RAND CORPORATION

Research Report

ABBIE TINGSTAD, PADMAJA VEDULA, ROBERT A. GUFFEY, KARISHMA R. MEHTA, LANCE MENTHE, JONATHAN ROBERTS

Outsmarting Agile Adversaries in the Electromagnetic Spectrum

Executive Summary

For more information on this publication, visit **www.rand.org/t/RRA981-2**.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-1058-0

Cover: Digital head and code: monsitj/Fotolia; pilot: U.S. Air Force photo.

Cover design: Rick Penn-Kraus

About This Report

This report summarizes research commissioned by the Plans, Program and Requirements Directorate, Air Combat Command (ACC A5/8/9) and fully documented in the report *Outsmarting Adaptive Adversaries in the Electromagnetic Spectrum*.[1] The research was conducted within the Force Modernization and Employment Program of RAND Project AIR FORCE as part of a fiscal year 2021 project, "Improving Speed and Security in Electronic Warfare Integrated Reprogramming."

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Resource Management; and Workforce, Development, and Health. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website:
www.rand.org/paf/

This report documents work originally shared with the DAF on September 24, 2021. The draft report, issued on September 30, 2021, was reviewed by formal peer reviewers and DAF subject-matter experts.

[1] Padmaja Vedula, Abbie Tingstad, Lance Menthe, Karishma R. Mehta, Jonathan Roberts, Robert A. Guffey, Natalie W. Crawford, Brad A. Bemish, Richard Payne, and Erik Schuh, *Outsmarting Agile Adversaries in the Electromagnetic Spectrum*, Santa Monica, Calif.: RAND Corporation, RR-A981-1, 2023.

Contents

Figures and Tables

Figures

Tables

Chapter 1. Introduction

Gaining access to and superiority in the electromagnetic spectrum (EMS) is becoming increasingly important for securing military advantage. This importance was first recognized in World War II by Britain, which leveraged the knowledge of radio waves to conduct information warfare (particularly in the areas of signals intelligence [SIGINT] gathering and electronic jamming of radio waves) in the Allied effort to defeat Germany. Since then, military uses of the EMS, typically focused in the radio frequency (RF) part of the spectrum,[2] have expanded in scope and complexity. For example, aircraft depend on the EMS (particularly RF) for sensing, navigating, and communicating. Aircraft crews employ RF to detect and communicate about potential threats. At the same time, adversaries sense activity in the EMS to track and target airborne (and other) platforms, including through the use of RF jamming to disrupt sensing and communications.

Now, military uses of the EMS are undergoing another renaissance; past capabilities will no longer be relevant in a world where control over information and the means to communicate it dominate historical weapons and concepts of employment. Adversaries and competitors are seeking to offset the United States' historical ability to operate within and through the EMS by making their systems more complex and adaptable—and, therefore, more difficult for U.S. platforms to detect, identify, evade, and counter. For these reasons, the U.S. Department of Defense (DoD) Spectrum Superiority Strategy articulates the need to develop "an electromagnetic spectrum . . . enterprise that is fully integrated, operationally focused, and designed for great power competition," with future EMS capabilities that must be able to "perform, operate, and adapt" to an increasingly complex threatscape.[3]

Within the U.S. Air Force (USAF), necessary adaptations to changes in the EMS have traditionally been accomplished through a process termed *electronic warfare integrated reprogramming* (EWIR). The USAF's EWIR enterprise is responsible for the fully integrated operations of compiling intelligence on adversary threats that emit in the EMS (in particular, radars and jammers) and configuring[4] electronic warfare (EW) equipment to enable aircraft or other USAF resources to react to and/or respond to adverse changes in the EMS environment. Affected aircraft include fighters; bombers; intelligence, surveillance, and reconnaissance (ISR)

[2] Note that the EMS covers a range, from infrared to very low frequency. The portion of the EMS of most concern for the USAF and militaries more generally is the radio frequencies used by radars and radios, although there is increasing use of higher-frequency light detection and ranging equipment and laser-based digital communications links.

[3] DoD, *Electromagnetic Spectrum Superiority Strategy*, October 2020.

[4] This configuration is generally done digitally and may include new uploads of data or code. Therefore, it is termed *reprogramming*. However, we note that it may also include changes to switches, dials, and other manually manipulated controls of the EW equipment.

platforms; tankers; and transporters. EWIR-related reconfigurations can take three forms: (1) changes to an aircraft's onboard computer code (i.e., its operational flight program [OFP]); (2) changes to an aircraft's onboard data files (i.e., a mission data file [MDF] containing expected threat characteristics linked to predetermined responses);[5] and (3) hardware adjustments[6] to support sensing and reaction to threats. Both OFP and MDF changes are considered software per DoD software development standards.[7] In the current EWIR process,[8] MDFs often contain stopgap solutions to deficiencies in capabilities that would require more time-intensive OFP updates—at least until the threat environment changes to such an extent that these stopgaps are no longer adequate or a routine OFP update has a fix for the identified deficiencies.

Historically, threats that manifest in the EMS did not change very quickly, and the EWIR enterprise could take months to execute updates without negative operational impacts. Now, U.S. adversaries are building more-advanced, complex, and diverse EW assets that are difficult to identify and track using historical methods and require faster updates than the EWIR enterprise was originally designed for. To remain competitive, USAF systems that operate in the EMS must be capable of rapidly (i.e., within seconds to minutes) evaluating the threat environment, including the emergence of new threats and the detection of adversary attempts to deceive or defeat U.S. EW detection and identification software. Additionally, USAF systems must be able to synthesize that evaluation into an interoperable tactical picture that is sharable across the battlegroup to formulate a coordinated response. To rapidly build and deploy these capabilities, the USAF would require more-agile software development methods, faster hardware upgrades, and autonomous threat intelligence processing than it has now.

---

[5] An MDF contains data to define a parameterized model that expresses the range of known or anticipated threat characteristics and responses. The collection of MDFs is often referred to as the "threat library" or a "digital encyclopedia" of the waveforms and frequencies used by an adversary's radar and communication systems. It may also include those waveforms and frequencies used by friendly systems to more fully characterize the battlespace. An MDF cannot express threat characteristics or responses that are outside of the domain for which it (and the code that uses it) was designed. While MDFs are designed to be more readily deployable into operations than flight program changes, their content impacts the aircraft's behavior in nontrivial ways that must be fully validated and verified prior to their being deployed to operational aircraft.

[6] Types of adjustments include, for example, changing sensors or adding processing capacity.

[7] While DoD software development has been governed by various military and Institute of Electrical and Electronics Engineers standards over the last 40 years, depending on acquisition philosophy, the definition of software as being inclusive of both code (instructions) and data (whether hardcoded or in data files) has been constant across that range of standards.

[8] When originally conceived in the mid-1960s, MDF changes offered a quicker path to deployment across the force given the rudimentary state of software delivery and deployment practices, which, at that time, relied on physically burning software into read-only memories. Over the years, as software delivery and deployment practices have changed to emphasize rapid deployment of working code, this distinction has become less true. MDF, in today's use of the term, has come to specifically refer to the threat library produced for a mission by the EWIR process. For more on the history of the development of electronic countermeasures for aircraft self-defense, see Robert L. Simmen and Bjorn M. Fjallstam, *Threat Warning for Tactical Aircraft: A Technical History of the Evolution from Analog to Digital Systems*, Xlibris, 2006.

The USAF is actively exploring how best to achieve adaptive and cutting-edge EMS capabilities.[9] To assist in this effort, RAND Project AIR FORCE (PAF) explored how adversary capabilities in the EMS are evolving, how fast current EW-related responses need to be to keep up, what obstacles exist within the current intel-to-reprogramming process, and what advanced technologies are needed to achieve necessary improvements. Primary data sources for the research included interviews, documents, and live observation of USAF concept rehearsals,[10] which fed three intermediate analyses: process documentation and analysis, technology mapping (which linked objectives to specific types of investments over time, including using doctrine, organization, training, materiel, leadership, personnel, facilities, and policies [DOTMLPF-P]), and illustrative vignette development. Finally, we derived recommendations based on our analysis of problems with the current process (establishing needs) and of four structured case studies of interrelated technologies (highlighting solutions). PAF's work centers on what is currently known as EWIR but is scoped to cover the broader range of issues related to the role of software in enabling EMS operations. This research, commissioned by the Plans, Program and Requirements Directorate, Air Combat Command (ACC A5/8/9), is fully documented in the report *Outsmarting Agile Adversaries in the Electromagnetic Spectrum*.[11] This summary presents major findings from that research.

