RAND CORPORATION

Research Report

PADMAJA VEDULA, ABBIE TINGSTAD, LANCE MENTHE, KARISHMA R. MEHTA,
JONATHAN ROBERTS, ROBERT A. GUFFEY, NATALIE W. CRAWFORD, BRAD A. BEMISH,
RICHARD PAYNE, ERIK SCHUH

# Outsmarting Agile Adversaries in the Electromagnetic Spectrum

For more information on this publication, visit **www.rand.org/t/RRA981-1**.

### About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

### Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

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

ISBN: 978-1-9774-1057-3

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

*Cover design: Rick Penn-Kraus*

### Limited Print and Electronic Distribution Rights

# About This Report

Adversaries and competitors are seeking to offset the United States' historical ability to operate within and through the electromagnetic spectrum (EMS) by making their systems more complex and adaptable—and therefore more difficult for U.S. platforms to detect, identify, evade, or counter. This presents an enormous challenge to the U.S. Air Force (USAF) electronic warfare integrated reprogramming (EWIR) enterprise. 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[1] electronic warfare (EW) equipment to enable aircraft or other USAF resources to react to and/or respond to adverse changes in the EMS environment. The USAF is actively exploring how best to achieve faster, cutting-edge EMS capabilities. To assist in this effort, RAND Project AIR FORCE (PAF) examined how adversary capabilities in the EMS are evolving, how fast EW-related software reprogramming needs to be to keep up with the threat, what obstacles exist within the current intel-to-reprogramming process, and what advanced technologies are needed to achieve necessary improvements. PAF's work is centered on what is currently known as EWIR but is scoped to cover the broader range of issues related to the role of data and software in enabling EMS operations and is intended for a broad audience concerned with military planning, budgeting, and operations.

The research reported here was commissioned by the Plans, Programs and Requirements Directorate, Headquarters Air Combat Command (ACC A5/8/9) and 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." A related executive summary provides an overview of conclusions and recommendations.[2]

## 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.

[1] This configuration is generally done digitally and may include new uploads of data, software code, and firmware. 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.

[2] Abbie Tingstad, Padmaja Vedula, Robert A. Guffey, Karishma R. Mehta, Lance Menthe, and Jonathan Roberts, *Outsmarting Agile Adversaries in the Electromagnetic Spectrum: Executive Summary*, Santa Monica, Calif.: RAND Corporation, RR-A981-2, 2023.

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.

## Acknowledgments

The research team would like to thank our sponsor, John C. Vona, SES, Deputy Director of the Plans, Programs and Requirements Directorate (ACC A5/8/9), Headquarters Air Combat Command, for sponsoring this study and for his input on the direction of the project. We also thank our project action officers, Gary “GMan” Woltering and Charles “Kent” Stitt, also at ACC A5/8/9.

Furthermore, we extend our gratitude to the multiple representatives of organizations within the broader EW, intelligence, and software communities. These include, but are not limited to, the 350th Spectrum Warfare Wing and component groups and squadrons, the National Air and Space Intelligence Center, platform program managers, several testing and development organizations, and several offices within United States Air Forces Europe.

Finally, we thank our many RAND colleagues who offered insight into this project. Emily-Kate Chiusano and Kathryn Giglio were instrumental in finalizing the report. We are also grateful to our research reviewers, Bonnie Triezenberg and Christopher Lynch.

# Summary

## Issue

Superiority in the electromagnetic spectrum (EMS) is increasingly important for securing military advantage. Adversaries and competitors are seeking to offset the United States' 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 threats.

This presents an enormous challenge to the U.S. Air Force (USAF) electronic warfare integrated reprogramming (EWIR) process, which relies on key organizations such as the National Air and Space Intelligence Center and the 350th Spectrum Warfare Wing. 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[3] electronic warfare (EW) equipment to enable aircraft or other USAF resources to react and/or respond to adverse changes in the EMS environment. Until recent years, EMS threats did not change very quickly. The EWIR enterprise could execute mission data file (MDF) updates as well as months-long operational flight program updates without a negative impact to operations. With the growing advancements in U.S. adversaries' electronic warfare assets, however, enabling complex and diverse EMS capabilities, identifying, tracking, and responding to these assets requires much faster updates than the EWIR enterprise was designed for.

## Approach

RAND Project AIR FORCE (PAF) considered how adversary capabilities in the EMS are evolving, how fast EW-related software reprogramming needs to be to keep pace with threats, what obstacles exist within the current intel-to-reprogramming process, and what advanced technologies are needed to achieve necessary improvements. PAF's work is centered on what is currently known as EWIR but is scoped to cover the broader range of issues related to the role of data and software in enabling EMS operations.

To conduct this work, PAF relied on subject-matter expert interviews and field observations (e.g., of air component rehearsal of concept drills), process analysis, technology forecasting analysis, and vignette development. Central to the methodology was the development of four interrelated technology case studies that together comprise the fundamental elements necessary

[3] This configuration is generally done digitally and may include new uploads of data, software code, and firmware. 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.

for developing a near-real-time, autonomous, inflight software reprogramming capability and, more specifically, artificial intelligence–enabled *cognitive electronic warfare*.[4]

## Conclusions

- To remain competitive and adapt to changing threats, USAF systems that operate in the EMS must be capable of rapid reprogramming (including evaluating the environment, detecting adversary activity, and synthesizing an appropriate response), at least on the order of seconds to minutes.
- Agile software solutions, hardware upgrades, data engineering, and interoperability with other systems are all required to achieve the needed speed.
- Accompanying changes in policy, organizational mission alignment, personnel and computing availability, and personnel professional development are also needed.

## Recommendations

- The USAF should start working today to *accelerate and integrate technologies needed to realize cognitive EW*. Steps include supporting a shift toward software architectures, such as containerized microservices, that would allow faster deployment of capabilities and upgrades to increase the reprogramming speed and provide support for the deployment of cognitive EW algorithms on platforms in the future; enhancing onboard high-performance computing; expanding experimentation and early technology adoption; prioritizing policies and technologies that will allow better data collection, standardization, classification, access, and integration processes; and ensuring coordinated investment and implementation of these activities given high interdependencies among key technologies.
- The USAF should also take immediate steps to *adopt new software deployment architectures to enable faster fielding of capabilities and implement rapid and airborne MDF updates in theater*. This necessitates important changes to existing policy; personnel professional development; technological reviews; and investments in software architecture standards, onboard processing, and computing and connectivity at the "edge" of combat (i.e., by the aircraft during the mission).

[4] *Cognitive electronic warfare* is the use of machine learning algorithms that enable USAF platforms to learn, reprogram, adapt, and effectively counter threats in flight.

# Contents

# Figures and Tables

## Figures

## Tables

# Chapter 1. Introduction

Gaining access to and effectively using capabilities in the electromagnetic spectrum (EMS) is becoming increasingly important for securing military advantage. The importance of the EMS 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.[5] Since then, military uses of the EMS, typically focused in the radio frequency (RF) part of the spectrum,[6] 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, these threats sense activity in the EMS to track and target airborne (and other) platforms, including through the use of the RF part of the spectrum itself to disrupt sensing and communications using jamming.

Now, military use of the EMS is undergoing another renaissance. Broader parts of the EMS are being explored and exploited. Specialized tactics (e.g., use of decoys, advanced intelligence tradecraft) can be employed to gain advantage in detecting threats and in evading them. Some capabilities of the past will no longer be relevant in a world where control over information and the means to communicate it dominate kinetic weapons and concepts of employment. It is becoming more important than ever for the U.S. Air Force (USAF) to be able to sense and understand the electromagnetic operating environment (EMOE).

## The Importance of Operating in the Electromagnetic Spectrum

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. military platforms to detect, identify, evade, or counter. This creates an issue for U.S. employment of EW, which is divided into electromagnetic support (ES), electromagnetic protection (EP), and electromagnetic attack (EA).[7] In brief, ES covers activities designed to gather data critical to effective execution of EW. EP involves threat identification and employment of appropriate countermeasures involving technologies (e.g.,

[5] See, e.g., Thales Group, "A War to Win the Airwaves—The History of UK Electronic Warfare," September 27, 2020.

[6] 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.

[7] U.S. Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations*, Joint Publication 3-85, Washington, D.C., May 22, 2020.

flares) and tactics (e.g., avoidance) using information collected in the EMS. EA, in turn, is the use of offensive approaches to neutralize threats in the EMS.

In 2020, the U.S. Department of Defense (DoD) released the *Electromagnetic Spectrum Superiority Strategy*,[8] which followed a 2018 *DoD EMS Strategy*, a 2017 *DoD Electronic Warfare (EW) Strategy*, and an even earlier 2013 *Electromagnetic Spectrum Strategy*.[9] The 2020 document articulates the need to develop "an electromagnetic spectrum (EMS) 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.[10] Indeed, freedom of maneuver within the EMS may in the near future be less of a "leading indicator"[11] of impending kinetic conflict and instead be the primary focus of power play between competitors. The EMS could be exceptionally well suited for this role, given that its capabilities cut across all of the four instruments of power—diplomacy, information, military, and economy—in the context of growing reliance on access to data and information across sectors and around the world.

The 2020 strategy also clarifies that both EW and EMS battle management fall underneath the umbrella of electromagnetic spectrum operations (EMSO) in order to develop and coordinate an effective EMS enterprise across DoD. EMS battle management, though separate from EW doctrinally, goes hand in hand with ES, EP, and EA in that it enables the planning and direction of operations in the EMS and the ability to monitor and assess activities.[12] The strategy also describes the growing complexity of the global EMS environment as increasingly contested, congested, and constrained.[13] In other words, the EMS is a space in which militaries seek advantage. Additionally, the increasing use of the EMS by commercial and other entities, along with militaries, is resulting in high levels of traffic across the spectrum and elevated risk of unintended interference, and this is necessitating policies that limit the amount of spectrum available for military use.

The 2020 strategy argues that freedom of maneuver in and responsible use of the EMS requires a responsive capability to recognize and effectively react to activity in the EMS. Historically within the USAF, necessary adaptations to changes in the EMS have been accomplished through a process termed *electronic warfare integrated reprogramming* (EWIR). Recognizing that the months to years currently needed for developing and executing the software configuration updates[14] at the heart of EWIR are not sufficient against current and future threats,

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

[9] Mark Pomerleau, "DoD Unveils Electromagnetic Spectrum Superiority Strategy," *C4ISRNet*, October 29, 2020b.

[10] DoD, 2020b, p. 8.

[11] DoD, 2020b, p. 3.

[12] U.S. Joint Chiefs of Staff, 2020, p. I-9.

[13] DoD, 2020b, p. 4.

[14] These software updates include what is presently known as the operational flight program (OFP) and the mission data file (MDF) or threat library.

the USAF is exploring how best to achieve adaptive and cutting-edge EMS capabilities.[15] The need for more-advanced EMS capabilities is further driven by the newer, more data-intensive EMSO capabilities that the USAF and Joint community have recently brought into their inventories (e.g., fifth-generation fighter aircraft) or are developing (e.g., planned unmanned systems).

In fiscal year (FY) 2021, the Plans, Programs and Requirements Directorate, Headquarters Air Combat Command (ACC A5/8/9) asked RAND Project AIR FORCE (PAF) to examine how the USAF can integrate key technological advances in algorithm development, data engineering, software, and hardware to support a redesign of the EWIR enterprise to enable much faster, more accurate reprogramming and secure software configuration updates. To do this, PAF has considered 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. 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 focuses on the fundamental investments needed to realize in-flight software reprogramming, with the ultimate goal of using machine learning (ML) algorithms to enable USAF platforms to learn, reprogram, adapt, and effectively counter threats in flight. This ML-enabled capability is referred to as *cognitive EW*. We begin by providing some historical context for EWIR below.

## Historical Context

Radar technology—and the EWIR process—have evolved over time.[16] The first operational military radar, Chain Home (United Kingdom, 1938), was a copse of steel towers and unshielded cables literally hardwired to generate 25 pulses per second of 20 microsecond duration in the 20–30 megahertz (MHz) frequency band.[17] Confirming a repeated "blip" was sufficient to detect a target,[18] and operators became highly adept at this, tracking fleeting returns from aircraft well below the ambient noise level.[19] Over the next few decades, radar circuitry was greatly miniaturized and upgraded to allow employment of ever-more sophisticated waveforms—even

[15] U.S. Air Force, *Spectrum Integration Group Conference Report*, October 2020b.

[16] A quick note on terminology: Here we use *radar* to mean the transmitting threat radar and *radar warning receiver (RWR)* to be the receiver. An EW system can refer to the radar, the RWR, or both.

[17] The receiving towers were also fixed in design. They were separated from the transmitters—technically a bistatic radar. Subsequent variants of Chain Home extended the range of pulse duration and frequency (B. T. Neale, "Chain Home—The First Operational Radar," *GEC Journal of Research*, Vol. 3, No. 2, 1985).

[18] "Two blips received on successive scans and seen by the operator is the detection criterion" (E. W. Paxson, *Detection by Airborne Intercept Radar*, Santa Monica, Calif.: RAND Corporation, RM-256, 1949).

[19] How the Women's Auxiliary Air Force operators managed this feat remains unknown, but it is thought to be related to the "cocktail party" effect (Neale, 1985).

switching between highly distinct waveforms on command[20]—but radar signals remained highly constrained by, and carried the clear fingerprints of, the particular hardware that generated them.

For these reasons, identifying an adversary radar system was understood largely as a memory game. A receiver would scan known RF bands looking for bursts of power, which it would summarize in terms of a handful of standard parameters: average frequency, pulse repetition rate, pulse duration, etc.[21] That parameter set was then compared to a library of known, parameterized radars, painstakingly constructed by electronic intelligence (ELINT) analysts based on previous encounters. A clear match was a positive identification, and partial or missing matches were recorded for further analysis.

Initially, the parameterization and comparisons were done by hand, as skilled sensor operators analyzed the signals and leafed through lookup tables. In time, the comparison process became more automated: Parametric data for many waveforms were automatically extracted and encoded as pulse descriptor words (PDWs), and the physical lookup tables became MDFs. The process by which MDFs are programmed with the right parametric libraries and loaded onto aircraft systems is one aspect of what we now call the EWIR process and is described in more detail later in this chapter.

Starting in the 1970s, engineers began to design radars with increasingly clever digital encoding schemes that enabled multiple systems to share the same portion of the RF spectrum and required dozens of extra parameters to be properly characterized.[22] Meanwhile, beam-shaping techniques that focus radar power from a floodlight to a flashlight made it increasingly difficult to detect signal sidelobes.[23] This increasing sophistication of waveforms demanded corresponding improvement in the sophistication of the techniques used to decipher them—which led to the development of technical electronic intelligence (TECHELINT).[24] However, while the arms race between radar design and TECHELINT techniques made the EWIR matching process far more complex, it was still essentially a memory game. As we describe in Chapter Two, a matching process—even a complex one—that is entirely reliant on pre-existing information is no longer sufficient for keeping up with newer, advanced adversary radars and jammers.

## The Role of Software Reprogramming in Electronic Warfare

Underpinning effective EMSO, including both EW and EMS battle management, is a need to understand the EMOE and to translate conditions therein into a format that machines—via software—can understand. This involves a series of key organizations, people, and materiel

[20] Before their components were sufficiently miniaturized, circuit boards were swapped out to change waveforms.

[21] Early RWRs recorded only a handful of parameters; modern systems might now record hundreds.

[22] Phase-shift and frequency-shift keying schemes allow radars to switch nimbly between EM spectrum bands and to share them with other systems.

[23] Evading the main beam of a targeting radar is highly desirable for obvious reasons.

[24] Other intelligence sources and methods also play an important role here.

capabilities (encompassing both software and hardware) that play important roles in ensuring that adversary radars and jammers and other activity in the EMS can be detected and appropriately reacted or responded to. Enabling the detection of and response to threats in the EMS entails abstracting intelligence into a format or language that machines with a diverse range of characteristics can individually understand, developing and updating software using different tools, and conducting the appropriate testing and maintenance to get those software updates operating on different platforms.

In practice, this involves an ongoing series of interrelated activities which, in the USAF, is conducted by the EWIR enterprise. EWIR as a concept, process, and enterprise has persisted in the USAF for decades. EWIR is a key enabler for many types of aircraft, including fighters; bombers; intelligence, surveillance, and reconnaissance (ISR) aircraft; tankers; and transporters. The USAF EWIR enterprise includes a diverse range of organizations, notably the National Air and Space Intelligence Center (NASIC), which leads the effort with partners in the intelligence community (IC) to make tactical SIGINT data available through the EWIR database, and the 350th Spectrum Warfare Wing (SWW), which was stood up in the summer of 2021 and includes the 36th Electronic Warfare Squadron (EWS) and the 453rd EWS, each of which plays key roles in supporting software reprogramming for a subset of USAF platforms. In addition, other USAF wings, such as the 55th and 363rd, support the broader intelligence effort, and the air components around the world enable updates to be uploaded to aircraft. The USAF EWIR enterprise also exists within a larger ecosystem of intelligence processes, including the collection, processing, and exploitation of TECHELINT conducted by the National Security Agency (NSA) and the service production centers. These organizations must work together to ensure that

- updated intelligence mission data (IMD) are available
- changes to threats are detected
- an impact analysis is performed
- updates to MDFs and OFPs are initiated
- software updates are generated
- updates are loaded onto platforms.

As defined in Air Force Instruction (AFI) 10-703 (specific to EWIR), the EWIR process at a macro level consists of four steps: detect a change, determine its impact, reprogram, and field the change.[25] EWIR consumes a vast amount of time—at least several weeks, if not months to years, depending on the scale of the changes needed, the priority, the personnel and computing available, and the availability of support from existing IMD and tools.[26]

EWIR-related changes can take three forms: (1) alterations to an aircraft's onboard computer code—i.e., its OFP; (2) updates to an aircraft's onboard data files—i.e., an MDF containing

[25] This process is also known as PACER WARE.

[26] Project interviews are listed in Appendix A. See USAF, *Air Force Instruction 10-703: Electronic Warfare Integrated Reprogramming: Ellsworth Supplement*, October 19, 2010, Supplement January 5, 2016.

expected threat characteristics or predetermined responses to that threat;[27] and (3) hardware adjustments[28] to support sensing and reaction to threats. Both OFP and MDF changes are considered software per DoD software development standards.[29] 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.[30] 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 refer, specifically, to the threat library produced for a mission by the EWIR process. Having said that, even in the current EWIR process, MDFs also 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.

The reprogramming changes are requested via an Operational Change Request and have three priority levels: routine, urgent, and emergency. Figure 1.1 shows the timelines for each priority level. OFP updates for both bug fixes (based on deficiency reports) and new capabilities[31] can be made at specific priority levels,[32] though *urgent* and *emergency* changes are usually accomplished through MDF updates[33] for timing feasibility reasons and because the

[27] 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 used by friendly systems to more fully characterize the battle space. 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 code 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 (USAF, Det 8, ACC TRSS, "*Electronic Warfare Fundamentals*," Las Vegas, Nev.: Nellis Air Force Base, 2000).

[28] Hardware adjustments could include, for example, changing sensors or adding processing capacity. Hardware changes have to comply with the guidance in USAF, *Air Force Instruction 63-131, Modification Management*, 2015; USAF, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming*, February 22, 2017.

[29] 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.

[30] An intriguing history of the development of electronic counter measures for aircraft self-defense is 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.

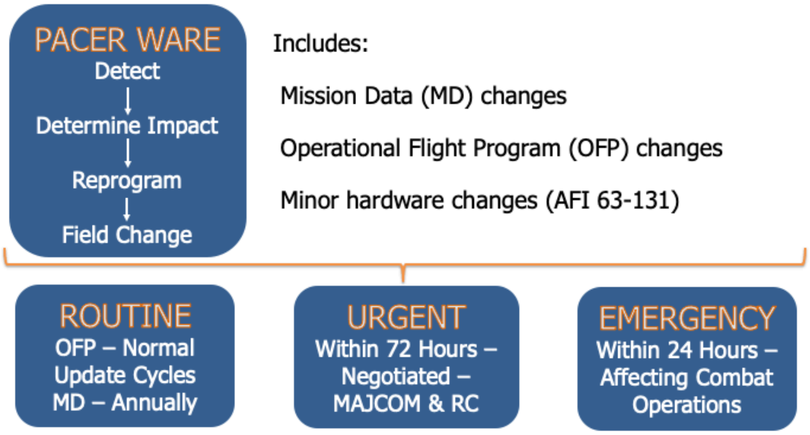
[31] New capability development is usually pushed back—i.e. downgraded in priority—to cater to bug fixes. Sometimes new capabilities take several iterations of the OFP update to be developed. This is more often true for newer, fifth-generation platforms than legacy platforms (subject-matter expert [SME] interview, March 11, 2021).

[32] AFI 10-703, 2017.

[33] AFI 10-703, 2017; Richard E. Neese, Scott A. Brantley, and Marc J. Pitarys, "Partitioned Software Support for Modular Embedded Computer Software," *Proceedings of the IEEE 1991 National Aerospace and Electronics*

change requests are often scoped to threat library lookup table adjustments. These MDF updates can be done relatively quickly when there are existing threat data from another area of responsibility or a sensor engineering issue that has caused an incorrect identification of a threat is found. In other words, emergency or urgent updates can be executed more quickly not only because of their high priority and associated ability to secure scarce resources quickly but also because they often do not need additional foundations in intelligence and preliminary testing to execute.

**Figure 1.1. EWIR Process: PACER WARE**


PACER WARE
Detect
Determine Impact
Reprogram
Field Change
Includes:
Mission Data (MD) changes
Operational Flight Program (OFP) changes
Minor hardware changes (AFI 63-131)
ROUTINE
OFP – Normal Update Cycles
MD – Annually
URGENT
Within 72 Hours – Negotiated – MAJCOM & RC
EMERGENCY
Within 24 Hours – Affecting Combat Operations

*Routine* OFP updates are generally based on the typical OFP update cycles and take up to two years to field.[34] In some cases, an OFP change would also theoretically be required as part of an *urgent* or *emergency* change request. However, as mentioned above, MDF programmers that we interviewed reported sometimes resorting to adding workarounds or stopgap solutions because OFP updates are time consuming. These stopgap solutions are used to trick the system to perform or respond in a particular way until a routine software change provides the necessary full functionality.[35] An additional downside to these types of stopgap solutions is that they might make the software inflexible to future OFP updates.[36]

*Conference NAECON 1991*, Vol. 12, 1991. Also, mission data updates are supported by Mission Data Generator tools and loaded with field loading equipment Program Loader Verifiers, Memory Loader Verifiers, the Enhanced Diagnostic Aide, and Common Aircraft Portable Reprogramming Equipment (AFI 10-703, 2017; USAF, 2000).

[34] The assumption is that these updates are inline with the normal update cycles proposed or agreed upon by the vendor of the EW subsystem or suite.

[35] See interviews listed in Appendix A.

[36] Any new OFP update might create a mismatch with the MDF stopgap solutions and could require additional testing to ensure consistency.

## Research Objective and Approach

The USAF recognizes that the current overarching process for conducting EWIR is too slow to compete with the adversary EMS capabilities it is likely to encounter in the future, for reasons[37] we detail in Chapter Two. The research discussed in this report was therefore intended to examine the current state of the EWIR process and the types of (particular materiel) investments that might be required to make it substantially faster, without sacrificing (and even improving) quality and security.[38] The research had two main objectives:

1. Document the existing EWIR process and gather lessons from the associated community regarding the reasons for slowdowns.
2. Articulate, to an order of magnitude, how fast the end-to-end EWIR process would need to be to counter advanced adversary radars and jammers, and elucidate the types of materiel investments that would establish the foundations for achieving the needed speed.

The PAF team also sought to document other types of investments across the doctrine, organization, training, materiel, leadership, personnel, facilities, and policy (DOTMLPF-P) framework to support the materiel investments.

PAF's research approach is summarized in Figure 1.2. Primary data sources included interviews, documents, and live observation of USAF concept rehearsals.[39] We cite specific primary sources, where relevant, throughout the report. These primary sources fed extensive process documentation and analysis; technology mapping (i.e., from objectives to specific types of investments over time, including by using DOTMLPF-P); and illustrative vignette development. We next conducted structured case studies of four interrelated technologies to enable potential solutions. These case studies were defined by the following elements:

- description of the technology type (what it is)
- application to EWIR (what problem does it solve)
- current state of development (what exists and how is it being used)
- likely future development path (what's next).

