://www.mars.af.mil/, http://www.marsradioglobal.us/). EDTF recommends inviting American Radio Relay League (ARRL) and MARS representatives to future EDTF discussions. Finally, any new comprehensive plans must examine how to ensure continued propagation of the timing signal, whether from GPS (space) or terrestrial sources. These plans and policies should also address prioritization and restoration actions. For example, first responders must have communications restored before basic users do, as should priority locations like Washington, DC, to ensure continuity of government.

Leadership

In terms of leadership, EDTF recommends that a strategic messaging policy for the United States with respect to EMS be developed and communicated. In general, the US should message that any attack with a HEMP is an act of war and a crime against humanity.

Leaders need to understand the threat of EMS, advocate for resourcing and governance, and provide focus. This will require organizations to take ownership of their assets and not rely on top-down direction to undertake mitigation efforts. The whole-of-government methodology, to date, has allowed responsibility to be shifted and even set aside until someone else made a decision. In many cases, a decision simply never happened. Because EMS attacks have the potential to affect the population as a whole, whether through transportation, communications, or basic

necessities, it is important to have a single focal point for advocacy within government, individual or organization, be an advocate for EMS protection across the whole of government. However, in the interim, organizations must begin to own this issue individually.

Finally, in terms of leadership, EDTF recommends that a strategic messaging policy for the United States with respect to EMS be developed and communicated. In general, the US should message that any attack with a HEMP is an act of war and a crime against humanity. This messaging is necessary to help deter able actors who believe a HEMP is not considered an act of war against the United States.

Personnel

A critical piece of enhancing EMS resilience is the accession of personnel (including military, civilian, and contractors) who have the right skill sets, aptitude, and desire to address EMS risks. This issue was discussed widely—the US is losing (or has lost) its corporate knowledge regarding EMS. Moreover, the nation is failing to recruit the best talent. Some potential accession options to "join the cause" within the DOD should include defining future challenges and then attracting those interested in solving those challenges.

Facilities

To minimize the effect of an EMS attack, DOD buildings and critical infrastructure need to be hardened. This must be accomplished through a hardening plan prioritizing critical assets due to the cost associated with hardening assets that are already built. New military construction plans and standards should be reviewed to determine which buildings to harden, because it is more cost effective to incorporate hardening standards into new construction than into existing structures. Incorporating EMP shielding, for example, in new construction is believed to only increase the cost of construction by five percent of the total capital costs.

Conclusion

The United States and NATO are at an unprecedented strategic crossroad. It is a crossroad because bold decisions must be made about commanding outcomes that will soon reshape the international environment. It is unprecedented because there has never been a time in history when all domains (space, air, land, sea, and cyber) and nearly all activities within them, both civil and military, have merged and become principally controlled by a single powerful overarching domain—the electromagnetic domain.

The inconceivable is no longer a distant inspiration, it is on our doorstep. We are, in many ways, experiencing a transformation from science fiction to science fact where technologies have begun to comparably behave and evolve like living organisms. Technologies are forming, splitting, merging, mutating, and even becoming intelligent. In this environment, it is plausible that as our understanding of the electromagnetic spectrum fuses with quantum physics, the communications architectures of today, which consist of transmitters, receivers, and networks, will no longer be required to move information and data across space and time.

Our pursuit of understanding and the implications of these new realities must be driven by compassion and a desire to improve the human condition. However, such knowledge must also be informed by a candid and intelligent understanding that human nature does not change. Thus, with new discoveries, there will be new risks. Such risks will require us to advance beyond reactive strategies to develop proactive strategies that invest in promising opportunities and help guide new sciences and technologies such as 5G, 6G, quantum communications, and even risky embryonic ideas not yet known to the world.

However, despite our rapid advancement into the digital and information ages, we continue to pull against a tremendous inertia derived from our first understanding of the electromagnetic environment, an environment that extends to the very boundaries of our universe and which permeates all forms of life and physical matter. The electromagnetic domain envelops us so entirely we usually take its existence lightly. Yet, the electromagnetic domain is, in every way, connected to everything else. The electromagnetic spectrum works in and through all we do.

Frequently ignored, sometimes minimized, commonly misunderstood, and many times at the edge of our deliberation, where the electromagnetic domain is concerned, what is often the last thought must become a forethought as we look to shape the future to ensure our freedom and maintain power over tyranny. The electromagnetic domain will become the dominant

and controlling feature in how modern nations and their defense elements engage in competition and strife. Even if unseen, the nefarious manipulation of this domain below the threshold of war is being used to aggress and often harm the US, its allies, and the public.

Once there is a recognition of the complexities present within the electromagnetic domain and a demonstrated willingness to lead, we must educate and teach our communities about the challenges and opportunities in this environment. Without pooling the intellectual capital of the wider force and collaboration with our allies, industry, academia, and civic organizations and citizens, the critical mass needed for substantive change will not likely materialize. Therefore, efforts like the Electromagnetic Defense Task Force (EDTF) must be cultivated, supported, and replicated.

The EDTF is not a panacea for dated doctrine, a fix for decision paralysis, a corrective for stagnant acquisitions, or even a wake-up call to the government and public. This effort could not be so ambitious. However, the ideas and information within this report are offered with sobriety and candor to credibly inform the deepest conversations and deliberations of our age.

As a stakeholder in our future, whether senior leader or senior citizen, junior officer or student, you are vitally important to the successful shaping of our future and the future of the electromagnetic domain. As we prepare this future, we must not be held captive by uncertainty or fear of the unknown, but rather take hold of the opportunities in front of us. If we comprehend the shape of what can be and work together, we can sculpt the future for the benefit of all humanity. Such vision requires, first and foremost, leadership that recognizes when the environment has changed, even against seemingly impossible odds. Like the young British officers discussed in the introduction to this report, we can use all within our reach to ensure successful outcomes. But we must act.

The opportunities now demand we think to win, and such thinking requires us to consider everything. If we fail in this regard, we will have failed cognitively. We can avoid a future where the US and its allies are humbled by an adversary who imagined better—whose ideas were unbounded and whose determination and audacity we failed to match. We are in a contest of imaginations, and those who imagine best, and follow next with actions, will shape things to come.

If we remain on our present course, the terrain may seem familiar, but adversaries will take the initiative. Given the ubiquity of the electromagnetic spectrum, this future outcome is and must be unthinkable.

Imagine an actor who decides to dominate space, the ultimate high ground, not for peaceful purposes but for ambition and conquest. Imagine, space assets

stationed above all humanity controlled by unthinkable tyranny. Imagine, dominance or terrorism from space platforms capable of projecting directed energy on cities, communities, and towns. Imagine the widespread disruption of communications or the use of electromagnetic systems to lock out positioning, navigation, and timing (PNT or GPS). What we do next will shape the ability of the US and our allies to prevent such futures.

As we demonstrate courage, leadership, and a willingness to learn and compete with novel ideas, there must be a demand for accountability in the critical areas that sustain our national welfare. Such accountability requires uniform standards, rigorous physical component testing, and incentives for manufacturers and customers to both demand and integrate electromagnetic spectrum (EMS) resilience into new and existing systems and designs. For example, estimates for end-to-end electromagnetic pulse (EMP) hardening of the US power grid and critical infrastructure range from $5 billion to $50 billion, and while it is recognized that an ideal outcome would be the complete protection of the nation's infrastructure, resource constraints make this outcome unlikely. Yet, the use of military standards to harden nuclear power stations, for example, is a justifiable investment from a risk and security standpoint. Where such improvements cannot be made, the US and its allies must find intelligent, low-cost, and practical solutions that enhance resilience in peace and in times of conflict.

We are in an electromagnetic age, and we must be ready to articulate a vision for how to preserve lasting peace, the rules-based order, the sanctity of life, our sacred liberty, and the pursuit of happiness.

We are in an electromagnetic age, and we must be ready to articulate a vision for how to preserve lasting peace, the rules-based order, the sanctity of life, our sacred liberty, and the pursuit of happiness. Part of this communication is an ability to inform future actors about the position of the United States of America with respect to EMS threats. The employment of such strategic means, including EMP, the disruption of PNT/GPS, and the employment of EMS activities against terrestrial or space-based targets, must be considered an act of aggression and, in some cases, a crime against humanity.

Communications with the public about the wider risks of EMS, EMP, geomagnetic disturbance (GMD), and other emergent risks is an essential component in maintaining the trust and confidence of the American people. As this trust is enhanced, the Department of Defense (DOD) and other agencies should, as much as practical, declassify and release information that can help facilitate broader knowledge on the issues, assist in the development of better EMS technologies, and promote accountability. Without a sound knowledge

of the facts, the American people are at a disadvantage. In an effort to lead by example, the EDTF has ensured this report is releasable to the public and encourages the widest possible dissemination.

Another low-cost measure is promoting public awareness of the limitations of the DOD and government in an EMS-degraded environment. Under certain conditions, strategic threats may be presented that bypass traditional deterrence schemes. Such threats may emerge from gray zone areas and rapidly deploy to create widespread outages and disruptions. However, similar effects of GMD may arise that interact with Earth's magnetic field to cause similar disruptions. By guiding the public to an accurate and realistic understanding of the EMS environment, the public will be served by (1) enhanced household and community resilience, (2) increased support for government measures and strategies that can further ensure the US and its allies are prepared to mitigate challenges, and (3) improved government transparency.

It is the strongest recommendation of this task force that USNORTHCOM develop concepts of operations and contingency plans for major EMS impacts (including EMP, GMD, and space-based PNT/GPS degradation) to the lower contiguous 48 states. Such plans may be built for little to no cost. However, the degree to which the resilience of the United States and Joint Force will be enhanced by this straightforward strategy cannot be overstated. Providing unified direction to the disposition of the US-based Joint Force will allow, in the unlikely event of a crisis, an organized and prioritized response that builds toward capability and speeds recovery.

At the nexus of technology, strategy, and our national power is an electromagnetic domain that is allowing our world and society to be resculpted. If we hold fast to that which shaped our first understanding, the grand design of what is to come will be crafted without the benefit of our value system. As sweeping changes occur, it is up to our nation's leaders and visionaries to form an image of what should come. The future will not answer to our wants, desires, or beliefs. The future will respond to our will and the intelligent steps we take to shape it.

We must consider the course to choose at this strategic crossroad. We can maintain the status quo by affirming our existing understanding of the environment and be faced with the prospect of conforming to a system designed for us by our adversaries and peer competitors. We can make modest improvements to our existing infrastructure and pursue incremental gains by incorporating better standards with physical testing and validation. Or the United States can transcend many of the most challenging aspects of the electromagnetic domain by redesigning the US critical infrastructure in such a

way that every community, family, and home has access to uninterruptible energy, data, and communications from a resilient architecture.

While the gears of progress have turned and advanced with our understanding of the electromagnetic spectrum, such progress can be crippled if we fail to grasp its incredible potential to help humanity on its journey forward. Thus, the electromagnetic domain must be understood, shaped, and positioned as a dominant enabling force for the defense and health of our nation and society.

How to accomplish this positioning is nothing short of a fantastic problem. If we are guided by a willingness to learn, lead, and understand fresh opportunities, we may advance our thinking, reshape our paradigms, and preserve and enhance our way of life.

These are times like no other. The task force thanks you for your interest, consideration, and ongoing support.

Selected Resources

The following are helpful resources on electromagnetic pulse (EMP).

Resource 1: Executive Order 13865. *Coordinating National Resilience to Electromagnetic Pulses*, 26 March 2019, https://www.govinfo.gov/app/details/DCPD-201900176.

This executive order implements core recommendations of the Congressional EMP Commission on an accelerated basis. It combines cybersecurity and security against electromagnetic spectrum threats, building upon executive branch orders and actions from previous presidential administrations to address threats from solar weather. Further, it requires that "the Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the nation's resilience to the effects of EMPs."

The order states that the assistant to the president for National Security Affairs, working with the National Security Council and the director of the Office of Science and Technology Policy, "shall coordinate the development and implementation of executive branch actions to assess, prioritize, and manage the risks of EMPs."

It directs the secretary of the Department of Homeland Security (DHS) to coordinate with the Energy and Defense secretaries, other agencies, and the private sector to "develop a plan to mitigate the effects of EMPs on the vulnerable priority-critical infrastructures."

Since there is not a substitute for EMP testing of equipment, one critical feature of the executive order is its requirement that the vulnerability of essential, critical infrastructure equipment is established through empirical testing by an EMP simulator rather than computer modeling.