[9] Department of the Air Force (DAF), *Spectrum Integration Group Conference Report*, October 2020.

[10] For example, these include practice drills conducted by an air component.

[11] Padmaja Vedula, Abbie Tingstad, Lance Menthe, Karishma R. Mehta, Jonathan Roberts, Robert A. Guffey, Natalie W. Crawford, Brad A. Bemish, Richard Payne, and Erik Schuh, *Outsmarting Agile Adversaries in the Electromagnetic Spectrum*, Santa Monica, Calif.: RAND Corporation, RR-A981-1, 2023.

Chapter 2. How Are Adversary EMS Capabilities Evolving?

Some historical context is helpful to appreciate the challenge that the USAF now faces.[12] In the early days of radar, there were only a few systems with simple, well-known, and largely unchanging waveforms that could be characterized by only a few parameters. Thus, it was relatively easy to collect electronic intelligence (ELINT) about an adversary's radar systems and for intelligence squadrons to develop and periodically update MDFs (and, less frequently, OFPs), so that sensor systems could identify enemy radars. The EWIR process of determining and analyzing the impact of threats and making the necessary configuration updates has become far more challenging as adversary radars have become more technically sophisticated, the number and diversity of systems has grown, and the pace of change has accelerated.

Adversary radars and jammers are increasingly software-defined and adaptive, designed to evade accurate detection using straightforward means. Waveforms (i.e., the internal structures of signals transmitted in the EMS) have become more complex, and there are now tens of thousands of systems to keep track of. Dozens of parameters are needed to reliably distinguish one emitter from another. Radars that use (or deliberately mimic) modern digital modulation techniques, such as frequency- and phase-shift keying, can be especially difficult to distinguish from communications systems through conventional means. Furthermore, adversaries now utilize radars with software-defined waveforms that can switch rapidly between waveforms in a matter of seconds or can even generate new modes, thus confounding the entire approach of using preset lookup tables to identify those systems. Low-probability-of-intercept (LPI) radars, such as noise-like waveforms, are difficult to detect—let alone identify—because of their irregular[13] pulse patterns.

Many threats are also mobile, sometimes highly so, and thus relying on a static threat map in lieu of training software to recognize threats wherever and whenever they might occur is not a winning proposition. In addition, capable adversaries have recently begun to employ tactics in air defense that further complicate the interpretation of sensor data into threat information that can be acted on by U.S. weapon systems.

EMS operations are a race between ever-evolving threat capabilities and ever-improving methods of identifying and countering those threats. Given the above advances in adversary capability, USAF EWIR capability must become both faster and smarter to maintain U.S. advantage in EMS operations.

[12] For additional detail, see Chapter Two of Vedula et al., 2023.

[13] Having no fixed frequency and repetition rate, these waveforms do not lend themselves to parametric analysis and can only be identified as radar systems by how they are used and by correlating signals from multiple receivers.

Chapter 3. How Fast Does the EWIR Process Need to Be?

The EWIR process can be divided into eight sections that were defined on the basis of expert interviews, doctrine, and PAF team expertise:[14]

- collection (historically the start of the intelligence cycle)
- processing (automated data transformation into a format amenable to further signals analysis, as well as automated identification of known signals)
- analysis (human-machine teaming to sift through unidentified and misidentified data)
- dissemination and archiving (preparing data for storage in formats and locations accessible to others)
- intelligence data pull and analysis (subsequent data discovery, evaluation to construct an understanding of signal or emitter characteristics, and storage)
- software development or update (pulling highly analyzed data to abstract a change in the EMS environment into software)
- development testing/operational testing and evaluation (modeling the interaction between radar warning receiver or other EW equipment software and the emitter[s] in question and testing software changes)
- use (uploading new software changes to onboard hardware).

PAF interviews with subject-matter experts, examination of current processes, and analysis of operational vignettes suggest that future EWIR capabilities will need to be able to process information, characterize threats, and generate countermeasures for the most demanding threats autonomously in real time.[15] Ultimately, the need for speed in EWIR depends on the type of intelligence task being carried out and the sophistication of the threat environment, given that not all threats are sophisticated or operationally urgent (i.e., are not being used in an active conflict). This means that there can be some prioritization in how changes are made across the EWIR enterprise, even as a more autonomous real-time capability (i.e., leveraging machine learning [ML]) is being pursued.

Figure 3.1 shows a range of intelligence tasks, from foundational intelligence-gathering to wartime tactical intelligence, and threat environments, from less-capable adversaries to near-peer competitors. The boxes show the types of EW threats likely to be encountered in each situation and how quickly the EWIR process would need to react through software updates (currently by modifying MDFs or an OFP[16]) to keep ahead of changing threat conditions.

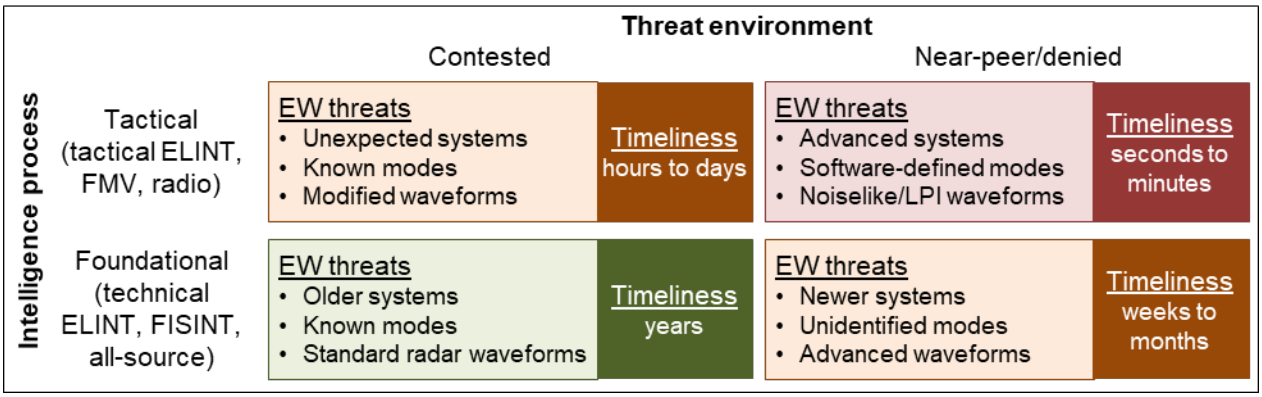
[14] For additional discussion of the current EWIR process, see Chapter Two of Vedula et al., 2023.

[15] See Chapter Two of the main project report (Vedula et al., 2023) for discussion of how fast future EWIR capabilities will need to be.

[16] Recall that the current construct favors MDF updates as a stopgap measure until the threat changes are so unanticipated that a code change is unavoidable.

Foundational intelligence activities are conducted to prepare for potential future conflicts and to survey a large range of threat information. These activities take place over comparatively long timescales. EWIR activities that take one or more years to incorporate changes discovered through foundational intelligence could be sufficient for EW threats that change more slowly, are less complex, and/or are not necessarily associated with priorities laid out in the National Defense Strategy and other strategic documents (lower-left box). For foundational intelligence on priority threats, including those that are quickly upgraded to continuously create a more challenging operating environment for the USAF (lower-right box), EWIR would need to generate the necessary configuration changes within weeks to months.

Figure 3.1. EWIR Speed Needed to Keep Pace with Threats



SOURCES: Subject-matter expert interviews, doctrine (Curtis E. LeMay Center for Doctrine Development and Education, *Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations*, Maxwell Air Force Base, Ala., 2015; DAF, *Air Force Instruction 10-703: Electronic Warfare Integrated Programming*, April 3, 2019; and DoD, *Department of Defense Directive 3222.04: Electronic Warfare (EW) Policy*, August 31, 2018), and vignettes.
NOTES: Colors conceptually indicate the acceptability of current EWIR timelines, with green signifying that the current general timeline of years might reasonably fulfill needs, whereas orange and red demonstrate decreasing acceptability of long timelines to keep up with the threat environment and associated intelligence process. FISINT = foreign instrumentation signature intelligence; FMV = full-motion video.