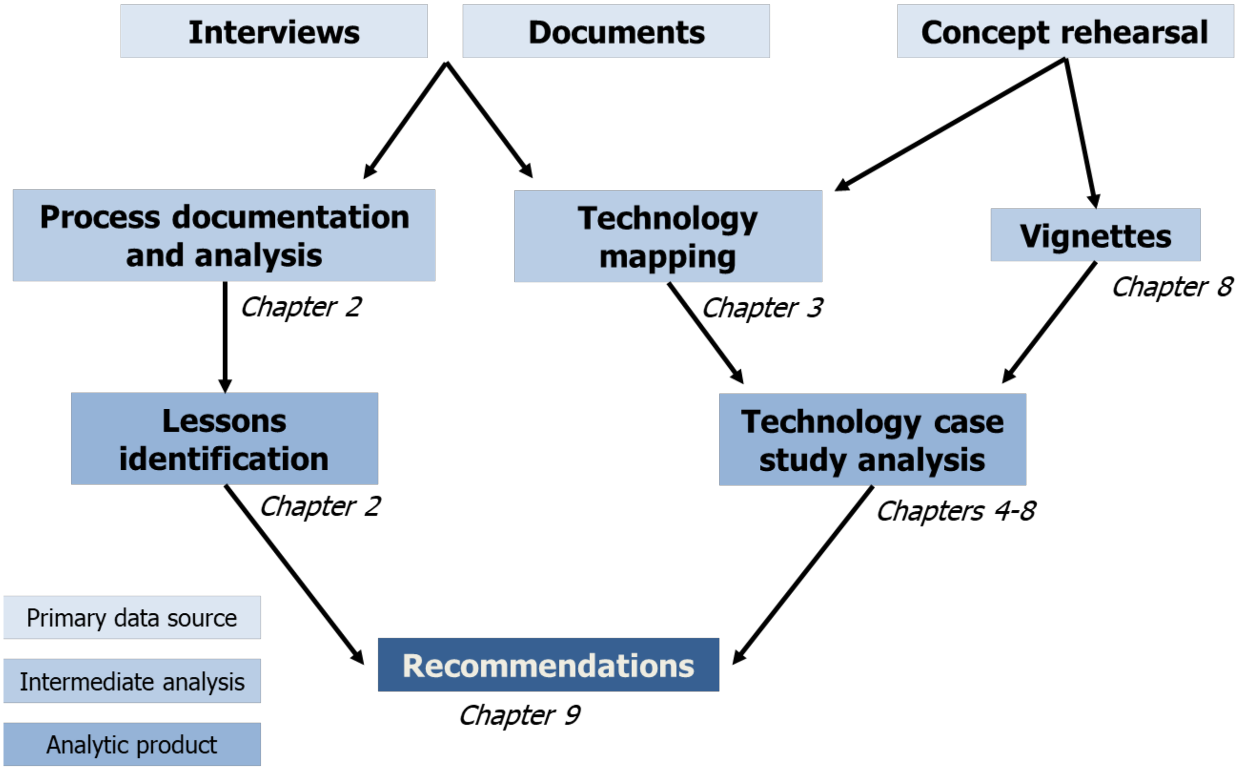
Finally, based on all of these analytic tasks, we recommended a vision and road map for future EWIR. More specifics on the research methodology are included in Appendix A.

[37] See, for example, Curtis E. LeMay Center for Doctrine Development and Education, "Electromagnetic Spectrum Support Activities," Air Force Doctrine Publication 3-51, Electromagnetic Warfare and Electromagnetic Spectrum Operations, last updated July 30, 2019.

[38] *Security* has numerous contexts; although we did not extensively explore this in the EWIR context, the project team scoped consideration of this to the security of aircraft software related to the RWR and any other elements that operate within the EMS.

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

**Figure 1.2. Project Approach**



## How This Document Is Organized

This report is organized into nine chapters and two appendixes. Figure 1.2 summarizes which aspects of the analysis are highlighted in each chapter. Chapter Two discusses how EMS threats are changing and explains why the EWIR process needs to be faster (in many cases) than the speeds summarized in Figure 1.1. In that chapter, we also examine the problems and obstacles that currently stand in the way of making reprogramming faster. Chapter Three lays out a vision for the USAF's future EWIR process that provides needed agility to counteract emerging advanced threats. Here, we articulate what exactly a faster EWIR process entails, the technological and policy achievements needed to advance this vision, and a summary of some primary needs across DOTMLPF-P, with an emphasis on technology, that are needed to support change.

Chapter Four presents the results of our first technology case study, which examines the concept of cognitive EW; how and why it applies to improving EWIR speed; and its unique technological facets and needs. Chapters Five through Seven detail three other types of technologies that underpin the cognitive EW system: Chapter Five examines the creation of a data pipeline through data engineering and cloud integration methods; Chapter Six focuses on ways to change the software deployment architecture to support faster OFP and MDF fielding processes and to build the infrastructure to support cognitive EW; and Chapter Seven looks at advances in high-performance computing (HPC) onboard aircraft that rely on EWIR and the need for processing power to support computationally intensive algorithms within size, weight, and power (SWaP) limitations.

Chapter Eight offers two vignettes that illustrate how a future EWIR process and capabilities (incorporating each of the technology case studies discussed in preceding chapters) could support operational objectives more effectively than today. Finally, Chapter Nine examines the interdependencies between the technology case studies and proposes how they might be integrated. We offer early-term ("fundamental") and later-term ("visionary") recommendations for USAF leadership to consider should they wish to move forward with pursuing a cognitive EW approach, and we discuss the intermediate capabilities needed to ultimately achieve that goal. Appendix A provides further detail about the research methodology. Appendix B presents additional information about the intelligence challenges that EWIR must address.

# Chapter 2. Assessment of the Current EWIR Enterprise

In Chapter One, we discussed some historical context for EWIR in which we referred to a reliance on preset rules adopted on the basis of careful intelligence inquiry along with subsequent computer modeling and software programming. In the past, radars grew more complex over time, and it was more challenging to identify their signatures in the EMS, but the basic EWIR approach of generating and periodically updating lookup tables kept pace with threats. Now, emerging adversary radar and jamming technologies are outpacing the historical approach around which the current EWIR process was designed. This chapter provides a brief overview of why this is the case, establishing the need for revisiting how EWIR is conducted. Next, we describe the end-to-end EWIR process and discuss some of the problems that will make it difficult for the current EWIR enterprise to keep pace with emerging advanced threats.

## The Threat Context

Systems operating in EMS leave signatures based on their physical characteristics and their use of the spectrum (particularly RF) for sensing and communications. As we have described, activities in the EMS were previously somewhat straightforward to detect once the appropriate sensing technologies and intelligence became available. Radar and jammer characteristics used to identify their operation by an adversary in the EMS did not change very quickly (or, if they did change, the change would generally be within some identifiable, relatively fixed envelope); most shifted slowly over several decades and adhered to the general rule that an emitter's unique thumbprint in the EMS could be pinned to a specific threat type and location. For example, the few radar systems that initially existed all had simple, well-known, and largely unchanging waveforms that could be characterized by only a few parameters. Thus, it was relatively easy to collect ELINT about an adversary's radar and jamming systems and for intelligence squadrons to develop and periodically update MDFs, and less frequently OFPs, so that sensor systems could identify enemy radars and jammers.

More recently, adaptability in the EMS has become an advantage for militaries that implement this type of adaptation effectively. In this context, *adaptability* refers to software-defined, hardware-related, and tactics-based actions that are intended in some way to disguise presence, location, and/or intent. Advanced adversary radar systems create a challenging EMOE by using waveforms, signal parameters, modes of operation, power and sensitivity, and other characteristics to reduce detectability. Because waveforms are becoming more complex, dozens of parameters are sometimes needed to reliably distinguish one emitter from another. Radars that employ low probability of intercept (LPI) techniques, such as ultra-wideband and noise-like waveforms, can be difficult to detect by conventional RWRs due to their reduced peak power[40] and random pulse patterns.[41] Radars that employ (or mimic) digital modulation, such as frequency hopping and phase-shift keying, can be difficult to distinguish from commercial communications systems, which increasingly compete for the same electromagnetic (EM) spectrum.[42] Software-defined radars (SDRs) can generate never-before-seen waveforms on the fly and shift rapidly between these, confounding traditional electronic warfare (EW) identification methods based on known pre-defined libraries.

Many threats are also mobile, sometimes highly so; therefore, relying on a static threat map in lieu of training software (via a smart system or ML) to recognize threats wherever and whenever they might occur is not a winning proposition. Furthermore, capable adversaries have recently begun to employ tactics in air defense (e.g., use of decoys) that further complicate the interpretation of sensor data into threat information that can be acted upon by U.S. weapons systems.

Thus, EMS operations are an "arms race" between ever-evolving threat capabilities and ever-improving methods of identifying and countering those threats. As described above, the changing complexity of threats and the EMS environment drive a need for EWIR to move faster and incorporate more data. The EWIR process of determining and analyzing the impact of threats and making the necessary software and MDF 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. Furthermore, new and developing USAF platforms capable of EMSO are increasingly data hungry, in that they are designed to rely on vast quantities of information about a fast-changing environment. EWIR configuration updates must keep up with these new designs in both speed and capacity for change.

Given these advances in threat capabilities and technologies to counter them, USAF EWIR must evolve to become *much* faster, deal with *much* higher data volumes, and become *much*

[40] "The principal idea of LPI radar is to escape interception by mismatching its waveform to those waveforms for which an ES [electronic support] receiver is tuned. Since the majority of ES receivers are tuned to detect pulse, CW [continuous wave]), and pulsed Doppler waveforms it is intuitively obvious that it should use some form of frequency or phase-coded high duty cycle signal. The wide bandwidth will negate the CW receiving channel and the high duty cycle with associated low peak power will make it difficult for the pulse channel to detect and identify the signal" (D. C. Schleher, "LPI Radar: Fact or Fiction," *IEEE Aerospace and Electronic Systems Magazine*, Vol. 21, No. 5, May 2006).

[41] Daniel Kellett, Dmitriy Garmatyuk, Saba Mudaliar, Nahlah Condict, and Isaiah Qualls, "Random Sequence Encoded Waveforms for Covert Asynchronous Communications and Radar," *The Institution of Engineering and Technology Radar, Sonar & Navigation*, Vol. 13, No. 10, 2019.

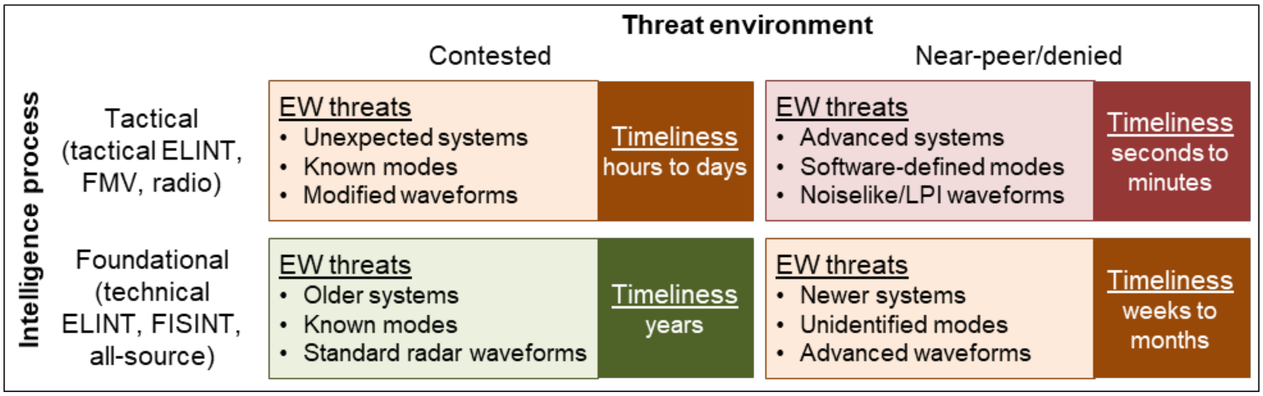
[42] "The proliferation of commercial mobile devices and consumer demand for streaming video and music applications have increased bandwidth requirements of mobile wireless communication networks. Frequency spectrum allocations for military and commercial radar systems . . . are normally segregated from other users to avoid interfering with these critical systems. However, the demand for increased bandwidth allocations by mobile network providers spurred innovation in developing systems and protocols that allow the coexistence of radar and communication systems within the same bandwidth while preventing or minimizing mutual interference" (Thomas W. Tedesso and Ric Romero, "Code Shift Keying Based Joint Radar and Communications for EMCON Applications," *Digital Signal Processing*, Vol. 80, September 2018).

smarter to maintain U.S. advantage in EMS operations. As we describe in more detail later, USAF systems that operate in the EMS must be capable of rapid reprogramming on the order of seconds to minutes because these are the speeds at which threats can or soon could adapt. Agile software solutions, faster hardware upgrades, advanced threat intelligence processing, and interoperability with other systems are all required to achieve the needed speed for EWIR. We show that this is presently not the case in the description of the current EWIR process that follows.

## The Need for Timeliness

How timely does the EWIR process need to be? Figure 2.1 summarizes four situations[43] that require software updates, but at different levels of urgency. The situations are defined by the intelligence context (from foundational [i.e., in peacetime] to tactical [i.e., direct mission support during crisis or conflict]) and by the threat environment (from less-capable adversaries [i.e., historical threats, not complex] to near-peer competitors [i.e., pacing threats, very complex and evasive]). The boxes in the figure 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 (MDFs or an OFP)[44] to keep ahead of changing threat conditions.

**Figure 2.1. EWIR Speed Needed to Keep Pace with Threats**



| Intelligence process | Threat environment: Contested | | Threat environment: Near-peer/denied | |
|---|---|---|---|---|
| Tactical (tactical ELINT, FMV, radio) | EW threats<br>• Unexpected systems<br>• Known modes<br>• Modified waveforms | Timeliness<br>hours to days | EW threats<br>• Advanced systems<br>• Software-defined modes<br>• Noiselike/LPI waveforms | Timeliness<br>seconds to minutes |
| Foundational (technical ELINT, FISINT, all-source) | EW threats<br>• Older systems<br>• Known modes<br>• Standard radar waveforms | Timeliness<br>years | EW threats<br>• Newer systems<br>• Unidentified modes<br>• Advanced waveforms | Timeliness<br>weeks to months |

SOURCES: SME interviews, doctrine (Curtis E. LeMay Center for Doctrine Development and Education, *Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations*, undated; USAF, *Air Force Instruction 10-703: Electronic Warfare Integrated Programming*, April 3, 2019c; DoD, *Department of Defense Directive 3222.04: Electronic Warfare (EW) Policy*, August 31, 2018), and vignettes (Chapter Eight).
NOTE: 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 processes.
FISINT = foreign instrumentation signature intelligence; FMV = full-motion video.

[43] These are distinct from the routine, urgent, and emergency updates referenced in AFI 10-703.

[44] Recall that the current construct favors MDF updates as stopgap measures until the threat changes are so significant that a major software 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 in Figure 2.1). For priority threats, including those that are capable of adapting waveforms to help evade detection (lower-right box), EWIR would need to generate the necessary OFP or MDF changes (depending on which is feasible) within weeks to months.

Tactical intelligence is more demanding for EWIR, because it is used to find, fix, and track threats 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 agile waveform variants (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. Another way to think about required speed in the context of tracking advanced threats is how fast alternatives to reprogramming would work. For example, one could employ procedures for intel sharing and coordination on kill chains, which could take a few dozen minutes. Improvements to reprogramming should aim to be faster than this type of solution, which has several potential points of failure if it is solely relied upon.

Next, we turn to why the existing EWIR process is fundamentally incapable of meeting needs in the more pressing or challenging contexts illustrated in Figure 2.2. We do so by focusing on lessons reported by experts reflecting their experiences in EWIR and supported by process analysis and literature.[45]

## EWIR Process Status Quo

As described in Chapter One, the USAF's EWIR enterprise has been developed, run, and supported by a diverse range of organizations, such as NASIC and the units that are now housed within the 350th SWW. These organizations have dedicated important efforts to EWIR for decades but have not had access to many of the fast-changing technologies that underpin an ability to enable continuous production and protection of data from all available sources and to conduct rapid reprogramming in flight.

[45] See, e.g., 87th Electronic Warfare Squadron Mission Briefing, April 29, 2021; 36th Electronic Warfare Squadron Mission Briefing, February 5, 2021; USAF, 2019c; and Michael Gilmore, "Key Issues with Airborne Electronic Attack (AEA) Test and Evaluation," presentation to 2011 Association of Old Crows AEA Symposium, 2011.

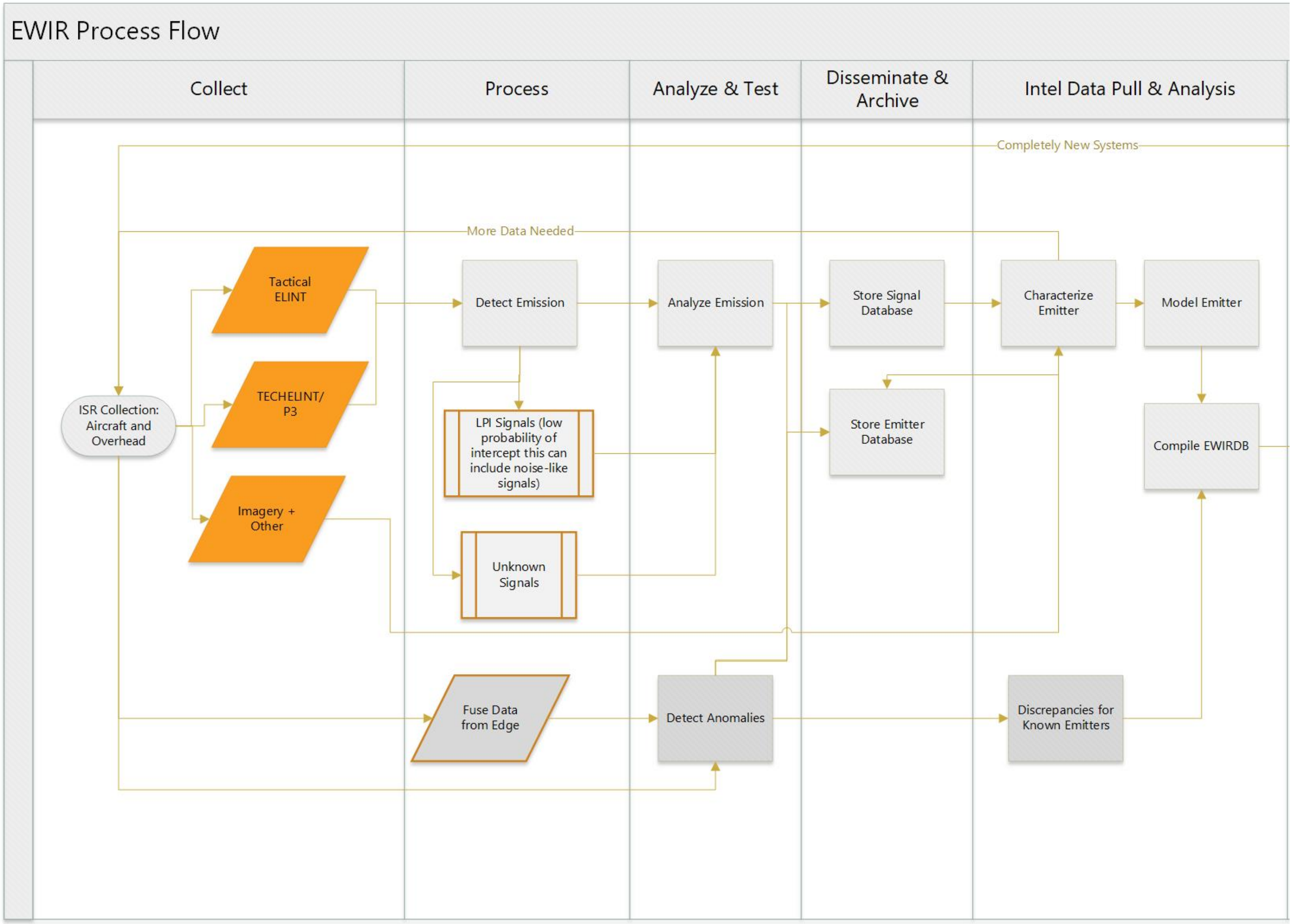
Figure 2.2 summarizes the EWIR process, dividing it into eight sections that were defined on the basis of expert interviews,[46] doctrine,[47] and PAF team knowledge:

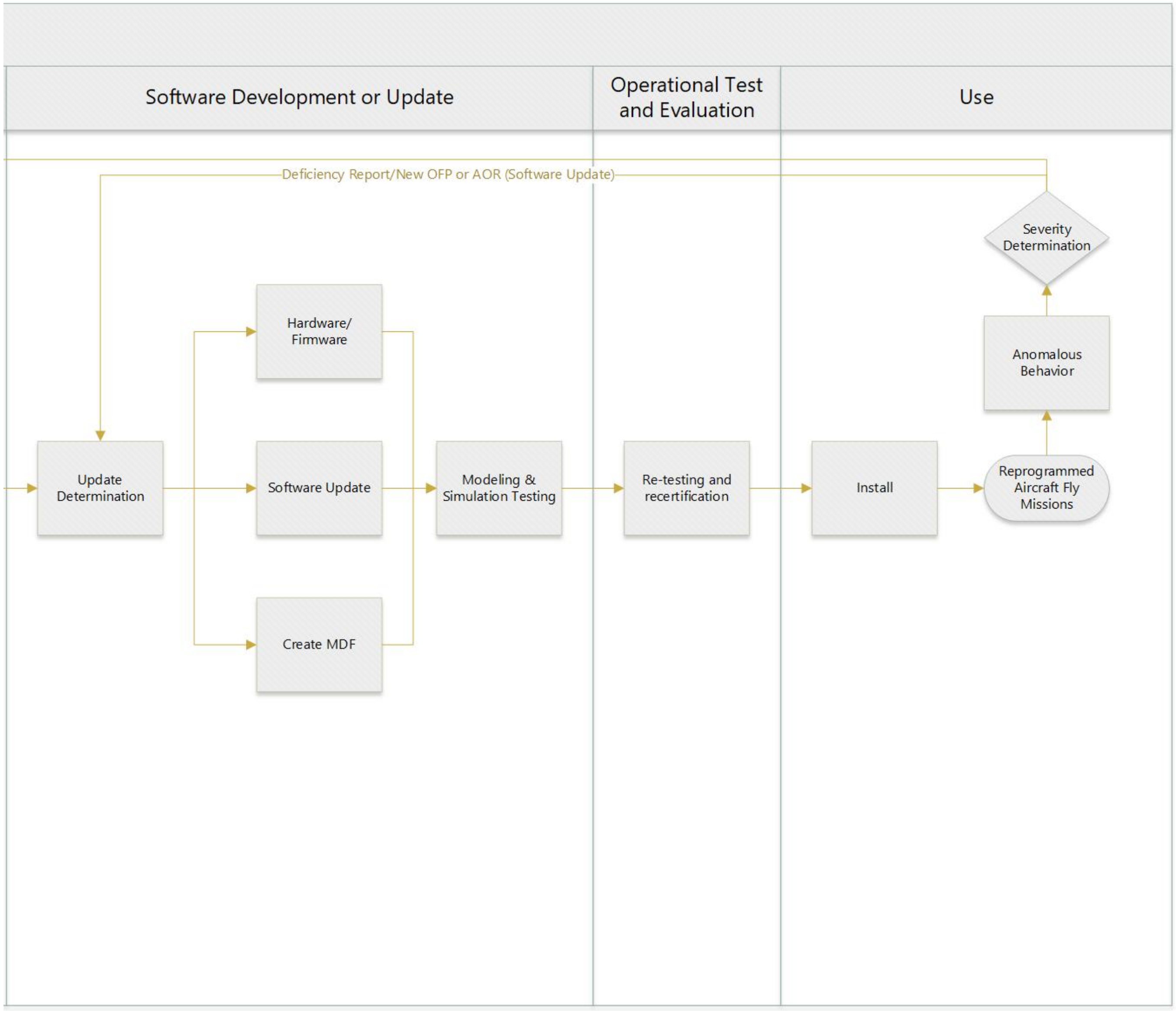
- collection (historically the start of the intelligence cycle)
- processing (automated data transformation into a format amenable to further signals analysis and automated identification of known signals)
- analysis (human-machine teaming to sift through unidentified and misidentified data)
- dissemination and archiving (preparing data for storage in formats and locations accessible to others)
- intel 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)
- developmental testing and evaluation (DT&E) and operational testing and evaluation (OT&E) (modeling the interaction between RWR or other EW equipment software and the emitter[s] in question and testing software changes)
- use (uploading new software changes to onboard hardware).

[46] See Appendix A.

[47] The doctrine consulted was primarily AFI 10-703, along with installation-level implementation documents for that instruction: e.g., USAF, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming, Aviano Supplement*, August 20, 2013; USAF, 2016; and USAF, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming: Beale Supplement*, April 3, 2019c.

**Figure 2.2. Generalized Summary of Current EWIR Process**




Software Development or Update
Operational Test and Evaluation
Use
Deficiency Report/New OFP or AOR (Software Update)
Severity Determination
Hardware/ Firmware
Anomalous Behavior
Update Determination
Software Update
Modeling & Simulation Testing
Re-testing and recertification
Install
Reprogrammed Aircraft Fly Missions
Create MDF

SOURCES: SME interviews and U.S. Air Force Instruction (AFI 10-703; U.S. Air Force, 2017).

A primary takeaway from Figure 2.2 is that EWIR is a complex process involving many decisions and transactions of data or information between humans, machines, or both. Figure 2.2 generalizes the EWIR process, despite the fact that the process can look a bit different depending on which platform is being supported. For example, different approaches and organizations are needed to reprogram fifth-generation aircraft, which need orders of magnitude more data to fully realize the capabilities inherent in their avionics. Conversely, without major hardware and software changes discussed later in this report, legacy aircraft struggle to use very complex inputs to support onboard decisionmaking. Adding further complexity, emergency or urgent MDF updates begin toward the latter steps in the process because they are driven by discoveries made during routine maintenance of intelligence. Thus, they can effectively skip the long lead times that are driven by intelligence-heavy steps at the front end of the process.