Table 1. Important deadlines specified in Executive Order 13865

Date	Government agency leads	Required actions summary	Secs.
26 Jun 2019	Sec. Homeland Security, SSA, and other agencies	List National Critical Functions and Critical Infrastructure Systems/Networks/Assets that, if disrupted, have catastrophic effects. Update as necessary.	6(a)(i)
26 Sep 2019	Sec. Homeland Security	Review test data and identify any gaps in test data regarding effects of critical infrastructure systems, networks.	6(b)(i)
26 Sep 2019	Sec. Homeland Security	Use the sector partnership structure to develop an integrated cross-sector plan to address identified gaps. Implement the plan in collaboration with the private sector as appropriate	6(b)(ii)

Table 1. Important deadlines specified in Executive Order 13865 *(Continued)*

Date	Government agency leads	Required actions summary	Secs.
26 Sep 2019	Sec. Homeland Security	Develop and implement pilot test to evaluate engineering approaches to mitigate EMP impacts on the most vulnerable critical infrastructure systems, identified in 6 (a)(ii).	6(c)(ii)
26 Sep 2019	Sec. Homeland Security, through administrator of FEMA	Review and update federal response plans, programs, and procedures to account for the effects of EMPs.	6(e)(i)
26 Dec 2019	Sec. Homeland Security (with Sec. Defense and Sec. Energy)	Develop plan to mitigate effects of EMP on critical infrastructure systems/networks/assets. Implement plan consistent with DHS. Update plan as required by results derived from in 6(b) and 6(c).	6(d)(i)
26 Mar 2020	Sec. Homeland Security (with Sec. Defense and Sec. Energy)	Develop risk assessment on EMP, and then develop quadrennial risks assessment.	5(f)(vii)
26 Mar 2020	Sec. Energy	Review existing standards for EMPs. Develop or update quantitative benchmarks that describe physical characteristics of EMP that are useful and can be shared by owners and operators of critical infrastructure.	6(b)(iii)
26 Mar 2020	Sec. Energy	Identify regulatory and nonregulatory mechanism, including cost recovery, that can enhance private-sector EMP efforts.	6(c)(iii)
26 Mar 2020	Agencies supporting national essential functions (NEF)	NEF agencies shall update their operational plans to prepare for, protect against, and mitigate the effects of EMPs.	6(e)(ii)
26 Mar 2020 and then every 2 years	Sec. Homeland Security (with Sec. Defense and Sec. Energy)	Submit report to the president of the United States (POTUS) analyzing tech options to improve resilience to effects of EMP, and identify gaps in available technological and identify future R&D opportunities.	6(c)(i)
26 Jun 2020	All agencies supporting NEFs	Update EMP plans in terms of vulnerability.	6(a)(ii)
26 Jun 2020	Sec. Homeland Security	Identify which critical infrastructure systems/networks/assets are most vulnerable to EMPs effects.	6(a)(ii)
26 Sep 2020	Sec. Defense (with Sec. Homeland Security and Sec. Energy)	Conduct pilot test to evaluate engineering approaches to harden strategic military installation and supporting infrastructure against EMPs.	6(d)(ii)

Table 1. **Important deadlines specified in Executive Order 13865** *(Continued)*

Date	Government agency leads	Required actions summary	Secs.
26 Dec 2020	Sec. Homeland Security	Provide to POTUS Staff assessment of EMP effect on communication infrastructure, and recommend changes to operational plans for response and recovery after EMP event.	6(e)(iii)
26 Mar 2021	Sec. Defense	Report cost and effectiveness of 6d(ii) test to POTUS.	6(d)(iii)
26 Jun 2021	Sec. Homeland Security	Develop plan to address EMP Effect Test Data gaps.	6(b)(ii)
26 Mar 2023	Sec. Interior	Complete in four years magnetotelluric survey of contiguous US to help critical infrastructure owners and operators to conduct EMP vulnerability assessments.	6 (b)(iv)

Resource 2: National Coordinating Center for Communications (NCC). *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment,* 5 February 2019, https://www.dhs.gov/.

The DHS's NCC has been working on this information product for at least four years, having published its first version in 2016 and updated it in 2019.

This document provides guidelines to assist federal, state, and local officials and critical infrastructure owners and operators to protect mission essential equipment against EMP threats. It was created to help fulfill the Secretary of Homeland Security's responsibilities to:

- "Provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the nation's critical infrastructure." [*Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience*]
- "Ensure . . . the necessary combination of hardness, redundancy . . . to obtain, to the maximum extent practicable, the survivability of NS/EP {national security/emergency preparedness} communications" [Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*]
- "Be the focal point within the Federal Government for all EMP technical data and studies concerning telecommunications." [Title 47 Part 215 of the Code of Federal Regulations (CFR)]"

The document also responds to the US Congressional EMP Commission's recommendation that the "Department of Homeland Security should play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences."

The document establishes four EMP protection levels "initially developed at the request of the federal Continuity Communications Managers Group but are applicable to any organization that desires to protect its electronics and critical infrastructures."

"In addition to making recommendations on how to physically protect electronic equipment from different types of EMP, this document provides guidance on how to help ensure communications and information systems (and their supported missions) can continue to function or be rapidly restored after one or more EMP events. Hence, Appendix C contains information on priority service programs (like Government Emergency Telecommunications Service, Wireless Priority Service, and Telecommunications Service Priority) as well as on the SHARES alternate communications service that can be used to support critical missions and to facilitate and coordinate restoration activities. The document supports the concepts of resiliency and recovery. The intention is to provide different levels of protection that should allow less damage and/or loss of data as one moves to a higher level of protection. This also should result in shorter outages of the system mission."

The DHS NCC specifies that "these guidelines do not endorse any referenced product, company, service, or information external to DHS" and that "The audience for this document is all governmental and civilian officials and owners and operators of critical infrastructures, particularly those using sensitive electronics for their operations. This includes the 16 critical infrastructure sectors identified under 'Presidential Policy Directive 21 (PPD21): Critical Infrastructure Security and Resilience.' "

Resource 3: Air University Library Research Guide on EMP, http://fairchild-mil.libguides.com/Electronic_Warfare.

This collection includes Air University research, books, documents, journals, articles, databases, websites, and electronic resources selected by Air University Library research librarians.

Appendix 1

Electromagnetic Pulse (EMP) Impacts on Nuclear Power Plants and the Role of the Nuclear Regulatory Commission (NRC)

In 2018, the Electromagnetic Defense Task Force (EDTF) identified potentially major concerns relating to the safety of US nuclear power stations in the event of an EMP. In particular, two primary issues were raised: The first was the sparsity of literature addressing the topic of how an EMP may interact with nuclear power stations, and the second was the total absence of any physical testing data to validate the assumptions made by the few studies on the subject.

In the NRC's parlance, an EMP is a "beyond-design-basis event" (BDBE) that does not have to be taken into account in facility design or be protected against with the use of "safety-grade" systems, structures, and components. Thus, no nuclear power plant was specifically designed to survive an EMP event. The key question in assessing the vulnerability of nuclear power plants to EMP is to what extent an EMP could cause damage both to nuclear plant systems and to the surrounding infrastructure and whether that damage would exceed that which the plant, its personnel, and its support systems are currently required to withstand or mitigate.

The primary impact of an EMP on a nuclear power plant would be a loss of off-site power due to failure of the grid. Such an event is a design-basis accident, and nuclear power plants are required to have safety-grade emergency diesel generators (EDG) to ensure that adequate cooling of the reactor fuel is maintained.

Nuclear plants are also required to cope with the possible failure of the EDGs, an event known as a station blackout. Station blackouts are considered BDBEs. Prior to the 2011 Fukushima accident, nuclear plants were only required to cope with a station blackout for a relatively short time, typically four to eight hours, based on estimates of how long it would take to restore access to power from the grid. However, after Fukushima, which suffered a station blackout for 10 days, the NRC required nuclear plants to prepare to cope with a loss of AC power indefinitely in the event of a beyond-design-basis external event (BDBEE; e.g., a natural disaster).

Nuclear plants have complied with the NRC's post-Fukushima requirements by procuring and staging portable emergency equipment, such as diesel-powered pumps and EDGs, that could be used to ensure reactor and spent fuel pool cooling in the event of a long-term blackout. This strategy is called

FLEX. FLEX equipment does not have to meet the same standards as safety-grade equipment to protect against design-basis events, but only must be "reasonably protected" against external hazards. The FLEX strategy also includes two national response centers, one each in Memphis and Phoenix, that would be able to supply additional sets of FLEX equipment to up to four reactors in distress. Nuclear plant owners are required to make arrangements with commercial companies to provide transport of replacement FLEX equipment from the national response centers, as well as to provide additional diesel fuel supplies to power the equipment.

Therefore, the threat posed by EMP to nuclear plants depends on how such an event could challenge the strategies currently in place to deal with electrical system disturbances, from loss of off-site power to indefinite station blackout. Key considerations are whether the safety-related EDGs and/or electrical distribution systems would be disabled, whether FLEX equipment would remain functional and FLEX strategies executable, and whether supply of diesel fuel and replacement equipment would be disrupted by a large-scale high-altitude electromagnetic pulse (HEMP) event. The NRC has not done such an analysis. These potential gaps need to be fully analyzed to better assess the current vulnerabilities of nuclear plants to EMP.

One major deficiency of the FLEX strategy is the absence of any NRC requirements for training, drills and exercises, staffing, and communications related to their implementation. While the NRC approved the inclusion of such requirements in its draft final rule on mitigation of BDBEs in 2016, in January 2019 the current commission voted to strike all such requirements from the final rule.

Although nuclear plants are required to conduct training to safely handle design-basis natural and man-made catastrophes, BDBEs such as extended station blackouts fall outside of these planning and training scenarios. This does not mean that such events cannot be mitigated; it just means, from a definition and design risk standpoint, operators and staff are not trained, do not exercise, do not plan, or do not have facilities and hardware intentionally designed to withstand such events. Any ability to address electromagnetic spectrum (EMS) or EMP concerns would require on-the-spot innovation, ad-hoc procedures, and whatever equipment remained functional.

To address these concerns in a comprehensive and transparent manner, EDTF hosted members of the US NRC with EDTF Fellows from more than a dozen organizations and labs with experience in electromagnetics and nuclear power and power generation. Also present were members of the White House Staff, Office of the Secretary of Defense, Joint Staff, Idaho National Labs, Sandia National Labs, Union of Concerned Scientists, and a number of scientists and

electrical and nuclear engineers. In total, 29 participants took part in three meetings over two days. One meeting was conducted at the unclassified level and two were conducted at the classified level. The meetings were organized and moderated by Maj David Stuckenberg and led by Lt Gen Steven Kwast and Brig Gen David Gaedecke.

Classified discussions raised a number of issues that will not be discussed in this paper. Further information on these meetings is available by briefing and may be requested by appropriate agencies.

In the paragraphs that follow, the major discussion points regarding nuclear power plant safety in relation to EMP will be discussed. It should be noted that the EDTF appreciates the spirit of cooperation, collaboration, and goodwill demonstrated in the lead-up to and during the meetings. The EDTF also acknowledges the mutual goal of the EDTF and NRC to faithfully ensure all stakeholders and the public are well informed on these technical issues and unknowns. Notwithstanding, there was both consensus and a lack of consensus on a variety of points summarized below.

EDTF-NRC Discussion Areas

Italicized text signifies agreement.

Area 1. Lack of credible research on EMP impacts to nuclear power stations.

EDTF position: Other than the 1983 report from Sandia National Labs, no credible research has been done on this issue. The Sandia study is faulty on more than a dozen assumptions and was not well received even within the nuclear power community at the time it was released.

NRC position: The 1983 study was not the only report done to study EMP impacts. Another study was conducted in 2009, which validated the first.

Recommended action: Since no comprehensive testing has been conducted at an operating or recently closed power station, modeling assumptions, irrespective of literature source, are not reliable. Many EMP tests conducted on actual equipment show modeling can be wrong by orders of magnitude. Suggest actual physical testing.

Area 2. Lack of comprehensive physical facility testing.

EDTF position: This means that how a nuclear power station will react to EMP as a complete system is largely a total unknown.

NRC position: NRC has tested the nuclear power stations with accurate computer-based simulations.

Recommended action: Since no actual testing has been conducted, such assumptions are gravely imprudent. EMP tests conducted on actual equipment show that modeling can be wrong by orders of magnitude. Suggest actual physical testing.

Area 3. *EMP is by definition a BDBE.*

EDTF position: *This means, with limited exceptions, that no staff or operators are required to be trained in how to react or mitigate unanticipated and unforeseen impacts*. Thus, present guidelines for responding to certain beyond-design-basis actions are not required by the NRC, but are done on a voluntary basis by licensees (and therefore not subject to NRC enforcement actions).

NRC position: *NRC agrees*.

Recommended action: *Detailed guidelines should be developed both on a plant-wide and nationwide level to address mitigation of potential EMP effects, and periodic training should be conducted among all parties involved in the response.*

Area 4. EMP will cause a prolonged station blackout (loss of off-site power and on-site EDG and/or electrical distribution systems). This issue area is linked with issue area 6.

EDTF position: All electronic devices are subject to impact and disablement by an EMP where there is sufficient field strength.

NRC position: Sufficient backup systems will maintain/allow: safe shutdown, core cooling, and spent fuel cooling. These are also the NRC's safety priorities.

Recommended action: These cannot be guaranteed due to a lack of actual testing. NRC suggests EDG will work and that fuel will be available from off-site in the event of a long-term blackout. However, NRC admits that without these logistical provisions there are no guarantees. There is an apparent contradiction in planning as the NRC admits that fuel delivery, for example, cannot be guaranteed, but it still relies on such deliveries for plant safety.

Area 5. EMP may impact control rooms and sensitive electronics.

EDTF position: All electronic devices are subject to impact and disablement by an EMP where there is sufficient field strength.

NRC position: NRC does not anticipate significant penetration of EMP fields into a nuclear power station due to design of the structures.

Recommended action: Since no actual testing has been conducted, such assumptions are imprudent. EMP tests conducted on actual equipment show that modeling can be wrong by orders of magnitude. Suggest actual physical testing. USAF nuclear command and control facilities and missile silos are often underground and even covered by tens of feet of concrete and metal rebar. This does not negate the need for EMP hardening. Such facilities are hardened to careful military specifications.

Area 6. Post-shutdown EDGs may not function. This issue area is linked with issue area 4.

EDTF position: EDGs have circuitry that can be impacted and incapacitated by an EMP, especially their control systems. They may not be reliable unless hardened to military standards.

NRC position: EDGs are normally disconnected from safety-related systems, this should protect them from induced EMP currents.

Recommended action: Consideration has not been made for secondary attacks. This means that any surviving generators, once connected and providing backup power, may be subsequently impacted. Moreover, even unpowered and unconnected devices can fail from EMP, as was demonstrated in Soviet HEMP tests over Kazakhstan in 1962, where backup generators were later found to be damaged. Recommend NRC investigate control circuit board bypass options with which to backfit EDGs to ensure manual operation is possible in post-EMP conditions.

For example, EDG modules are available which allow the bypassing of complex microcircuits. Recommend all station operators be required to maintain an ability or "kit" to bypass circuits to ensure an ability to operate EDGs in manual mode.

Area 7. *Post-EMP logistics to the nuclear power station, including diesel, would be exhausted after one week (seven days).*

EDTF position: *This means that the EDGs that would continue supplying electricity to the spent fuel pools and other vital components could stop if there is no way to replenish fuel.*

NRC position: *Assurance of core and fuel spent fuel pool cooling in a long-term power grid outage is needed.*

Recommended action: *EDTF suggests evaluating the viability of immediately providing both EMP-hardened EDGs and at least six months of diesel fuel at each site. EDTF also suggests rapid exploration of technological solutions such as the application of long-term EMP-resilient power generation assets to power cooling systems. Such could include technical evaluation of Rankine or Brayton Cycle technologies, solar photovoltaic systems, and thermoelectric generators that can use heat from the spent fuel pool to generate power.*

Area 8. Post EMP, spent fuel pools may not have adequate electrical power to the cooling pumps.