Tactical intelligence is more demanding because it is used to find, fix, and track threats in real time or on the fly. Even in more-permissive threat environments (upper-left box), updates must be made within hours or days to be relevant to warfighters. For tactical tracking of rapidly evolving threats, such as advanced integrated air defense systems and adaptive radars with digitally programmable waveforms (upper-right box), the USAF would need to update information in real time or in a few minutes (at most) to keep pace with a very agile adversary.

Chapter 4. How Does the Current EWIR Enterprise Measure Up?

Many factors determine how quickly the EWIR enterprise can make the necessary updates. Subject-matter experts indicate that in the best case, a nonroutine MDF update for a single known threat can currently take weeks or months. A typical EWIR-related OFP update can take nearly two years. Times vary based on the type of platform (newer platforms use more data and can thus take longer to update), update urgency, availability of resources, and other factors. For example, schedule-intensive activities include extensive modeling and simulation of the threat (needed for both MDF and OFP) and verification of the security hardening and safety or airworthiness certification of the software (for OFP changes). These activities are pacing items for the developmental testing and evaluation and operational testing and evaluation required before changes can be deployed into operations.

The USAF is reducing these times by working to implement continuous software delivery and deployment pipelines, but this practice has not yet become commonplace.[17] Additionally, because OFP changes typically have longer fielding timelines than MDF changes, the USAF sometimes employs workarounds to, or as, MDF updates for issues that would be better addressed through code changes. In theory, this could lead to compromises in performance and the USAF's ability to counter adversary weapons and tactics. The current EWIR process is unable to support faster reprogramming updates, and changes to the overall process are needed to address these bottlenecks.[18]

Several additional obstacles slow the current EWIR process and inhibit it from keeping up with rapidly adapting EW threats:

- There is a **proliferation of manual steps** in which products wait for input or resources. These steps make the end-to-end process transaction-heavy and not agile. Because there are so many bottlenecks, *automating any one step in this process will have only a limited impact on overall speed and accuracy*.
- **Long security hardening and safety certification timelines cannot be avoided** with current software architectures and deployment processes and result in significant delays in moving software updates forward in the process. All software and hardware updates require a platform to undergo verifications for software security hardening, safety and airworthiness, and end-to-end regression testing. It can take anywhere from several months to nearly two years to complete these tests on the platform, because of limitations in human and computing resources. A software fix or an update

[17] Modern software development processes that automate security hardening and verification processes are a goal of the Air Force "One" initiatives (USAF, Office of the Chief Software Officer, homepage, undated). Commercial software companies that employ similar practices are able to deliver code within hours of when a developer checks in the necessary code modifications.

[18] Chapter Two of the main project report (Vedula et al., 2023) discusses the current EWIR process, timelines, and obstacles to faster updates.

for a single existing or new capability necessitates all the verifications and testing schedules mentioned above.

- **Lack of sufficient resources and inefficient use of available resources** further exacerbates how long it takes to complete manual steps. For example, it is inefficient for intelligence experts to proactively scan available databases to learn of changes in the threats, rather than to receive push notifications. The limited availability of testing equipment, including computers, causes both OFP and MDF updates to sit in a queue. Regional maintainers do get notifications of MDF updates for their particular platforms, but they must review the notifications to ensure that an update is relevant for their area and work out a strategy to take platforms offline to deploy the updates without disrupting other demands (e.g., training).
- **Limited communication of requirements and context for updates** appears to slow down the EWIR process and could impact software update efficiency and efficacy (in the sense that slow updates could be behind the pace of threat changes). Some units communicate together better than others. To communicate new needs, flying units must first be tipped off about a change in threat characteristics (often based on intelligence data to which they do not have access but instead gather from people they know in the intelligence community) and then make requests up the chain of command. Requests are then coordinated among multiple parties, such as the relevant program office and ACC.
- It is **difficult to create data pipelines** from the majority of platforms that carry EMS-related sensing equipment to relevant SIGINT databases. The availability of ISR platforms to collect characterizing data is limited. When available, many ISR platforms lack features that enable operation in close proximity to emitters during conflict. These factors prohibit ISR platforms from gathering data that accurately reflect how adversary capabilities are used in wartime.

Obstacles such as these suggest that the current EWIR process was not designed to operate at the tempo required for future threats or to cope with highly adaptive adversaries that can change the parameters of their systems in real time. Speeding up the EWIR process is therefore a priority. However, focusing on the *speed* of the existing process is not enough; more-fundamental changes are needed to *remove* the time constraints imposed by the large number of sequential transactions, as well as to improve *how* data are interpreted in order to stay competitive in the evolving threat environment.[19] As discussed in the next section, transforming the EWIR process in this way will require fundamental changes, and not simply automating steps in the current process.

[19] Although we do not explicitly address security here, this is also a critical issue that will require changes to how the current software update process is architected to remain ahead of capable adversaries.

Chapter 5. What Should Be the Vision for Future EWIR?

Over the years, the USAF has taken steps to fix specific problems within the EWIR enterprise. Some component organizations, for example, have experimented with automation and other forms of innovation for years. This is how the Specialized Electromagnetic Combat Tools and Reprogramming Environment (SPECTRE) tool suite came into being.[20] Other services are also looking at the problem; for example, the Army is working to develop the Electronic Warfare Planning and Management Tool to support coordination on EW in a Joint environment.[21] It is generally believed that increased automation can bring further improvements, and we recommend that these efforts be continued in the near term. Automation of existing processes can improve timeliness for some intelligence tasks (such as those in the lower-right and upper-left boxes of Figure 3.1) in the near term, and the USAF should seize opportunities to make those improvements.

However, we emphasize the limited utility of automating existing processes. The urgent and long-term problem of being competitive and capable in EMS operations requires new processes. There is a limit to how much faster the USAF can be as long as the bulk of the EWIR enterprise takes place *off* the aircraft and *after* the mission. A more far-reaching goal would be to have a significant portion of the current EWIR process take place *on* the aircraft *in real time*, first by using algorithms that execute predefined rules to identify adversary capabilities (*adaptive EW*, described below), and later by using ML algorithms on the aircraft to figure out novel or rapidly changing adversary capabilities without predefined rules (*cognitive EW*, described below).

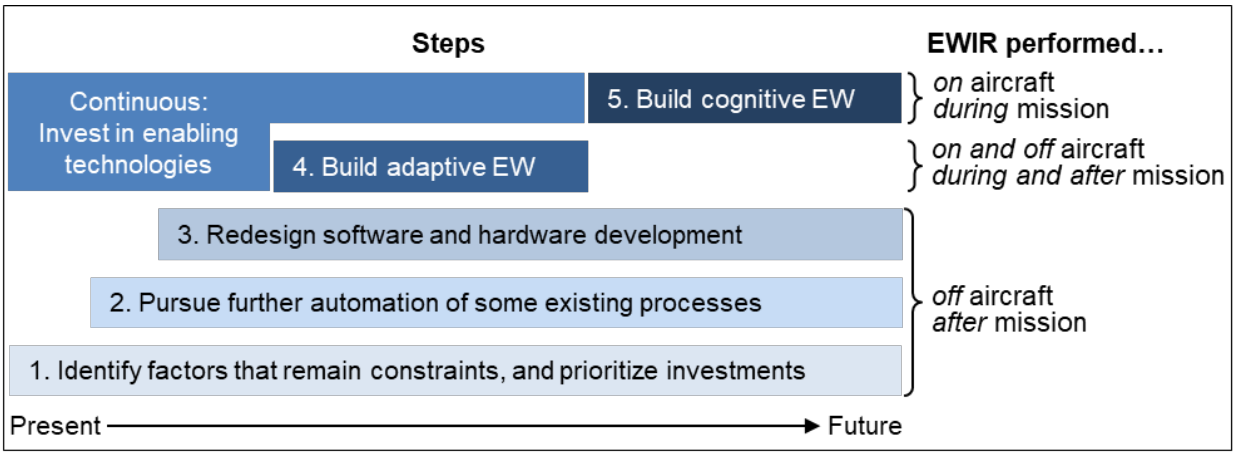
To move toward the vision of real-time, autonomous reprogramming, however, several steps are required to address problems in the near term while investing in the foundational enhancements for more far-reaching changes in the long term. This vision and its component steps are illustrated in Figure 5.1 and described below.[22]

[20] USAF, *Air Force Doctrine Publication (AFDP) 3-51: Electromagnetic Warfare and Electromagnetic Spectrum Operations*, July 30, 2019; Curtis E. LeMay Center for Doctrine Development and Education, *AFDP 3-51: Electromagnetic Spectrum Support Activities*, Maxwell Air Force Base, Ala., July 30, 2019.