PAF did not attempt to time aspects of the EWIR process through observation or simulation because we did not need a precise baseline to evaluate potential options for improvement at a specific point in the process. Nor did we assess any particular organization's timeliness in depth. Our research scope was to take a broader view of the end-to-end EWIR process[48] to identify endemic problems that no single organization is responsible for fixing.

Table 2.1 documents, in a general sense, how long each step takes to better contextualize some of the lessons we describe below. For each step, we interviewed SMEs responsible for the work involved to answer two questions:

1. How would a best case, average, and worst case be defined for this step?
2. What is an approximate time for step completion in each case?

We defined *average* as a SME's typical day-to-day or expected working experience. Aircraft receive software updates with fairly predictable regularity, and it was this case that we used to discuss *average*. In contrast, *best case*, somewhat counterintuitively, was defined as an emergency update—one that would receive the highest priority over other activities that experts might be expected to perform. We also constrained this case to only MDF updates for a single adversary radar or jammer. Finally, *worst case* was defined as the circumstances leading to the slowest experienced execution of a step or series of steps. This was typically associated with lower-priority changes and assuming multiple procedural holdups (e.g., lack of network access, broken computer, key personnel unavailable for some period).

[48] This process is also called PACER WARE (AFI 10-703).

**Table 2.1. Generalized Time Estimate for Portions of the Current EWIR Process**

| Step | Relevant Unit | Best Case Scenario | Average | Worst Case Scenario |
|---|---|---|---|---|
| Collection | Per signal | 24 hours | Days to months | Years |
| Processing | Per signal | A few seconds | A few seconds | A few minutes |
| Analysis | Per signal | Real time (automatic); 1 hour | 1–4 days | 3 months |
| Dissemination and archiving | Per signal | Minutes | 4 hours | 3 days |
| Intel data pull and analysis | Per emitter | Days | 1 month | 6 months<br>Recollection needed |
| Software development or update | MDF (dependent on intel) | Within 1 week | 6 months | Intel is never found |
|  | OFP | 6 months (F-16)[a] | 6 months (F-35)<br>12 months (F-16) | 3 years (F-16) (re-architecture) |
| DT&E and OT&E | Per update | 9 months (F-16) | 12 months (F-16)<br>6 months (F-35) | 24 months (F-16)<br>12 months(F-35) |
| Use | Per update | 48 hours | 72 hours | Don’t make the update; 18 months |

SOURCES: SME interviews, Appendix A, AFI 10-703 (U.S. Air Force, 2017).

[a] We did not include a best-case scenario for F-35 because the massive data requirements for training this platform’s systems sufficiently burden the process so that we did not assess there to be a substantial difference between “average” and “best.”

Several factors could cause shifts between these scenarios and, in turn, timeliness at each step in Table 2.1. *Collection* is one of the least predictable steps in terms of timing because there are a variety of factors that could lead to failure, principal among them the emergence of an opportunity (“the enemy gets a vote”) and the availability of the right sensor at the right place at the right time. *Processing* is automated and should generally occur in seconds but could work more slowly—on the order of minutes—if the hardware in question is near capacity (e.g., due to high data volume or particularly low processing power). This occurs on board the collection platform. *Analysis* is dependent on how unique the signal is and how sensitively the collector’s onboard system—or a system on the ground post-flight—can associate the processed data to an emitter. The more time humans need to intervene in this process, the longer this step takes. For *dissemination and archiving*, key dependencies include connectivity with centralized databases, data volume, and any formatting or system glitches.

The next steps constitute the process for adapting general-purpose intelligence to EWIR. The time it takes to complete *intel data pull and analysis* depends on how complete the intelligence available is for the purposes of understanding how to identify an adversary radar or jammer. If all needed data are available, the timing comes down to the priority of the threat and whether highly trained analysts are available. *Software development or update* timing largely depends on whether the change in the EMS environment that triggered further analysis requires an OFP update (longer) or an MDF update (shorter). A single change of limited departure from prior activity can generally be recorded in an MDF update. Other factors important to timing in this step include the availability and efficacy of automated tools, which this project did not evaluate, such as the Specialized Electromagnetic Combat Tools and Reprogramming Environment (SPECTRE), to flag the change and propose the necessary update. *DT&E/OT&E* is constrained by the number of computers, processing power, availability of personnel, number of certification steps, and availability of other testing infrastructure and equipment (e.g., hangar space).

*Use*—or the uploading of updates—is fairly constrained by doctrine (AFI 10-703), and timing is primarily based on whether the update is designated as *routine*, *urgent*, or *emergency*. Some variation also occurs based on the ability of flying wing staff to identify necessary updates, access the correct networks, and develop an efficient approach to conducting the required maintenance.

As demonstrated in this section, many factors determine how quickly the EWIR enterprise can make the necessary updates. SMEs 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. Schedule-intensive activities include extensive modeling and simulation to simulate 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 DT&E and OT&E required before these changes can be deployed into operations.

The USAF is planning to implement continuous software delivery and deployment pipelines to reduce these timelines, but this practice is not commonplace, particularly for weapon systems software.[49] Additionally, because OFP changes typically have longer fielding timelines, the USAF sometimes adds stopgap solutions or workarounds to MDF updates for issues or behaviors that would be better addressed through software code changes. Such workarounds eventually lead to inflexible software and compromises in performance affecting 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.

## Lessons: What Problems Does the Current EWIR Process Face?

Several obstacles slow down the current EWIR process and make it ill suited to keep up with rapidly adapting EW threats. Based on our interviews, we found that individual organizations involved in the EWIR process are generally quite aware of the bottlenecks inherent to their portion of the process and in many cases know of or are even working on fixes to those issues.

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

Thus, we relied on well-established techniques for gathering and articulating lessons,[50] for which one relevant definition is "Validated observation(s) that summarize a capability, process, or procedure, to be sustained, disseminated, and replicated (best practice); or that identifies a capability shortfall requiring corrective action (issue)."[51] We worked to compile observations from across different organizations with key roles in the process to establish high-level lessons that set the stage for the vision of future EWIR presented in Chapter Three. Although these lessons focus on problems, we acknowledge ways in which the status quo is working to support USAF and Joint needs in the EMS throughout the report when relevant. In particular, we emphasize that a modified version of the existing approach can and should have a role in the future, to ensure a smooth transition toward newer technologies and also as a key component of any cognitive EW approach, which we describe in Chapter Three.

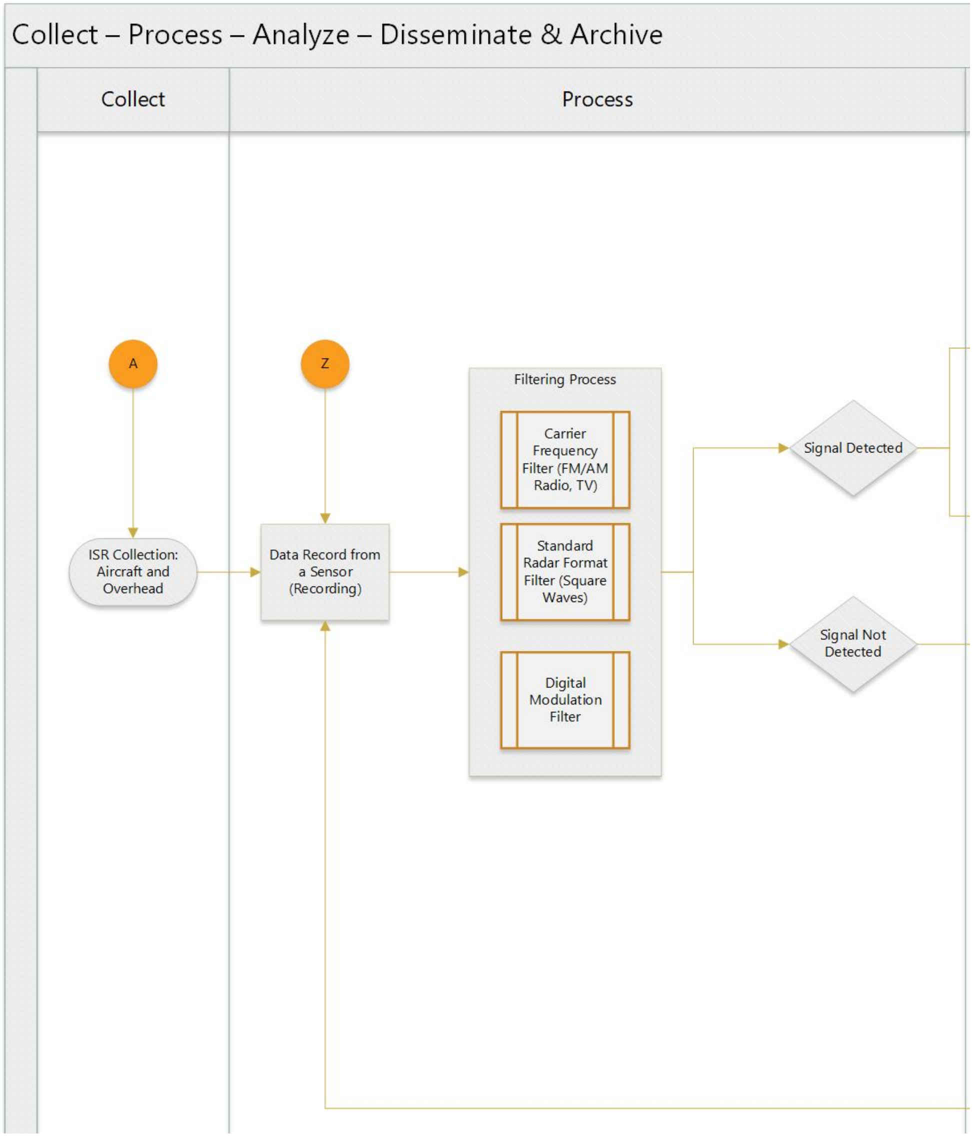
### *The Proliferation of Manual Steps Limits Process Improvements Gained from Discontinuous or Stopgap Solutions*

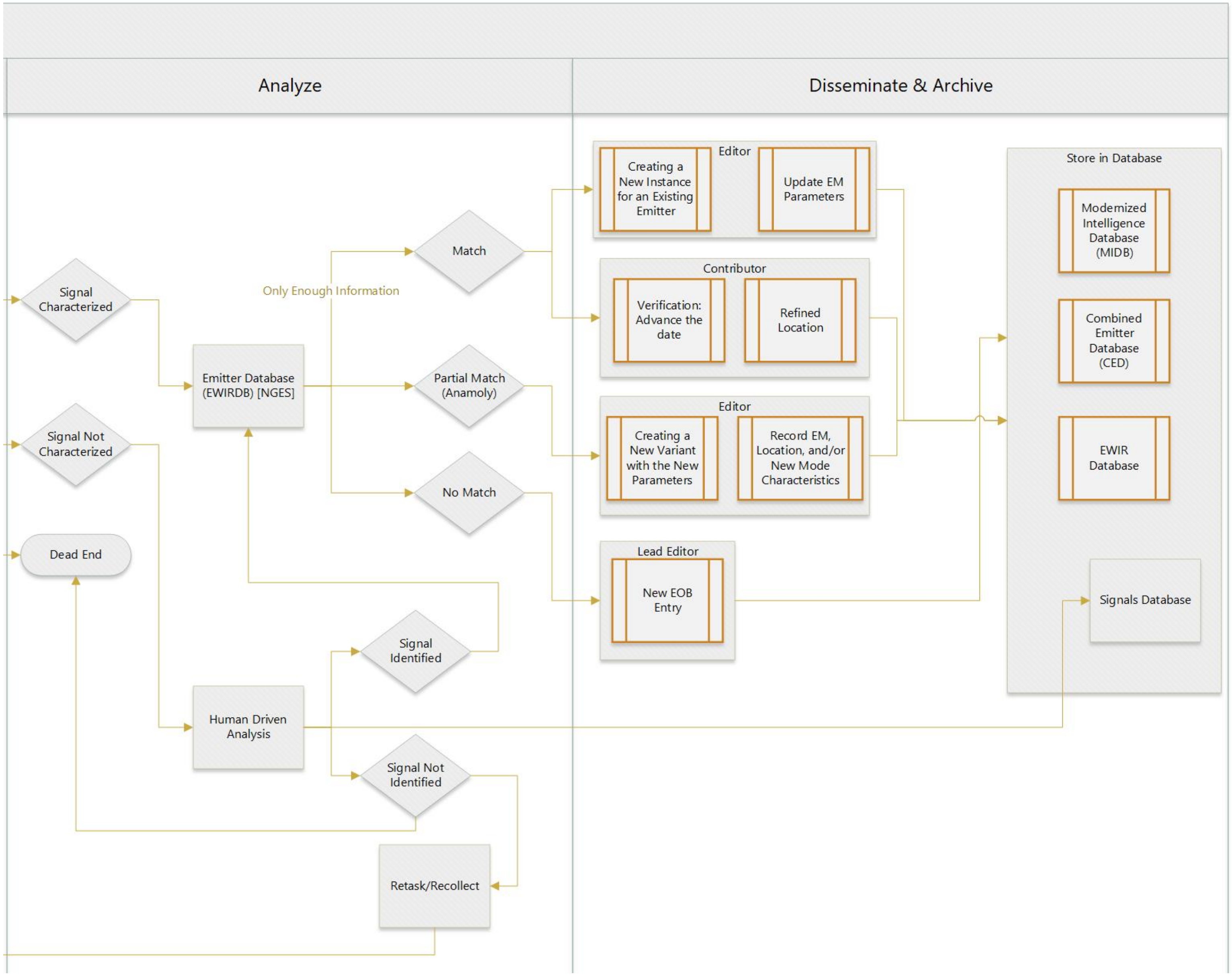
Figures 2.2 (examined earlier), 2.3, 2.4, and 2.5 help demonstrate the proliferation of substeps in the EWIR process. Many of these, save for those involved in the *processing* step, are manual or only partially automated with people in the loop.

[50] See, e.g., Brien Alkire, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Elena Danescu, William Fry, D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie Riposo, Timothy William James Smith, and Alexander Stephenson, *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, Santa Monica, Calif.: RAND Corporation, RR-1330-AF, 2016.

[51] Chairman of the Joint Chiefs of Staff, *Joint Lessons Learned Program*, Manual 3150.25B, October 12, 2018.

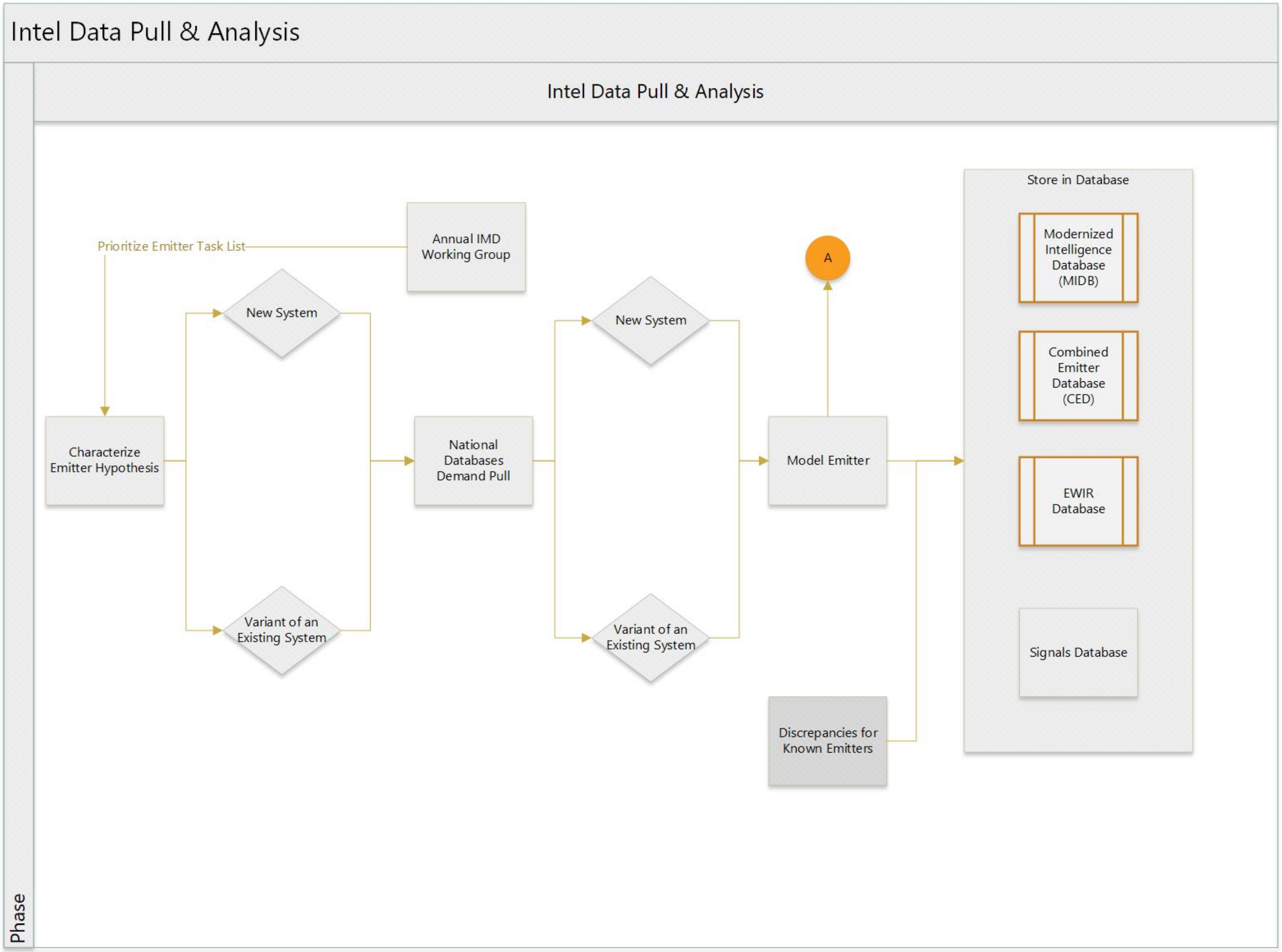
**Figure 2.3. Representation of Collection, Processing, Analysis, and Dissemination and Archiving Steps**


Collect – Process – Analyze – Disseminate & Archive
Collect
Process
A
Z
ISR Collection: Aircraft and Overhead
Data Record from a Sensor (Recording)
Filtering Process
Carrier Frequency Filter (FM/AM Radio, TV)
Standard Radar Format Filter (Square Waves)
Digital Modulation Filter
Signal Detected
Signal Not Detected



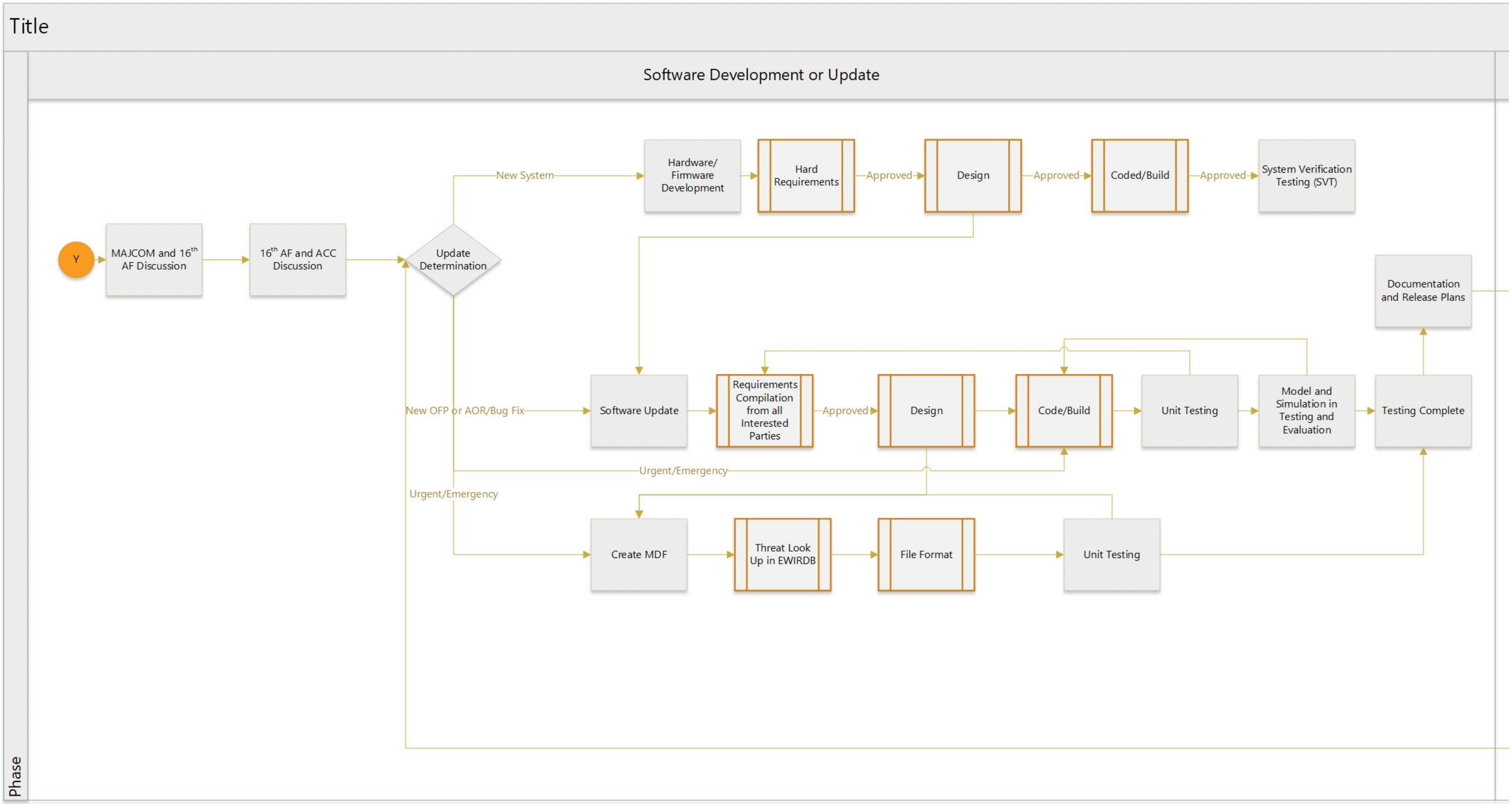
SOURCES: SME interviews and U.S. Air Force Instruction (AFI 10-703; U.S. Air Force, 2017).