EDTF position: See above/below.

NRC position: See above/below.

Recommended action: See above/below.

Area 9. Before an EMP or station blackout, it might make sense to have more spent fuel in dry cask storage in order to reduce the risk of a self-sustaining zirconium fire in the spent fuel pool in the event of an extended loss of cooling.

EDTF position: Expedited transfer of spent fuel to dry cask storage can significantly reduce risks posed by potential loss of cooling to spent fuel pools. (Reference 2018 EDTF report for tables and figures.)

NRC position: While the NRC expects spent fuel pools would boil off in days or weeks without electrical power for cooling, they do not expect EDG failures. Post-Fukushima safety improvements include instrumentation of spent fuel pools. Potential inability to obtain fuel delivery is a concern. Suggest the Department of Defense (DOD) provide a logistics option/guarantee.

Recommended action: The imperative remains to move as much spent fuel into dry cask storage as practical. Spent fuel can be transferred to dry storage after about five years of cooling. By moving more fuel out of the pool, if the pool does lose power and boils off, the likelihood of a pool fire decreases and there will be less material to cause radioactive release (for more information on this area reference the 2018 EDTF report). This is a passive safety measure. EDTF recommends that the NRC does not rely on DOD for logistics support in the event of a severe EMP event.

Area 10. ***Nuclear power plant physical security was not addressed in 2018 but was addressed in 2019.***

EDTF position: *There is currently no plan to extend or support security personnel in a prolonged station blackout.*

NRC position: *NRC agrees.*

Recommended action: *Part of a holistic plan for EMP issues should include how to support staff that will not receive immediate relief due to potential off-site impacts to food, water, transportation, communications, etc. During the Fukushima disaster, this issue created many concerns. EDTF strongly recommends that NRC create the conditions whereby nuclear plant owners/operators can provide both access and resources to care for the immediate families of nuclear power station personnel during a blackout.* Moreover, the question must be posed as to whether nuclear plants in a post-EMP weakened state would become targets of opportunity for terrorists/extremists, and whether it is appropriate to consider provisions for addressing this increased threat. State and local law enforcement, FBI, etc., may be limited in the ability to provide an effective response under post-HEMP conditions. Also, the impact of EMP on digital systems important for security—alarms, access authorization, assessment tools, communications—may not have been fully evaluated.

Area 11. Component hardening standards were not addressed in 2018 but were addressed in 2019.

EDTF position: No US nuclear power station is hardened to military standards. It makes sense that if the DOD would harden nuclear assets with known standards the NRC would require the same.

NRC position: Agree NRC does not harden to DOD or military standards. However, some nuclear power station features do meet military standards by design.

Recommended action: The EDTF questions these assertions. The safety of a nuclear power station must be absolute in order to maintain the public trust. As a confidence-building measure, a physical testing baseline should be established from which inferences and modeling can be done. It also seems reasonable that NRC licensees would be required to harden to military standards given the risks posed to nuclear power sites. Recommend the NRC consider requiring military-standard EMP hardening of facilities or proof of equivalency for individual sites.

Area 12. Site security and small EMP attacks were not addressed in 2018 but were addressed in 2019.

EDTF position: HEMP is a large-scale attack that may arise of state or nonstate actions. However, there are additional concerns that smaller vehicle-borne EMS devices (which have been created) could affect a nuclear power station by simply directing energy toward critical facility nodes.

NRC position: It is believed that such impacts would be negligible due to the attenuation of signals by the physical structure. In addition, modeling for EMP indicated there will be practically no impact to safety systems.

Recommended action: This issue is significant and un-mitigated. Modeling does not adequately establish reliable information without at least a physical testing baseline. To date no nuclear power facilities have been subjected to an actual EMP field to establish a baseline.

Area 13. Ability to safely conduct a shutdown in the event of an EMP blackout.

EDTF position: A station shut down by an EMP is a station suffering from a BDBEE. Such means training may not address any particularities arising out of unexpected circumstances associated with EMS effects.

NRC position: While EMP is a BDBE, stations are expected to shut down correctly and orderly. There are no digital components connected to equipment required for shutdown; most nuclear station control systems are still analog.

Recommended action: Lack of physical testing leaves many questions about what may or may not work in a shutdown. During the accident at Three Mile Island, an incorrect reading of a valve position on a digital readout caused an inadvertent release of radiation. Recommendation is to harden facilities to DOD EMP standards.

Area 14. Efforts under way to digitize most plant controls were not addressed in 2018 but were addressed in 2019.

EDTF position: There is concern that digital components will fail if subjected to EMP field strength above 8kV per meter.

NRC position: There is a strong campaign to digitize plant control room electronics. However, approval is slow and the process is expensive. When approval is made the NRC attempts to evaluate second- and third-order effects.

Recommended action: Digital components being installed in nuclear power stations have not been subjected to EMP testing. However, most Chinese nuclear power stations and many Russian facilities have tested components. The apparent disparities continue to be a concern.

Area 15. The ability to maintain FLEX facilities for power station supply/ reach back.

EDTF position: Delivery of FLEX assets will likely be unreliable due to failures in logistics and supply chains for reasons ranging from potential loss of satellite positioning, navigation, and timing (PNT) to inability to fuel trucks, to choked highways/transportation infrastructure due to immobilized autos, to societal chaos.

NRC position: FLEX assets are now maintained on several sites in separate storage facilities. These facilities are not EMP hardened nor is delivery assured. For example, FLEX strategies often involve the use of solid-state battery chargers and inverters that could be affected by EMP.

Recommended action: Consideration should be given to advancing the FLEX program to provide more regional depositories (beyond AZ and TN warehouses) and creating EMP-hardened structures for spare EDGs. Many structures may now be hardened with aftermarket materials at a low cost. More information is available through the Air Force Research Laboratory.

Area 16. Issues impacting the public health and military assets downwind from power stations. The important question here is whether occupationally significant doses of released radiation could affect downwind DOD facilities, triggering either protective actions (see, e.g., the repositioning of US naval vessels after Fukushima when low levels of radiation were detected) or requiring personnel to be exposed to needless radiation exposure to carry out essential duties. This could result both from passage of the initial plume from core melt and from long-term land contamination by cesium-137 from both core melt and spent fuel pool fires.

EDTF position: Psychological issue. These stations are the "crown jewel" of the US infrastructure. The DOD has no plan for impacts to personnel and equipment issues in this area. However, there could be major impact if planning is not conducted.

NRC position: Modeling indicates there will be no early radiation dose fatalities far from the plant [distance not specified; modeling not provided].

Recommended action: More information is needed to determine if the extended plume release (beyond 10 miles) will impact the public and military assets and personnel. The potential release of radiation can trigger panic. More information is needed to inform military planners on how to prepare for contingencies.

Area 17. What are the assumptions for the restoration of off-site power to the facility? Current diesel fuel storage for EDGs only require one week (seven days) of fuel.

EDTF position: It could take between weeks and months to restore on-site power and restart the power station. This is in part due to long replacement times for assets such as power transformers that, according to EMP experts, will likely fail from an EMP or geomagnetic disturbance (GMD) and also due to the need for the external grid to be ready to accommodate the load.

NRC position: Currently the NRC does not require stations to maintain fuel beyond one week (seven days). Additionally, the NRC does not require security beyond that which is reasonable for a contractor security company. The NRC does not consider state-level threats or intentional acts to be within the scope of its mitigation schema.

Recommended action: Within the wider US critical infrastructure nuclear power stations are the crown jewel. The NRC should consider measures to achieve mitigation that considers both state and nonstate actors in the security of facilities. In addition, planning is not conservative as assumptions for restoration of off-site power—which is essential to spent fuel pool cooling—may take months to restore. This issue continues to pose a substantial risk to the public and DOD assets. While off-site power is not the responsibility of the NRC, the NRC should plan to success, not failure. By failing to close the loop with Federal Energy Regulatory Commission on where transformers would be sourced and how long they would take to install, the NRC is likely basing its planning on unsupportable assumptions.

Appendix 1.1

NRC Staff Comments on EDTF 2.0 Report

Overall Comments

1. Nuclear power plants in the US are extremely robust structures designed with safety margins, as well as defense-in-depth safety capabilities. The facilities are capable of withstanding a broad range of beyond-design-basis events.
2. The NRC's authority to regulate and to issue orders to its licensees is consistent with its authorizing legislation, including the Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, and the Energy Policy Act of 2005, as amended. The NRC continues to implement Executive Order (EO) 13865, "Coordinating National Resilience to Electromagnetic Pulses," and will continue to take actions determined to be necessary through the EO's implementation process. Appendix 1 should appropriately recognize the regulatory framework within which the NRC operates and should also recognize that NRC is evaluating whether additional actions regarding EMP are needed for commercial nuclear power plants, consistent with EO 13865.
3. The NRC staff appreciates the opportunity to comment on Appendix 1. However, EDTF allotted limited time to NRC staff to review it and no time to engage with the EDTF on the substance. NRC staff is concerned that the rush to publication of appendix 1 without addressing NRC staff comments may result in inaccuracies. We remain ready to interact further to ensure that the appendix pertaining to commercial nuclear power plants is accurate.
4. Appendix 1 contains several statements without providing a readily apparent basis through citation to authoritative references, and dismisses others, such as the Sandia National Laboratory (SNL) study, without providing a basis for their dismissal (e.g., "The Sandia Study is faulty on more than a dozen assumptions . . .").
5. EO 13865 was not mentioned in appendix 1. The NRC and other federal agencies are currently implementing the EO and will take certain actions as determined through the EO's implementation process.

Comments on the Text of Appendix 1

1. On the first page, in paragraph 2, the EDTF states, "In the NRC's parlance, an EMP is a 'beyond design basis event' (BDBE) that does not have to be taken into account in facility design or be protected against with the use of 'safety-grade' systems, structures, and components (SSC). Thus, no nuclear power plant was specifically designed to survive an EMP event." The Commission addressed this issue beginning in 1967, holding that NRC licensees are not required to protect against enemies of the state conducting an act of war which would include a high-altitude electromagnetic pulse from a nuclear detonation by a nation State. The Commission announced its policy in the final rule, "Exclusion of Attacks and Destructive Acts by Enemies of the U.S. in Issuance of Facility Licenses" (32 FR 13445), which amended 10 CFR Parts 50 and 115:

> The amendments codify the Commission's practice of not requiring applicants for licenses to construct and operate production and utilization facilities to provide for design features or other measures for the specific purpose of protection against (1) the effects of attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, or (2) the use or deployment of weapons incident to U.S. defense activities. The protection of the United States against hostile enemy acts is a responsibility of the nation's defense establishment and of the various agencies having internal security functions. The power reactors which the Commission licenses are, of course, equipped with numerous features intended to assure the safety of plant employees and the public. The massive containment and other procedures and systems for rapid shutdown of the facility included in these features could serve a useful purpose in protection against the effects of enemy attacks and destructive acts, although that is not their specific purpose. One factor underlying the Commission's practice in this connection has been a recognition that reactor design features to protect against the full range of the modern arsenal of weapons are simply not practicable and that the defense and internal security capabilities of this country constitute, of necessity, the basic "Safeguards" as respects possible hostile acts by an enemy of the United States.
>
> The circumstances which compel this recognition are not, of course, unique as regards a nuclear facility; they apply also to other structures which play vital roles within our complex industrial economy. The risk of enemy attack or sabotage against such structures, like the risk of all other hostile attacks which might be directed against this country, is a risk that is shared by the nation as a whole.
>
> Furthermore, assessment of whether, at some time during the life of a facility, another nation actually would use force against that particular facility, the nature of such force and whether that enemy nation would be capable of employing the postulated force against our defense and internal security capabilities are matters

> which are speculative in the extreme. Moreover, examination into the above matters, apart from their extremely speculative nature, would involve information singularly sensitive from the standpoint of both our national defense and our diplomatic relations.

Specifically, Section 50.13 of Title 10 of the *Code of Federal Regulations* (CFR), "Attacks and destructive acts by enemies of the United States; and defense activities," states, "An applicant for a license to construct and operate a production or utilization facility, or for an amendment to such license, is not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities."

Thus, under NRC's regulations, nuclear power plants are not required to defend against enemies of the state. However, 10 CFR 73.1(a)(1) requires that power reactor facilities protect against the radiological sabotage design basis threat (DBT) committed by nonstate actors. Electromagnetic weapons are not included in the description of the DBT in 10 CFR 73.1.

The Commission has continued to consider these issues. In 1984, the Commission denied three petitions for rulemaking seeking to mandate that licensees protect against electromagnetic pulses. The Commission denied the petitions of Ohio Citizens for Responsible Energy, Marvin I. Lewis, and Mapleton Intervenors (19 NRC 1599 (1984)) and stated:

> Based upon results of studies done by the NRC and for the NRC (Sandia National Laboratory Report, NUREG/CR-3069, "Interaction of Electromagnetic Pulse with Commercial Nuclear Power Plant Systems") there is no reason to believe that an EMP would prevent any commercial nuclear power plant from achieving a safe shutdown condition. In addition, the rationale behind the issuance of 10 CFR 50.13, which was upheld in the U.S. Court of Appeals, was that Congress did not intend to implement legislation that would require nuclear power plants to be capable of warding off the effects of hostile enemy acts. This rationale has been reevaluated in the light of the petitions and at this time the Commission finds no information to support a change in policy.

The above regulatory construct notwithstanding, the NRC is addressing the EMP issue consistent with EO 13865. The appendix should recognize the regulatory construct and the fact that the NRC is, nevertheless, addressing EMP consistent with EO 13865.