[21] Mark Pomerleau, "The Army May Have the Electronic Warfare Tool the Pentagon Needs," *C4ISRNet*, June 15, 2020.

[22] These steps are described in greater detail in Chapter Three of Vedula et al., 2023.

Figure 5.1. Vision for Improving USAF EWIR Enterprise



1. Identify Factors That Could Remain Constraints and Prioritize Investments Accordingly

In the near term, not all slower processes need to be prioritized for improvement. One important example is the necessary months or years it takes to build foundational intelligence: Capturing the right data sometimes means being in the right place, at the right time, with the right collector. As has been commonly observed, "the enemy has a vote." Naturally, data-driven and machine-aided collection requirements and strategies can help in this regard. More-sophisticated intelligence tradecraft or approaches can also help. But there is a limit to how quickly reliable foundational intelligence can be collected. Given this constraint, limited investment resources are better allocated elsewhere.

Another example is the necessary time it takes for new avionics, including software, to be deployed onto a platform. This will likely remain at least a somewhat manual process, with the necessary safety requirements encountered by all physical maintenance procedures, such as the need to remove any equipment that could initiate combustion. Once basic networking infrastructure is installed, however, subsequent software deliveries can be installed over the network. Even then, there will be necessary operational precautions that must be taken. Careful scheduling of software deployment onto the platforms to avoid adverse operational impacts will always be needed.

2. Pursue Further Limited Automation of Some Existing Processes

In the near term, the USAF should continue to pursue automation of some steps in the existing EWIR processes. Such improvements will be of benefit in certain situations, such as when threats are not quickly changing or when making preparation for wartime during peacetime.

One such near-term example is to automate the process by which data collected at "the edge" of combat (i.e., by the aircraft during the mission) are used to inform MDF updates. Automated machine-to-machine transfer of potential threat information collected during flight immediately after landing, paired with local processing and storage capability, may allow for on-site model-building capability. One effort already under way is referred to as "crowd-sourcing data," which adds hardware both on the combat platforms and on the ground to enable rapid data capture and dissemination.[23] In addition to having a near-term benefit, the ability to rapidly get data into the pipeline would contribute to the vision for cognitive EW described below.

Near-term automation that is less relevant to fully transformed future EWIR may still be important to today's EWIR enterprise. For example, the SPECTRE tool for making intelligence data visible and creating models to support software updates continues to evolve and could provide analysts greater support as they navigate the current EWIR process. Another example is implementing a "pushed" distribution system that automatically routes the right updates to the right users.

Note, however, that these near-term automation solutions have a limited benefit in terms of reducing the total time it takes from detection of a new threat to deployment of aircraft with the onboard capability to counter that threat. According to several experts familiar with the time it typically takes to conduct various steps of the current EWIR process, basic automation within the constraints of the current process might improve speed by up to one order of magnitude. *At best, further automation of the current process could reduce the time required for a part of the process that currently takes months down to days*.

3. Redesign Software and Hardware Development Processes to Increase the Speed of Fielding EWIR Capability and to Develop and Sustain Future Autonomous Capabilities

The remaining steps of the vision in Figure 5.1 are concerned with more-transformational changes to the EWIR process. One of the major bottlenecks for fielding new or upgraded EW capability is the long duration required for security hardening, end-to-end regression testing, and safety and airworthiness certification of the software and hardware that compose an aircraft's avionics. The rigor incorporated within each of these processes is necessary for determining the safety, stability, and performance of the platform with any new upgrade of software or hardware. Therefore, the processes themselves may not see significant changes, although new avionics acquisition programs that often levy requirements on the speed of software updates or the

[23] Air Force Technology, "USAF Selects Intelligent Waves for Flight Data Collection Support," webpage, October 10, 2019.

addition of what is termed a *test harness*[24] may reduce the overall process timelines. Part of the issue is that the avionics design is proprietary and oftentimes was not designed to enable rapid update and testing. Additionally, modular software architectures of the current platforms still do not support deployment time modularity, or the packaging of the deployed service, in such a way that upgrades to a single service could be tested and fielded rapidly.[25] What is required is an immediate threefold approach to increase the agility of EW-related avionics development and deployment:

1. Redesign OFP software to decouple flight control and EW software components and dependencies from one another to the extent possible, identifying elements that may be most subject to future change. A decoupled design, or simply an understanding of the coupling inherent in the design of software, will facilitate use of newer paradigms for integrating, delivering, and deploying software into operations. These paradigms are specifically formulated with the goal of minimizing the scope of end-to-end regression testing, shortening security hardening, and automating many of the steps required for flight safety and information security certification of the aircraft.
2. While decoupling is a key element of producing reusable and interoperable software, open interfaces at the coupling points and at external data exchange points will allow the USAF to (a) incrementally develop future capabilities to counter evolving threats and (b) enable processing and sharing of information in a complex system-of-systems environment, where information regarding threat identification and the system's use of the EMS must be consistently and immediately distributed among all systems involved.
3. Due to the rapidly changing EW threat environment, platform avionics not only have to support the faster fielding of EWIR but also should be designed to support future algorithms with substantial computational resource needs. Additionally, EW software design should have a deployment architecture, including packaging and delivery, for these algorithms. One way to minimize the total compute resources required is to provide for autoscaling[26] and sharing of resources using cloud-based computing and networking techniques (i.e., enabling efficiency on the fly). Investments in future programmable and high-performance hardware with significantly reduced size, weight, and power (SWaP) is another important priority, as it will improve the speed of today's EWIR and provide critical infrastructure for adaptive and, ultimately, cognitive capabilities in the future.

4. Build an Adaptive EW Capability

More far-reaching capability enhancements will be needed to keep the EWIR enterprise competitive. This is because advances in threat capability, complexity, and sheer numbers make it impossible to remain competitive in the EMS "arms race" simply by speeding up the EWIR

[24] A test harness contains interfaces that are needed in test but not in operations. For example, test interfaces allow testers to inject specific fault signatures or to view intermediate results of algorithms. Using these test interfaces allows for more-rapid and direct verifications but is not a substitute for true end-to-end testing.

[25] See Chapter Six of Vedula et al., 2023, for more discussion of deployment time modularity.

[26] *Autoscaling* refers to dynamically allocating computing resources within a set of servers.

process in its current form. To support mission analysis and requirements, future EWIR must be deployed as close to the edge, where data is created or captured, as possible. Additionally, the EWIR enterprise will need to field products that autonomously detect, identify, and respond to both (1) previously unknown or unidentified threats and (2) known threats that behave in an agile, adaptive way, all within a congested electromagnetic environment in which friendly interference can be as detrimental as adversary action.

The first step to building an autonomous reprogramming capability is to create an adaptive EW capability that uses on-aircraft processing to identify changes to adversary systems based on preprogrammed rules. Instead of using a single lookup table, adaptive EW systems would use complex decision trees that anticipate possible variations in threat behavior and allow for extrapolation. In this construct, the software recognizes small variations in systems, or systems in unexpected locations; interprets those variations using predefined rules; and provides information regarding possible threats to the pilot or other decisionmakers.

The 350th Spectrum Warfare Wing (SWW) and partners are already taking some important steps in this direction. For example, capability and interoperability can be improved in the near term by creating a layer of lightweight, service-specific applications (apps), developed and deployed by the USAF, that interface with existing OFPs.[27] This can be done even as the USAF pushes toward more-encompassing changes required to execute more-advanced adaptive—and ultimately cognitive—EW concepts.