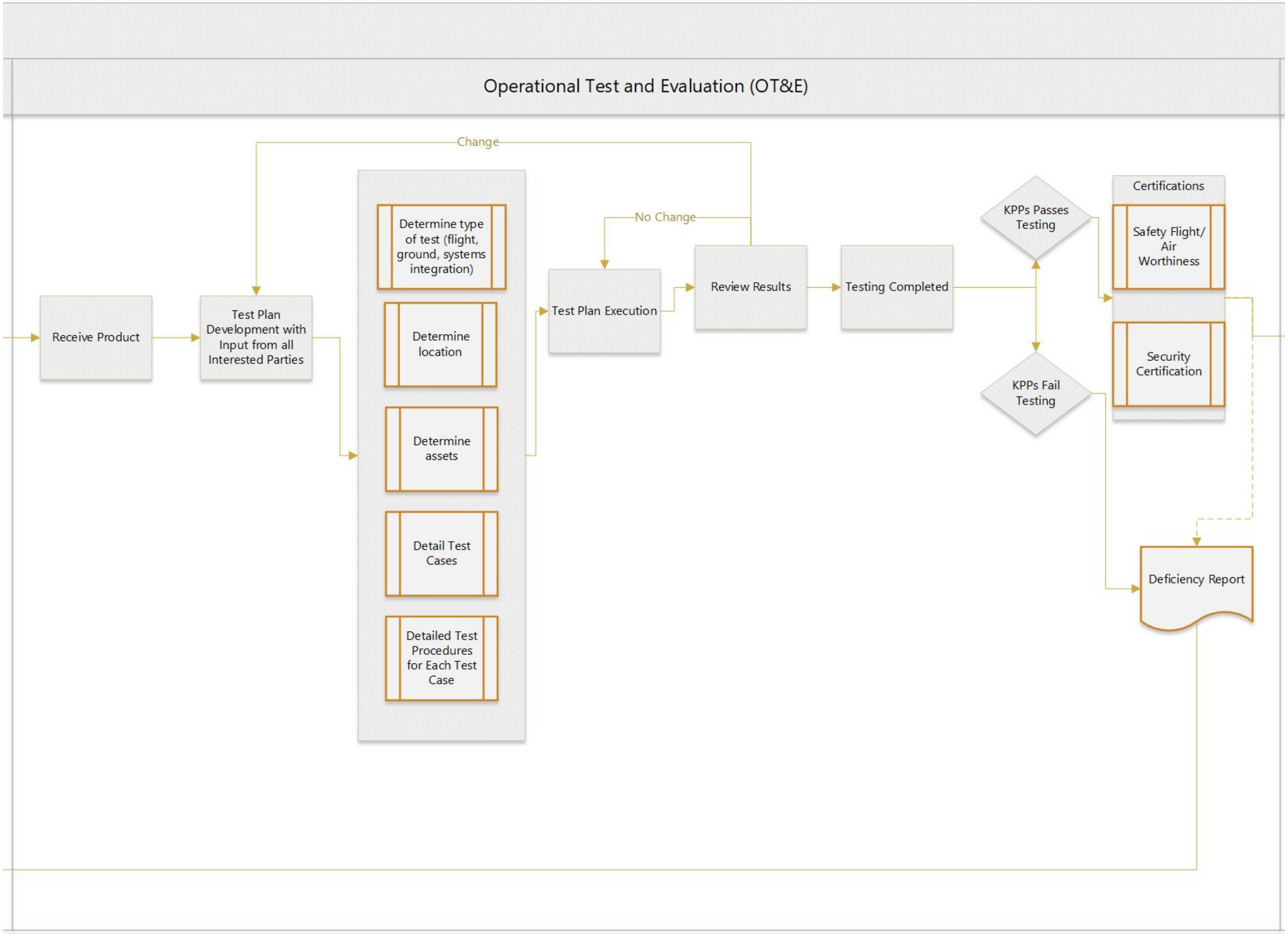
**Figure 2.4. Representation of Intelligence Data Pull and Analysis Step**

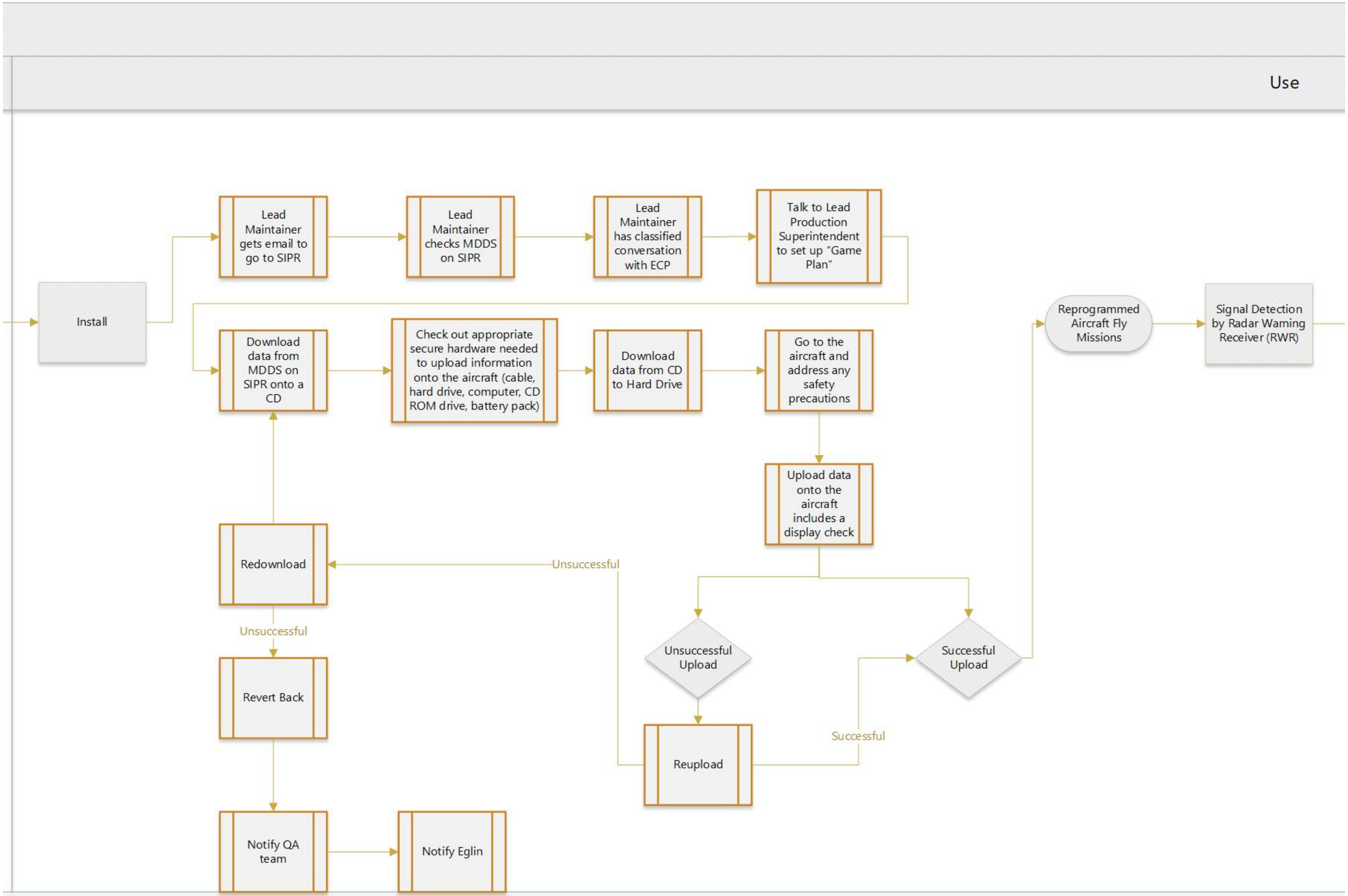

Intel Data Pull & Analysis
Intel Data Pull & Analysis
Phase
Prioritize Emitter Task List
Annual IMD Working Group
Characterize Emitter Hypothesis
New System
Variant of an Existing System
National Databases Demand Pull
New System
Variant of an Existing System
A
Model Emitter
Discrepancies for Known Emitters
Store in Database
Modernized Intelligence Database (MIDB)
Combined Emitter Database (CED)
EWIR Database
Signals Database

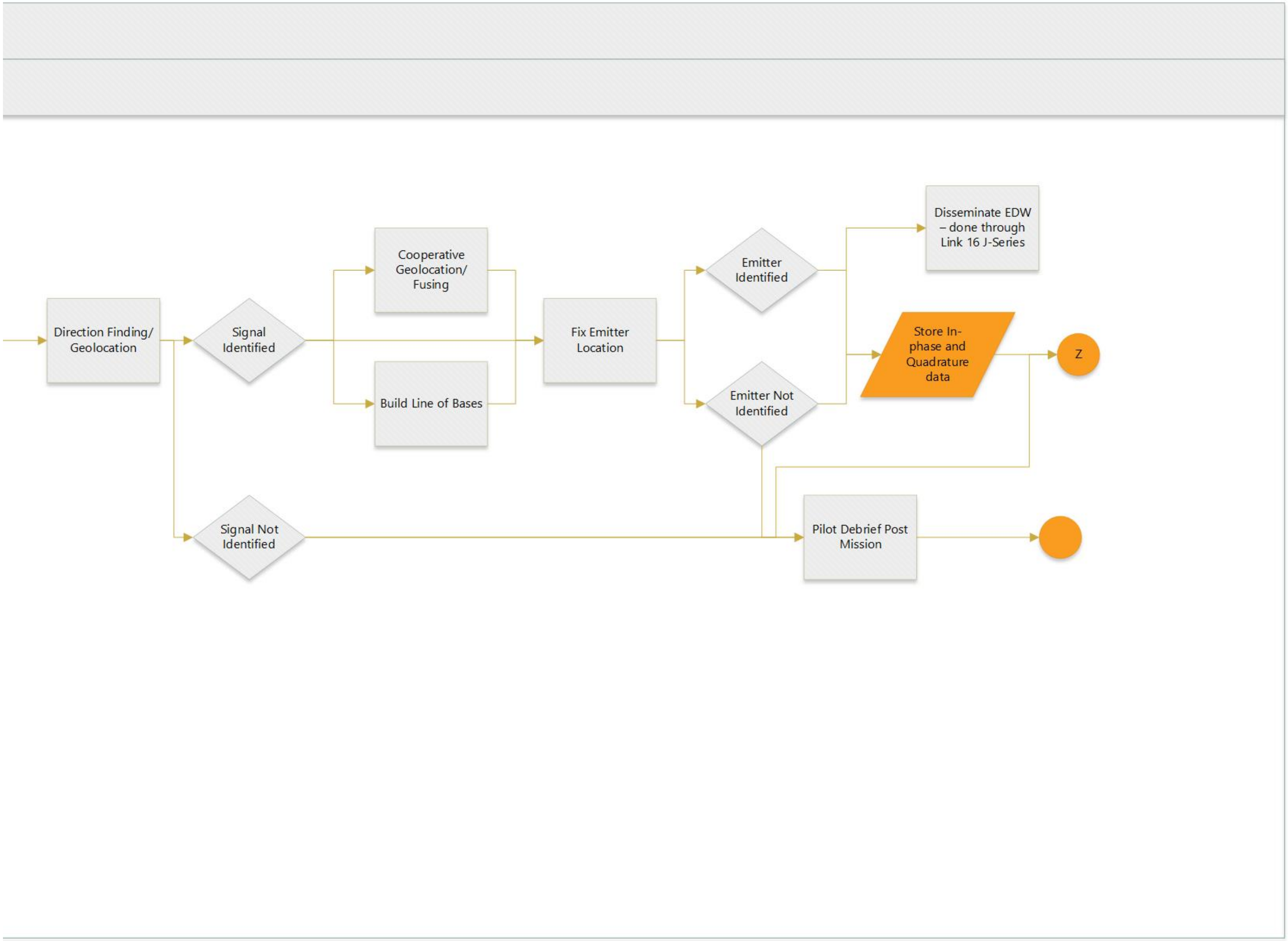
SOURCES: SME interviews and U.S. Air Force Instruction (AFI 10-703; U.S. Air Force, 2017).

**Figure 2.5. Representation of Software Development/Update, Developmental Testing and Operation and Operational Testing and Evaluation, and Use Steps**


Title
Software Development or Update
Phase
Y
MAJCOM and 16th AF Discussion
16th AF and ACC Discussion
Update Determination
New System
Hardware/ Firmware Development
Hard Requirements
Approved
Design
Approved
Coded/Build
Approved
System Verification Testing (SVT)
Documentation and Release Plans
New OFP or AOR/Bug Fix
Software Update
Requirements Compilation from all Interested Parties
Approved
Design
Code/Build
Unit Testing
Model and Simulation in Testing and Evaluation
Testing Complete
Urgent/Emergency
Urgent/Emergency
Create MDF
Threat Look Up in EWIRDB
File Format
Unit Testing


Operational Test and Evaluation (OT&E)
Change
No Change
Receive Product
Test Plan Development with Input from all Interested Parties
Determine type of test (flight, ground, systems integration)
Determine location
Determine assets
Detail Test Cases
Detailed Test Procedures for Each Test Case
Test Plan Execution
Review Results
Testing Completed
KPPs Passes Testing
KPPs Fail Testing
Certifications
Safety Flight/ Air Worthiness
Security Certification
Deficiency Report


Use
Install
Lead Maintainer gets email to go to SIPR
Lead Maintainer checks MDDS on SIPR
Lead Maintainer has classified conversation with ECP
Talk to Lead Production Superintendent to set up "Game Plan"
Download data from MDDS on SIPR onto a CD
Check out appropriate secure hardware needed to upload information onto the aircraft (cable, hard drive, computer, CD ROM drive, battery pack)
Download data from CD to Hard Drive
Go to the aircraft and address any safety precautions
Upload data onto the aircraft includes a display check
Unsuccessful Upload
Successful Upload
Reupload
Successful
Unsuccessful
Redownload
Unsuccessful
Revert Back
Notify QA team
Notify Eglin
Reprogrammed Aircraft Fly Missions
Signal Detection by Radar Warning Receiver (RWR)


Direction Finding/ Geolocation
Signal Identified
Cooperative Geolocation/ Fusing
Build Line of Bases
Fix Emitter Location
Emitter Identified
Emitter Not Identified
Disseminate EDW – done through Link 16 J-Series
Store In-phase and Quadrature data
Z
Signal Not Identified
Pilot Debrief Post Mission

SOURCES: SME interviews and U.S. Air Force Instruction (AFI 10-703; U.S. Air Force, 2017).

Some aspects of *Collection, Processing, Analysis, and Dissemination and Archiving* in Figure 2.3 are among the most completely automated in the current EWIR process, especially in the case of known, unchanging threats. Indeed, if a particular adversary radar or jammer is frequently operational in an area of interest, has a well-characterized waveform based on many years of observation, and is not employing any mechanisms designed to evade detection, then its path will follow the upper part of the diagram from collection and filtering through signal detection, characterization, matching, and record creation and update with relatively little human intervention required. However, this ideal situation is not always the case, and these types of radars and jammers, though important to maintain awareness of, are not the pacing challenge for EWIR because they are so predictable.

Adversary radars and jammers that less frequently or rarely make an appearance (at least to the intelligence assets seeking them out) start slowing the steps in Figure 2.3 right from the beginning with collection. Not only does "the enemy have a vote" in this context, but any available automation of collection designed to detect adversary activity and automatically record it or flag it for an analyst is less likely to work. These more-difficult cases continue to require much more human intervention than the ideal situation because the associated signal that was collected cannot be easily characterized and may lead to the need for more collection (a human decision under most circumstances) and time for human analysts to study and compare the signal of concern to what is known to make a best attempt at identifying it. The records generated from this can also require additional steps because more information is needed when a signal is unknown or otherwise somehow unusual, as opposed to a known case where the detection is updated and verified.

In the *intel data pull and analysis* step illustrated in Figure 2.4, humans are responsible for characterizing an emitter (or changing a known emitter), pulling appropriate data from intelligence databases, modeling the emitter, and entering the newly characterized emitter into another database. Analysts are supported by some basic tools to help flag and extract relevant data and to model threats in a way that enables an RWR or EA system to recognize a threat. However, it is still a human that is manually running software to piece together a picture of each emitter. There is also some variation in how available software-based tools are or how well they work, depending on the specific RWR or EA system in question. This is because each system operates somewhat differently (e.g., the number and types of parameters used to identify adversary radars and jammers) and thus the EWIR solution will be different for each system, which prevents efficiencies that could be gained from applying a single solution to multiple systems.

Finally, the *software development/update, DT&E and OT&E, and use* steps summarized in Figure 2.5 demonstrate how much complexity and human intervention there is even after a proposed EWIR solution is found. First, the process works differently depending on whether the solution has to do with a hardware change (upper part of the diagram), OFP change (middle), or MDF/lookup table adjustment (bottom). Notice the number of approvals and testing required as part of the update design, all requiring a high level of human intervention. OT&E is a critical part of EWIR that is absolutely necessary for safety and effectiveness. There is heavy human involvement in planning tests, conducting tests, and deciding whether the results greenlight an EWIR solution to move forward to deployment. There are points at which a failure will lead to more development and testing, which further slows the process, because it is not unusual for a solution to not entirely work the first time in the operational test phase or in the certification substeps.

Once a change is deemed ready to deploy, a host of substeps are required to make changes on aircraft, starting with alerting maintenance staff at the unit level and creating a plan to conduct the maintenance to deploy new updates. Quite unlike the automated updates that are pushed to computers in a workplace or to smart phones, many of the decisions and procedures are not done behind the scenes or in an automated way. Conducting the necessary safety tests can involve multiple people, decisions, and hours.

With so many heavily manual steps, EWIR cannot be made substantially faster simply by automating a given substep. Doing so would only place additional emphasis on bottlenecks elsewhere. Improving the orchestration of intelligence collection would only cause queues at the emitter characterization substep, the solution computer simulation substep, or other substeps to grow longer. No amount of additional resources to speed test plan development or improve the consistency with which maintainers access updates can chip away at the time it takes to ensure that safety procedures are followed.

Furthermore, even automating individual substeps of the current process wherever possible would fail to reduce the end-to-end process to seconds or minutes. This is because automation cannot solve problems such as a lack of human or computing resources, limited or no access to data, or the impediments posed by regulations or processes external to EWIR.

The bottlenecks associated with the proliferation of manual steps are exacerbated at the enterprise level. The EWIR process must be conducted for every type of platform, and the requisite maintenance must be conducted for each individual aircraft (at least within a given theater). Running the EWIR process at scale in some cases makes bottlenecks worse due to competition over limited resources and the fact that different teams support different platforms. These factors lead to inefficiencies and unevenness in making updates across platforms.[52]

### *Long Security Hardening and Safety Certification Timelines Cannot Be Avoided*

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. As we mentioned earlier, all software and hardware updates require a platform to undergo verifications for software security hardening, safety and airworthiness, and end-to-end regression testing, including modeling and simulation, DT&E, and OT&E. It can take several months to nearly two years to complete these tests on the platform, due to limitations in human and computing resources. We discuss these issues in detail in

[52] Differences in level of mission risk and specialized hardware also contribute to this unevenness in making updates across platforms.

Chapter Six; however, to summarize, current software architecture on platforms lack deployment time modularity even while achieving run time modularity.[53] In other words, a software fix or an update for a single existing or new capability necessitates all the verifications and testing schedules mentioned above. Many USAF weapon systems have proprietary ownership of different systems (and their software) implemented in different development vendor environments and, depending on the platform, undergo system integration before deployment. This exacerbates the issue, as a flight test (DT&E) of an integrated system might reveal stability problems and other deficiencies in the integration environment and would require coordination of fixes and retesting. Testing and certification of MDF updates are much less time intensive but nevertheless take hours to execute and thus will soon reach a similar plateau in terms of how much automating existing EWIR substeps can help speed up the overarching process. Additional software-related issues are discussed in Chapter Six.

### *Lack of Sufficient Computing and Personnel Delay EWIR*

Lack of sufficient computing and personnel often further delay EWIR steps. The technical and policy barriers to creating robust data pipelines are compounded by the mismatch in the number of expert personnel and computing capabilities required to handle data analysis, and subsequent use of IMD and other intelligence, to create software updates as compared with the volume of requirements and data that are ingested into the EWIR process. Resources that are available are not necessarily used efficiently for reasons such as policy changes lagging needs and lack of communication between organizations.

EWIR depends on multiple types of specialized personnel. Some are skilled in ways that directly support steps in the EWIR process. EWIR personnel include ELINT analysts, threat experts, engineers that specialize in RWR software, and maintainers for particular platforms. Other important personnel, more generally, manage the EWIR process, requirements development, and employment of capabilities that depend on EWIR. This is a very wide-ranging group, but Electronic Warfare Officers are particularly central for guiding the planning and execution of many aspects of operating in the EMS. Another general skill that is increasingly relevant to software- and data-heavy areas such as EWIR is familiarity with programming and data science.[54]

[53] Run time modularity is a software design paradigm in which separate functions are designed and implemented as modules that the platform or the system is able to run independently by using the required resources, interfaces, and dependencies for each module. Additionally, the platform is designed to ensure that modules only interact with other modules based on well-defined dependencies and do not interact or interfere with other modules in the platform. Deployment time modularity adds the additional requirement that the software of a platform should be designed as separate single deployable and maintainable entities, usually specific to some function or groups of related functions of the platform. Such deployable units or entities are packaged along with their dependencies. This allows these single entities to behave consistently across various development or integration environments. This means that additions of new capabilities or updates to existing capabilities would be supported without disturbing the existing functioning of the platform software.

[54] Software programming and data science and engineering are specialized skills. However, the USAF would benefit from having or training personnel with a basic working understanding of how to employ them.

There is a dearth of analysis available on how many people with the right skill sets are needed to support EWIR and how this could change if EWIR is transformed as we describe in Chapter Three. However, our interviews suggest a general concern that there are too few specialized personnel in areas such as those introduced above. Too few people are trained to do different types of specialized work, and those that are may not be retained—they frequently move to new assignments, retire, or separate from the military.

Furthermore, those with specialized training may not be in roles that maximize the use of specialized skills. This is especially true for officers, whose career development focuses on broadening skills as opposed to specialization. In some cases, the basic training could be right, but personnel lack the experience to apply it in the right context. Additionally, even with new software delivery paradigms, such as those currently being implemented by USAF software factories, these development initiatives and skill sets are still being applied to ground-based and infrastructure components and not to software for weapon systems and platforms. Involving personnel and skill sets from software factories to collaborate with USAF software engineering groups to develop a breadth of experience—across different platforms, with multiple sources of intelligence, and varied architectures—is required.

Having too few personnel, or at least too few with the right skills or experience and in the right roles, can lead to additional slowdowns in the EWIR process. Data and software updates wait in the queue until someone can get to them. Consider the EWIR database as an example. Although the very few highest-priority database entries (e.g., sudden changes to the most dangerous threats) could be turned around very quickly, it is not surprising that some intelligence updates wait months or more to become available through the EWIR database.[55]

Another example is the limited number of experienced intelligence personnel within flying units. Having an up-to-date and nuanced understanding of intelligence is key for anticipating needs, understanding when software updates may become available, and understanding whether the software is working as it should. Flying units tend to have more-junior intelligence personnel and very few of them (if any). Furthermore, these personnel tend to lack access to many key intelligence databases.[56]

It is not clear that all the requirements even make it into the system because there may be too few intelligence experts, EW officers, and other personnel with the requisite knowledge to recognize what current and potential future needs are. Opportunities to leverage an airman's peripheral skills, to capitalize on cross-platform similarities, or to modify approaches for an airborne environment to increase EWIR process efficiency can easily be missed.

In addition, the limited availability of testing equipment, including computers, causes both OFP and MDF updates to sit in a queue. Computer simulations are used extensively for developing and testing new threat models. Not only is the availability of hardware itself limited, but the lack of recent hardware upgrades also means that the processing speed is relatively

[55] Interview with 772 Test Squadron staff members, November 4, 2020.

[56] Interview with EW expert, United States Air Forces Europe, February 4, 2021; interview with F-16 maintenance staff member, United States Air Forces Europe, March 3, 2021.

slow.[57] This serves to exacerbate some of the broader challenges with OT&E in the EMS, in which it can be very difficult to simulate the impacts or complexity of threats effectively and many hours are needed to meet reliability thresholds.[58]

### *Limited Communication of Requirements and Context Could Inhibit Update Quality*

Communicating requirements are pervasive in creating bottlenecks throughout the EWIR process. There are several requirements-related problems that impact different aspects of the status quo.

First, the identification and articulation of new requirements for EWIR is irregular and dependent on individuals and the health of their professional networks. Typically, someone working with or adjacent to reprogramming teams, or at the flying units, will notice a potential change in the threat environment (e.g., through an unidentified emitter). This need must then be communicated and vetted through the broader Air Combat Command (ACC) organization; those most likely to identify the need do not necessarily have the authority to immediately act on it. Naturally, vetting and coordination is important, but the lack of streamlining could cause both delays and unevenness in quality.

Second, intelligence requirements are separate from requirements that drive reprogramming. There are several issues here, ranging from end users not understanding the process for submitting a requirement to inefficient prioritization and management of collection and assessment of collection to determine whether needs are met.[59] Thus, there is great potential for problems in syncing needs for additional IMD with those for new software updates.

Third, there is currently little enterprise-level assessment of readiness for EMS operations, which would include the timeliness, availability, and quality of EWIR. For example, SMEs report that there is currently no USAF method for reporting or grading EW readiness through the Defense Readiness Reporting System (home station health of mission), USAF Air Expeditionary Force Reporting Tool (deployment-capable health of mission), and Status of Resources and Training System (unit-level self-reporting on skill-level progress and upgrades). However, the recently established Combat Shield program focuses on USAF EW assessment[60] and has great

[57] SME interview, March 5, 2021.

[58] Gilmore, 2011.

[59] This is an extensive subject of study. See, for example, Abbie Tingstad, Dahlia Anne Goldfeld, Lance Menthe, Robert A. Guffey, Zachary Haldeman, Krista Langeland, Amado Cordova, Elizabeth M. Waina, and Balys Gintautas, *Assessing the Value of Intelligence Collected by U.S. Air Force Airborne Intelligence, Surveillance, and Reconnaissance Platforms*, Santa Monica, Calif.: RAND Corporation, RR-2742-AF, 2021; Cynthia R. Cook, David Luckey, Bradley Knopp, Yuliya Shokh, Karen M. Sudkamp, Don Casler, Yousuf Abdelfatah, and Hilary Reininger, *Improving Intelligence Support to the Future Warfighter: Acquisition for the Contested Environment*, Santa Monica, Calif.: RAND Corporation, RR-A537-1, 2021; and Bradley Knopp, David Luckey, and Yuliya Shokh, *Documenting Intelligence Mission-Data Production Requirements: How the U.S. Department of Defense Can Improve Efficiency and Effectiveness by Streamlining the Production Requirement Process*, Santa Monica, Calif.: RAND Corporation, RR-A241-1, 2021.

[60] 87th EWS mission briefing, April 29, 2021.

potential to expand its scope or inspire a spinoff program that could focus directly on IMD and EWIR.

Fourth, there is also an issue of communication at the tail end of the EWIR process. Personnel at flying units have to pull updates after receiving a generic push notification and help make an assessment of whether the update applies to their theater and platform. This makes update timeliness partially dependent on their network access on any given day and on their experience.

### *Restrictions on Data Recording, Storage, and Sharing Inhibit Data Pipelines*

Without continuous access to all the relevant data, there may be aspects of threats that are missed, leading to problems with accurate identifications. Just getting to the point of being able to get data (i.e., being at the right place at the right time) can be time consuming, and this is compounded by policies, contracts (e.g., vendor lock-ins[61]), and technological means required to extract data collected by some sensors which may just happen to have capitalized on a rare opportunity to gather the right data. Although initial intelligence assessments can be made quickly (and indeed sometimes are made on the fly), the production of verified and precise threat characteristics that can be published and widely used in the relevant communities takes much longer because of the important operational and tactical risks of having faulty data.