2. Also on the first page, paragraph 2, the EDTF provides incomplete information on the design and vulnerability of nuclear power plants to

EMP. The US commercial nuclear power plant fleet includes inherent design features (i.e., reactor containment and reactor auxiliary buildings with ceilings and walls that are several feet thick with rebar) that provide protection against the E1 and E2 components of a HEMP. In assessing the vulnerability of nuclear power plants to HEMP, it is important to understand to what extent a HEMP event is capable of degrading nuclear plant systems and the surrounding infrastructure, and whether that damage would exceed the capability of the nuclear power plant (NPP) and its support systems to maintain core cooling.

There are three distinct reactor phases to consider after an EMP event: shutdown, long-term core cooling, and spent fuel pool cooling. All reactors in the US fleet are designed to automatically shut down regardless of the source of the loss of off-site power. Cooling of the spent fuel pool is maintained by the continual addition of water, which is available from a wide variety of sources. The large volume of water present in spent fuel pools renders immediate action regarding the pool following loss of power unnecessary. The NRC is currently evaluating the assets necessary for long-term core cooling as part of the evaluation phase mandated by EO 13865.

The appendix should be revised to address these points.

3. In paragraph 4 of appendix 1, the EDTF describes station blackout. The following information is provided for your consideration in modification of this paragraph. Station blackout (SBO) would occur with failure of redundant EDGs. The NRC adopted regulations that require nuclear plant operators to ensure that a NPP can withstand and recover from a station blackout for a specified duration at 10 CFR 50.63 "Loss of All Alternating Current Power." The duration is plant specific and takes into consideration the reliability and availability of on-site and off-site power sources and vulnerability to weather related events.

   NRC Regulatory Guide (RG) 1.155 "Station Blackout," provides guidance for plant operators to meet the requirements of 10 CFR 50.63. The guidance describes the procedures NPP operators may use to cope with SBO and the recommended actions to restore emergency AC power. The SBO procedures are integrated with plant-specific technical guidelines and emergency operating procedures. Nuclear reactor operator training identifies all operator actions that are necessary to cope with a station blackout for the applicable duration. Although SBO events are BDBEs, all NPPs have taken measures to cope with a SBO event of limited dura-

tion. Generally, all nuclear power plants assume off-site power will be restored within four hours; this information is detailed in NUMARC 87-00.

The NRC's post-Fukushima Order on Mitigation Strategies expanded US NPPs' ability to safely withstand SBOs of indefinite duration. Enhanced procedures to sustain installed battery and steam-driven core cooling systems, additional on-site generators and pumps to supplement those installed systems, and the ability to bring supplies and equipment from off-site sources mean NPPs are well positioned to maintain public health and safety under SBO conditions.

4. In the sixth paragraph of appendix 1, the EDTF states: "Therefore, the threat posed by EMP to nuclear plants depends on how such an event could challenge the strategies currently in place to deal with electrical system disturbances, from loss of off-site power to indefinite station blackout. Key considerations are whether the safety related EDGs and/or electrical distribution systems would be disabled; whether FLEX equipment would remain functional and FLEX strategies executable; and whether supply of diesel fuel and replacement equipment would be disrupted by a large-scale HEMP event. **The NRC has not done such an analysis** [emphasis added]." The bolded text is not accurate.

   The NRC staff performed a preliminary evaluation of impact of a HEMP based on analyses and limited physical testing performed by Sandia National Laboratory (Assessing Vulnerabilities of Present Day Digital Systems to Electromagnetic [EM] Threats at Nuclear Power Plants, December 2009). Taking into consideration the combination of the inherent design features of a typical nuclear plant which can withstand external events (severe weather, earthquakes, lightning strikes) and the standby mode (electrical disconnection) of safety related EDGs, the NRC staff concluded that there is reasonable assurance that core cooling and spent fuel pool cooling will be maintained with permanently installed equipment at US nuclear plants. Consistent with EO 13865, the NRC is currently conducting an analysis which it expects will further validate this position. Additionally, the NRC is currently coordinating with the Department of Homeland Security to evaluate the question of diesel fuel availability.

   Appendix 1 should be revised to address these facts.

5. FLEX Equipment: In paragraphs four through eight, the EDTF describes FLEX equipment and BDBE strategy, though it does not accurately capture the nature and scope of these activities. In particular

paragraphs seven and eight, which begin with "One major deficiency" and conclude with "whatever equipment remained functional," are not accurate, almost in their entirety.

NRC Order EA-12-049, "Order Modifying Licenses with Regard to Requirements for Mitigation Strategies for Beyond-Design-Basis External Events" (Reference 3), requires a phased approach for mitigating BDBEs. The initial phase requires using installed equipment and resources to maintain or restore key safety functions, including core cooling, containment, and spent fuel pool (SFP) cooling. The transition phase requires licensees to provide sufficient, portable, on-site equipment and consumables to maintain or restore key safety functions until off-site resources are brought to the facility. The final phase requires maintaining sufficient off-site resources to sustain key safety functions indefinitely. Order EA-12-049 requires NPP operators to develop and implement strategies to maintain or restore core cooling, containment, and SFP cooling capabilities. Full compliance with the order requires procedures, guidance, training, and acquisition, staging, or installing of equipment needed for the strategies following a BDBE.

NEI 12-06 provides specific guidance for the US fleet of operating NPPs on compliance with Order EA-12-049. In order to comply with the post-Fukushima requirements, the NPP operators have purchased and positioned non-safety-related portable emergency equipment such as portable diesel generators to charge station batteries and portable pumps to ensure reactor and spent fuel pool cooling in the event of a long-term SBO. The plants have also made modifications to facilitate connection points for additional equipment (pumps and generators) that may be located external to plant. The NRC inspected and confirmed that all US reactors are in compliance with these post-Fukushima requirements.

While FLEX equipment does not have to meet the 10 CFR Part 50, Appendix B, quality standards, they do meet commercial standards and are required to be maintained in a condition to perform their required actions. As part of its activities addressing the EO, the NRC is determining how best to prevent off-site release of large amounts of radioactivity following an EMP event. The role of FLEX equipment in achieving that objective is being considered.

Appendix 1 should be revised to address these facts.

6. In paragraph six, the EDTF states: "Therefore, the threat posed by EMP to nuclear plants depends . . . The NRC wishes to point out what is being discussed is the *risk* posed by EMP to nuclear power plants, not the *threat*." Please change "threat" to "risk."

   In the same paragraph, the EDTF inaccurately asserts the NRC has not analyzed vulnerabilities of nuclear plants to possible consequences of an EMP event, for example, whether safety-related EDGs would be disabled, whether FLEX equipment would function as expected, and whether the resupply of diesel fuel would be available. The NRC conducted two studies, in 1983 and again in 2009, that analyze the risk of EMP to nuclear power plants. Additionally, consistent with EO 13865, the NRC is currently conducting a follow-on analysis again reviewing this information in-depth.

   The appendix should be revised to address these facts.

7. The NRC staff recommends deletion of paragraph 10, which mentions classified discussions. The sharing of this information should only be to those individuals with the appropriate clearance and the need-to-know basis.

Comments on the EDTF-NRC Discussion Areas

1. Global comments:
   a. The positions under "NRC Position" are not official NRC positions but rather the positions of NRC staff. The NRC Commission has not weighed in on these positions. Please add the word "Staff" so it reads "NRC Staff Position."
   b. EDTF recommendations should not be italicized, because the legend suggests that the NRC agrees with the EDTF recommendation. The NRC has not been provided the opportunity to take positions on these statements.
   c. Please change all stated "NRC Positions" (which, as discussed above, should be referred to as "NRC Staff Positions" to ensure clarity) to the language stated below under Discussion Area Inputs. If the comment to combine issues that are very similar is accepted, please combine responses.
2. Editorial comments:
   a. In the "Recommended actions" column, many are general statements and opinions rather than actions. Recommend they be revised to include actions or the information deleted.

b. Recommend combining issue areas 1, 2, and 5. The issues are very similar as well as the recommended actions.

c. Recommend combining areas 4, 6, 7, and 8. All are related to emergency diesel generators with similar recommendations.

2. Discussion Area Inputs:

a. Area 1, NRC Staff Position: Multiple studies have been conducted by the NRC on EMP effects at nuclear power plants, first in 1983; that study was updated in 2009 to account for instrument and control digitization. Those studies conducted limited physical testing and then input the results to a complex computer-based modelling system to analyze EMP impacts. The 2009 study validated the 1983 results. In 2010, the 2009 study was supplemented to analyze the effects of geomagnetic disturbances on nuclear power plants. The NRC is further addressing this subject in response to EO 13865.

b. Area 2, NRC Staff Position: The NRC has conducted low-level testing at two facilities and used that data to better understand EMP impacts with accurate computer-based modelling. The NRC is further addressing this subject in response to EO 13865.

c. Area 3, NRC Staff Position: The Commission's practice of not requiring applicants for licenses to construct and operate production and utilization facilities to provide for design features or other measures for the specific purpose of protection against (1) the effects of attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, or (2) the use or deployment of weapons incident to US defense activities was set forth in 32 Federal Register 13445 and 10 CFR 50.13. The NRC has clearly asserted that it is the responsibility of the United States defense framework to protect against enemies of the State. An EMP attack perpetrated by an enemy of the State would be an act of war. Nuclear power plants are civilian-owned and operated infrastructure and not part of the national defense framework. Consequently, EMP attack was not considered to be a design basis event when nuclear power plants were designed and constructed.

d. Area 4, NRC Staff Position: According to SNL studies and internal NRC staff reviews, sufficient back-up systems will maintain/allow:

1. Safe shutdown

2. Long-term core cooling

3. Spent fuel cooling

A consistent and on-going supply of diesel fuel will be required to maintain the safe shutdown configuration. The NRC is working with the Departments of Homeland Security and Energy and the National Security Council to address the logistics associated with these deliveries.

The NRC staff is further addressing this subject in response to EO 13865.

e. Area 5, NRC Staff Position: NRC staff does not anticipate significant penetration of EMP fields into a reactor containment and auxiliary buildings due to design of the structures. Both types of structures are category 1 seismic buildings with significant amounts of concrete and rebar. The NRC is further addressing this subject in response to EO 13865.

f. Area 6, NRC Staff Position: EDGs are normally de-energized, disconnected from safety-related systems, and typically located in a seismic category 1 building made of cement with rebar. Based on the Sandia studies as well as National Institute of Standards and Technology's concrete signal attenuation standards, significant signal attenuation exists with these types of structures. The robust design should protect the EDGs from induced EMP illumination and transmission currents. The NRC is further addressing this subject in response to EO 13865.

g. Area 7, NRC Staff Position: The NRC staff generally agrees that greater assurance is needed for an on-going diesel fuel supply to the nuclear power plants. The NRC staff has been working with the Departments of Homeland Security and Energy and the National Security Council to establish the logistics necessary to ensure timely diesel delivery.

h. Recommend deleting area 8 entirely because it is addressed by prior items.

i. Area 9, NRC Staff Position: Spent fuel pools will remain safe as long as sufficient water is replenished. Because the pools are unpressurized and contain large volumes of water, replenishing the water is neither difficult nor of great urgency following an EMP event. Furthermore, consistent with previously-established Commission positions, wet- and dry- spent fuel storage are considered safe.

j. Area 10, remove "The NRC agrees." NRC Staff Position: NRC licensee site security is required to prevent radiological sabotage regardless of

the conditions. According to 10 CFR 73.55(o), Compensatory Measures, when a degradation occurs, nuclear power plants are required to implement compensatory measures to ensure they maintain the ability to detect, assess, interdict, and neutralize the design basis threat. A site's ability to carry out these procedures for weeks to years has not been analyzed. The NRC is further addressing this subject in response to EO 13865.

k. Area 11, NRC Staff Position: The NRC staff agrees to the extent that NRC licensees are not required to harden to DOD or military standards. However, some nuclear power station features may meet military standards by virtue of how they were designed for other purposes.

l. Area 12, NRC Staff Position: The 2009 SNL study specifically analyzed the "smaller" EMP weapons and indicated that such impacts would likely be low. The NRC staff is further addressing this subject in response to EO 13865.

m. Area 13, NRC Staff Position: While EMP is a BDBE, the NRC staff has high confidence that nuclear power plants will shut down safely as designed. Regardless of the reason for the loss of power, all shutdown instrumentation and controls are fail-safe and automatic.

   Also, in Recommended actions, the EDTF states, "During the accident at Three Mile Island, an incorrect reading of a valve position on a digital readout caused an inadvertent release of radiation." TMI 2's core melt situation is completely unrelated to EMP; the discussion should be deleted

n. Area 14, NRC Staff Position: Some nuclear power plants have upgraded their safety systems with digital technology, and others have an interest in performing these upgrades in the near future. In approving the use of digital safety systems, the NRC staff considers diversity of actuation means, defense-in-depth, and possible failure modes. Note that on loss of power, safety systems are designed to fail in a safe mode. The NRC is further addressing this subject in response to EO 13865.

o. Area 15, NRC Staff Position: FLEX assets are maintained on-site at all reactors and in two additional sites in separate storage facilities: one in Memphis and the other in Phoenix. All FLEX equipment is stored de-energized and disconnected from the grid. The NRC, in addressing EO 13865, is considering the role of FLEX equipment in

preventing significant release of radioactivity off-site following an EMP event.

p. Area 16, NRC Staff Position: If all engineered and proceduralized mitigation measures failed and a meltdown were to occur, there is a very large uncertainty in off-site consequences due to the large uncertainty in size of releases and variability in meteorological conditions (wind speed, direction, precipitation, etc.). Early fatalities from high acute exposures are not expected. Early severe health effects require both high doses and high dose rates; these conditions, if they were to exist, are expected to be limited to areas near the site. With prompt protective actions, off-site doses can be kept to low levels. The NRC staff has not analyzed scenarios with extended and widespread failure of off-site protective actions, which continue for more than several days. Without prompt protective actions, off-site doses may reach levels where there is an elevated lifetime risk of cancer to off-site populations. For the population, failure of access to food and clean drinking water would likely prove much more hazardous to health and safety. The NRC is further addressing emergency planning impacts from EMP in response to EO 13865.

q. Area 17, NRC Staff Position: Off-site power restoration is outside the NRC's statutory authority. In performing the analyses required by EO 13865, the NRC will follow the off-site power assumptions provided by the Department of Homeland Security.