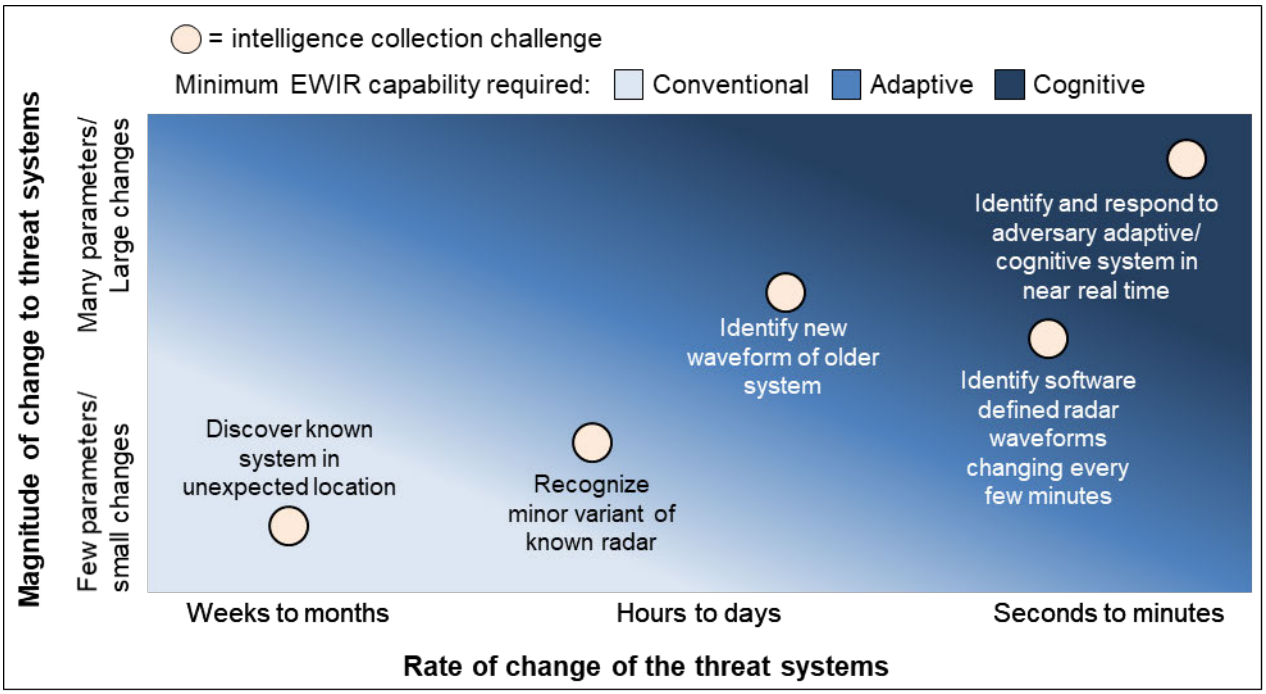
The key advantage of adaptive EW is that it would allow the USAF to keep pace with a wider range of enemy behaviors than it can today, as illustrated in Figure 5.2. The y axis represents the magnitude of changes to adversary systems, ranging from few or small to many or large. The x axis represents the speed at which the adversary can make those changes. Current (conventional) EWIR capabilities are good at detecting small changes over long timescales (such as discovering known systems operating in unexpected locations, as illustrated in the lower left of the figure). A rules-enabled adaptive capability would be able to identify software-defined waveforms that change every few minutes or modes that have never before been seen on known systems, such as those that an adversary might use only in wartime (i.e., in the middle color band of the figure). An adaptive system can also adjust radar and communications waveforms in response to adversary jamming and EM suppression measures. In other words, adaptive EW would be able to keep up with faster and more-complex changes.

---

[27] Although this is a promising option that might be executable in one or two years and will give the USAF complete ownership of this lightweight apps layer providing the flexibility of rapid changes, there are some important factors making this approach untenable as a final, long-term solution, including the following:

1. The apps will need to be updated whenever an interfacing OFP updates its external interface. Both the interfacing OFP and the apps then will require testing and safety certification. Although the scope of the retest and recertification can be reduced by architecting the new apps' software as microservices and encapsulating the existing OFP in a container (as suggested later in this summary), some test and recertification will still need to occur.
2. App software that is supported by older OFPs (even if those OFPs are designed to be modular) remains a relatively heavy and brittle solution, rendering the prospect for cognitive EW at scale unlikely.

Figure 5.2. Minimum EWIR Capability Needed for Intelligence Collection Challenges



Despite their advanced capabilities, adaptive systems are only as good as the logic programmed into them, usually prior to the mission.[28] To cope with adversary systems that can switch nimbly between modes in real time or use no fixed mode at all (i.e., the upper right of the figure), and to learn from experience to adapt and rapidly develop countermeasures in real time, aircraft will need an onboard cognitive capability that can quickly think beyond the preprogrammed rules.

5. Build a Cognitive EW Capability

Cognitive systems are designed to adapt based on learned experience rather than predefined rules. The algorithms developed for this purpose are extensively trained and tested on existing data to enable advanced problem-solving. A cognitive EW system would be able to enter an environment without full knowledge of the adversary systems, learn from how those systems react in real time, and rapidly devise countermeasures against them. Cognitive systems can also recognize threats by their behavior alone over time (e.g., how and when they are used, where they are located, how the mainbeam is oriented and moves) and classify radars, jammers, or other electronic signals as potentially threatening (or nonthreatening) *without* identifying the actual system. A cognitive system can effectively act like a ride-along intel analyst who

[28] Although there are rules engines that accept runtime "over the air" updates to their rulesets, modifying a ruleset while in flight is not without danger. Assuring the security and safety of such an update is difficult, and the residual risks of implementing such an interface may not be acceptable.

examines unknown signals in the EMS and draws on their experience to rank the likelihood that those signals are threats. When dealing with new or not-previously-characterized enemy systems, this may be the only approach that can assist pilots in near-real time, especially when reachback is not available. Without the need of preprogrammed rules, a cognitive system can recognize and identify major and/or large changes to an emitter or to the parameters of an emitter, as indicated in the upper right of Figure 5.2.

Chapter 6. How Can the USAF Operationalize This Vision?

The goal of real-time, autonomous response cannot be achieved within the context of the current EWIR process for three reasons:

1. the policy and process obstacles described above
2. lack of necessary technologies that are available now
3. insufficient investment in development of new or advanced technologies.

Commercial companies and parts of the U.S. defense industry are working on new and advanced technologies. PAF research examined these efforts using case studies focused on identifying relevant technologies, their application to the EWIR problem, their current status, and their future development. The vision in Figure 5.1 recommends continuous investment in four areas starting now: cognitive EW, cloud integration and data engineering, software architecture and containerized microservices, and onboard high-performance computing. Based on that vision, we recommend a road map for achieving real-time autonomous reprogramming through a series of integrated increments by 2035.

Figure 6.1 presents our recommended road map, which identifies advancements in the four areas that require immediate and continuous investment if the USAF is to achieve adaptive and cognitive EW capabilities by 2035.[29] These advancements will incrementally build capabilities and include early wins that improve existing processes, as well as the infrastructure to support future autonomy. The latter includes a refactoring of the software architecture to accommodate

1. independent deployment of decoupled modules (using containers and other design best practices) to allow EW sensing and response software to be updated independently of aircraft flight control software
2. standardized and well-structured data to support ML algorithms.

In the area of hardware capacity, improved infrastructure includes the development of more-efficient (and, in some cases, specialized) hardware with the processing power to support computationally intensive algorithms within SWaP limitations.

For the EWIR enterprise, process improvements include

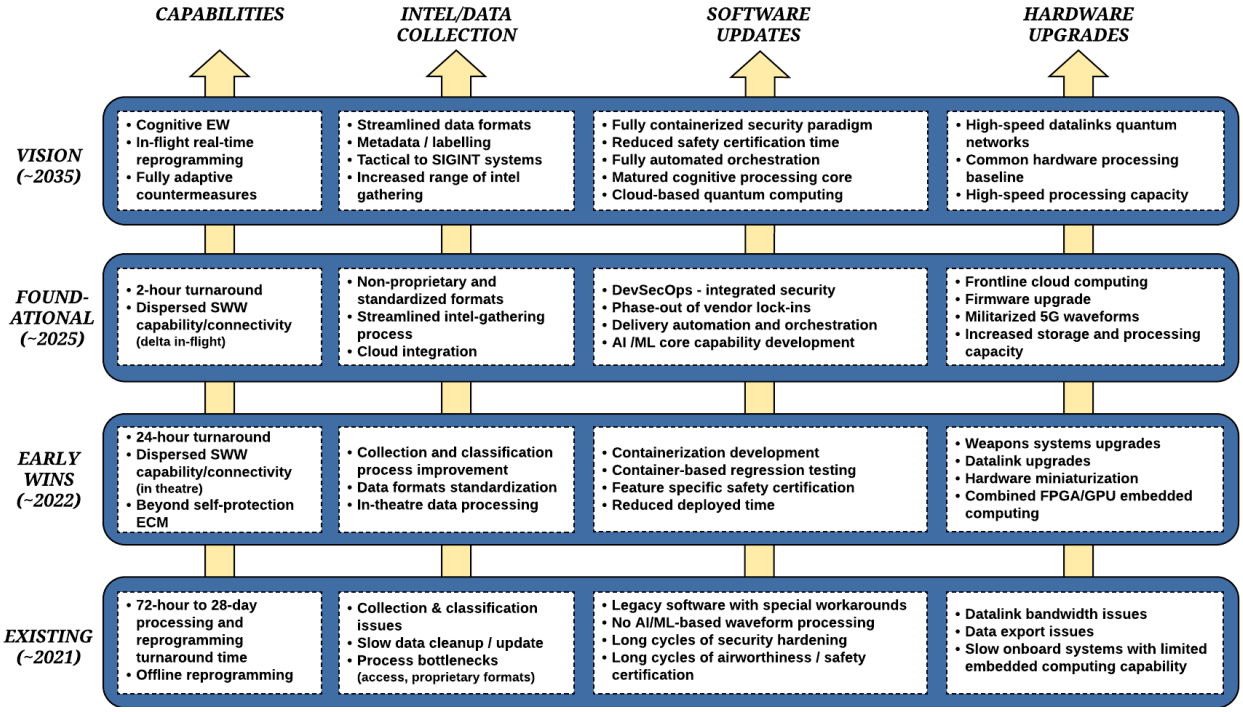
1. implementation of emerging paradigms for data collection, standardization, classification, and integration[30]
2. incremental upgrades in all of the above to make current EWIR processes more efficient and eventually enable airborne reprogramming and cognitive EW.