This is compounded by the fact that ISR platforms that can collect IMD are limited in availability and lack features that would enable them to fly close to threats during conflicts. These factors prohibit a proliferation of ISR platforms from gathering data that accurately reflect how adversary capabilities are being used in wartime. Thus, there is an emerging need to incorporate data collected from sensors (e.g., RWRs) on non-ISR platforms, especially those that are expected to operate in close proximity to threats.

However, it is difficult to pipe data from most platforms that carry EMS-related sensing equipment to relevant SIGINT databases. Specific issues vary by platform but may include one or more of the following:

- lack of data recording technology
- lack of storage capacity or practice in place to store data
- access limitations due to data ownership rights in contracts
- access limitations due to classification
- lack of requirements for data-sharing
- lack of procedures in place for data-sharing.

These types of issues result in unaccounted-for data or data that are known but not accessible. Unaccounted-for data can include information that remains undocumented or unrecorded by transport and other aircraft that historically have no role in contributing to a common intelligence picture but in the quest for more data could become part of an ecosystem. Inaccessible data come

[61] *Vendor lock-ins* are contractual rules by which the commercial provider controls or otherwise limits access to data gathered by the platform.

from platforms that heavily collect and use data, such as fifth-generation fighter aircraft, but for which there are multiple barriers to making these data discoverable to the broader community who might use them.

Generally speaking, the types of problems encountered when trying to make a greater variety of (especially SIGINT) data available for EWIR include restrictive classification and stovepiping. Restrictive classification is necessary for protecting U.S. national security. However, this also means that both the rules for determining classification and the culture of working in classified environments restricts the flow of data, even when data-sharing would be potentially beneficial. This issue cannot necessarily be changed, although classification policies and procedures can be reviewed. However, it is important to recognize that there is a trade-off between classification and availability of data. More-recent approaches to data security—involving permissions at the level of data as opposed to a network—can help in limiting classification-related issues by preventing lower classification data being swept into a more classified (and hence overly restricted) environment.

Stovepiping can be related to restrictive classification but can also simply result from contractual agreements with a vendor as well as historical organizational structures and culture.[62] In many cases, vendors control data collected by a platform. If some aspects of data-sharing are not included in the agreement between the vendor and the USAF, then data are bound to remain "dark" for any USAF applications. Furthermore, there are important policy and procedural boundaries between ISR aircraft and combat or other aircraft that limit the use of data collected by the latter for intelligence purposes. Principal among these boundaries are those interpreted on the basis of the United States Code, which outlines the respective roles of the armed forces and intelligence (Title 10, Title 50[63]). Finally, data access policies tend to assume that users do not have a need to see or use data unless permission is explicitly sought or access is tied to a particular role the user is assuming. These policies are necessary for protecting data but also contribute to stovepiping by only permitting access as needed as opposed to assuming that data have wide usability and only restricting access if this is proven otherwise.

## Conclusion

In this chapter, we have discussed the challenges that the EWIR enterprise faces as adversaries become more agile and the EMS environment becomes more important to military operations. We have further illustrated the current EWIR process and surveyed five key lessons demonstrating why the current EWIR process is not well suited to address the most challenging future requirements. The current EWIR process lags for various reasons at every step summarized in Figure 2.1. In particular, the "heaviness" of the process due to the numerous

[62] James B. Bruce, Sina Beaghley, and W. George Jameson, *Secrecy in U.S. National Security: Why A Paradigm Shift Is Needed*, Santa Monica, Calif.: RAND Corporation, PE-305-OSD, 2018.

[63] See, for example, U.S. Code, Title 10, Armed Forces, 1956, and U.S. Code, Title 50, War and National Defense, 1947.

manual steps, extensive OT&E and certification processes, lack of personnel and computing resources, limited requirements communication, and feeble data pipelines cause extensive slowdowns and, in some cases, may also inhibit quality and security.

However, this analysis does not necessarily mean that the current EWIR process is not responsive or appropriate for some software reprogramming needs, at least in the near term, as described earlier in this chapter. The current EWIR process could continue to meet needs for baseline shifts in intelligence about threats (generally legacy systems) that are not expected to adapt very quickly. In fact, prioritizing situations that require the fastest updates will help implement the incremental changes that we discuss in subsequent chapters; wholesale changes across the board and all at once would not only be expensive and disruptive to current operations but also would be unachievable. In the next chapter, we turn to a vision for transforming the EWIR process, bearing in mind that there is still benefit and functionality in the current process that will be key to maintain in order to enable a gradual transition and (in some format) to support more-autonomous capabilities.

# Chapter 3. A Vision for Future EWIR

Over the years, the USAF, in some cases with IC and Joint partners, has taken steps to fix specific problems within the EWIR enterprise. Automating certain tasks and upgrading data storage are worthy improvements, and these types of efforts can continue to bridge some of the gaps in generating software updates based on insights from intelligence. Although this research project did not explicitly evaluate any of these efforts, we note some examples here to emphasize that effort has been and is being undertaken to resolve some of the problems identified in Chapter Two, though none encompass all of the issues.

One very important shift was the redesign of the EWIR database[64] to diversify available data fields, maintain standardized data formats, and better support computer simulation.[65] The SPECTRE tool suite is supporting the work of organizations such as the 36th EWS in pulling in key intelligence data and developing threat models that ultimately form the basis for software reprogramming.[66] The Next Generation EW Environment Generator is a development that has supported testing needs across the board for EW-related needs.[67] Most recently, the newly established 350th SWW has worked with partners to establish options for software-based approaches to conducting EMSO. Although the USAF is working on reducing software update timelines by implementing continuous software delivery and deployment pipelines, this practice has not yet become commonplace.[68]

Some component organizations have also experimented with automation and other forms of innovation for years. For example, the 453rd EWS has a history of internal tool development made possible by a small contingent of engineers and information technology experts.[69] These tools help the squadron conduct day-to-day tasks such as detecting changes in threats. The use of mission data generators has helped to automate and speed up aspects of MDF updates by the 36th Electronic Warfare Group (EWG) for some time.[70] Other services are also looking at the

[64] The EWIR database is sometimes referred to as NGES: Next-Generation EW Integrated Reprogramming Database System.

[65] NASIC and Missile and Space Intelligence Center (MSIC) SMEs, interview via Microsoft Teams with Abbie Tingstad, Padmaja Vedula, and Lance Menthe, May 24, 2021.

[66] USAF, *Air Force Doctrine Publication (AFDP) 3-51: Electromagnetic Warfare and Electromagnetic Spectrum Operations*, July 30, 2019e; USAF, *Air Force Doctrine Publication (AFDP) 3-51: Electromagnetic Spectrum Support Activities*, July 30, 2019d; and 36th Electronic Warfare Squadron (EWS) SME, interview via Microsoft Teams with Abbie Tingstad and Padmaja Vedula, March 5, 2021.

[67] Gilmore, 2011.

[68] Modern software development processes that automate security hardening and verification processes are a goal of USAF's Platform Air Force "One" initiatives. See USAF, undated-a. Commercial software companies that employ similar practices are able to deliver code within hours of when a developer makes the necessary code modifications.

[69] 453rd EWS SME, interview via Microsoft Teams with Abbie Tingstad and Padmaja Vedula, March 24, 2021.

[70] 36th EWS, March 5, 2021.

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.[71]

For the long term, however, our research suggests that more fundamental changes are needed to address the urgent problem of continuing to be competitive and capable in EMS operations. Learning from the lessons presented in Chapter Two—in other words, taking action to rectify the problems they illuminate—requires a comprehensive rethinking of how EWIR works and even what it is. Gaining and maintaining advantage in the EMS will require flexibility and survivability to stay ahead of threats that are increasingly designed to be evasive and lethal.

## From Lessons to Actions: Overarching Vision for Improving EWIR

One way to address the challenges and lessons articulated in Chapter Two is to build a cognitive EW capability that enables systems to leverage ML algorithms to learn, reprogram, adapt, and effectively counter threats in flight. Whereas the bulk of the current EWIR process takes place *off* the aircraft and *after* the mission, building toward a cognitive EW capability would help enable a significant portion of what is currently known as the EWIR process to take place *on* the aircraft *in real time*, first by utilizing basic algorithms that can execute complex preset instructions to identify adversary capabilities (referred to as *adaptive EW* below), and later by using ML on the aircraft to figure out novel or rapidly changing adversary capabilities and how to respond to them without preset instructions (referred to as *cognitive EW* below).

As we demonstrate over the next several chapters, achieving a cognitive EW future requires dramatically different technological foundations than what the EWIR enterprise, or much of the broader USAF, can support today. Indeed, both DoD as a whole and the USAF itself have several initiatives (e.g., the System of Systems [SoS] Technology Integration Tool Chain for Heterogeneous Electronic Systems–STICHES,[72] DoD's Center of Excellence in Artificial Intelligence and Machine Learning at Howard University,[73] and USAF's Platform One[74]) underway with goals that align with the vision described here even if these are not mature or scaled to the level of being common practice. However, making such changes does not imply that the current EWIR process—at least in some form—is no longer needed. Not only does there need to be a capability in place to support a transition toward a cognitive future, but leveraging ML will also require substantial support for algorithm development (as we describe in Chapter Four), as well as a less computation-intensive option for software updates that lack urgency to conserve resources.

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

[72] Evan Fortunato, "Stitches: SoS Technology Integration Tool Chain for Heterogeneous Electronic Systems," Apogee Research, Abstract #18869, undated.

[73] Office of the Under Secretary of Defense for Research and Engineering, "DoD Launches Center of Excellence in Artificial Intelligence and Machine Learning at Howard University," January 28, 2021.

[74] Office of the Under Secretary of Defense for Research and Engineering, 2021; USAF, Office of the Chief Software Officer, "Software Ecosystem Innovation Hubs—One Platform," webpage, undated-b.

To move toward a vision of real-time, autonomous reprogramming, several steps are required in the near term to address immediate problems while investing in the fundamental enhancements for more far-reaching changes in the long term. Here, we first articulate this vision and its component steps (Figure 3.1) and then describe some specific actions to help meet this vision and address lessons identified from the current EWIR process. We start with step 1 of the vision, which articulates the concept that some factors that impact the current EWIR process will remain constraints in the future; improvements described later in this report should be made with this assumption.

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

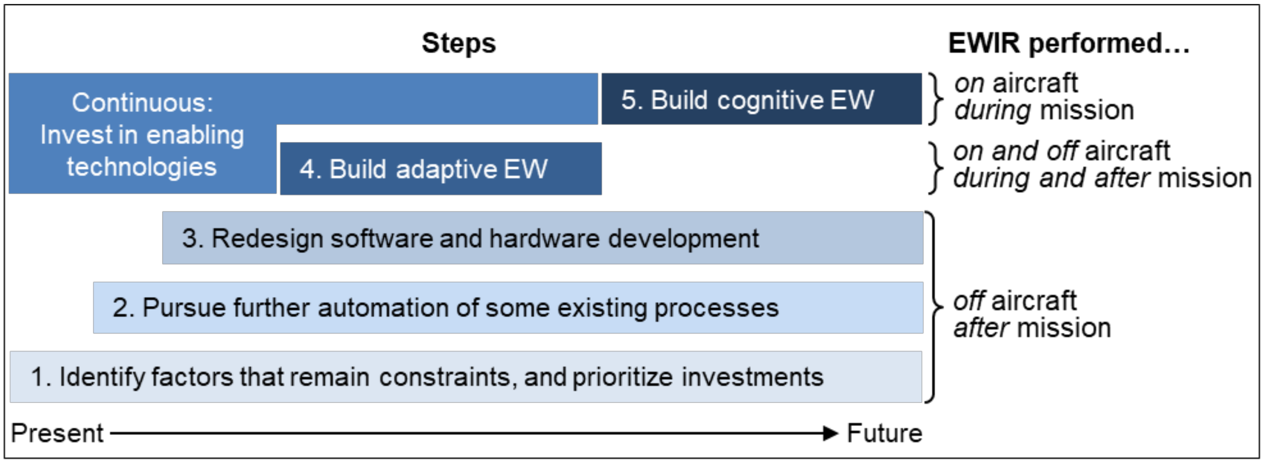
In the near term, not all slower processes need to be considered priority obstacles. Some are important constraints that may require solutions but not under reprogramming initiatives because responsibilities for them fall well outside of the EW community. Consider, for example, the necessary months or 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 is 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.

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, because of 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, it may enable subsequent software deliveries to be installed over the network. Even then, there will be necessary operational precautions that must be taken.[75] Careful scheduling of software deployment onto the platforms to avoid adverse operational impacts will always be critical.

EWIR improvements discussed later on in this report should assume that some constraints may remain in place, or at least that there are reprogramming-relevant problems that are or should be handled by organizations outside of the reprogramming community. This assumption will shape how improvements are designed and investments are prioritized and may imply strategic partnerships (e.g., between the USAF and the IC).

[75] We have to note that not all software needs to be delivered over networks or to airborne platforms. The need is more for ensuring that software deployment architectures mitigate the need for extensive safety certifications and end-to-end regression testing, thereby enabling faster software and capability deployments.

**Figure 3.1. Vision for Improving USAF EWIR Enterprise**


Steps
EWIR performed…
Continuous: Invest in enabling technologies
5. Build cognitive EW
on aircraft during mission
4. Build adaptive EW
on and off aircraft during and after mission
3. Redesign software and hardware development
2. Pursue further automation of some existing processes
off aircraft after mission
1. Identify factors that remain constraints, and prioritize investments
Present
Future

### *Step 2. Pursue Further 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 are employing other means of evasion or when making preparation for wartime during peacetime. Further automation will also support the building of software and ML models for better sensing of advanced threats.

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) is 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 *crowdsourcing data*, which adds hardware both on the combat platforms and on the ground to enable rapid data capture and dissemination.[76] In addition to having a near-term benefit, the ability to rapidly get data into the pipeline contributes to the vision for cognitive EW described below.

Near-term automation of less relevance for 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 from when a new threat is detected to when the deployed fleet of aircraft have 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

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

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 a part of the process that currently takes months to the order of days*.

Furthermore, the current EWIR process contains some substeps that are not amenable to automation and cannot be skipped in favor of faster updates. Safety measures conducted by maintenance prior to uploading new software are a good example of this. The only way to avoid the handful of hours it takes to remove certain equipment prior to a software update and then emplace it again afterward is to use containerization of software so that the software being updated does not touch the software controlling the hazardous equipment that must be removed. This goes beyond automating individual substeps of the current process and is a key element to developing an adaptive and cognitive capability, as we describe in detail in Chapter Six.

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

As described in Chapter Two, 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 process in its current format. To keep the EWIR enterprise competitive, the USAF will need far-reaching capability enhancements such as adaptive (step 4) and cognitive (step 5) EW capabilities described below. Before moving to those steps, however, the USAF should redesign the software and hardware development processes to address the near-term issues of software deployment speeds and the hardware needed to support emerging deployment architectures. Without these processes already in place, the changes in steps 4 and 5 below cannot be operationalized.

Current legacy platforms have individual avionics subsystems with dedicated mission computers and OFPs. The design and development of the OFP suite is either partly owned by the USAF or has proprietary hardware, software, and OFPs supplied by various vendors for each subsystem. An EW suite or an individual EW subsystem, for example, could be supplied by one or more vendors. Even for fifth-generation platforms with integrated avionics architectures, various operational modules could still be provided by different vendors and the system OFP(s) need to be integrated for every update. Additionally, many platforms have software written in legacy languages and are not hardware agnostic.

As described in Chapter Two, one of the major bottlenecks for fielding new or upgraded EW capability is the long timelines 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. Hence, 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 addition of what is termed a *test harness* may reduce the overall process timelines.[77] 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.

An immediate threefold approach is needed to increase the agility of EW-related avionics development and deployment in order to make platforms ready to support scalable modular architectures that would allow faster software updates:

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 in which information regarding threat identification and the system's use of the EMS must be consistently and immediately distributed among all systems involved.

Because of the rapidly changing EW threat environment, platform avionics not only have to support the faster fielding of EWIR but should also 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, that supports regular updates and run time fault and failure tolerance. One way to minimize the total computing resources required is to provide for autoscaling 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 SWaP is another important priority to support processing overheads of new software deployment and cloud orchestration tools (see Chapter Six) to improve the speed of today's EWIR and to provide critical infrastructure for adaptive—and, ultimately, cognitive—capabilities in the future. Implementing new software deployment architectures and enabling supporting tools via hardware upgrades would be the first step to creating a development and integration pipeline for faster deployments, employing what is called development, security, and operations

[77] 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.

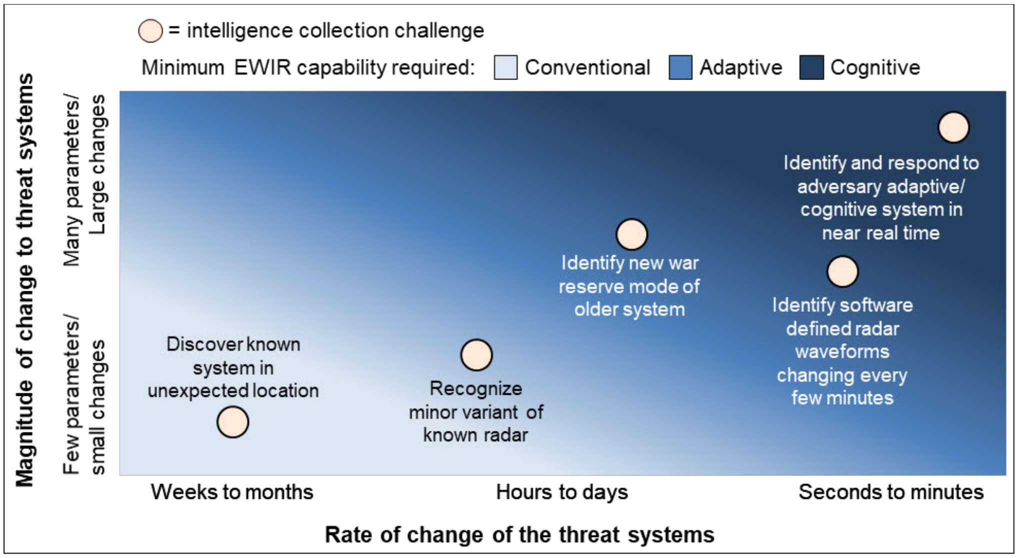
(DevSecOps)—a development and integration pipeline incorporating security as a part of the cycle.

### *Step 4. Build an Adaptive EW Capability*

As described above, adaptive EW capability uses advanced algorithms to execute preset instructions onboard the aircraft (beyond the basic threat library lookup that is provided by an MDF) to identify changes to adversary systems based on preprogrammed human-in-the-loop rules. Instead of using a single lookup table, adaptive EW systems would use a complex decision tree that anticipates possible variations in threat behavior and allows for extrapolation. In this construct, algorithms would enable the recognition of small variations in systems, or systems in unexpected locations, and would modify the interpretation of sensed information for the pilot or other decisionmakers.

The key advantage of adaptive EW is that it would allow the USAF to keep pace with a wider range of adversary capabilities than it can today, even if somewhat less capable (from a speed and automation standpoint) than cognitive EW (which we describe next), as illustrated in Figure 3.2. In this figure, 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. Whereas current (conventional) EWIR capabilities are good at detecting small changes over long timescales (such as discovering known systems operating in unexpected locations), a rules-enabled adaptive capability would be able to identify software-defined waveforms that change every few minutes or waveforms that have never been seen on known systems. An adaptive system can also adjust radar and communications waveforms in response to adversary jamming and EM suppression measures. In other words, adaptive EW will be able to keep up with faster and more-complex changes than current capabilities.

**Figure 3.2. Minimum EWIR Capability Needed for Intelligence Collection Challenges**



A precursor to truly adaptive EW that can be achieved already is the use of in-flight MDF updates, which essentially simulate (with intensive manual processes) a minimal capability that an adaptive system should be able to achieve. Additional progress toward adaptive capabilities in the near term can be achieved, for example, by creating a layer of lightweight service-specific applications (apps) that have been developed or are under development by the USAF. These apps would interface with existing OFPs[78] and could execute some adaptive EW functionality by enabling the employment of smart systems operating based on preprogrammed rules. As we describe in Chapter Four, such an approach would still present some important limitations; however, these could be overcome by changes to OFP software deployment architecture and management described in Chapter Six.

Despite offering improvement over current capabilities, however, even the most capable adaptive systems would still be only as good as the logic programmed into them by humans on the ground prior to the mission. To cope with adversary systems that can switch nimbly between waveforms in real time or use no fixed waveform at all 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.

### *Step 5. Build a Cognitive EW Capability*

Cognitive systems would employ artificial intelligence (AI) and ML on an aircraft to assess novel or rapidly changing adversary capabilities and develop countermeasures, without preset instructions in real time. Such systems are designed to adapt based on learned experience rather than predefined rules. A cognitive EW system would be able to enter an environment without knowledge of the adversary systems, learn those systems, and rapidly devise countermeasures against them. Cognitive systems can also recognize threats by behavior over time—e.g., how and when threats 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. 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. A cognitive system can

[78] 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 that make this approach unappealing 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 retesting 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 testing and recertification will still need to occur.
2) App software that is supported by older OFPs (even if that OFP is designed to be modular) remains a relatively heavy and brittle solution, rendering the prospect for cognitive EW at scale very unlikely.

effectively act like a ride-along intelligence analyst who 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 changes to an emitter, such as rapidly changing software defined waveforms or even an adversary adaptive or cognitive system, as indicated in the upper right of Figure 3.2. We discuss the operationalization of cognitive EW in greater detail in Chapter Four.

## DOTMLPF-P Considerations Needed to Support Future EWIR Vision

The vision, as laid out in Figure 3.1 and discussed above, has implications for every aspect of DOTMLPF-P, a DoD framework and approach associated with the Joint Capabilities Integration Development System.[79] Table 3.1 illustrates at a cursory level some of the changes within DOTMLPF-P that are implied by the future EWIR vision described above and that are needed to address lessons identified in Chapter Two. This table was derived by compiling insights from interviews (Appendix A) and PAF team knowledge of USAF organizations and processes. We organize these changes based on the lessons from Chapter Two and further describe them in what follows, noting that information on some aspects is more detailed than others and not all of what we discuss here results in a recommendation because of differences in the depth to which we were able to investigate various topics. This DOTMLPF-P exercise represents a compilation of information gathered early in the research that was used to winnow down topics (primarily materiel) that we focused on for the remainder of this report and undoubtedly omits some important aspects of any future reprogramming capability. We start with an overview of some fundamental materiel changes needed to realize a cognitive EW vision and address the lessons from the current EWIR process before moving on to some examples of other types of changes that go hand in hand with technological modernization to support future operations in the EMS.

[79] Defense Acquisition University, "DOTmLPF-P Analysis," webpage, undated.

Table 3.1. Summary of Selected DOTMLPF-P Implications of Future EWIR Vision

| Lesson | Proliferation of manual steps limits process improvements from discontinuous or stopgap solutions | Long security hardening and safety certification timelines cannot be avoided with current software architectures | Lack of sufficient computing and personnel often further delay EWIR steps | Limited communication of requirements and context could inhibit update quality | Restrictions on data recording, storage, and sharing inhibit data pipelines |
|---|---|---|---|---|---|
| **DOTMLPF-P Implications** | | | | | |
| **Doctrine** | Create doctrine for advanced (adaptive and cognitive) EW concepts | Update AFI 10-703 to specify when in-flight MDF updates (near term) and advanced EW concepts (long term) can be used, along with procedures to follow | Introduce concept of a minimum viable EWIR product and standards into doctrine | Explicitly include roles and responsibilities for communicating requirements in AFI 10-703 | Examine ways in which doctrine changes could help break down data stovepipes between ISR and combat communities |
| **Organization** | Set conditions for 350th Wing to serve as focal point for USAF advanced EW concepts | House a suborganization within the 350th Wing to enable experimentation and development of a minimum viable product for adaptive/cognitive solutions | — | Set up capability within 350th Wing to maintain visibility on requirements to enable coordinated troubleshooting as needed | — |
| **Training** | Review training needs across personnel with role in reprogramming | — | Train additional personnel and expose people to different systems | Allow some personnel (e.g., software programmers, EW officers) to train on more than one system | Encourage more live training opportunities that experiment with data from multiple sources |
| **Materiel** | Invest in technological foundations to support advanced EW concepts (algorithm development, containerized software, hardware upgrades, and cloud-enabled data pipelines) | Create foundations for and use containerized software for current and next-generation platforms; include legacy platforms if service life is expected to continue for > 10 years | Upgrade computing hardware, including that to enable edge cloud services and ML applications | — | Invest in technologies needed to record, store, and transfer data |

| Lesson | Proliferation of manual steps limits process improvements from discontinuous or stopgap solutions | Long security hardening and safety certification timelines cannot be avoided with current software architectures | Lack of sufficient computing and personnel often further delay EWIR steps | Limited communication of requirements and context could inhibit update quality | Restrictions on data recording, storage, and sharing inhibit data pipelines |
|---|---|---|---|---|---|
| **DOTMLPF-P Implications** | | | | | |
| **Leadership** | Articulate a consistent message supporting a paradigm shift toward advanced EW concepts while recognizing the need for maintaining aspects of current EWIR | Develop and enforce mechanisms to encourage shifts toward updated software architectures and upgraded hardware | — | Review authorities to submit requirements; ensure that the highest-priority EWIR requirements for both intel and software updates are being submitted by the highest-priority office | Coordinate with other leaders to pave the way for improved data sharing |
| **Personnel** | Assess needs for new skill sets and establish means of tracking airmen with AI and software skills across disciplines | | | Continue to develop the pipeline for growing EW officers, which are needed for various EW platforms and also to advise and plan within air components | Review and expand personnel access to different data sources—for example, by ensuring timely access to networks and databases |
| **Facilities** | Designate appropriate spaces within 350th Wing and flying units to develop (e.g., via experimentation) or apply (e.g., through maintenance) advanced EW concepts | | | — | Invest in facilities needed to support edge cloud architecture |
| **Policy** | Focus on integrated investments, rather than discrete programs of record, to acquire advanced EW capabilities | Update test, evaluation, and certification processes for situations in which in-flight MDF updates or advanced EW concepts are being used | More-explicitly report metrics for personnel and computing resources to make problems more visible | Review whether current prioritization schemes inhibit more-rapid reprogramming and investigate whether any necessary policy changes can be made | Work with USAF, Joint, and IC partners to enable improved data-sharing, particularly at the edge |

SOURCES: SME interviews (Appendix A) and RAND analysis.