Appendix 2

Enterprise Capability Collaboration Team (ECCT)

Background on EMS Superiority in the Spectrum

Imagine driving on a two-lane road through a small town with very little traffic. That was the extent of the electromagnetic spectrum (EMS) according to a Federal Communications Commission (FCC) chart produced around 1970. However, today's EMS can be likened to trying to fit Atlanta or Washington, DC, traffic during rush hour through that same small town. Use of the EMS has expanded exponentially, and the current FCC radio frequency allocation table[1] now includes telecommunications (4G), weather radar, datalinks, satellite communications, radio navigation, and much more.

Modern warfare is highly dependent on the EMS, and maintaining an advantage within this domain is necessary to enable Joint Force commanders to gain tactical, operational, and strategic advantage. Joint doctrine defines electromagnetic spectrum operations (EMSO) as coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment to achieve the commander's objectives. EMSO refers to all actions taken in the EMS or involving the EMS regardless of their nature or adversary involvement to compete and win against peer and near-peer adversaries in modern conflict.

Current joint and service doctrine emphasizes a view of the EMS as a resource to support operations in the other operational domains, at the expense of the view that the EMS is a distinct domain in which conflicts can be won or lost. US and allied platforms, weapon systems, and kill chains rely on the EMS—a reliance increasingly challenged by competitors and adversaries, especially impacting the air and space domains.

The EMS is defined by rapid technological change, contested and congested battlespace, and intense competition for control and superiority. In an era refocused on great power competition and readiness for the peer fight, controlling the EMS is irrefutably linked to our combat lethality and societal resilience.

Peer and near-peer competitors have organized, trained, and equipped with advanced EMS capabilities, integrating cyberspace, space, and air assets into comprehensive, integrated air defense systems; these combined manned and unmanned aircraft, sophisticated air and missile defenses, ballistic missiles, cruise missiles, hypersonic vehicles, as well as ground-, maritime-, air-,

1. "Radio Spectrum Allocation," Federal Communications Commission, 7 May 2019, https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation,https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf.

space-, and cyberspace-based electronic warfare (EW) capabilities, present growing challenges to the Joint Force's ability to achieve control of the air, space, cyberspace, land, and maritime domains.

Competing powers have witnessed America's dominance on the battlefield and perceive our reliance on the spectrum as a major vulnerability. In some instances, the US has not kept pace, and our technological advantages are eroding. Some of the contributing factors include (1) lack of a comprehensive and coherent EMS strategy and doctrine; (2) EMSO not perceived as a US military core competency; and (3) deteriorating knowledge, expertise, and acumen of the EMS in almost all Americans.

EMS experts have agreed that the preponderance of EMS knowledge resides within the US's older generation, working on specific projects and having limited awareness of other EMS capabilities ongoing with other military or civilian institutions. The lack of EMS training provided over time has produced Americans with limited knowledge in the EMS. Over the last three decades, this has diminished EMS advocacy, strategy, and vision within US leadership circles.

The intent of this paper is to adjust America's Joint Force and civilian (including industry, academia, defense contractors, etc.) policy perspectives on the importance of gaining and maintaining dominance in the EMS, enabling superiority in the air, space, cyberspace, land, and maritime domains.

ECCT Recommendations

The Chief of Staff of the Air Force (CSAF) is addressing this lack of EMS management, from a service-specific point of view, by directing the ECCT to deliver executable courses of action to gain and maintain EMS superiority across the range of military operations in an increasingly congested and contested EMS. Brig Gen David Gaedecke, director of EMS Superiority, presented the ECCT outbrief during the January 2019 Weapons and Tactics Conference. CSAF approved three recommendations: (1) establish an EMS Superiority Directorate within Headquarters Air Force, (2) restructure the EW reprogramming enterprise, and (3) reinstill a culture of EMS awareness across the Air Force.

Presently, the Headquarters Air Force (HAF) staff is standing up the directorate and corporate panel. This plan, once implemented, will drive development of policy and changes to current guidance on EW and EMSO and management. HAF and the Air Force major command (MAJCOM) staffs will provide new policy and revised guidance to squadrons employing EMS-dependent platforms or systems. It may drive changes to tactics, tech-

niques, and procedures and present improved doctrine, training, and education related to attaining and sustaining EMS superiority.

Improving the US doctrine, education, training, and exercising/war gaming with regard to the EMS will (1) identify and define characteristics and requirements for the EMS warriors; (2) assess and formalize training and education of EMS capabilities for all US personnel throughout their careers; (3) review and determine changes in doctrine and strategy to integrate EMS responsibilities, operational objectives, acquisitions, and concept of operations across the US military, industry, and private sectors; and (4) review and incorporate EMS objectives into US exercises and war gaming to prepare military and civilian procedures in the advent of catastrophic EMS degradation due to an electromagnetic pulse, intentional/inadvertent EMS disruption, or natural negative effects due to a geomagnetic disturbance (GMD).

During the conference, the commanders of Air Combat Command (ACC) and Air Education and Training Command (AETC) agreed to restructure the reprogramming enterprise and reinstill a culture of EMS/EW awareness. CSAF approved a holistic review of education, training, and exercises/war gaming. Correspondingly, AETC will take action to combine separate EMS, EW, signals intelligence (SIGINT), and Weapons School academics into standardized EMS force development academics (basic [EMS100] through advanced [EMS400]) for all Airmen. AETC will consolidate all inputs and develop EMS courseware to be instructed/planned across the Air Force at all levels of commissioning/enlistment, initial qualification, upgrade training, professional military education, and live-fly/virtual exercises and war gaming.

Executing similar recommendations across the US in a whole-of-government approach will enable the US military and civic leaders, military and civilian populace, industry, academia, and infrastructure personnel to be better educated on the challenges of understanding and dominating the EMS, provide a more robust and resilient populace and infrastructure, and ensure our ideals of individual freedom and our way of life.

Actions Completed

In December 2018 the LeMay Center hosted an EW/EMS Doctrine Rewrite Summit to update EW/EMS doctrine. There were approximately 20 experienced personnel from RC-135 and EC-130 aircraft, 53rd Wing, Air Force Special Operations Command, Air Force Space Command (AFSPC), Air Force Global Strike Command (AFGSC), ACC, Air Force Mobility Command, and Cyber Command to rewrite the Air Force (AF) Annex 3-51 Electronic Warfare Doctrine. After reviewing the current doctrine and the

draft JP 3-16 Joint Electromagnetic Spectrum Operations (JEMSO) documents, the group composed a draft Annex 3-51 *Electronic Warfare and Electromagnetic Spectrum Operations*, which defined EW in air, space, and cyber and incorporated JEMSO concepts into Air Force structure. The Annex 3-51 EW/EMS Doctrine is in final coordination, which was published 30 July 2019.

The LeMay Center drafted a review process for AETC coordination, at the direction of CSAF, to review all EW, SIGINT, Weapons School, and EMS academics. Correspondence between AETC and MAJCOMs will allow for the creation of standardized EMS force-development academics for all Airmen. The academics/courseware will provide EMS education for every Airman at a basic level to a more specific advanced EMS course for war gamers and joint planners.

The Way Forward

The Deputy Chief of Staff, Strategy, Integration and Requirements (AF/A5) will establish an EMS Superiority Directorate. A general officer will lead this new directorate that will be responsible for enterprise-wide actions and unity of effort to deliver EMS superiority in all domains.

The Director, EMS Superiority will assess the value of creating an EMS Enterprise Integration Group linking MAJCOM staffs and Air Force Warfighting Integration Capability counterparts. This group will be responsible for developing enterprise-wide EMS strategy and corresponding investment and divestment priorities. The director will chair the group and establish linkages with AF/A8P and A8X for program objective memorandum planning and programming actions.

AF/A5 will stand up a functional integration team in AF/A5A, led by a colonel who synchronizes with the EMS Superiority Directorate. AF/A5 will embed EMS experts in all A5A functional areas (e.g., Capability Development, Futures/Concepts, etc.), and establish an EMS Superiority Panel.

The Deputy Chief of Staff of Plans and Programs (AF/A8) will establish an EMS Superiority Panel that will manage all AF EMS/EW equities. A colonel will lead the panel and will report to the EMS Superiority Director and identify an office of primary responsibility and a point of contact for EMSO.

All MAJCOMs should designate a dedicated EMSO staff element (recommend Division) with effective linkage to the EMS Superiority Directorate.

Consolidate and Modernize EW Reprogramming Enterprise

ACC will migrate the existing Specialized Electronic Combat and Reprogramming Environment (SPECTRE) infrastructure into an Air Force com-

mon integrated programming platform for EW. Acting as an application store, the enhanced SPECTRE will securely develop, test, host, and deliver the EW missionware using modern, industry-standard developer tool chains. SPECTRE will integrate EMS effects while identifying and mitigating EMS fratricide by employing appropriate model-based systems engineering and advanced modeling and simulation.

Offices under the Secretary of the Air Force will develop an appropriate continuous authority to operate that will facilitate the rapid fielding of secure missionware and consolidate reprogramming centers. To accomplish this, ACC will consolidate the Air Force's two Operational Reprogramming Centers into a single organization that will program and reprogram EMS/EW systems as well as sensor engineer Combat and Mobility Air Forces systems and platforms. Individual MAJCOMs will continue to set the programming and updating priorities within their portfolios. ACC will also work with AFSPC to identify mechanisms to ensure unity of effort while deconflicting EW effects. Applicable Air Force Life Cycle Management Center organization(s) will partner with the Operational Reprogramming Center to develop a system-specific missionware capability that supports portability of threat-specific techniques, threat simulations, and other system attributes. SAF/CN will identify and accredit a suitable Secure Development Ops Environment for this interchange.

EMS Culture and Awareness

To ensure EMS culture and awareness across the range of military operations, this paper recommends a three-phase approach: Near-Term, Mid-Term, and Long-Term. The knowledge of an EMS war fighter is not limited only to EW but constitutes the entire domain. To make certain a cohesive understanding and integration of the entire EMS among Air Force civilians, active duty, and leadership for future EMS superiority, the following minimum recommendations are provided for implementation across the US:

Near-Term:

1. Author US EMS policy and doctrine
2. Facilitate AF service support to joint doctrine's plan for Joint EMS Operations (JEMSO) and provide the AF's position on service execution for the commander of Air Force Forces (COMAFFOR)'s staff to execute EMSO operations in support of the Joint Force Commander's Theater Campaign Plan
3. Review and consolidate US EW/EMS academics and courses

Mid-Term:

Consolidate EMS academics and create standardized, multi-layered academics to instill a culture of EMS awareness in the US. Instill EMS objectives into all major exercises, large force employment, and war gaming.

EMS 100: Basic EW and EMS education to be taught at basic training, service academies, Reserve Officer Training Corps, officer training school, and so forth.

EMS 200: Intermediate EW and EMS academics and tabletop exercises to be reinforced at all military initial qualification training and technical schools; special emphasis to identify and instruct future EMS subject matter experts. This course will also be used as a refresher course for general officers.

EMS 300: Advanced EMS education for military planners, industry leaders, academia, and EMS leaders of tomorrow. The course would include academics, strategic/operational doctrine, and tabletop exercises and requirements for participation in exercises where attendees ensure they execute EMS objectives in a contested environment against a peer adversary or due to a GMD.

EMS 400: Additional advanced EMS academics for military and civilian planners and military EMSO staffs. Requirements include advanced academics/doctrine and tabletop exercises, with a graduation exercise—participation in an exercise where attendees ensure they execute EMS objectives in a contested environment against a peer adversary or due to a GMD.

Long-Term:

Focus on three critical lines of effort collectively required for protecting this core competency:

1. Expertise and Operating Concepts;
2. Bridge to Advanced Technology and Competitive Capability;
3. Institutionalize EMS Resurgence and Leadership.

To develop EMS doctrine and training, AETC will explore, develop, and produce new and innovative concepts and doctrine that expand on historic EW principles in favor of enterprise EMSO. Outdated doctrine and instructions will be rewritten emphasizing the EMS as a war-fighting maneuver space addressing joint and multi-domain EMSO. Correspondingly, AETC will act to combine components of separate EW, SIGINT, Weapons School, and EMS academics into standardized EMS force development academics (basic through advanced) for all Airmen—military and civilian.

AETC will assess the creation of an EMS Center of Excellence made up of Airborne EW, Space EW, Cyber EW, and Joint expertise responsible for EMS education, leadership training, exercises, war games, and sophisticated technical acumen.

The EMS Superiority Directorate, in coordination with Air Force Manpower and Personnel (AF/A1), will provide oversight for talent management of EMS experts to ensure development of future joint EMS leaders. This will enable the US to develop and manage EMS talent.

MAJCOMs and the LeMay Center will emphasize exercising and training in a realistic EMS-contested environment in order to develop tactics, techniques, and procedures and build situational recognition and proficiency in a degraded EMS environment.

Summary

Lacking recognition of the EMS as a war-fighting domain, there is no true forcing function to drive the US to do the hard thinking, experimentation, and war gaming required to develop and validate the theory and doctrine we lack. The tasks included in this Implementation Plan are designed to begin the process of restoring the Air Force's ability to gain and maintain EMS superiority. As champion, the Director, EMS Superiority, will stand up and lead the directorate and provide oversight of the creation of an EMS Superiority Panel, the modernization of EW reprogramming, and instantiation of a culture of EMS/EW awareness across the Air Force. The support of Airmen across the Air Force is necessary to assure effective implementation.

Appendix 3

A "Typical State's" Perspective on EMP and EMS Threats to the Electric Grid

Overview

As in many other states, policy makers in Alabama have heard constituents are interested in learning what utilities and state government are doing to protect the state and nation's security and prosperity, including threats to the electric grid. Policy makers and their constituents have engaged utilities in Alabama to discuss and discover the magnitude of the threats faced by the grid and the strides taken by utilities to protect and secure infrastructure against natural and man-made hazards.