[29] See Chapter Three of the main project report (Vedula et al., 2023) for a more-detailed discussion of the reprogramming road map.

[30] Vedula et al., 2023, details various emerging technologies and efficient methods for data collection, data integration, and data engineering.

The reprogramming road map identifies the technology transformations required to achieve future cognitive EW capabilities. Importantly, this road map connects some tractable early wins with additional steps required for the longer-term vision. The time estimates in Figure 6.1 are based on PAF's analysis of current and expected technology readiness and the assumption that the USAF will actively pursue integrating those technologies into its EWIR process.

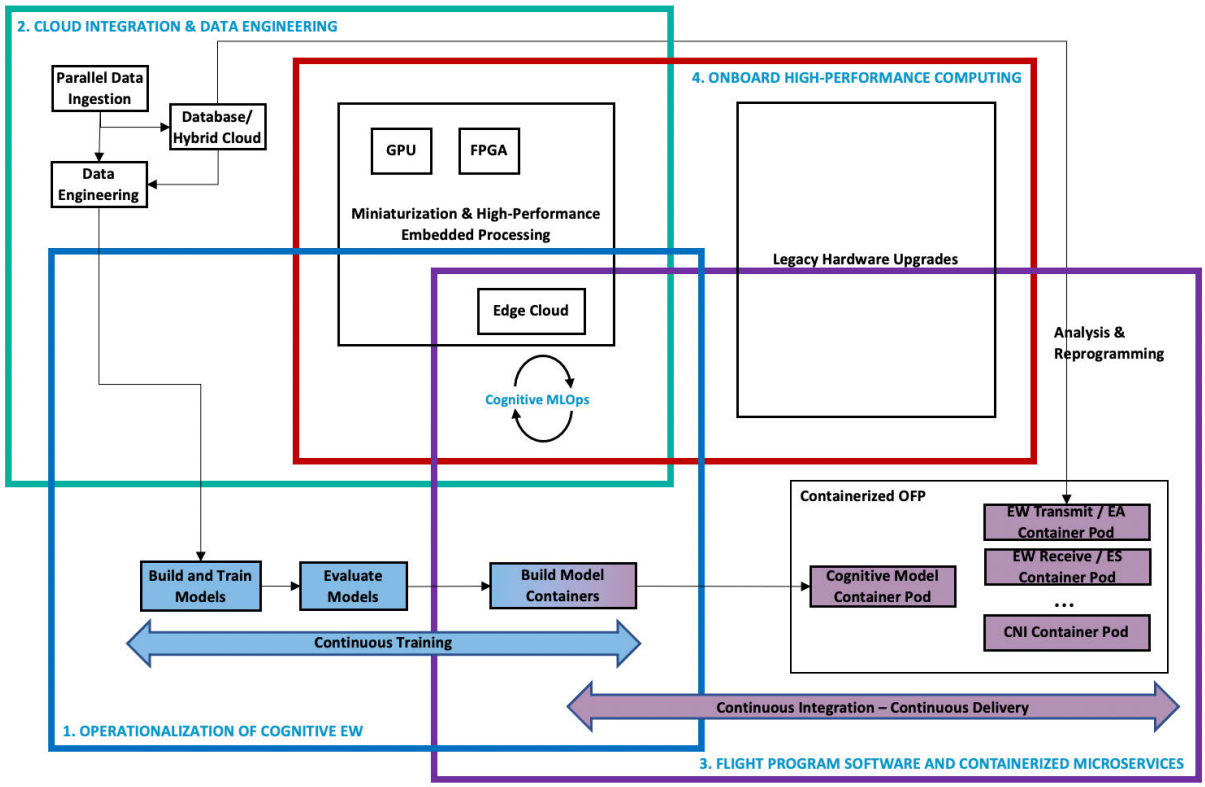
Figure 6.1. A Road Map for Achieving Real-Time, Autonomous Reprogramming



NOTE: AI = artificial intelligence; ECM = electronic countermeasures; FPGA = field-programmable gate array; GPU = graphics processing unit.

While several emerging technologies will play a part in bringing about the long-term vision, PAF investigated the state of development for four essential technologies described below. Figure 6.2 illustrates these technologies (represented by a set of colored boxes) and how they support the requirements for the development of future EW autonomy. Though separate, the four technologies interact in ways that collectively support incremental enhancement of the EWIR process. Due to these interdependencies, parallel investments are needed if the USAF is to reap the benefits of these technologies.

Figure 6.2. Interdependencies of Key Technologies for Cognitive EW



NOTE: EA = electromagnetic attack; CNI = container network interface; ES = electromagnetic support; MLOps = machine learning operations.

Operationalization of Cognitive EW

The ultimate goal is to operationalize a cognitive EW system for the USAF that can assess situations, make decisions, and continuously learn from experience. The first step is to define the desired end state. Adaptive and cognitive EW systems will require a well-defined data pipeline, a process for building and training ML models, and rapid deployment into the warfight. USAF software developers will need a lifecycle workflow that supports the training/retraining, tuning, and deployment of cognitive and adaptive models. Continuous training (CT) is necessary, as the predictive power of the models decrease with continuously changing data profiles. *Containerization* (discussed below) is a key technique that will allow the USAF to sustain future iterations of model updates. The main project report examines current DoD and industry efforts in building adaptive EW and cognitive EW capabilities.[31]

[31] These are detailed in Chapter Four of Vedula et al., 2023.

Cloud Integration and Data Engineering

Real-time autonomy for EWIR will require standardized data definitions that support the collection, retrieval, and classification of raw data from multisensor platforms and from future distributed and complex systems of systems. Data, in short, must be engineered. Real-time autonomous EWIR will require sustainable methods for data ingestion and data pipeline management, as was shown in Figure 6.2 (boxes 1 and 2). These methods are tightly integrated with the ML model development, training, and deployment (i.e., MLOps) discussed above. The main project report[32] examines current development efforts, including edge data collection, storage, computing, and data transfer options with supporting devices, such as Quick-Reaction Instrumentation Package (QRIP)–Knowledge Management/Rapid Analysis Processing Independent Deployable System (KM/RAPIDS).

Flight Program Software and Containerized Microservices

Containerization is a software deployment architecture that allows packaging of software into service-specific components, or microservices,[33] that run consistently on any platform or environment. Containerization simplifies the deployment of capabilities and upgrades. It is well suited to large-scale deployments onto dissimilar platforms (i.e., platforms that have widely different computing infrastructures, including operating systems and computing hardware). However, it requires the design of containerized service-specific components, or microservices, to have relatively few dependencies on each other. In fact, the goal of a container is that it includes the complete runtime environment for an application, databases, libraries, etc. The deployment architecture of the current EW-centric OFP software should be updated to allow containerization of services that execute in different containers and can be independently upgraded with enhanced capabilities (or new capabilities) without affecting other aircraft flight control software.

A containerized software architecture enables rapid software development, automated testing, and faster and airborne updates using a DevSecOps pipeline (i.e., automated tooling that

---

[32] See Chapter Five of Vedula et al., 2023, for detailed discussion of cloud integration and data engineering.