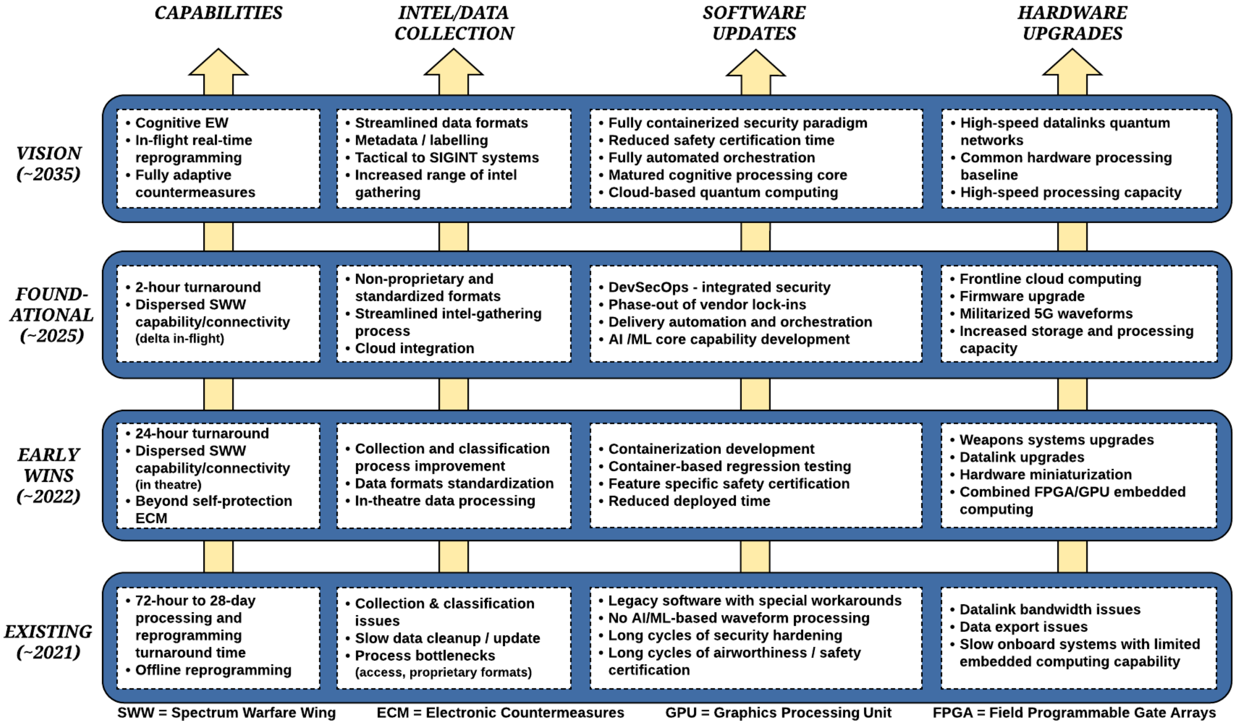
### *Materiel*

The five-step future EWIR vision walked through earlier in this chapter is multidimensional, but this research emphasizes the materiel aspects of getting there because technological change is what is needed to shape the overall envisioned outcome. Ultimately, making reprogramming much faster requires substantial automation. However, as we have argued, it is not sufficient to automate individual substeps within the existing process, because many bottlenecks exist. A slowdown in one part of the process will simply be shifted elsewhere if a piecemeal approach is used. Thus, the process must be redesigned with end-to-end automation in mind, with human support especially on the front end in guiding foundational intelligence activities and supporting algorithm development.

There are four fundamental, parallel materiel transformations needed to realize cognitive EW, which is, for the foreseeable future, the ultimate solution for automating reprogramming in real time. To guide our understanding of technological changes required to realize an end-to-end automated, cognitive EW future, we constructed a conceptual model summarized in Figure 3.3. Based on interviews[80] and PAF team member expertise, the model shows the interrelated aspects of increasing levels of autonomy in reprogramming ("capabilities"), data pipelines and flow ("intel/data collection"), software architecture and development approach ("software updates"), and computing capabilities and capacity ("hardware upgrades"). The bullets in each box are discussed more fully in the following chapters. Time increments in the figure represent early wins (toward the bottom of the figure) that improve existing processes. Moving up in the diagram, fundamental and "visionary" capabilities increasingly support future autonomous reprogramming through redesign of the software architecture to accommodate microservices-based development (i.e., to allow portions of software to be updated independently of the entire architecture) and ML. These also rely on increasingly efficient hardware with the processing power to support computationally intensive algorithms within SWaP limitations; emerging paradigms for data collection, standardization, classification, and integration; and incremental upgrades that enable airborne reprogramming and cognitive EW. The time estimates in Figure 3.3 are based on PAF's analysis of current and expected technology readiness (discussed in the following chapters) and the assumption that the USAF will actively pursue integrating those technologies into its EWIR process, as we recommend.

[80] See Appendix A for a full list of interviews conducted during the course of the research.

**Figure 3.3. A Road Map for Achieving Real-Time, Autonomous Reprogramming**



| | *CAPABILITIES* | *INTEL/DATA COLLECTION* | *SOFTWARE UPDATES* | *HARDWARE UPGRADES* |
|---|---|---|---|---|
| *VISION (~2035)* | • Cognitive EW<br>• In-flight real-time reprogramming<br>• Fully adaptive countermeasures | • Streamlined data formats<br>• Metadata / labelling<br>• Tactical to SIGINT systems<br>• Increased range of intel gathering | • Fully containerized security paradigm<br>• Reduced safety certification time<br>• Fully automated orchestration<br>• Matured cognitive processing core<br>• Cloud-based quantum computing | • High-speed datalinks quantum networks<br>• Common hardware processing baseline<br>• High-speed processing capacity |
| *FOUND-ATIONAL (~2025)* | • 2-hour turnaround<br>• Dispersed SWW capability/connectivity (delta in-flight) | • Non-proprietary and standardized formats<br>• Streamlined intel-gathering process<br>• Cloud integration | • DevSecOps - integrated security<br>• Phase-out of vendor lock-ins<br>• Delivery automation and orchestration<br>• AI /ML core capability development | • Frontline cloud computing<br>• Firmware upgrade<br>• Militarized 5G waveforms<br>• Increased storage and processing capacity |
| *EARLY WINS (~2022)* | • 24-hour turnaround<br>• Dispersed SWW capability/connectivity (in theatre)<br>• Beyond self-protection ECM | • Collection and classification process improvement<br>• Data formats standardization<br>• In-theatre data processing | • Containerization development<br>• Container-based regression testing<br>• Feature specific safety certification<br>• Reduced deployed time | • Weapons systems upgrades<br>• Datalink upgrades<br>• Hardware miniaturization<br>• Combined FPGA/GPU embedded computing |
| *EXISTING (~2021)* | • 72-hour to 28-day processing and reprogramming turnaround time<br>• Offline reprogramming | • Collection & classification issues<br>• Slow data cleanup / update<br>• Process bottlenecks (access, proprietary formats) | • Legacy software with special workarounds<br>• No AI/ML-based waveform processing<br>• Long cycles of security hardening<br>• Long cycles of airworthiness / safety certification | • Datalink bandwidth issues<br>• Data export issues<br>• Slow onboard systems with limited embedded computing capability |

SWW = Spectrum Warfare Wing ECM = Electronic Countermeasures GPU = Graphics Processing Unit FPGA = Field Programmable Gate Arrays

SOURCES: Interviews and RAND analysis.

This conceptual model served as a road map that led to the selection and execution of the technology case studies[81] highlighted in the next four chapters, which include cognitive EW algorithm development, data engineering and cloud integration, software containerization and orchestration, and increasing onboard processing (OBP) and other edge computing capacity. These are reflected in Table 3.1 above and directly address four of the five lessons identified in Chapter Two.

Achieving adaptive and cognitive EW capabilities by 2035 would require immediate and continuous investment by the USAF in these four types of technologies. It is important to note that the model in Figure 3.3 emphasizes the idea that incremental improvements can be realized along the way even as the USAF is priming the way for cognitive EW—in this sense, investing in such technology types represents a "win-win."

Though we focused this report on the application of technological changes to EWIR, these changes are relevant to a much broader set of needs across the USAF that relate to digital infrastructure and data management. The USAF has made several attempts to revitalize and upgrade this infrastructure at the speed relevant to the fast-moving software industry. Some of these latest efforts are encompassed within plans for the Advanced Battle Management System, which is envisioned as the technological backbone of the Joint All Domain Command and

[81] For each case study, we include technology definition, application to the EWIR problem, evaluation of current status, and exploration of future development.

Control (JADC2) approach. Thus, we suggest that investments made to improve the EWIR enterprise will also have benefits for the USAF-wide data infrastructure.

### *Doctrine and Policy*

The project team took a limited look at some key doctrine and policy changes that would be needed to support and enable the investment in and operationalization of the key technology areas summarized above. Here we highlight three of them, starting with the most complex:

- data-sharing policy
- acquisition approach
- updates to EWIR doctrine.

#### Data-Sharing Policy

There are several fundamental issues with data-sharing that would need to change from the status quo of largely sensor-centric processes for data-sharing to something much more holistic and encompassing. Two important and related policy issues are at the forefront of enabling data access, visibility, and usability:

1. allowing more data of different origin (and in some cases of different classification) to reside within the same infrastructure
2. being more discriminating with data classification.

Both of these policy areas emphasize reducing the burden of “dark” data on both EWIR and other USAF processes that rely on intelligence data. More-agile, lethal threats require more tools for understanding them. In particular, the focus of intelligence is moving from using single sources of intelligence to employing multiple sources and, in some cases, multiple intelligence disciplines with different strengths to understanding threats and adversary intent. Just as multiple data sources are critical for enabling autonomous vehicles to drive safely, so too will multiple data sources be key for enabling a cognitive EW concept, so that ML algorithms will have sufficient data of the necessary complexity to discriminate between threats and other activity in the EMS, given that advanced threats do their best to disappear or seem benign.

Continuing work to adapt policies on which networks can store and move different types of data, and how networks can connect to each other and to different users, will be a big improvement over data stovepiping. Being more discriminating in data classification will go hand in hand with this, if the USAF moves with the Joint community to a more software-based approach to data security. In a software-based approach, data will be able to reside on the same infrastructure, and access will be controlled and tailored through software-based tools. Even if a highly classified source pours data into this type of system, users without the appropriate level of access will not be able to see or utilize the data. In some cases, data classification could be situation-dependent; that is, not all data gathering activities or data types collected by a system may need to be at the same (high) level of classification. Software-based security, plus discriminating classification policies, will help make more data visible to more users (as appropriate for protecting national security).

#### Acquisition Approach

Acquisition or technology development policies that govern how EWIR modernization will be invested in and developed will also continue to need work and updates. The reprogramming road map in Figure 3.3 identifies the technology transformations required to achieve future cognitive EW capabilities using an agile software development process with a DevSecOps automation methodology. Note that this road map connects some tractable early wins with additional steps required for the longer-term vision. This approach emphasizes the need for continuous development and acquisition in a way that recognizes the many interdependencies between technology types. A review of the complex DoD acquisition process and legal framework is beyond the scope of this report, but we simply state that it will be a key factor in the successful development of cognitive EW capabilities.

#### EWIR Doctrine Updates

Finally, we also acknowledge that USAF doctrine for EWIR, in particular AFI 10-703 and facility-specific implementation documents, will need updating as faster reprogramming approaches emerge. We have already acknowledged that some form of the existing EWIR process is likely to remain, even in a cognitive EW future, to provide support to cognitive EW algorithm development and to ensure that resources required for advanced reprogramming can be allocated to the most urgent situations. Thus, the primary change needed in doctrine is to lay out the circumstances under which advanced reprogramming can and should be used, and this will need to be updated each time a new capability comes online.

### *Organization, Training, Leadership, Personnel, and Facilities*

Although we did not focus our investigation on organization, training, leadership, personnel, or facilities issues, we did make two observations that are especially pertinent to the establishment of a cognitive EW capability and came up repeatedly during the course of interviews.

#### Organizational Alignment to Mission

The standup of the 350th SWW in summer 2021 has presented several important opportunities to do things differently within the USAF's EW enterprise, reprogramming included. One topic of ongoing discussion is how to present applicable forces to support operational reprogramming needs. The status quo depends on what part of the EWIR process is being considered, but, generally speaking, personnel are largely centralized in terms of mission and organization, organized by function (supporting different aspects of the end-to-end reprogramming process as detailed in Chapter Two), and within those functions organized by sensor or platform. For example, NASIC is the central clearinghouse for much of the relevant tactical ELINT, and each sensor on each platform has a team specialized to their specific reprogramming needs.

Although very different in overall mission from the 350th SWW, USAF software factories,[82] such as Platform One, Kessel Run, SkiCAMP, and Kobayashi Maru, are also generally aligned either by function (e.g., some form of command and control [C2]) or platform. As described in more detail later in the report, USAF software factories design software with a centralized, ground-based computing architecture in mind.

Although the functional and platform-based alignments of the current EWIR enterprise and software factories are understandable from a funding and historical perspective, they may have some downsides. Functional and platform-based mission alignments do not necessarily enable strong links to important operational and tactical problems, such as a particular region in which an adversary has many difficult-to-track radars and jammers. This alignment can limit the effectiveness of products from reachback organizations, whether a software update or a new tool or software-based capability, as solutions to real-world problems. It may also mean that centralized reachback organizations cannot provide solutions fast enough in a dynamic crisis context.

Another question: What functions or capabilities should be centrally located within the 350th Wing? The extensive development required for cognitive algorithms, for example, might become uncoordinated with stops and starts if spread out among too many organizations that may, at times, have different priorities.

### Development of Personnel

For several years, there have been concerns regarding the reestablishment of a pipeline for EW-capable personnel, especially EW officers, as well as pipelines for other specific skills such as in ELINT and software design. There is also considerable training and professional experience that goes into creating and evaluating threat models and other aspects of updating software for particular platforms. An evaluation of personnel pipelines and development merits a deeper analysis that was outside the scope of this research. Here we note that our interviews with USAF SMEs indicated concern not only for the limited number of personnel but also for the limited breadth in personnel experience. Some of these fields are so specialized that it is difficult to release personnel into career-broadening assignments. Yet this also limits the crossflow of information between missions and platforms. These factors limit EW officers' ability to inform operational-level (as opposed to tactical-level) EW strategy at organizations such as an Air and Space Operations Center (AOC).

One additional personnel development area to consider is the ability of airmen throughout the EW and intel enterprises to gain experience in software coding and data science. The proliferation of digital tools has enabled more airmen to gain this type of on-the-job experience. We do not know of any current way that the Department of the Air Force (DAF) is tracking who has gained this kind of experience as on-the-job training and who has not. Anecdotally, we heard about several situations in which airmen gained knowledge on using data and tools in one assignment, only to be moved to an unrelated position for their next assignment. This practice

[82] U.S. Air Force Chief Software Office, "Department of the Air Force Software Ecosystem," webpage, undated-a.

may lead to missed opportunities for growing cadres of “software-smart” EW and intel personnel who need not be the lead engineers for such efforts but could very much lead the integration and practical use of such tools and practices.

## Conclusion

While several emerging technologies will play a part in bringing about the long-term vision described in this chapter, the following chapters discuss the state of development for four essential types: cognitive EW algorithm development, data pipelines, software architecture, and hardware capacity. Figure 3.3 above illustrates these technologies and how they support the requirements for the development of future autonomous reprogramming capabilities. Though separate in terms of future technology development and evolution, these four technologies have several interrelations that collectively support the incremental enhancements of the EWIR process. Parallel investments are needed to operationalize the benefits of each technology, as well as in some of the other DOTMLPF-P examples provided here.

# Chapter 4. Operationalization of Cognitive EW

This and the next three chapters examine the four interrelated technological advances summarized in Figure 3.3 that are required to achieve the vision for future EWIR. Here, we look at the concept of cognitive EW and its unique technological facets and needs as a way to further set up why parallel investments need to be made across different technologies to operationalize the ultimate vision. In Chapters Five, Six, and Seven, we detail three other technologies that underpin the cognitive EW system: data pipelines (data engineering and cloud integration), software containerization and orchestration, and hardware miniaturization and specialization.

To be effective in a rapidly developing EMOE, USAF EW systems must employ novel techniques to defeat advanced threats. As the DoD EM Superiority Strategy explains, "The modern EMOE is increasingly congested, contested, and constrained. . . . In order to maintain warfighting superiority, DoD must look to revolutionary, leap-ahead technologies and capabilities to be able to compete against a range of adversaries throughout the competition continuum."[83] As we describe in this chapter, adaptive and ultimately cognitive EW systems are critical to achieving these objectives.

## Understanding Adaptive and Cognitive EW

Adaptive and cognitive EW systems take advantage of modern hardware and software technologies to provide powerful new EW capabilities. In the same way, however, they also pose powerful new challenges to the current EWIR process. SDR technology, mentioned in Chapter One, is a key threat enabler that we discuss in some additional detail before moving to adaptive and cognitive EW.

Although technically not required to build adaptive and cognitive EW systems,[84] SDR is a family of game-changing technologies that make adaptive and cognitive EW systems practical, inexpensive, and essential.[85] The concept of software-defined radio was introduced by Mitola in 1992,[86] and its adaptation to radar is straightforward, if challenging. SDR uses reconfigurable

[83] DoD, 2020b, p. 11.

[84] "An intermediate step toward arbitrary waveform generation is the selection of waveforms or waveform parameters from a prespecified set. Many modern radars already have this capability" (Maria S. Greco, Fulvio Gini, Pietro Stinco, and Kristine Bell, "Cognitive Radars: On the Road to Reality: Progress Thus Far and Possibilities for the Future," *IEEE Signal Processing Magazine*, Vol. 35, No. 4, July 2018).

[85] "Cognition requires waveforms and circuits to be reconfigurable and optimizable in real time" (Greco et al., 2018).

[86] Joseph Mitola, "Software Radios: Survey, Critical Evaluation and Future Directions," *Proceedings of NTC-92: National Telesystems Conference*, 1992.

computing devices—usually field-programmable gate arrays (FPGAs)[87]—to allow software to set (and reset) radar parameters that formerly had to be hardcoded.[88] SDR technology allows a common set of hardware to generate a wide array of different waveforms. Because it allows rapid and repeated reprogramming, SDR technology allows radars to switch between waveforms in a matter of seconds or even change waveforms on each pulse.[89] SDRs can generate new waveforms on the fly, confounding the traditional approach of recognizing signals using preset lookup tables. SDRs even permit the generation of random, noise-like waveforms that follow few fixed statistical patterns and thus defy classical radar parametrization schema altogether.[90]

By liberating the signal from its hardware, SDRs make recognition much more difficult. But recognition is not impossible. Just as the 60 hertz (Hz) "mains hum" from a standard electrical outlet can be heard muttering in the background of older stereo systems, an SDR transmission carries within it telltale fingerprints of the hardware that created it. To make an analogy, a traditional radar system has a unique "sound," just as each musical instrument has a distinct timbre. SDR is like a synthesizer that can mimic any instrument in the orchestra by matching the tonal parameters sufficiently to fool the ear. But while this frustrates traditional means of identification, if one listens closely to pitch transitions and higher-order harmonics, one can learn to distinguish a Casio keyboard from a Sony keyboard (for example). Likewise, sophisticated TECHELINT sensors can tease out subtle differences that would fool a normal ELINT system.[91]

With this hard-won knowledge, special processing filters can, in principle, be designed in some cases to detect these characteristics and thereby identify the radar. These new capabilities can then be added to the RWR through an upgraded OFP. But this EWIR process is difficult and

[87] "A field-programmable gate array (FPGA) is an integrated circuit designed to be configured after manufacturing and is hence 'field-programmable'" (Thibault Debatty, "Software Defined RADAR a State of the Art," *2nd International Workshop on Cognitive Information Processing*, 2010); "Field programmable gate arrays (FPGAs) are integrated circuits with a programmable hardware fabric. Unlike graphics processing units (GPUs) . . . the circuitry inside an FPGA chip is not hard etched—it can be reprogrammed as needed" (Intel, "FPGA vs. GPU for Deep Learning," webpage, undated).

[88] "A software-defined radar applies the same principles as a software-defined radio: components that have typically been implemented in hardware (e.g. mixers, filters, modulators, demodulators, detectors etc.) are implemented using software on a computer or other programmable device, usually a field-programmable gate array (FPGA)" (Debatty, 2010).

[89] "Technology allows the emitted waveform to be altered on a pulse-by-pulse basis" (Hugh Griffiths and Chris J. Baker, "Towards the Intelligent Adaptive Radar Network," *2013 IEEE Radar Conference (RadarCon13)*, 2013).

[90] "Noise radar technology (NRT) is based on the transmission of random waveforms as opposed to the classical, often sophisticated, deterministic radar signals. . . . In a conventional radar, a single waveform (or a finite set of waveforms), is used for transmission and reception with matched filtering. Conversely, NRT is able to transmit a—virtually unlimited—set of realizations (i.e., "sample functions") of a random process" (Francesco De Palo, Gaspare Galati, Gabriele Pavan, Christoph Wasserzier, and Kubilay Savci, "Introduction to Noise Radar and Its Waveforms," *Sensors*, Vol. 20, No. 18, Article 5187, 2020).

[91] This is usually accomplished by identifying "unintentional modulations" of the pulse due to the specific hardware circuits. See Lawrence E. Langley, "Specific Emitter Identification (SEI) and Classical Parameter Fusion Technology," *Proceedings of WESCON '93*, 1993.

time consuming, often taking months or years to complete—if it is possible at all. Furthermore, as SDRs become increasingly sophisticated, the demands on this extended TECHELINT solution become increasingly arduous. A new approach is needed to make identification of SDRs practical in the field.

### *Adaptive EW*

Adaptive EW is one approach to addressing some of these challenges—yet it also poses new problems. Adaptive radar was initially developed in rough analogy to adaptive optics in astronomy as proposed by Babcock in 1953 and realized publicly in the early 1990s.[92] The initial idea was to improve the performance of radar receivers in detecting faint signals by accounting for ambient environmental effects, in much the same way that astronomical observatories now adjust for atmospheric disturbances to improve telescopes' ability to discern faint starlight.[93] In this approach, environmental effects are measured by observing the difference between received and expected signals.

This approach was later extended to the broader radar identification process, as returned signals are compared to the library of expected signals. The adaptive approach augments the fixed lookup table with a complex decision tree that assesses environmental effects and anticipates how some changes—e.g., minor damage to the adversary's transmitting antenna or various forms of deliberate tinkering with the signal generation circuitry—can alter the received waveform so that it falls outside the boundary of known signals in the library. A "smart" adaptive system can recognize partial matches and recalibrate expectations accordingly. This effectively enables the adaptive system to revise the library on the fly to account for potential variations.

In a sense, the conventional EWIR process is adaptive in that it seeks to update the library based on new information—but, as noted in this report, it can take months for analysts to extract the data, analyze it, generate modified MDFs, and load them onto the aircraft. The adaptive EW systems that we propose can take humans out of the EWIR loop for basic signal variations that can be realistically anticipated in advance. As Werner Dahm, chair of the USAF Scientific Advisory Board, put it, "Adaptive solutions . . . allow for basic operation in these environments, but are not capable of rapid understanding and countermeasures. [But] there are a surprising amount of benefits from relatively simple levels of adaptability in EW systems. . . . These simpler systems are something that's 'no kidding' achievable on time scales of the Air Force."[94]

[92] Jacques M. Beckers, "Adaptive Optics for Astronomy: Principles, Performance, and Applications," *Annual Review of Astronomy and Astrophysics*, Vol. 31, 1993.