Alabama is a diverse state in terms of electrification. A variety of electric providers, including Alabama Power, the Tennessee Valley Authority (TVA), and the state's many nonprofit rural electric cooperative and municipal electric utilities, operate together to provide power to the state. The strong relationships among these partners are characterized by cooperation, a passion for community engagement, and sustained forward progress in growth and industrial development that has measurably increased the quality of life for all Alabamians. Additionally, Alabama's electric sector stakeholders enjoy productive and cooperative relationships with the state's policy makers and regulators. In the face of hazards including hurricanes, tornadoes, ice storms, heat waves, and severe windstorms, these partners cooperate to ensure the reliability and prompt restoration of service to customers.

Alabama is also a diverse state in terms of its infrastructure and economy. While not as populous as some states, it is home to a deep-water port, a robust automotive manufacturing industry, and several military installations. The state also has a robust agriculture industry and a long history with aerospace manufacturing and technology. Additionally, Alabama continues to capitalize on its strong partnership with the Department of Defense (DOD) to develop and host next-generation war-fighting technologies, such as the Air National Guard's 187th Fighter Wing's F-35 Lightning II aircraft.

The Alabama Emergency Management Agency (AEMA)—due to its unique position as the nexus of infrastructure protection and restoration from all hazards, its mission to coordinate with partners on enhancing the state's capacity for community resilience, and its interfaces with military partners—was tasked to convene a series of discussions among industry leaders and key stakeholders on the topic of grid resilience. These discussions

identified opportunities and barriers for how a "typical state" would protect its infrastructure and citizens.

As a capstone to this effort, AEMA worked with Air University and the Curtis E. LeMay Center for Doctrine Development and Education to invite representatives from Alabama's energy sector and other interested stakeholders to participate in the Electromagnetic Defense Task Force (EDTF) 2.0 summit held at Maxwell Air Force Base in May 2019. Attendees included representation from Alabama Power, the TVA, the Alabama Rural Electric Association of Cooperatives, PowerSouth Energy Cooperative, and the Alabama Municipal Electric Authority, as well as representation from the Montgomery Area Chamber of Commerce, the Air Force, the Alabama Air National Guard, the Department of Homeland Security, and the office of Alabama Governor Kay Ivey.

After participating in EDTF discussions and hearing perspectives from other states, utilities, and federal partners, Alabama's attendees met to develop a list of open questions and consensus points about how a typical state might move forward with mitigation. The items listed below summarize what work remains to be done in closing the information and mitigation gaps for electromagnetic pulse (EMP) and electromagnetic spectrum (EMS) threats to the grid. This is not an Alabama-specific plan for addressing the issues; rather, it is intended as a guide for policy makers and presents the current condition of the state regarding EMP and EMS electrical grid protection. While the participants expressed confidence that counterparts in other states would hold a variety of views on these topics, the participants also felt the major issues and questions raised would likely be representative of a typical state.

The thoughts and perspectives provided by the Alabama focus group have been distilled into a list of nine open questions that must be answered to enable the nation to tackle EMP and EMS hardening of the electric grid. Additionally, three overarching strategic obstacles were identified; these will need deliberate and collaborative public-private solutions for the nation to progress toward resilience against these threats.

Disclaimer: The reader should note that the issues outlined below present only a general synthesis of themes and questions discussed during the EDTF. The material presented should not be construed as representing the opinion or position of any individual who participated in the summit, any employer or institution represented, or the state of Alabama.

Discussion: Open Questions, Moving Forward

1. The nation needs to decide if it will implement EMP/EMS mitigation measures in either a holistic or a piecemeal fashion.

There are two primary concepts of applying EMP/EMS mitigation measures across the grid.

a. An approach that focuses only on identified critical paths and nodes in the generation, transmission, distribution, and load chains. Such an approach might provide a means of mitigation for known critical infrastructure and loads that are essential to national defense and homeland security. This might be dubbed a critical path approach.

b. Applying "defense in depth." Such an approach would see EMP/EMS mitigation measures applied across the entire grid ecosystem. It would also include efforts to enhance the redundancy and survivability of the grid against a variety of other known threats, including natural hazards such as geomagnetic disturbance (GMD).

It is possible that some combination of both approaches might be realized. By focusing first on critical paths, some level of survivability could be attained today, while further resilience for the system could be achieved tomorrow as mitigation measures are applied across the grid.

2. Resilience against EMP/EMS threats must be incentivized.

Utilities in any state will need to be incentivized before undertaking significant mitigation projects. In general, questions arose around two facets of incentivization: the incentives themselves and the lens through which the stakeholders will understand the incentives.

What are the factors that will ultimately drive the utility industry on the one hand, and the DOD on the other, to commit to implementing grid resilience measures as a collective undertaking?

What framework will be used to analyze incentives? Attendees expressed confidence that industry analysis will be financially driven while the DOD is likely to take a threat-based approach to analysis.

Incentivization of EMP/EMS mitigation measures is a wicked problem due to the complex factors involved. Primarily, the attendees felt that the principal factors were (a) funding, (b) the evident unknowability (at least at the time of this report) of what constitutes a proper and prudent mitigation strategy, and (c) disagreements among the data regarding the magnitude of EMP/EMS threats to the grid and its infrastructure.

3. Better data and information sharing is essential.

While it is in principle a basic concept, participants felt achieving an enhanced commitment to information and data sharing across industry, government (both regulators and policy makers), defense, and homeland security stakeholders should be prioritized.

4. Business cases for EMP and EMS mitigation must be developed.

More work is needed to build the business case for investing in mitigation measures. This is an area where a contrast between defense and industry officials becomes evident.

From a defense perspective that views the employment of EMP and EMS techniques as weapons of war, the nation's survival cannot be measured with cost-benefit analysis; that is, in the face of existential threats, ensuring survival is—on its own merits—a complete business case.

On the other hand, industry requires mitigation measures being bought at a defined cost—regardless of whether that cost is currently known or agreed to. Thus, mitigation is by necessity a matter of managing limited resources, both financial and material.

The attendees agreed that hyperbolic language about EMP and EMS threats was generally unhelpful in moving discussions forward on these issues. A useful approach is anchoring discussion on the topics of technical vulnerabilities and mitigation challenges, leaving aside speculation about the socioeconomic impacts of a cascading infrastructure failure.

5. The mindset regarding EMP and EMS threats must change across industry, government, and other interested stakeholders.

It is important to note the dark tone of some conversations around EMP and EMS threats belies the underlying mindset about tackling the problem; that is to say, the discourse around these issues has become securitized. To make progress, conversations around EMP and EMS threats must be desecuritized and reconceptualized. They must be viewed as challenges to the resilience of our nation's infrastructure and as opportunities for industry and public-private partnerships to drive increased economic and national security in the future.

6. Effective coordination structures are needed to implement EMP/EMS mitigation measures.

At the state level, formalized coordination structures will be needed to bring together industry, utilities, government, subject matter experts from defense and homeland security, and the research community, to collectively address the challenge of EMP and EMS mitigation. It is essential that states and their utilities be empowered to control their own affairs to the maximum extent possible while also being provided with an opportunity to function as one cohesive team in the undertaking.

Likewise, states will need to develop shared, cooperative strategies that integrate vision, goals, and objectives across all stakeholders. Such strategies must be sufficiently broad to allow for future refinement in data and mitigation measures, while also synchronizing stakeholders around resilience activities.

7. A comprehensive vantage point must be maintained that considers EMP and EMS threats in the balance of all hazards and threats.

A fundamental principle of emergency management in the United States is the "all hazards" approach. In this framework, government and the private sector coordinate to address both natural and man-made hazards through a comprehensive system that applies mitigation, preparedness, response, and recovery plans and resources in a consistent manner regardless of any threat. This all hazards approach must be maintained when dealing with EMP and EMS threats. Any resilience and mitigation measures must be implemented with an eye toward other threats, especially natural hazards such as hurricanes, tornadoes, windstorms, ice storms, and GMD. Furthermore, mitigation efforts must also consider unconventional threats such as cyberattacks and terrorism.

8. An effective risk communications strategy must be developed.

Decision makers in both the public and private sectors frequently make decisions in the context of risk. As such, efforts to mitigate against EMP and EMS threats must be communicated to stakeholders using the language of risk. Simplified, this means talking about the risks of investing in mitigation (sunk costs, lost productivity in other areas of effort) and the risks of not investing in mitigation (failure of the grid, degraded national security). Ultimately, there is risk in every scenario and outcome; as such, it is imperative that the issues of EMP and EMS mitigation not be reduced to a binary question of identifying a single, low-risk course of action among a pool of evident alternatives. A combination of

many different measures must be weighed in the context of the complex environment in which those measures will be implemented.

9. Mitigation efforts must focus not only on infrastructure hardening but also on policies, plans, and procedures.

The electric utility industry has made significant progress over the past several decades by optimizing plans, procedures, and operational protocols with an eye toward increased safety and enhanced efficiency. In the energy industry, resilience is—in large part—due to intensive training of highly skilled professional system operators and relying on good policies and procedures that are continually improved. There is a culture of high reliability in the industry. Lessons learned through achieving that culture should be considered when contemplating the path forward for addressing EMP and EMS threats.

Perceived Barriers to Progress

In addition to the areas of opportunity identified during the Alabama discussions, participants spoke broadly to three overarching strategic obstacles that must be overcome if the nation is to effectively mitigate EMP and EMS threats to the electric grid. These obstacles were perceived by the participants as threats to the resiliency and national security of the United States.

Strategic Obstacle no. 1: Aligning public policy interests at the state and federal levels.

At the state level, the most evident strategic obstacle is education. This includes education of both the public and policy makers.

K–12 education: Electric utilities, like all industries, rely on a trained, qualified, and engaged workforce. The delivery of high-quality science, technology, engineering, and mathematics (STEM) education is a strategic priority for the energy industry. Without successful STEM programs, the industry will suffer, as will the nation's resilience. **State-level policy makers must understand STEM education as an essential pillar in our nation's national security.**

Policy-maker education: Awareness of the complexity and vulnerabilities of our nation's infrastructure is limited among state-level policy makers. This is a problem across all infrastructure sectors and is especially true regarding the electric grid, EMP and EMS threats, and the nexus of electric power with all other aspects of life in a modern society. **A deliberate program should be undertaken to educate state-level appointed and elected leaders about enhancing the resilience of the nation's electric grid.**

At the federal level, three closely related concerns constitute a strategic obstacle: politics, funding, and regulation.

Politics: The politics of the energy industry on the national stage are complex. With regard to mitigating against EMP and EMS threats, many opinions exist as to the magnitude of the threat, the most appropriate means to mitigate against the threat, and who should be leading the decision-making process for mitigation efforts. At a basic level, the public-private policy apparatus that drives the energy industry is optimized to address the day-to-day delivery of clean, efficient power to the American public. **Tackling a complex problem such as EMP and EMS threats is well outside the norm of issues for many of those involved in energy policy discussions and will require a realignment of policy interests within the broader context of our nation's ongoing energy debates.**

Funding: Obtaining funding for EMP and EMS mitigation efforts is a necessity, and the federal government must facilitate a solution to this need. Currently, EMP and EMS threats are collectively viewed as either "a national security/defense issue" or as an "inherent vulnerability of the electric grid." Those who view the issue as one of national defense tend to point toward Congress and defense appropriations as the best funding source for mitigation efforts and leadership in defining the nature and extent of threats. On the other hand, those who view the issue as one of the inherent complexities of the nation's infrastructure tend to look toward industry to find its own solutions within the confines of existing rate structures, regulation, and business income. **The nation must decide whether the EMP and EMS threat is a national defense issue. Further, the nation must collectively determine how best to drive mitigation efforts: through federal appropriations and incentives, through regulation and existing utility funding streams, or through some combination of those avenues.**

Regulation: Lastly, at the federal level, regulators with influence in the energy production and transmission domains should work to gain awareness of how EMP and EMS threats are impacting electric utilities across the nation and work to provide effective regulatory guidance and support for future mitigation activities. **Importantly, the attendees stressed that no material progress on mitigating against EMP and EMS threats would be possible without strong and clear support from federal regulators.**

Strategic Obstacle no. 2: Articulating clear and measurable near- and long-term action items.

Stakeholders in the energy sector need actionable plans for mitigating against EMP and EMS threats. Action plans are needed for mitigation measures and implementation processes and to further define requirements and standards.

Planning element 1: Mitigation courses of action. States and utilities need courses of action and alternatives for mitigation measures that include cost/benefit estimation tools.

Planning element 2: Implementation processes. States and utilities need roadmaps and templated processes for mitigation measures. These should include alternatives such as incremental mitigation measures—such as leveraging the attrition of old and obsolete components as an opportunity to introduce EMP- and EMS-hardened systems.

Planning element 3: Requirements and standards. There is currently no clear consensus across interests in the defense and energy domains to the extent of appropriate mitigation measures. Once such a consensus is achieved, a requirements- and standards-setting framework will be needed to guide necessary changes in rules, regulations, laws, and baseline minimum mitigation levels. Such a framework must provide a mechanism for coordinating efforts across both technical and policy domains.

Strategic Obstacle no. 3: Overcoming the state/regional dichotomy.

Currently, energy production and transmission in the United States are operationally regulated and managed at two primary levels: states and regions. Depending on the system in question and the level of analysis, there is overlap between these two domains. To proceed with EMP and EMS mitigation measures, congruence between the domains must be achieved. Fundamentally, the nation must decide whether EMP and EMS mitigation is to be pursued within the geographic boundaries of any particular state or at the regional—or national—level. Resolving this question and determining the best level at which to focus mitigation efforts are a challenge of feasibility—technically, financially, and politically.