[33] The microservices architecture advocates the development of independent services within an application or platform with well-defined interfaces. Microservices generally facilitate ease of development and deployment, particularly in a continuous integration (CI), continuous delivery (CD), and development, security, and operations (DevSecOps) software deployment paradigm. The other benefits of microservices are separation of development, reusable and portable modular services, and fault tolerance. In this report, the term *microservices* is used to refer to independent containerized services; the term does not prescribe a specific level of granularity of the services themselves. Ideally, the EWIR-related software would be refactored into relatively small microservices that each execute in their own separate containers. For instance, it might seem prudent to place each ML algorithm, including its data, in its own container to allow for it to be upgraded independently of the rest of the EWIR-related software, thus lowering the time between software code completion and fielded software. However, too much granularity could produce latency issues and CPU and memory constraints. As will be discussed in the accompanying report (Vedula et al., 2023), weapon systems software would require an optimum number of containerized microservices to overcome the current issues with the speed of software deployments and to support future deployment infrastructure.

is designed around the idea of passing a container along a conveyor belt as it is hardened, tested, verified, and deployed into operations). This paradigm is based on the principles of CI, CD, and CT. The CI/CD-CT relationship is shown in Figure 6.2 (boxes 1 and 3).

Finally, the tools supporting the deployment of containers generally provide autoscaling and workload management services when executed in a cloud computing environment (or a mini-cloud or edge cloud created using existing on-aircraft computing systems).[34] These services allow computing resources to be optimally utilized based on need, which would be crucial for the high-speed processing of an adaptive or cognitive model. As examples, the main project report discusses the recent tests of Kubernetes, a container orchestration tool, on platforms such as the F-16. The report also discusses the work of USAF software factories, such as Platform One and Cloud One, which are providing core container repositories and other services to various automation initiatives within the DAF.[35]

Onboard High-Performance Computing

Current platforms, particularly legacy platforms, do not have the computing power necessary to process large amounts of data on the aircraft and for cognitive algorithms. Additionally, containerized OFPs with supporting orchestration tools would have computing resource demands that not all legacy platforms can support. The main project report discusses the hardware upgrades required for legacy platforms and current options that have ML computing powers, such as FPGAs and GPUs. The report also addresses recent innovations in hardware miniaturization and onboard high-performance embedded processing capabilities that would support ML processing on the edge, such as Agile Condor[36] and edge cloud,[37] as shown in Figure 6.2 (boxes 1 and 4).[38]

[34] Both containerization and the orchestration tools used for the resource management and auto-scaling of containers can be deployed and run on local on-premise systems or on platforms. However, cloud-based deployments provide additional networking, load-balancing, and storage support, and they reduce development and deployment times. We discuss this concept of mini cloud or edge cloud in the main project report, both in terms of the storage and processing power required for containerized software while overcoming the limitations of latency and in terms of data storage and processing of data closer to the point of collection to conserve and overcome the issues with bandwidth.

[35] Chapter Six of Vedula et al., 2023, discusses flight program software and containerized microservices.

[36] SRC, Inc., "Agile Condor High-Performance Embedded Computing," webpage, undated.

[37] Tina Francis and Madhiajagan Muthiya, "A Comparison of Execution Mechanisms: Fog and Edge Cloud Computing," presented at 2017 International Conference on Electrical Engineering, Computer Science and Informatics, Yogyakarta, Indonesia, September 19–21, 2017.

[38] Onboard high-performance computing is discussed in detail in Chapter Seven of Vedula et al., 2023.

Chapter 7. Conclusions and Recommendations

The EMS is a critical arena for great power competition. U.S. adversaries are looking to offset the United States' historical capabilities in this arena by developing smarter, more complex, and more rapidly adaptable systems. For the USAF, this means being able to more rapidly evaluate signals on the battlefield to identify both mobile and stationary threats to aircraft, air defenses, and the ability to project military power in and through the air domain. Threats include radars; communications jammers; and the electronic emissions of adversary aircraft, missiles, or related air warfare systems. Historically, this has been accomplished through a relatively manual and slow EWIR process. Fixing problems that slow the existing EWIR process is a necessary step to keeping the United States competitive in the EMS. However, the USAF should be thinking much further ahead about the kind of EWIR capability it will need to meet the most challenging competitors in the future—and it should start investing now in the enabling technologies required to realize that vision.

Some of the recommendations below will have immediate benefits for the existing EWIR process, and all will move the USAF toward the autonomous, onboard reprogramming capability necessary to survive in future denied and congested EMS environments. To that end, we offer recommendations in two areas: those that focus on generating faster and more-accurate reprogramming in the next two to five years while also preparing for cognitive EW and those that focus on accelerating and integrating technology development and adoption in order to support the cognitive EW vision over the longer term. These recommendations and the organizations involved in implementing them are summarized in Tables 7.1 and 7.2.[39]

[39] See Chapter Nine of Vedula et al., 2023, for detailed discussion of recommendations.

Table 7.1. Recommendations Impacting Today's EWIR

Alter how software is architected and supported		
1	Work with senior service and DoD leadership to determine the feasibility of requiring delivery of EWIR-related software using containers, including maintaining a repository of core-portable, platform-agnostic containers.	HAF A2/6 HAF A5 USAF digital executives
2	Conduct an analysis to determine which operational and test platforms have processing capacity to utilize containerized software.	Program offices
3	Develop template requirements for the acquisition of avionics that use containerized software and provide examples for how and when to include the requirements in future contracts.	ACC A5/8/9 ACC A3 350th SWW
4	Better align software development factories for greater use for airborne (instead of ground-based) computing infrastructure.	Software factories
5	Identify ways to encourage cross-platform software knowledge-sharing, such as potentially rotating programmers between different systems.	350th SWW
Enable rapid MDF updates in theater		
6	Develop template requirements for the acquisition of edge cloud computing, hybrid cloud architecture, data recorders (e.g., QRIP), and onboard processing and storage. Accelerating the development of the SPECTRE tool may be an appropriate use case to consider when developing the template requirements.	ACC A5/8/9 ACC A3 350th SWW
7	Develop tactics for rapid (airborne, ground-based) MDF updates in theater.	350th SWW
8	Consider aligning teams to support specific theater (as opposed to individual platform) reprogramming.	350th SWW
9	Collaborate to include reprogramming in exercises and concept rehearsals conducted at the edge.	350th SWW National Air and Space Intelligence Center Air components
10	Update Air Force Instruction 10-703 to clarify under which circumstances MDF updates can be conducted in theater.	HAF A5
11	Update data quality assurance/quality control processes for intelligence to facilitate more-rapid data use at the edge.	HAF A2/6 Director of National Intelligence
12	Develop and employ "coder airman" special experience identifier.	HAF A1
13	Consider adding experience on at least two platforms for a subset of EW officers designated as "theater coordinators" or a similar term.	HAF A1

NOTE: HAF = Headquarters Air Force.

Table 7.2. Recommendations Impacting Tomorrow's EWIR

Accelerate technological development		
14	Continue pursuing an applications-based approach to rapidly realizing automated and adaptive capabilities. Simultaneously support longer-term changes to OFP architecture that would ultimately enable a seamless, fully autonomous, cognitive EW capability.	ACC A5/8/9 350th SWW
15	Gather and write requirements for increasing onboard high-performance computing, use of dedicated ML accelerators (e.g., Tensor Cores, which are a type of processing unit), development of data warehouses, real-time data fusion.	ACC A5/8/9 ACC A3 350th SWW
16	Scale up ability to employ ES, mobility, and tanker aircraft to pilot emerging adaptive and cognitive EW concepts.	ACC A5/8/9 USAF Life Cycle Management Center Big Safari Operational units
17	Establish an integrated team of EWIR engineers, data engineers, and software engineers to build a developmental pipeline and testing environment for a service-owned reprogramming and cognitive EW minimum viable product capability ("EWIR-X") focused on air domain operations.	ACC A5/8/9 350th SWW (Air Force Research Laboratory) (Software factories)
18	Update data classification policies for USAF platforms and the networks through which different data can be accessed; establish architecture and policies to support Title 10/Title 50 data flow.	HAF A2/6 HAF A3 HAF A5
Integrate technologies to enable cognitive EW vision		
19	Develop integrated enterprise strategy of investments and employment related to cognitive/adaptive EW algorithms, data engineering and cloud integration, software containerization and orchestration, and hardware miniaturization.	HAF A5 ACC A5/8/9 USAF digital executive
20	Organize, train, equip, and provide EMS operations-capable forces that i. employ interoperable and extensible software components and microservices across platforms ii. analyze real-world data sets necessary to train cognitive EW systems iii. develop ML algorithms to facilitate cross-correlation of data from multiple sources iv. marry data to miniaturized hardware and containerized software v. enable access to high-speed datalinks to prime algorithms with the most recent data pre-mission vi. facilitate data extraction post-mission to share with other aircraft before their missions vii. enable personnel to develop platform related software knowledge to inform the development of applicable software and software services.	ACC directorates (implemented by operational units, supported by software factories)

In this research, PAF found that the current EWIR process is not designed for, nor is it fully adaptable to, responding to the newest types of threats in the EMS that are complex, fast-changing, and evasive. This situation is not unusual; processes are often designed with the past, present, and near-term future in mind and thus have limited flexibility to adapt to total regime or paradigm shifts, such as are emerging in the EMS.