[93] "Adaptive optics is now a fully mature technique to improve the angular resolution of observations taken with ground-based astronomical telescopes. It is available at most of the major optical/IR observatories" (François Rigault, "Astronomical Adaptive Optics," *Publications of the Astronomical Society of the Pacific*, Vol. 127, No. 958, 2015).

[94] Mark Pomerleau, "What Is the Difference Between Adaptive and Cognitive Electronic Warfare?" *C4ISRNet*, December 16, 2016.

Moreover, while adaptive systems can be developed and deployed in the near term and can offer some operational benefits, they are also a critical developmental stepping-stone toward more-capable cognitive EW.

### *Cognitive EW*

The concept of cognitive radar was first advanced in 2006, building on work in the late 1990s.[95] Cognitive radars expand on adaptive methods to create an active feedback loop between the receiver and transmitter.[96] They use intelligent signal processing and generally require some memory of previously received signals to learn from.[97] More generally, cognitive EW extends beyond adaptive EW, using ML algorithms to attempt to learn the changing EMOE and to account for unanticipated changes in the noise environment,[98] unanticipated variation in known threat radars and jammers, and even previously unknown radars and jammers. A simple example of a cognitive EW process would be using algorithms to predict frequency-hopping by an observed adversary system. What distinguishes adaptive from cognitive systems is the latter's ability to retrain or learn during use.[99]

An important feature of cognitive EW systems is that, at least to some degree of confidence, they have the potential to determine which radar and jammer systems are threats *without* relying on a preset library of parametric data—without having strong prior knowledge of the specific adversary systems they face.[100] As John Tranquili of BAE systems put it, "A system that's

[95] Greco et al., 2018; Simon Haykin, "Cognitive Radar: A Way of the Future," *IEEE Signal Processing Magazine*, Vol. 23, No. 1, January 2006.

[96] "The new feature of a cognitive radar that differentiates it from a classical radar is the active feedback between receiver and transmitter. . . . A classical adaptive radar is able to extract information from the target and the disturbance signals through appropriate signal processing algorithms and to use that information at the receive level to improve its performance. Conversely, a cognitive radar is able to use all of the extracted information not only at the receive level but also at the transmit level by changing, on the fly, the transmit frequency channel, waveform shape, time on target, pulse repetition frequency (PRF), power, number of pulses, polarization, and so forth" (Greco et al., 2018).

[97] "Three ingredients are basic to the constitution of cognitive radar: 1) intelligent signal processing, which builds on learning through interactions of the radar with the surrounding environment; 2) feedback from the receiver to the transmitter, which is a facilitator of intelligence; and 3) preservation of the information content of radar returns, which is realized by the Bayesian approach to target detection through tracking" (Haykin, 2006).

[98] "A radar detector must incorporate previously determined knowledge to estimate the statistical characteristics of the operating environment. . . . However, cognitive systems in nature are adept at adapting to new situations by leveraging prior knowledge. Therefore, a true cognitive radar should adaptively estimate an accurate threshold regardless of the distribution to which the clutter process belongs" (Justin Metcalf, Shannon D. Blunt, and Braham Himed, "A Machine Learning Approach to Cognitive Radar Detection," *Proceedings of the 2015 IEEE Radar Conference*, 2015).

[99] "[A] cognitive radar is able to use all of the extracted information not only at the receive level but also at the transmit level by changing, on the fly, the transmit frequency channel, waveform shape, time on target, pulse repetition frequency (PRF), power, number of pulses, polarization, and so forth. In an adaptive radar, all of these parameters are preset and cannot be changed on the spot" (Greco et al., 2018).

[100] "True cognitive EW systems . . . should be able enter into an environment not knowing anything about adversarial systems, understand them and even devise countermeasures rapidly" (Pomerleau, 2016).

cognitive is capable of two things: First, its operations are not reliant on a predefined threat database. . . . It can determine the meaning of the signals it receives and reason over the potential responses it can make. . . . Second, it makes use of learned knowledge so it can respond quicker and more effectively in subsequent engagements."[101]

The lack of reliance on preset databases and the ability to learn from experience make cognitive systems particularly compelling for designing countermeasures for adversary jammers enhanced with SDR. When dealing with new or not-previously-characterized enemy systems, cognitive EW may be the only approach that can assist pilots in near-real time—especially if reachback is not available.

Cognitive EW systems succeed where lesser measures fail because they apply what we often call "intelligent" processing to a wider set of data, extending analysis beyond signal parameters to include the *behavior* of a radar system—taking into account when, where, and how different radar waveforms are used, switched, and directed. For example, a radar system that suddenly turns on, changes waveforms, and maintains its main beam on a moving aircraft may be considered threatening. Or, in some cases, radar operators might reveal themselves through habitual behavior that the cognitive EW system observes.[102] Karen Haigh writes:

> A cognitive radar takes advantage of being aware of its environment and employs other cognitive traits such as problem solving, judging and remembering. A radar with these cognitive abilities that will collect information about the environment via spectrum sensing, GPS [Global Positioning System] location, system speed and bearing, temperature, real-time estimation of background clutter, etc., may use all of this to its advantage.[103]

Ideally, a cognitive system could provide the pilot with what a team of experienced intelligence analysts might offer if they could ride along in flight and operate at the speed of computers: to draw on experience and context to make the best educated guesses possible as to the origin and intent of the signals they detect. We should emphasize, however, that even though cognitive systems *can* make judgments without predefined libraries, they must still be trained on data from such libraries, and they are far more effective when their knowledge of the current EMOE is augmented with good foundational intelligence. In other words, cognitive EW is best thought of not as a replacement for foundational TECHELINT, but rather as the best way to take maximal advantage of it. Furthermore, we would expect these algorithms to feed back into priming intelligence foundations because their educated guesswork in situations where signals do not quite behave as prior intelligence would suggest can provide valuable new insights, not just for the algorithm in question, but also for the development of future algorithms for other purposes.

[101] J. R. Wilson, "Adaptive and Bistatic Electronic Warfare," *Military & Aerospace Electronics*, February 1, 2018.

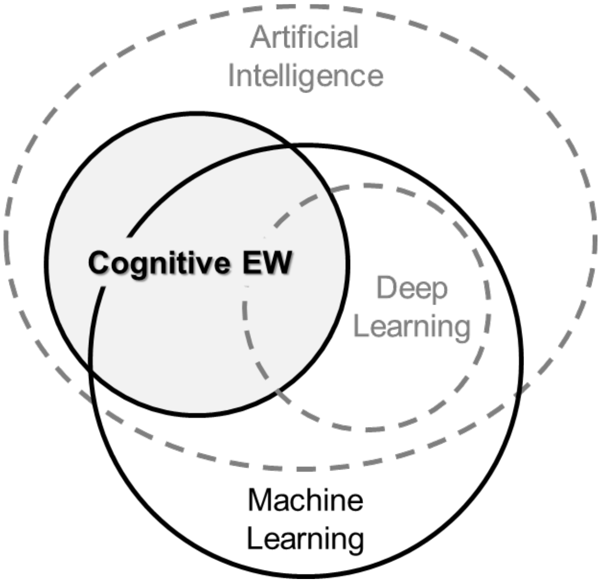
[102] An example of habitual behavior could be turning on the system for a test at the same time each day.

[103] Karen Haigh and Julia Andrusenko, *Cognitive Electronic Warfare: An Artificial Intelligence Approach*, Boston, Mass.: Artech House, 2021.

### Artificial Intelligence and Machine Learning

Before we turn to the status of adaptive and cognitive EW systems and the challenges to adoption, it is worth taking a moment to discuss some of the technologies that make cognitive EW possible and some of the confusion in terminology surrounding this subject. Terms such as *AI*, *ML*, and *deep learning* are often used in the same breath as cognitive EW and intelligent processing. Figure 4.1 illustrates the semantic relationships between these terms as we use them in this report.

**Figure 4.1. Terminology**



As indicated by the gray dotted oval, *AI* is a fairly loose umbrella term. While the term continues to evolve, we can roughly define *AI* as "the use of computers to carry out tasks that previously required human intelligence."[104] Some consider adaptive EW to be a form of AI, while others reserve the term AI to describe cognitive EW.

*ML* is more specific: It is a set of computing techniques, including artificial neural networks (NNs), best known for their application to AI systems. However, despite common association between AI and ML, ML is a broad academic discipline, and there remain many less prominent subfields that do not fit neatly under the AI umbrella.[105]

[104] This wording comes from Edward Geist as found in Lance Menthe, Dahlia Anne Goldfeld, Abbie Tingstad, Sherrill Lingel, Edward Geist, Donald Brunk, Amanda Wicker, Sarah Soliman, Balys Gintautas, Anne Stickells, and Amado Cordova, *Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 2, Technical Supporting Analysis*, Santa Monica, Calif.: RAND Corporation, RR-A341-2, 2021b, updating Marvin Minsky's seminal (if now slightly problematic) definition: "the science of making machines do things that would require intelligence if done by men" (Marvin Minsky, ed., *Semantic Information Processing*, Cambridge, Mass.: MIT Press, 1968, p. v).

[105] "[M]any ML applications, such as logistic regressions and clustering algorithms, are not really 'artificial intelligence,' even under the most expansive definitions of the field" (Menthe et al., 2021b).

*Deep learning* is an important subset of ML—specifically a subset of NNs—that has revolutionized the field. Automated assistants such as Siri, Alexa, and Cortana and facial recognition software from Facebook and Google all use forms of deep learning. Deep learning refers to varieties of NNs that have multiple hidden layers, although there is no specific number or size, so the term can be somewhat loose.[106] As Schmidhuber describes:

> A standard neural network (NN) consists of many simple, connected processors called neurons. . . . Learning or credit assignment is about finding weights that make the NN exhibit desired behavior. . . . Depending on the problem and how the neurons are connected, such behavior may require long causal chains of computational stages. . . . Deep Learning is about accurately assigning credit across *many* such stages [emphasis added].[107]

Finally, cognitive EW systems can be built with more-general ML or specific deep learning networks—but they may also be constructed as an *expert system*, an earlier form of AI that falls outside what we think of as ML today.[108] Indeed, although the older method may not be as powerful as today's ML, it has merit in that it may be constructed through interviews with and observations of human analysts rather than requiring vast amounts of training data from the battlespace, which, as we describe later, may be the single biggest challenge to the construction of effective cognitive EW.

## Current Status

Various adaptive EW and cognitive EW systems have been under development for some time, but their capabilities remain limited, and the full application of AI techniques remains in its infancy.[109] For example, the Air Force Lifecycle Management Center put out a request in March 2021 for cognitive EW and ML applications for the F-15. The goal of the proposal is "to develop and build cognitive EW technologies at least as mature as a laboratory breadboard version (TRL-4), and investigate challenges of adaptive, agile, ambiguous, and out-of-library

[106] Menthe et al., 2021b.

[107] Jürgen Schmidhuber, "Deep Learning in Neural Networks: An Overview," *Neural Networks*, Vol. 61, January 2015.

[108] "The term expert system is used here to describe a computerized system that encapsulates human knowledge, without resorting to any machine learning or data mining technique. . . . The end product of this process is a computer program that tries to mimic the way the experts solve the particular problem, usually in some sort of rule-based form" (Arie Ben-David and Eibe Frank, "Accuracy of Machine Learning Models Versus 'Hand Crafted' Expert Systems—A Credit Scoring Case Study," *Expert Systems with Applications*, Vol. 31, No. 3, Part 1, April 2009).

[109] "Like any other intelligent system, cognitive EW must overcome challenges associated with each AI concept or stage of the cognition loop. The domain is challenging to understand, and the decision space is large and complex. . . . In other domains, AI techniques have addressed the full richness of most of these challenges. In the Cognitive Radio and EW domains, AI techniques are just beginning to scratch the surface. . . . We need to bring these techniques into EMS operations, and address them in depth" (Haigh and Andrusenko, 2021).

complex emitters that operate inside RF background noise . . . [and] cognitive technologies that provide rapid EW reprogramming."[110]

Although the description clearly indicates that the technology is in its early stages of development, we note that assigning a technology readiness level (TRL) for AI systems is problematic because TRLs were originally developed to assess the maturity of hardware.[111] Because TRL definitions refer to things such as "prototypes" and "breadboards," the difficulty of applying them to software has been understood for some time.[112] Two recent RAND reports devised their own scales to attempt to account for the importance of the data sets involved. An FY 2018 project defined a TRL-like scale for AI/ML algorithms. On this scale, levels 2–9 are distinguished by the size and complexity of the data sets used to train them—ranging from a "toy" data set (level 2), to a "real-world" data set (level 6), to widespread commercial use (level 9).[113] On these TRL-like scales, we would rate cognitive EW systems in the mid-range because the algorithms have yet to be fielded and trained with significant real-world data sets.

We emphasize the importance of using real-world data in AI systems because such data are more than just a final test—for AI systems, it is an integral part of the development and maturation process. As Haigh and Andrusenko note, "Data collection and management is perhaps the hardest part of building a system based on AI and machine learning. A rule-of-thumb for all machine learning-enabled systems is that 80% of the work goes into collecting and curating the data."[114]

Without carefully curated data and methods, naïve use of ML may not offer performance beyond what can be achieved through more traditional models.[115] And deciding when the system has learned enough is also a challenge. Haigh and Andrusenko write, "Traditional [validation and verification] approaches . . . have not yet caught up to the needs of learning-based AI. Data quality, data storage, model security, and validation objectives are lacking."[116]

[110] John Keller, "Air Force Asks Industry for Artificial Intelligence (AI) Cognitive Electronic Warfare (EW) for F-15 Jets," *Military & Aerospace Electronics*, March 15, 2021.

[111] They were first developed by NASA in the 1970s. The current nine-point scale was defined formally in 1995 and adopted by DoD following a Government Accountability Office review in 1999. See John C. Mankins, "Technology Readiness Assessments: A Retrospective," *Acta Astronautica*, Vol. 65, 2009, and U.S. Government Accountability Office, *Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects*, GAO-20-48G, January 2020a.

[112] DoD initially created separate criteria for software TRLs, but they were later abandoned. See Deputy Under Secretary of Defense for Science and Technology, *Technology Readiness Assessment (TRA) Deskbook*, Washington, D.C.: U.S. Department of Defense, May 2005.

[113] Menthe et al., 2021b, pp. 105–107.

[114] Haigh and Andrusenko, 2021.

[115] "Our results indicate that a naive user of machine learning, who is not schooled in the intricacies of the machine learning methods that are at his or her disposal, will struggle to beat the performance of a carefully hand-crafted expert system" (Ben-David and Frank, 2009).

[116] Haigh and Andrusenko, 2021.

Programs are underway to build cognitive EW, but reported outcomes still involve simpler data sets.[117]

Because of the lack of data in general, and the lack of high-quality labeled data in particular, commercial AI methods, which have worked so well for facial recognition and other familiar tasks in recent years, are difficult to apply to EW out of the box. Significant development efforts are needed to make them work for this context. Adams notes, "Pertinent signal data is typically low in signal quality, not labeled and not timely. . . . Because of the paucity of data, more modeling and simulation are required, which are challenging and expensive processes. Commercially derived approaches to machine learning don't work well in EW."[118]

Nevertheless, even in their early stages of development, cognitive EW and ML can still play an important role in improving and speeding up the EWIR process in the near term and the mid-term—and giving proper attention to development would position the USAF to attain and maintain dominance of the EM battlespace for years to come.

## Early Wins and Fundamental Development

Today's EW systems rely on an accumulated library of parametric data about adversary systems stored in the EWIR database,[119] compiled by intelligence analysts at the NASIC, sister intelligence production centers, and other intelligence organizations through careful and deliberate analysis of millions of signals collected by a wide variety of platforms.[120] But this collection and analysis can take months or longer to complete.[121] As noted earlier, the EWIR process is struggling to keep up with the increasing proliferation of new conventional systems,

[117] "DARPA [the Defense Advanced Research Projects Agency] has done some initial studies on 'sample problem sets that are somewhat more simple in nature,' Tilghman said. In one effort, researchers built a convolutional neural network to understand what modulation a signal was using—AM, FM or phase-shift keying, for instance. . . . Tilghman added it proved that machine-learning systems 'can abstract additional features and information out of the RF spectrum to help us better understand [the signal environment]'" (Charlotte Adams, "Cognitive Electronic Warfare: Radio Frequency Spectrum Meets Machine Learning: A Look at the Technologies That Will Power the Aircraft of Tomorrow," *Avionics International*, August-September 2018).

[118] Adams, 2018.

[119] "The [EWIR database] is a database that contains parametric and select C&P [characteristics & performance] data describing EW systems. It is the primary source for mission and reprogramming data. It is the primary DOD approved source for technical parametric and performance data on non-communications electronic emitters and associated systems. Scientific and technical intelligence and other centers (including NASIC, NGIC [National Ground Intelligence Center], NMIC [National Maritime Intelligence Center], MSIC, 453 EWS, and NSA) provide the data to NASIC for inclusion in the database" (AFI 10-703, 2019c).

[120] The EWIR database (EWIRDB) was replaced in the mid 2010s by what was initially named the Next Generation EWIR Database System (NGES). (The original version is now called the "legacy" version and remains in use by some units, because it contains some information in formats not found in the newer version.)

[121] "This foundational library . . . is created by scouring thousands of hours of collection, looking for every . . . emitter that exists. . . . This process is labor intensive with results taking months to complete even for the most benign signal" (John G. Casey, "Cognitive Electronic Warfare: A Move Towards EMS Maneuver Warfare," *Over the Horizon*, July 3, 2020).

let alone the advent of SDR-powered radars and jammers that undermine the parametric paradigm altogether.

The following steps in fundamental development of adaptive and cognitive EW capabilities could help the USAF achieve early wins and prepare for the larger transformations necessary to succeed in tomorrow's EMOE.

### *Enhance Capabilities to Compare Signals with Parameterized Emitter Data*

First, it is critical for the USAF to significantly enhance its capabilities to compare signals taken from the aircraft ("sensorized" data) with parameterized emitter data as stored in the EWIR database, the information and methods within the SPECTRE environment,[122] and other repositories related to the electronic order of battle. It is currently an unavoidable reality that each EW system analyzes waveforms slightly differently and may use different bins, cutoffs, and false-alarm thresholds to categorize and parametrize signals. As a result, comparing new EW data with existing EW data—a critical part of any intelligence-updating process—is difficult to achieve to the requisite level of quality for analysis. As one SME we interviewed explained, "Regarding the challenges with EWIR database, I believe it is mostly formatting issues and possibly missing data on occasion. . . . The bottom line is that the automatic loading process for the mode-comparison tool produces a large number of errors requiring manual intervention."[123]

A key advance in this area may be found within the Vigilant Protector (VIPR) system of the 453rd EWS.[124] Currently, VIPR compares signal intercepts to the appropriate databases automatically, allowing for close matches, as opposed to requiring exact matches. The next generation (VIPR-2G, currently under development) will include limited ML capabilities to attempt to make the matches faster and potentially more accurate and to deal with the more flexible EWIR database format, which can make data-matching difficult.[125] Additional support is needed to ensure that subsequent generations of the software realize this vision and can work to provide automated pathways for data that go beyond what the 53rd EWG requires for its own purposes to lay the foundation for future data exchange in general. Until data matching can be made automatically to a high degree of confidence, it will be difficult or even infeasible to train and develop cognitive EW systems that work effectively with real-world data.

[122] SPECTRE is an environment developed by the 53rd EWG to allow "machine-to-machine transfer of intelligence data and programming information into mission data generator tools" (USAF, 2019e).

[123] Discussions on background were nonattributional.

[124] SMEs noted that this is a longstanding problem and that there have been other attempts at innovation in automation over the years as well. VIPR is not the first tool to attempt this.

[125] The new EWIR database has a much more complex format and can take more complicated entries in each. One entry for contact information, for example, uses a graphical scan of a business card.

### *Increase Commitment to Developing and Deploying Adaptive EW Systems*

Second, the USAF should increase its commitment to developing and deploying adaptive EW systems. Adaptive EW systems require less data than cognitive EW systems, so it is not necessary to wait until the IC has labeled a sufficient amount of high-quality data to train the ML models. Adaptive EW systems are also narrower in focus and more modest in ambition. For example, adaptive EW systems can be used on board aircraft to improve robustness against jamming and even self-interference—and this has already begun.[126] Other systems are the Adaptive Radar Countermeasures program and Behavioral Learning for Adaptive EW, led by DARPA.[127]

The Angry Kitten platform—and its family—provide another interesting pathway in this regard.[128] Initially developed starting in 2012 to simulate adversary systems using open-source architecture and commercial off-the-shelf hardware, the program has grown to include the Technique Description Language, which provides a nearly universal language for coding adaptive systems, so a single coding structure might in principle be used to write MDFs for many systems. This kind of generalization is likely to be part of any future development cycle that seeks to move away from hand-built EWIR toward an automated system. In general, the earliest wins in this push toward more sophisticated EM operations will come from adopting adaptive EW systems into the fleet, as we wait for cognitive EW systems to mature.

Building capabilities such as adaptive EW as an applications layer or as an app-enabled design that interfaces with existing OFPs is a near-term way forward to operationalize adaptive systems (see Figure 4.2). An applications-based approach allows for rapid innovation without the need to completely change the architecture of existing OFP software. In the long term, however, this approach does not present as a sustainable and maintainable option when it comes to achieving real-time responsive reprogramming. This is because, as shown in Figure 4.2, the functionality of the applications layer will still be subject to the OFP layer, which is generally proprietary with inherent design issues and very slow update processes. The OFP layer still defines the fundamental behavior of the platform's capabilities and forms the layer of interaction between the proposed apps and the operating system and hardware. Hence, the applications and their interfaces with the underlying OFP would need to be updated with each OFP update. With multiple layers of interfacing software, the flexibility that the applications layer would provide in the near term might easily be offset by the maintenance and performance issues in the long run. This approach might not be conducive to the development of an ML and

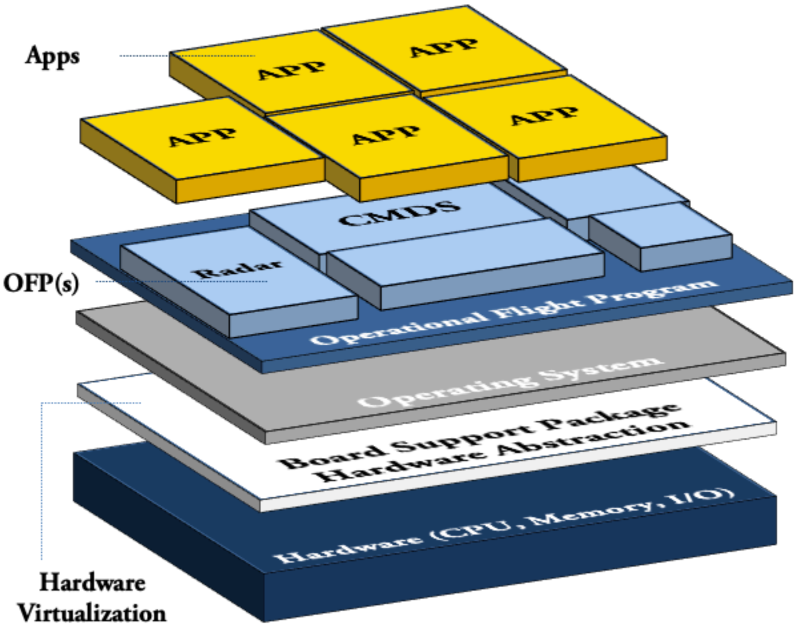
[126] "L3Harris is working on adaptive EW systems, such as its HalcyonLink equipment. These systems employ interference cancellation techniques to maintain critical tactical communications even during an adversary's efforts at jamming. In some cases, it may even be a pilot's own equipment that's doing the jamming, since an aircraft's EW suite has been known to block the same aircraft's communications equipment" (Jack Browne, "Digital Techniques Train Cognitive EW Systems," *Microwaves and RF,* August 12, 2020).

[127] The Adaptive Radar Countermeasures program is supported also by the U.S. Navy and USAF; the Behavioral Learning for Adaptive EW program is supported by the U.S. Army. See Wilson, 2018.

[128] Angry Kitten is developed by the Georgia Tech Research Institute.

cognitive EW capability. Hence, a parallel effort for a more robust, albeit disruptive, long-term solution is required. Chapter Six deeply explores a parallel approach for rearchitecting software that would enable cognitive EW and avoid the issues referenced above.