Appendix 4

Recommendations Checklist

- ☐ Establish information sharing within the government, industry, and academia
  - ☐ Create a national repository to track infrastructure resiliency initiatives to help minimize duplication of efforts and enhance benchmarking of successful projects
- ☐ Garner public support through public outreach and media campaigns
- ☐ Develop a nationwide plan with Department of Homeland Security (DHS), US Northern Command (USNORTHCOM), and US Strategic Command, and include local communities
- ☐ Ensure electric power grid and supervisory control and data acquisition is not dependent on 5G
- ☐ Build a community of experts
  - ☐ Invest in science, technology, engineering, and mathematics (STEM)
  - ☐ Incentivize STEM graduates and engineering disciplines to research the mechanics of EMS hardening
- ☐ Develop a cohesive strategic plan involving national and local governments
  - ☐ Involve the Federal Emergency Management Agency and establish geomagnetic disturbance (GMD) / electromagnetic pulse (EMP) as a natural disaster
  - ☐ Ensure 5G's recovery steps are included as 5G becomes more prevalent
  - ☐ Harden and utilize cells-on-wheels
  - ☐ Partner with American Radio and Relay League and Military Auxiliary Radio System to integrate ham radio into the national emergency and redundant communications strategy
- ☐ Incentivize industry to implement shielding standards and protect equipment
  - ☐ Research implementation of EMP-Star rating
  - ☐ Set standards for tiered rating
  - ☐ Award cities for EMP resiliency

- ☐ Increase the pace and reduce the cost of 5G development by allocating mid-band spectrum (sub 6Ghz) for mobile assets
  - ☐ Ensure supply chain integrity of 5G equipment for security
  - ☐ Educate students and military on vulnerabilities of 5G and potential threats
  - ☐ Ensure 5G networks are resilient, redundant, and resistant to GMD/EMP
- ☐ Recognize the electromagnetic spectrum (EMS) as a domain and incorporate EMS into doctrine
  - ☐ Create a culture of EMS awareness
  - ☐ Translate/publish/understand adversary doctrine
  - ☐ Develop golden hour response plan for EMP recovery
- ☐ Educate military members on EMS utilization and vulnerabilities beginning with initial military training and continuing through career
  - ☐ Incorporate EMS training into LeMay Wing and Group Commander's course
- ☐ Train and exercise in an EMS-degraded environment
  - ☐ Incorporate GMD/EMP into community and base exercises
  - ☐ Stand up EMS attack "Red Team"
- ☐ Develop cognitive electronic warfare and artificial intelligence to deliver mass alert from GMD/EMP
  - ☐ Develop software-defined/reconfigurable radios and laser-based communications
  - ☐ Research UAV or balloon-based repeaters for radio communication
- ☐ Invest in pre-positioned shielded assets, including generators, fuel, and communications equipment, which are placed throughout the nation and in allied countries
- ☐ Streamline the acquisition process for EMP-shielded equipment to allow quicker development and unit testing
- ☐ Develop tax incentives for implementing EMP-hardening standards
- ☐ Develop micro-grids that are hardened for EMP and cyber for critical facilities and then branch out to all military bases
- ☐ Evaluate ways to detect and prevent threats across 5G networks

- ☐ Institutionalize EMS awareness in leadership positions
- ☐ Partner with universities to develop "whole of society" EMS education programs and strategies
- ☐ Strategically message that the US is prepared for EMP attack and will regard it as a crime against humanity
- ☐ Develop leadership roles for specific situations; for example DHS will lead recovery after GMD, while USNORTHCOM will lead recovery and retaliation after EMP
- ☐ Manage the workforce to find and retain experts in EMS operations and maintain corporate knowledge
- ☐ Ensure EMP shielding is implemented in new military construction as the cost is much lower

Appendix 5

EDTF 2.0 Executive Outbrief Slides

Track I: EMSO

What sustainable, efficient, and cost-effective approaches do we need to invest in/develop right now to keep Joint Force capability operational (viable) in a severe EMS-degraded environment?

1. Doctrine: common understanding/lexicon, war fighting
2. Organization: integrated across staff/echelon, institutionalized in military and civic arenas
3. Training/Education (individual/collective): whole force, readiness, demand signal, objectives, OPFOR, venues, M&S, T&E (OT/DT)
4. Material: cognitive/AI, meshed networks, distributed, autonomy, man-machine, software-defined/reconfigurable, multi-mission, MDC2/EMBM (J2/3/6 operationalized)
5. Leadership: advocacy/influence, resourcing, governance, focus, "seat at the table"
6. Personnel: available expertise, workforce management (traceable, career)
7. Facilities: ranges, LVC, COE (virtual distributed? DEVOPs: tech/ops?)

Deterrence

What sustainable, efficient, and cost-effective approaches do we need to invest in/develop right now to keep Joint Force capability operational (viable) in a severe EMS-degraded environment?

1. Whole of Government Strategic Messaging
   a. Attack with HEMP is act of war and crime against humanity
   b. Expect severe repercussions from US, allies, and coalition
2. Educate, train, exercise, war game to real-world scenario and make resources available
   a. Military capabilities emphasis
   b. Civic/DOD interoperability, cooperation, and training
   c. Degraded EMS-focused exercises—realistic replication

   d. EMP/EMS Red Team creation
3. NORTHCOM/STRATCOM/DHS integration and sharing resources, knowledge (command relationships)
4. Resiliency, redundancy, and hardening plan (physical/long term)
5. Responsive and reliant communications for military/civilian response

Deterrence: Left of Bang

1. Reenergize the DOD to train and exercise Contingency and Emergency communication plans (PACE plan)
   a. Mandate to unify communities w/ EMP plan to include municipal entities, utilities, etc.
2. Infrastructure protection
   a. Prioritized list of what industry/power/financial networks need to be hardened—EMP survivability rating?
   b. Incentivize protected commercial assets that provide military comm services, with sufficient EMP shielding for future satellites
   c. Mandate future asset development with EMI/EMP protection capabilities
   d. Implement micro-power grids according to a prioritized list (regional commands)
   e. Fiber lines, software based radios, laser communications
   f. HF/ham radio assets with people trained and proficient in TTPs
3. Prepositioned comm assets in EMP facilities or containers
   a. Regional military commands
   b. Data pods in FVEY countries
4. Launch micro-sat system to be repeaters for UHF/VHF/etc. communication
5. Autonomy of decision making (centralized control/decentralized execution—mission type orders)

Recovery

What are our strategic blind spots in regard to EMSO, and how do we counter/frustrate enemy efforts (place near-term bets)?

1. Public buy-in and "user pull" with public leaders, military leadership and industry

   a. Lack of investment strategy and civil coordination
   b. Day without EMS
2. No grounded understanding in E1, E2, E3 effects on spectrum of systems and capabilities
   a. Increase modeling and simulation across DOD, industry, academia
3. Execute recovery plans and capabilities across CONUS regions and multi-national
   a. Gain awareness of situation
   b. USNORTHCOM/DHS cooperative execution of command and control
4. Execute dispersal and positioning of minimum essential equipment list (COOP plan)
   a. Establish communications (NC3 L2 from SAC?); nuclear mobile communications teams, civilian telecommunications
   b. Launch CubeSats/micro-sats
5. Expectation management to DOD and civilian sectors
6. Execute prioritized restoration of critical infrastructure

Retaliate

How can industry, academia, and military work together to counter our strategic blind spots and improve the nation's resilience?

1. Include more industry, energy companies, data analysis personnel in R&D, capability
2. Invest in STEM! Public education baseline must support this fight
   a. Educate the populace through civil defense programs—strengthen will of the people
   b. Take advantage of community relationships with military bases
   c. Benchmark relationships, synergy of investment dollars
   d. Find those civ/mil SMEs and organizations (AFIT, RAND, AF/A9, AF Office of Scientific Research)
3. Develop quantum computing, cognitive EW, and advanced AI to provide I&W and support to attributing responsibility
4. Action on strategic messaging

Track II: HPEM/DE/Spectrum

What sustainable, efficient, and cost-effective approaches do we need to invest in/develop right now to keep Joint Force capability operational (viable) in a severe EMS-degraded environment?

1. Share existing test and mitigation information—reach consensus
2. Identify & prioritize critical infrastructure & defense dependencies
3. Single accountable agency & shared strategy
4. Test, assess, plan, exercise

Strategic blind spots & counter/frustrate enemy efforts (near term)

1. Strategic blind spots
    a. Disagreement on anticipated effects
    b. Inadequate testing and integrated exercises
    c. Lack of national and military strategy and plans
    d. Lack of R&D integration with users and acquisitions
2. Counter/frustrate enemy efforts (near term)
    a. Share existing test information – update environmental standards

Work together to counter our strategic blind spots and improve the nation's resilience?

1. What roles should industry, academia, and military play?
    a. Team approach – integrated planning and exercises
    b. Differing lanes – natural disasters versus national defense
2. How can the convergence of industry, academic, and military efforts counter strategic blind spots and improve the nation's resilience?
    a. Incentives/disincentives for innovation & mitigation
    b. Information sharing among stakeholders
    c. Public outreach programs
    d. Best practices programs

Track III: EMP and GMD

What sustainable, efficient, and cost-effective approaches do we need to invest in/develop right now to keep Joint Force capability operational (viable) in a severe EMS-degraded environment?

1. Investments
    a. Education, training and policy/doctrine
        i. Develop corporate knowledge and properly capturing historical documents, data, knowledge
    b. Continue effort to identify and harden DOD mission critical infrastructure (black start cap)
    c. Identify and harden essential infrastructure (power stations, water/sanitation, comms, etc.)
2. Developmental Requirements
    a. Policy/doctrine/standards
        i. Golden hour standards, drills, and exercises (civilian and military)
    b. Hardening standards and testing (tiered solution for military/civil/infrastructure)
    c. Marketing campaign for response and preparedness
    d. Critical personnel and family plans
    e. Streamlined acquisition process (i.e., AFWERX/SOFWERX/Army Futures command-like capabilities) CVC

What are our strategic blind spots in regard to each track (EMSO, HPEM/5G/DE, EMP/GMD, and EMS/Quantum) and how do we counter/frustrate enemy efforts (place near-term bets)?

1. What are our strategic blind spots?
    a. Adversary policy and doctrine for EM warfare
        i. Adversary understanding of our policy and doctrine for response/First use
            ii. Adversary views of readiness and vulnerabilities
    b. Identifying, understanding and testing our internal vulnerabilities, gaps, capabilities
    c Inadvertently/knowingly building vulnerabilities with tech advances

d. Remove barriers for sharing information (classification/political/bureaucratic/patent process)

2. Prioritize near-term responses to counter/frustrate enemy efforts.
    a. Deterrence/strategic messaging/denial and deception
    b. Codify achievable requirements for future system design to include EM protection/resilience
    c. EDTF outreach

How can industry, academia, and military work together to counter our strategic blind spots and improve the nation's resilience?

1. What roles should industry, academia, and military play?
    a. *Government/Military set the example with deterrence/resilience
    b. Academia train the next generation of experts
    c. Industry invest/develop incremental hardening plans and technologies
2. How can the convergence of industry, academic, and military efforts counter strategic blind spots and improve the nation's resilience?
    a. Remove barriers for sharing information (classification/political/bureaucratic)
    b. *Government/Military/Industry strategically funding/incentivizing resilient systems
    c. *Government/Military/Academia developing education, training and expertise

***Government=federal/state/local**

Track IV: Quantum/5G Working Group

How resilient is 5G?

1. Not very as it is vulnerable to the effects of EMP just as 4G
2. Mobile network is VERY dependent on power
3. Large macro-cell stations may have some emergency power, but small cells are unlikely to have any useful emergency power
4. Existing power grid relies on a SCADA (survey control and data acquisition) network that for resiliency needs to be independent of the general 5G network

Recommendations

1. Test for effects of EMP against base station infrastructure
2. Retrieve technical inputs on SCADA resiliency

How does 5G relate to computing at the edge?

1. 5G standards allow the integration of edge computing located at base stations
2. 5G's ability to embed compute services inside mobile network greatly increases the attack surface
3. In severely degraded environment (i.e., EMP), without connectivity to control elements inside the core network, communication ceases

Recommendations

1. Test distributing the core network (if it is possible)
2. Test shutting down network in localized area on the ground, running the network via airborne platform (i.e., UAV)

How does the RF-degraded environment affect data retrieval at the edge (i.e. impact to the cloud)?

If the base station is disconnected from the network, then there is no connectivity to the cloud.

What happens when we lose PNT (upon which all transpiration layers are reliant)?

If properly designed, it is possible to communicate timing data via fiber-optic connectivity (rarely done at present).

Additional Quantum/5G Question

How do we establish/preserve/regenerate joint 5G/quantum computing capabilities now?

1. Networks need to be China-free
2. Supply chain integrity
3. Encryption improvement (zero-trust model for communications)
4. Need more mid-band spectrum in commercial service for economies of scale

What are our strategic blind spots in regard to 5G/Quantum?

1. Lack of education of what 5G is, why it affects everyone, and how to harden before emergency
2. US is deploying 5G in different spectrums
3. Unknown interdependencies between power, SCADA, and mobile that may prohibit recovery from HEMP event
4. US telecom providers unaware of viability of EMP

How can industry, academia, and military work together to address these strategic blind spots?

1. Formally recognize EMS as a domain
2. Establish training within services for EMS scenarios (total force training)
   a. Educate—EMS should be taught at entry level training and up (e.g., OTS and BMT). Strategic thinking with regard to EMS should start much younger than where we are now.
   b. Train—on basic and continuation training/at unit-directed level
   c. Evaluate—define operational metrics (mission/people) to determine if training is effective
3. Train industrial base on significant risks
4. Lower level recruitment (whole-of-society efforts)
   a. Set up something similar to Palace Acquire (sets career path for recruited STEM grads)
   b. Create programs for younger kids, not just college grads; not just recruiting into the military—develop civilian/reserve option
   c. Define what we want the future to be and work toward it
5. DOD needs to plan for operations in a post-Western internet environment

How can we organize, train, equip, and provide for each strategy?

1. Organize: create linkages between AETC and internal and external organizations (e.g. AFRL linking with AETC); tap into UARC/EWI; develop new process/policy for spectrum collaboration/sharing (whole-of-society efforts)
2. Train: ensure every Airman understands EMS and becomes responsible as a stakeholder in protection of EMS (strategic thinking at all levels); create operational exercises with real-life impact (e.g. two days post-IOS update shut down all without update); strengthen red team capability/feedback Air Force wide
3. Equip/provide: right equipment to accomplish mission; determine level of hardening based on mission

We should develop a DOTMLPF-P for a national response framework to a HEMP scenario that pre-plans federal/state responsibilities, details evacuation plans for large cities to simplify resupply efforts, reassesses existing utility of organizations like the Civil Air Patrol, and ensures an effective, high-bandwidth emergency communication systems that integrates all elements.