The current EWIR process is capable of managing the day-to-day needs associated with legacy or less-complex threats, especially if afforded the opportunity to increase the use of

automation and the capacity of personnel and computing at certain bottlenecks in the process. Some form of the current process will also be required not only to manage future transition to new technologies, but also to support day-to-day operations in at least two ways: first, to maintain a capability to develop and curate algorithms, and, second, to manage system updates in lower-urgency situations because personnel and computing resources to support adaptive and ultimately cognitive EW will be limited.

Several technology, process, and policy changes need to come together to achieve the vision of advanced autonomous reprogramming. The reprogramming capability needed to succeed in combat against the most advanced threats in the EMS cannot be bought with modest progress in automating a few EWIR substeps or by acquiring a few new desktops. Rather, a paradigm shift is needed, one that is defined by a transition toward cognitive algorithm development and use and is supported by software containerization, hardware upgrades, and cloud computing architectures. We have suggested that systems will first be able to take advantage of more-advanced rules-based mechanisms (e.g., "smart" systems or adaptive algorithms), and, indeed, cognitive approaches may only be needed for the subset of threats that are most capable of evading conventional tracking and countermeasures.

The USAF can and should make use of these developments to advance toward a future EWIR capability through *continuous investment* in enabling technologies, starting now. Though disruptive, many of the changes on the path toward cognitive EW described here and in the accompanying report could be incrementally achieved to enable some early capabilities, which could then support the next steps.

On a final note, the changes described in the accompanying report—though articulated in the context of reprogramming for EMS operations—are really much more broadly relevant to USAF modernization. Rearchitecting software, taking advantage of small and specialized hardware, fielding innovative cloud capabilities to support advanced data fusion, and developing and operating with specialized algorithms will also be at the heart of operating in and through all warfare domains in the future. It is becoming more clear that the future of warfare is not so much about superior platforms operating alone, but instead about how all players are connected and pool information between them to outsmart an adversary.

Abbreviations

ACC	Air Combat Command
CD	continuous delivery
CI	continuous integration
CT	continuous training
DAF	Department of the Air Force
DevSecOps	development, security, and operations
DoD	U.S. Department of Defense
DOTMLPF-P	doctrine, organization, training, materiel, leadership, personnel, facilities, and policies
ELINT	electronic intelligence
EMS	electromagnetic spectrum
EW	electronic warfare
EWIR	electronic warfare integrated reprogramming
FPGA	field-programmable gate array
GPU	graphics processing unit
HAF	Headquarters Air Force
ISR	intelligence, surveillance, and reconnaissance
KM/RAPIDS	Knowledge Management/Rapid Analysis Processing Independent Deployable System
LPI	low-probability-of-intercept
MDF	mission data file
ML	machine learning
MLOps	machine learning operations
OFP	operational flight program
PAF	Project AIR FORCE
QRIP	Quick-Reaction Instrumentation Package
RF	radio frequency
SIGINT	signals intelligence

SPECTRE	Specialized Electromagnetic Combat Tools and Reprogramming Environment
SWaP	size, weight, and power
SWW	Spectrum Warfare Wing
USAF	U.S. Air Force

References

Air Force Technology, "USAF Selects Intelligent Waves for Flight Data Collection Support," webpage, October 10, 2019. As of August 27, 2021: https://www.airforce-technology.com/news/usaf-intelligent-waves-data-collection/

Curtis E. LeMay Center for Doctrine Development and Education, *Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations*, Maxwell Air Force Base, Ala., 2015.

Curtis E. LeMay Center for Doctrine Development and Education, *AFDP 3-51: Electromagnetic Spectrum Support Activities*, Maxwell Air Force Base, Ala., July 30, 2019. As of December 2, 2021: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-51/3-51-D08-EW-EMS-Support.pdf

DAF—*See* Department of the Air Force.

Department of the Air Force, *Air Force Instruction 10-703: Electronic Warfare Integrated Programming*, April 3, 2019.

DoD—*See* U.S. Department of Defense.

Francis, Tina, and Madhiajagan Muthiya, "A Comparison of Execution Mechanisms: Fog and Edge Cloud Computing," presented at 2017 International Conference on Electrical Engineering, Computer Science and Informatics, Yogyakarta, Indonesia, September 19–21, 2017.

Pomerleau, Mark, "The Army May Have the Electronic Warfare Tool the Pentagon Needs," *C4ISRNet*, June 15, 2020. As of August 27, 2021: https://www.c4isrnet.com/electronic-warfare/2020/06/15/the-army-may-have-the-electronic-warfare-tool-the-pentagon-needs/

Simmen, Robert L., and Bjorn M. Fjallstam, *Threat Warning for Tactical Aircraft: A Technical History of the Evolution from Analog to Digital Systems*, Xlibris, 2006.

SRC, Inc.,"Agile Condor High-Performance Embedded Computing," webpage, undated. As of July 6, 2021: https://www.srcinc.com/products/intel-collection-and-analysis/agile-condor-high-performance-embeded-computing.html

USAF—*See* U.S. Air Force.

U.S. Air Force, *Air Force Doctrine Publication (AFDP) 3-51: Electromagnetic Warfare and Electromagnetic Spectrum Operations*, July 30, 2019. As of August 12, 2021: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-51/3-51-AFDP-EW-EMSO.pdf

U.S. Air Force, *Spectrum Integration Group Conference Report*, October 2020.

U.S. Air Force, Office of the Chief Software Officer, homepage, undated. As of December 1, 2021: https://software.af.mil/

U.S. Department of Defense, *Department of Defense Directive 3222.04: Electronic Warfare (EW) Policy*, August 31, 2018.

U.S. Department of Defense, *Electromagnetic Spectrum Superiority Strategy*, October 2020. As of August 27, 2021: https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF

Vedula, Padmaja, Abbie Tingstad, Lance Menthe, Karishma R. Mehta, Jonathan Roberts, Robert A. Guffey, Natalie W. Crawford, Brad A. Bemish, Richard Payne, and Erik Schuh, *Outsmarting Agile Adversaries in the Electromagnetic Spectrum*, Santa Monica, Calif.: RAND Corporation, RR-A981-1, 2023. As of January 19, 2023: https://www.rand.org/pubs/research_reports/RRA981-1.html

PROJECT AIR FORCE

The U.S. Air Force's electronic warfare integrated reprogramming (EWIR) enterprise examines intelligence on adversary threats that emit in the electromagnetic spectrum (EMS) (in particular, radars and jammers) and configures electronic warfare software and hardware to enable aircraft or other resources to react to and/or respond to adverse changes in the EMS environment. With the growing advancements in U.S. adversaries' electronic warfare assets that enable complex and diverse EMS capabilities, identifying, tracking, and responding to these threats requires much faster updates than the existing EWIR enterprise was designed for. The research team conducted four interrelated technology case studies that together comprise the fundamental elements necessary for creating a near-real-time, autonomous, inflight software reprogramming capability and, more specifically, artificial intelligence–enabled *cognitive electronic warfare* capabilities—the use of machine learning algorithms that enable platforms to learn, reprogram, adapt, and effectively counter threats in flight. The research team also highlighted important continuing roles for the existing EWIR enterprise even as the U.S. Air Force moves toward a cognitive future.

$18.50

ISBN-10 1-9774-1058-8
ISBN-13 978-1-9774-1058-0

www.rand.org

RR-A981-2