What do we need to invest in/develop to implement the strategy?

1. Invest: Sub-6 technology vs mmWave; buy and test (e.g. OSD Foreign Comparative Testing Office)
2. Develop: Cooperative model to test/evaluate 5G/Quantum (including academia, industry, and specific foreign partners)
3. Terrestrial alternative to GPS; 5G/Quantum can assist with providing high-precision timing to ensure that there is an alternative to GPS should the satellite system be inaccessible due to ionization

Are quantum communications resilient to EMS?

Theoretically, quantum communications *should* be more resilient; more research is needed.

Appendix 6

List of Attendees and Contacts

This appendix is a sample list of more than 100 agencies represented at the 2019 Electromagnetic Defense Task Force summit.

- Air Education and Training Command
- Air Force Civil Engineering Center
- Air Force Global Strike Command
- Air Force Institute of Technology
- Air Force Materiel Command
- Air Force Research Laboratory
- Air Force Special Operations Command
- Air University
- Alabama Rural Electric Association
- Argonne National Laboratory
- Defense Innovation Board
- Defense Spectrum Organization
- Defense Threat Reduction Agency
- Department of Homeland Security
- Federal Energy Regulatory Commission
- George Mason University
- Georgia Tech Research Institute
- Idaho National Laboratory
- IHS Markit
- Johns Hopkins University
- Joint Chiefs of Staff (Joint Staff)
- *Journal of Electronic Defense*
- Lockheed Martin
- Los Alamos National Laboratory
- National Aeronautics and Space Administration (NASA)

- National Defense University
- North Atlantic Treaty Organization (NATO)
- Nuclear Regulatory Commission (NRC)
- Office of the Secretary of Defense
- Royal Australian Air Force
- Royal Australian Navy
- Sandia National Laboratory
- Southwest Research Institute
- State of Alabama, Governor's Office
- Texas State House of Representatives
- Texas State Office of Risk Management
- The Curtis E. LeMay Center for Doctrine Development and Education
- The White House
- Union of Concerned Scientists
- United States Strategic Command
- University of Colorado
- University of Texas
- Wyoming National Guard

Appendix 7

EMS Resilience and Preparedness for Government and Society

Background

During the Electromagnetic Defense Task Force (EDTF) 2.0, a fellow with more than 33 years of uniformed service provided a historic reflection demonstrating the importance of assuring the protection of civilians and supporting civil infrastructure to ensure mission accomplishment. The fellow had been part of the first operational readiness exercise conducted by Strategic Air Command (SAC) in 1964. During the exercise, conducted in Minot AFB, North Dakota, with an outside temperature of 20 below zero, all power to the base housing area was turned off. Not a single aircraft was able to get airborne due to the number of military personnel who stayed home to tend to their families.

A 2019 exercise at Fort Bragg, North Carolina, led to similar outcomes. During the exercise, a mock cyberattack induced a blackout of approximately 12 hours in conjunction with the exercise deployment of an Army Airborne Division, "to test the community's ability to rebound from an attack and still get troops off on their mission."[1] The half-day exercise resulted in sufficient turmoil from the local civilian and military population that the installation issued an apology and the garrison commander's office had to coordinate with the post's judge advocate general to assist residents with claims for losses caused by the exercise-induced blackout. This contemporary exercise demonstrates that the criticality of residential and family resilience has not changed since the 1964 exercise.

With these exercises as a contextual backdrop, EDTF experts explored modern cultural resilience, the human psychological dimension of a long-term electric grid collapse, and existing US government guidance on resilience and preparedness associated with electromagnetic spectrum (EMS) threats. The discussion produced several insights that are presented below.

1. Meghann Myers, "You Can Claim Damages if the Fort Bragg Power Outage Ruined Your Stuff," *Army Times*, 2 May 2019, https://www.armytimes.com/news/your-army/2019/05/02/you-can-claim-damages-if-the-fort-bragg-power-outage-ruined-your-stuff/.

Federal Guidance on EMS Resilience and Preparedness

The Department of Homeland Security's (DHS) 5 February 2019 release *Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment* is the most recent authoritative document dealing with the resilience and preparedness specifically associated with EMS threats. It describes four EMP protection levels for infrastructure and equipment that underscore the importance of food, water, and critical supplies and spares to assure the human sustainment and health.

While the DHS resource is informative about infrastructure protection and associated costs of EMS threat mitigation, it does not provide recommendations or cost estimates associated with the storage of food, water, or critical supplies that may be required to support military personnel or their families. Nevertheless, DHS's focus on a 30-day period of preparedness corresponds to the EDTF 1.0 consensus view that 30 days of food and water is a reasonable and realistic target to ensure the families of military personnel are sustained during a prolonged power outage. However, it was noted during Federal Emergency Management Agency's (FEMA) National Preparedness Symposium in 2018 that "current [FEMA] planning does not include any contingencies for very long or extremely widespread power outages."[2]

Furthermore, the National Infrastructure Advisory Council's (NIAC) December 2018 report, titled "Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation," contained a recommendation to "develop guidance and provide resources for states, territories, cities, and localities to design community enclaves—areas that colocate critical services and resources to sustain surrounding populaces, maintain health and safety, and allow residents to shelter in place." A subtask recommended the following: "Identify the critical lifeline functions that communities need (even in a limited capacity or degraded state)—such as communications, electricity, fuel, limited financial services, food, water and wastewater, and medical facilities—and for how long (i.e., 30–45 days)."[3]

In its specific analysis on the topic of individual preparedness, the NIAC report provides examples of state government initiatives for community

2. Lonnie Lawson, Brenda Vossler, and William Byrd, "Private and Public Cyber Security Issues in Rural America" (PowerPoint presentation, National Preparedness Symposium, Anniston, AL, 24 May 2018), https://training.fema.gov/nationalpreparednesssymposium/_assets/2018/2018%20private%20&%20public%20cyber%20security%20issues%20in%20rural%20america.pptx.

3. The President's National Infrastructure Advisory Council (NIAC), *Surviving a Catastrophic Power Outage*, December 2018, 11, www.dhs.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power %20Outage%20Study_508%20FINAL.pdf.

preparedness and references three states (Washington, Oregon, and Hawaii) that encourage citizens to maintain a 14-day supply of essentials.[4]

Consequences to Government and Society from an EMS Attack

EDTF is assessing existing data pertaining to EMS threats and the effects such threats could have on government and society. Since adversaries exploiting EMS would likely focus attack(s) to cause the most widespread and long-term damage, EDTF experts specifically explored the human dimension of life without electricity, examined existing government-sponsored reports on this topic, and invited the participation of subject matter experts in this area.

According to research conducted by the US Congress's EMP Commission, there is an assumption that an EMP-induced blackout could cause a long-term nationwide grid collapse and the loss of up to 90 percent of the population through starvation, disease, and societal collapse. While this mathematical assessment is based on population metrics, it is not without debate. However, the basis of this calculation is not unreasonable from a logistics standpoint. America is no longer the benefactor of widespread off-grid farming or nonelectric farming equipment. In 1820, farmers made up approximately 72 percent of the US population.[5] Today, only about 2 percent of the US population works in agriculture.[6] The ability to continue providing food to approximately 165 million people with a 70 percentage point drop in farming is enabled through large-scale, computer-controlled, just-in-time farming operations. Such operations rely on computers, the internet, access to large-scale commercial trucking logistics, distribution algorithms, open lines of communication between the various stakeholders, and access to fuel—all of which rely on the nation's interconnected commercial power grid.

One of the experts invited to participate in this discussion was Jonathan Hollerman, a former USAF SERE (survival, evasion, resistance, and escape) instructor. He was asked to provide his perspective on this topic of how a long-term blackout would affect the American populace and, specifically, the US military.

Hollerman's informed analysis focused on three overarching factors that he suggests are absent in most government-sponsored plans: (1) human desper-

4. NIAC, *Surviving*, 13.

5. Associated Press, "Farm Population Lowest since 1850s," *New York Times*, 20 July 1988, https://www.nytimes.com/1988/07/20/us/farm-population-lowest-since-1850-s.html.

6. "Fast Facts about Agriculture," American Farm Bureau Federation, accessed 22 July 2019, https://www.fb.org/newsroom/fast-facts.

ation, (2) starvation, and (3) living without rule of law (WROL).[7] Hollerman's work is his own professional assessment/opinion and not reflective of an official position of EDTF or its fellows; however, it does evoke an understanding of the potentially troubling consequences of a long-term, nationwide blackout and emphasizes the reality that America must secure its critical national infrastructure against EMS threats.

A Way Forward

EDTF 2.0 began the preliminary process of generating strategies that could be applied to enhance EMS resilience and preparedness for government and society. Strategies ranged from encouraging citizens to stock larger quantities of food, water, and basic supplies to encouraging gas stations to maintain backup generators to pump fuel to the EMS hardening of municipal water and wastewater systems.

EDTF will continue to focus on generating sensible recommendations in the area of emergency management, consequence management, continuity of operations, and food and water resilience with three goals in mind:

1. Identifying and expanding the array of technological assets and physical measures that can be applied to infrastructure and equipment to increase EMS resilience.
2. Identifying the best way to prioritize these measures to increase survivability and resilience of society and government personnel and organizations.
3. Identifying methods of incentivizing governmental organizations as well as the owners and operators of life-sustaining infrastructures to make their assets resilient to EMS threats and their personnel (and families) more capable of maintaining health and welfare in an EMS-degraded environment.

7. Jonathan Hollerman, *Grid Down: Death of a Nation* (self-pub., 2019), https://www.griddownconsulting.com/grid-down-report.

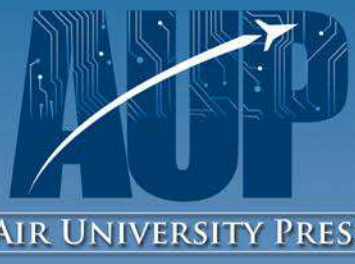
Abbreviations

Abbreviation or acronym	Spelled out form of term or organization
ACC	Air Combat Command
AER	Atmosphere and Environmental Research
AEMA	Alabama Emergency Management Agency
AETC	Air Education and Training Command
AFIT	Air Force Institute of Technology
AFLCMC	Air Force Life Cycle Management Center
AFRL	Air Force Research Lab
AFSPC	Air Force Space Command
AFWIC	Air Force War-fighting Integration Capability
AGC	automatic generation control
AI	artificial intelligence
APNSA	Assistant to the President for National Security Affairs
ARRL	American Radio and Relay League
ATSO	ability to survive and operate
AU	Air University
BDBE	beyond-design-basis event
BDBEE	beyond-design-basis external event
BIL	basic impulse level
BMT	basic military training
BST	Black Start team
CCMG	Continuity Communications Managers Group
CISA	Cybersecurity and Infrastructure Security Agency
CME	coronal mass ejection
COA	course of action
COE	center of excellence
CONUS	continental United States
COOP	continuity of operations
CSAF	chief of staff, United States Air Force
CVC	combat vehicle crewman (helmet)
DBT	design basis threat

DE	directed energy
DEVOP	developers and operations
DHS	Department of Homeland Security
DIB	Defense Innovation Board
DIME	diplomatic, informational, military, and economic
DOD	Department of Defense
DOE	Department of Energy
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
DPR	digital protective relay
DSB	Defense Science Board
ECCT	Enterprise Capability Collaboration Team
ECD	Emergency Communications Division
EDG	emergency diesel generator
EDTF	Electromagnetic Defense Task Force
EHV	extra high voltage
EM	electromagnetic
EMBM	electromagnetic battle management
EME	electromagnetic environment
EMI	electromagnetic interference
EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EPRI	Electric Power Research Institute
EW	electronic warfare
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FVEY	Five Eyes
GDP	gross domestic product
GIC	geomagnetically induced current
GMD	geomagnetic disturbance

HAF	Headquarters Air Force
HEMP	high-altitude electromagnetic pulse
HF	high frequency
HPEM	high-powered electronics and microwaves
IADS	integrated air defense system
IEC	International Electrotechnical Commission
IEMI	Intentional Electromagnetic Interference
IOS	internetwork operating system or internet operating system
IoT	internet of things
ISR	intelligence, surveillance, and reconnaissance
JEMSO	Joint Electromagnetic Spectrum Operations
L2	lessons learned
LVC	live, virtual, and constructive
M&S	modeling and simulation
MAJCOM	major command
MARS	Military Auxiliary Radio System
MDC2	multi-domain command and control
NAOC	National Airborne Operations Center
NC3	nuclear command, control, and communications
NCC	National Coordinating Center for Communications
NDS	National Defense Strategy
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NMCA	National Military Command Authority
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSS	National Security Strategy
OPFOR	opposing force
OSD	Office of the Secretary of Defense
OT/DT	operational testing/developmental testing
OTS	officer training school
PACE	primary, alternate, contingency, emergency
PNT	positioning, navigation, and timing

POTUS	president of the United States
PTN	Pilot Training Next
R&D	research and development
RF	radio frequency
ROMO	range of military operations
SBO	station blackout
SCADA	supervisory control and data acquisition
SCADAS	supervisory control and data acquisition systems
SERE	survival, evasion, resistance, and escape
SFP	spent fuel pool
SPECTRE	Specialized Electronic Combat and Reprogramming Environment
SSA	Sector-Specific Agency
STEM	science, technology, engineering, and mathematics
T&E	test and evaluation
TTX	tabletop exercise
TVA	Tennessee Valley Authority
UARC	university affiliated research center
UAV	unmanned aerial vehicle
UHF	ultrahigh frequency
UPS	uninterrupted power supply
USG	United States government
USNORTHCOM	US Northern Command
USSTRATCOM	US Strategic Command
VHF	very high frequency
WROL	without rule of law



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

ISSN 2575-6737
LP-4