**Figure 4.2. Applications-Based Realization of Adaptive EW**



### *Introduce Cognitive EW in Supporting Roles*

Third, cognitive EW systems may be introduced gradually into parts of the EWIR cycle (away from the edge) where they can play a supporting role—as opposed to pushing them into fighter cockpits. One excellent testbed in which cognitive EW systems could show their merit and learn on real-world EMOE data would be to install them in airborne EW support systems such as the RC-135V/W Rivet Joint, the U.S. Army's Guardrail Common Sensor, and the U.S. Navy's E/A-18G Growler. These cognitive systems would seek to disambiguate signals, including miscalls and miscues, that are uncommon but far from rare. They can also account for variances, such as "short" measurements that fail to capture an entire pulse or incomplete pictures of waveforms. Note that cognitive systems would also be able to acquire data for later training of other systems. However, additional memory capacity is likely needed for such cognitive EW systems, which may constrain initial use.[129]

Another essential proving ground for cognitive EW systems would be to apply them to stored data—to the libraries within the EWIR database, inherent within the SPECTRE environment, and others. (As noted earlier, this requires effective and efficient machine-to-

[129] "Extended memories are needed in cognitive EW systems in companion with threat-recognition algorithms to locate known or anticipated threat emitters and respond with an ECM [electronic countermeasure] such as a jammer" (Browne, 2020).

machine pathways to connect these systems.) The support of the IC would be critical in linking up test systems to these databases, likely through the intelligence production centers. Such cognitive EW algorithms could be run on enormous fused data sets from multiple platforms, looking to identify LPI signals and other radar that may have been missed entirely in the initial sweeps of the data.[130] They can also be used to look for the "unintentional modulations" that could be used to reprogram RWRs to identify elusive SDR systems. In this way, they could exceed what experts or expert systems can achieve:

> A machine-learning-based system could learn and react in ways that experts would never have thought. . . . Machine learning might be able to discover hitherto unimagined distinctions between emitters based on "unintentional modulations" of waveforms caused by factors such as manufacturing flaws. This data might be thrown away by an expert-system-based device.[131]

### *Apply Adaptive and Cognitive EW to Post-Mission Data Directly from Fighters*

Fourth, adaptive and cognitive EW capabilities should be applied to post-mission data gathered directly from fighter aircraft. This is the most stringent real-world test, and the data sets gathered here may provide the best way to develop cognitive EW that will be truly effective when needed.

The Quick-Reaction Instrumentation Package (QRIP), together with the Knowledge Management/Rapid Analysis Processing Independent Deployable System (KM/RAPIDS) programs, provides one means of doing this. Other methods may be developed later, but this one is available now—and every mission flown without capturing the data by some means is wasted data, which ultimately slows down the progress toward developing cognitive EW systems. To use this method effectively, however, some security classification, proprietary data, and related policy issues remain to be overcome. We address these in Chapters Five and Six.

### *Invest in Machine Learning to Correlate Radar Returns from Multiple Receivers*

Finally, the USAF should invest in developing the ML algorithms necessary to correlate radar returns from multiple receivers in near-real time. The AI algorithms necessary to do this are different from but related to what will be required to work with fused data mentioned above. This will prepare the USAF for real-time, multiplatform analysis of radar signals by developing the algorithms necessary to compare returns from moving targets in this detailed manner. As others have noted:

> Bistatic or specially distributed systems provide simultaneous looks at the same signal, which gives you spacial diversity and may provide some elements you couldn't get from a single system. But it is technologically difficult—

[130] "Cognitive EW toolkits would not just be critical on the battlespace but also within the EW processing centers across the globe conducting the EW reprogramming cycle. Vast servers hosting cognitive EW algorithms would comb through various feeds of raw EMS data searching for the new and unusual signals" (Casey, 2020).

[131] Anthony Nigara, director of EW Mission Solutions at Harris Corporation, as reported in Adams, 2018.

> coordinating across separated receivers, how to share information—and other levels of complexity that still need to be solved.[132]

Together, building the machine-to-machine data pathways, gathering the data, and starting to train adaptive and cognitive EW systems on these data will pave the way for genuine cognitive installation on fighter aircraft and moving more of what is now known as the EWIR process to the edge.

## Future Development Path

As advanced radars proliferate around the globe and SDR technologies allow the number of possible new waveforms to grow almost without bound, the USAF will lose the ability to dominate such a battlespace with prewritten rules, however complex and adaptive they may be. At that point a true cognitive system will be needed—and it must be at the edge, onboard the very aircraft that survive in this deadly EMOE without the aid of more vulnerable electronic support systems and without recourse to intelligence analysts back home.[133] Ideally, cognitive systems would permit fighter aircraft not only to survive the future EMOE but also to dominate it.

To make this happen, a host of technological advances are required. First, the real-world data sets necessary to train cognitive EW systems must be acquired and analyzed. This requires fixing the pathways and devising the algorithms as described in the previous section. Next, cognitive systems must be married to miniaturized hardware and containerized software, as described in the following chapters. Finally, cognitive systems require access to high-speed datalinks to prime the systems with the most recent data before the mission and to pull data after the mission to share with other aircraft, in a virtuous cycle.

As we look to a future in which cognitive EW systems replace the static, rules-based systems we have today, we note a few additional concerns. First, ML-enabled systems have the capacity to improvise in the face of the unknown. This is, of course, an essential and desirable characteristic given the expected advances in the EMOE. But it is worth nothing that different instantiations of the same EW system on different aircraft could “learn” differently based on exposure to different EMOEs—and, thus, they might, at least in theory, reach different determinations concerning whether an emitter represents a threat. In practice, fighter aircraft in a multiship formation would normally be expected to exchange data, and differences are likely to apply to fairly fine distinctions. But, as noted earlier, a system that can learn like this poses a challenge to current validation and verification methods. It is important that these systems be tested on the range and that testing and evaluation (T&E) wings receive the support necessary to do so. It is worth noting that this is not a trivial need, because the ability to mimic unknown enemy systems itself requires complex SDR, and, if testers are not careful, cognitive systems

[132] Wilson, 2018.

[133] And, of course, once the enemy has cognitive EW capabilities as well, nothing less will suffice.

will learn the unintentional modulations of our own T&E systems, rather than those they are meant to be tested against.

Second, while this future vision of a fully automated cognitive EW system is the ultimate goal, we cannot get there without tremendous human effort. In other words, human-driven EWIR will not be obsolete in the foreseeable future: The demands on trained intelligence analysts in this field will only grow as cognitive EW algorithms are developed. And the need for more collection and analysis will continue. As one observer put it:

> This is not to say that human-derived EW and forensic based reprogramming is no longer needed. On the contrary, human-enabled reprogramming would become more vital than ever. . . . Machine learning tools are enabled by vast arrays of data to train the machine to understand what is occurring within the spectrum.[134]

For this reason, investment in human skills in EWIR and spectrum warfare in general remains critical. As RAND researchers have noted elsewhere: "AI/ML technologies alone do not solve these challenges; rather, if properly implemented and complemented by human analysts with the right skills and training, they can . . . meet warfighter needs. Automation is best understood as a means to reshape human effort toward more productive ends, not to remove it entirely."[135]

## Conclusion

In June 2017, Bill Conley, deputy director of the Pentagon's Office of Electronic Warfare, told the Air Force Association that the United States has done little to address a quarter century of adversary advances in EW capabilities. This deficit has led DoD to develop a new EW strategy that is predicated on the ability to control the EMS. This new strategy focuses on a crucial central goal: "agile, adaptive, and integrated electronic warfare to offensively achieve electromagnetic spectrum superiority across the range of military operations."[136] The path toward cognitive EW is a crucial part of this story.

The following chapters discuss three further technologies that support the vision of advanced, autonomous reprogramming: cloud integration and data engineering (Chapter Five), flight program software and containerized microservices (Chapter Six), and onboard HPC (Chapter Seven).

[134] Casey, 2020.

[135] Lance Menthe, Dahlia Anne Goldfeld, Abbie Tingstad, Sherrill Lingel, Edward Geist, Donald Brunk, Amanda Wicker, Sarah Soliman, Balys Gintautas, Anne Stickells, and Amado Cordova, *Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 1, Findings and Recommendations*, Santa Monica, Calif.: RAND Corporation, RR-A341-1, 2021a.

[136] Wilson, 2018.

# Chapter 5. Cloud Integration and Data Engineering

In the previous chapter, we discussed what a cognitive EW system is and what it means to operationalize it. Here, we turn to creating a data pipeline, another key technology that supports cognitive EW—and, incidentally, many capabilities that the USAF is looking to develop, such as the Advanced Battle Management System to support JADC2. Cognitive EW (or anything else employing ML) will not work without data, and lots of it. The DoD Data Strategy emphasizes the need to leverage data in the near term and long term as a strategic asset. The collection of data at "the point of creation"[137] and the creation and management of data sets for training and modeling of AI capabilities are among the eight guiding principles for supporting the vision of a "data-centric organization that uses data at speed and scale for operational advantage." Hence, the need is to convert raw data to actionable intelligence.

To do so in real time, autonomous reprogramming will require data engineering methods that support the collection, retrieval, and classification of primary data that have not yet been processed for use, or are minimally processed, and thus retain many or all of their original attributes. Autonomous reprogramming also requires cloud integration strategies for cost-effective ways to store large amounts of data (data centers), to create and train AI models, to enable algorithms to process real-time data on airborne platforms (with hardware capability enhancements, discussed in Chapter Seven), and to enable edge cloud computing to enable processing of large amounts of data without encountering bandwidth and latency issues of network traversals (discussed in Chapters Six and Seven).[138] The data will need to come from multiple sensors and from future distributed and complex systems of systems. Autonomous reprogramming will also require the ability to sustain a future life cycle for data ingestion and data pipeline management, supporting ML model development, training, and deployment. In Chapter Six, we discuss cloud-based software architectural changes that would be required for faster EWIR deployments and for building and sustaining deployment pipelines (i.e., machine learning operations [MLOps]) for cognitive EW capabilities. We noted in Chapter Two the numerous technical, procedural, and policy issues involved with moving more data more quickly into the EWIR pipeline. In what follows, we focus on strategies for managing problems with the front end of the data pipeline: (1) making dark data visible, available, and analyzable; (2) structuring, sorting, and analyzing large volumes of data; and (3) further enabling multilevel data security. The interdependency of the various technologies discussed in the case studies, and, therefore, the need for parallel development of capabilities, is further elaborated in the concluding chapter of this report.

[137] DoD, "Data Strategy, Unleashing Data to Advance the National Defense Strategy," September 30, 2020a.

[138] Mahadev Satyanarayanan, Wei Gao, and Brandon Lucia, "The Computing Landscape of the 21st Century," *Ideas of the Future*, HotMobile '19, Santa Cruz, Calif., February 2019.

## Envisioning the Data Pipeline of the Future

EWIR has historically relied heavily on tactical-level SIGINT information to populate data fields required to generate models usable for software reprogramming (OFP and MDF updates). This approach is appropriate to threats that regularly emit in a reliable fashion in the EMS. In this case, the data pipeline might look like an unsteady stream of data from a few data sources in a single intelligence discipline.

Another version of a data pipeline, one that would meet the needs for a pathway to a cognitive EW capability, would differ in several ways from the historical approach. In what follows, we broadly describe five facets to an ideal data pipeline in this instance:

1. tailored tactical SIGINT data from all relevant sources
2. multiple data sources across intelligence disciplines
3. data that characterize general or baseline activity in the EMS
4. tolerance for different levels of data fidelity
5. streaming situational awareness and data availability.

Tailored access to all relevant sources of tactical SIGINT would reduce reliance on "high-demand, low-density" exquisite SIGINT collectors with well-defined processes for moving data into accessible databases. Several of these additional sources may not include data that are relevant to a particular platform's reprogramming needs because each sensor interprets data sensed from the EMS somewhat differently due to its particular hardware, and many (especially legacy) RWRs are not particularly complex in their sensing capabilities. Thus, it is necessary to tailor tactical-level SIGINT based on what is relevant in specific contexts.

Second, there is also increasing recognition that multiple intelligence disciplines are relevant for understanding activity in the EMS. Many of these sources do not include data that can be directly input to the EWIR process. Sources such as imagery and other types of SIGINT are valuable in focusing limited exquisite SIGINT collectors on high-priority needs by helping to direct collection decisions. The use of other types of intelligence data is also helpful in resolving ambiguity in the EMS environment to help with positive threat identification, in addition to tackling the problem of understanding the quality and appropriateness of the tactical SIGINT data collected.

Thus far, we have only focused on data about activity in the EMS that is associated with potential threats—in other words, anything that is not immediately known as friendly or neutral. A good data pipeline for cognitive EW would also provide insights into a broad spectrum of activity in the EMS. As we explain in the previous chapter, these fast-changing algorithms will probably work best if they are not entirely reliant on gaining high-quality information about a few very specific characteristics of a few very specific emitters. As we have described, this process can take a long time, and gaining opportunities to collect this information is not something that can be forced. Instead, these cognitive algorithms could rely on multisource information that could help characterize behaviors in the EMS that do not serve to identify a specific characteristic but, when combined with other data, can help identify an anomalous actor that might be a threat. To do this, the "other data" could be highly reliable in some cases where there is an ability to provide "ground truth." These data can then be used to at least determine what an unidentified actor is not, even if they cannot help directly determine what it is.

Finally, streaming data that are fused together is important for maintaining awareness in a rapidly changing environment. Interruptions in data access could, for example, result in important threats no longer being tracked because continuous information about them can be needed to follow their behavior. Next, we turn to the fundamental capabilities needed to architect such a data environment.

## Making Data Usable

The first piece of the puzzle is simply to make data available. This is not, of course, a simple task. It involves removing several key technological obstacles, resolving policy issues, and adapting procedures. We focus here on technologies that record, temporarily store, transfer, fuse, and stream data, noting other considerations (e.g., people, policies, processes) where applicable.

### *Current State*

The internet industry has made its money on the ability to record, store, and serve up data for a variety of future applications. Google, for example, would not be the commercial giant it is without the ability to catalog the internet and record how people use it. The growing Internet of Things relies heavily on the ability not only to sense the surrounding environment in a particular moment of time but also to record those data, store them, and deliver them to use in the broader ecosystem for the purposes of improving automation and ML, in addition to other applications, such as making sense of the broader environment. These feats within the commercial industry are accomplished through the employment of data loggers; data centers; other servers; a combination of (mostly) wireless and wired connectivity; and software to guide extract, transform, and load operations, in addition to other aspects of building, filling, and enabling others to use a data warehouse. Much, if not all, of this is orchestrated by specialized data engineers, which is generally accepted as a separate career field even if many underlying skills are similar to those of software engineers.

The defense industry has followed suit in the development of some new systems, though a seamless Internet of Military Things does not yet exist even among newer systems due to a variety of nontechnical factors. These include lack of USAF requirements for systems to connect and share data (although this appears to be changing) and contracts that enable vendor lock-ins in which vendors control data access. For legacy systems, the issue is more directly hardware related; many platforms lack one or more of the following: data recorders, sufficient onboard data processing (as described in Chapter Seven), sufficient onboard data storage, in-flight or post-flight external data processing and storage, and wired or wireless connection to external data processing and storage. One promising recent development is the QRIP and KM/RAPIDS discussed in Chapter Four.

Non–public sector[139] defense research and development has also largely embraced and technologically enabled new processes for data capture, storage, processing, and analysis. The Syracuse Research Corporation (SRC), a not-for-profit defense and intelligence research and development organization, for example, emphasizes the use of all-source intelligence about EMS threats to feed the reprogramming process as a guide for new tool development,[140] which is a substantial departure from the historical processes discussed in Chapter Two of this report. DoD writ large is working to modernize software practices and processes to manage data in the digital environment[141] but must account for ingrained legacy processes much as it must contend with legacy platforms that were not built for warfare in a software-defined world. There are numerous examples of USAF processes that were not built to optimize data capture and use.[142] The USAF Chief Data Office (SAF/CO) is spearheading a strategy to improve metadata standards and use, database architectures, legacy platform data visibility, and the overall management of the data life cycle.[143]

One step in the overarching data life cycle worth calling out is that of quality assurance (QA) and quality control (QC). This is a critical but potentially very time-consuming task if relying largely on manually completed steps, and it is impossible to do effectively if there are very large data volumes in question. QA/QC in the commercial computing industry is automated with humans in the loop at system and enterprise levels (i.e., above the level of individual data) to ensure that the broader process and systems are working. This is a much more manual process when it comes to intelligence data because of the persistence of legacy processes and division of roles and responsibilities between organizations that require hand-offs. Historically, this likely made sense for times when automation was less capable and reliable and could not be used to support military missions that literally could have life or death consequences. Given modern digital infrastructure, automation is now quite effective, and one can argue that the level of digitization of commercial industries and the public's reliance on them could now provide a more relevant analog to risk in military settings than they did before. In other words, use of automation for data QA/QC in commercial settings probably provides good reassurance that these tools work (for the most part) and can be further explored for military applications. Using such tools more expansively for USAF intelligence data, however, would require substantial changes to culture, process, and organizational boundaries. This would be difficult to do but is worthy of additional consideration, given the lengthy backlogs of unanalyzed intelligence data (for example) that by themselves could cause a quality problem because of the lack of relevance of old data.

[139] The non–public sector category includes both the commercial/private sector and the not-for-profit or voluntary sector.

[140] SRC, Inc., "Electronic Warfare Intelligence Production & Programming," webpage, undated.

[141] See, for example, DoD, *DoD Digital Modernization Strategy*, July 12, 2019.

[142] Tingstad et al., 2021.

[143] Air Force Chief Data Office (SAF/CO), *Data Services Reference Architecture*, USAF, March 2019.

The final part of this discussion is data fusion. There are numerous examples of robust data fusion, especially in the commercial world but also for military applications. In many cases, the fusion is used to generate visualizations that enable awareness. For example, FlightAware is a commercial company that integrates ground- and space-based Automatic Dependent Surveillance-Broadcast position data and information from flight plans and datalinks into real-time aviation picture maps.[144] FlightAware uses several different algorithms to manage data so that the service is able to crunch 10,000 aircraft position messages each second. In another example, integration of data from different sensors—and from different nearby vehicles—is how autonomous vehicles are able to work without crashing into objects around them. Autonomous vehicles may fuse information from cameras, radar, and lidar to combine the identification, speed, and distance data associated with obstacles.[145] One military example is the development of the Talon Thresher tool as an approach to fuse data from many different sources and present both a common operating picture (COP) and a common intelligence picture.[146]

### Future Development

The commercial industry is continuing to work to make data management more efficient. In particular, a current focus is on low-latency applications, such as autonomous vehicles. There is still a need for even faster responses between edge and more-centralized databases when it comes to data exchange to support applications such as “sense-and-avoid,” for which even a very marginal improvement in timing could make a variety of autonomous platforms safer. Future technological improvements in data management rely in improving technologies and concepts for things like hardware miniaturization (discussed in Chapter Seven) and cloud computing (discussed below). The more processing that can be packed into or very close to a small edge device (e.g., on an aircraft in flight), the faster data can be used to sense and respond to the environment. Part of this is managing processing across devices, which the commercial industry is continuously improving through the use of software that dynamically shares processing loads across devices to efficiently use spare capacity where it is available. One (potentially) useful advancement could be the development of new software-defined ways to batch portions of a job across devices with spare capacity, or even interrupt a job on a device that is suddenly prioritized for some other purpose and transfer the work mid-job to another available device with spare processing capacity.

[144] FlightAware, “FlightAware’s Data Sources,” webpage, undated.

[145] See, e.g., J. Kocić, N. Jovičić and V. Drndarević, “Sensors and Sensor Fusion in Autonomous Vehicles,” 2018 26th Telecommunications Forum (TELFOR), 2018.

[146] Brent N. Harms, *Data Fusion as Software Solution for 2018 OIR Lessons Learned and JADC2*, Air War College, Air University, March 27, 2020.

## Handling Large Data Volumes

The second piece of the puzzle is about data management when there are large volumes of data. USAF sensing systems produce growing quantities of data—so much that existing humans and machines cannot sort, store, and examine anywhere near all of it. Thus, work needs to be done to manage the large data volumes that are key for training and improving ML algorithms and to avoid the potential for critical data loss simply because there is so much of it. We focus here on cloud-based storage and data integration.

### *Current State*

Several major commercial technology companies offer and are continuously developing cloud-based solutions for data storage and management. With the volume of data created through internet use and networked devices, and with the advent of technologies such as supercomputing (e.g., to run weather and climate models, and in computational biotechnology), it quickly became clear that very few data users had the infrastructure, space, and funds to sustain sufficient data storage and processing capabilities to meet their needs. Furthermore, it is difficult to share and integrate such a large volume of data.

The initial cloud concept was that users could tap into some centrally located data center or other server infrastructure via network connections to meet data storage and processing needs. This idea then quickly evolved in several directions to help meet emerging needs. Use of centralized servers expanded to include more services beyond basic data management—for example, to host applications for users to manipulate data. Now, a user can access a virtual machine through cloud services. A virtual machine mimics a physical computer and is accessed through a physical computer but allows users to share specialized software and analyze cloud-stored data, as examples. Some cloud providers, such as Google, offer different virtual machine options, ranging from general purpose to those optimized for processing power, memory, and ML.[147]

Although a public cloud was a useful way to distribute services to the widest possible audience, private clouds also emerged for specialized users with a need to maintain more-secure access to their data and services. As previously mentioned, low-latency applications such as autonomous vehicle operation require faster connections with data processing, storage, and analysis centers than is generally possible with the centralized cloud model. Increasing the number of cloud physical points of presence around the world has begun to resolve this issue. But the more significant advance has been the advent of the hybrid cloud concept, in which software directs some processing and a little storage space to hardware that is on or physically close to a sensor that ultimately connects with more-centralized processing and storage for work that is beyond the capacity (and is not relevant for operation of) hardware at the edge of a network.

[147] Hanan Youssef, “Compute Engine Explained: Choosing the Right Machine Family and Type,” Google Cloud blog post, July 9, 2020.

Recent cloud engineering has been substantially supported by other development, such as growth in computer chip processing power (though the historical ability to incrementally increase power is waning because of physical limitations), as well as network connectivity (speed and diversity of connections). The development of ML accelerators, computer chips optimized for ML as opposed to general processing, brings even more specialization to cloud services that can include environments that exclusively support ML.

We discuss the particular hardware needed for more rapid OBP in Chapter Seven, but we note here that other forms of hardware, such as datalinks, will continue to be critical for other key aspects of cognitive EW, even while cognitive EW capabilities could be supported by edge clouds that are entirely composed of infrastructure at the edges of networks. These edge clouds also rely on additional hardware to support distributed metadata storage and sync services to account for times when the edge is off network.[148] An edge cloud also delivers the cloud computing capabilities at the tactical edge, circumventing the bandwidth and latency issues of datalinks and of the computational tasks of cloud-based software by reducing the need for network traversals to traditional data center-based cloud infrastructures.[149] In other words, edge cloud computing allows the migration of computational tasks to the edge, thereby supporting low-latency requirements of a weapon system and its software, hardware, and capabilities.[150] This capability of an edge cloud is discussed further in Chapter Six.

Cloud technology is one area in which the defense industry and government organizations have more or less unilaterally chosen to look to commercial industry partners for services. DoD continues to examine which commercial cloud service it will select to support its cloud needs at scale. As of June 2021, Microsoft Azure and Amazon Web Services were considered the primary contenders, with a prior Azure contract under the Joint Enterprise Defense Infrastructure program having been terminated.[151] Amazon Web Services also reports having 22 national security and defense partners, including some major contractors, such as Northrop Grumman and Lockheed Martin.[152]

### *Future Development*

From a USAF perspective, future innovations would include operationalizing a cloud wherever the air component needs it. One relatively simple idea is exploring how aircraft

[148] See, e.g., Yung Xiong, Yulin Sun, Li Xing, and Ying Huang, "Extend Cloud to Edge with KubeEdge," *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, October 25–27, 2018.

[149] Ikhwan Ismail Bukhary, Ehsan Mostajeran Goortani, Mohd Bazli Ab Karim, Wong Ming Tat, Sharipah Setapa, Jing Yuan Luke, and Ong Hong Hoe, "Evaluation of Docker as Edge Computing Platform," *IEEE Conference on Open Systems*, 2015.

[150] Ali Elgazar and Khaled. A. Harras, "Enabling Seamless Container Migration in Edge Platforms," *CHANTS: Challenged Networks*, Los Cabos, Mexico, October 25, 2019.

[151] DoD, "Future of the Joint Enterprise Defense Infrastructure Cloud Contract," July 6, 2021c.

[152] AWS, "Explore AWS Partner Profiles, Solutions, Case Studies, and Locations," webpage, undated.

without grave limitations on SWaP, such as the C-130 or RC-135, could be used as physical points of presence for a highly mobile hybrid cloud.

In the further future, packing even more processing and storage capability into smaller spaces using next-generation chip and other minimized hardware technologies will essentially enable the cloud itself to disappear, creating more of a "swarm" of nodes that share data, processing loads, and storage space. In addition to relying on even more HPC in even smaller spaces, this envisioned technology will require a new generation of high-speed datalinks.

## Enabling Multilevel Security

A cloud-based model in which data centers are used efficiently for various purposes and software controls access to various components therein (rather than relying on air gaps between disconnected hardware) presents a potential data security challenge. Thus, a third puzzle piece has to do with the necessary security measures to keep data, and ultimately the U.S. national security enterprise, safe. Here, we discuss some recent commercial and open-source partnerships that are holding promise not only to resolve this problem but also to create a *more secure* situation.

### *Current State*

Intelligence data and information have long had multiple levels of classification, and thus data streams used for EWIR (among other needs) require multiple levels of security. As we discuss here, multiple levels of security need not necessarily mean siloing data to the greatest extent possible. Rather, there are some methods of making more data available to users that have the right accesses. However, this does not take the place of the necessary policy discussions about which data require various levels of security.

The current model employed to enable data security is to keep data on different secure networks that cannot talk to each other. This results in data becoming trapped on one network or another and/or duplication of data across networks. This also means that, in some cases, there are multiple instances of different applications, which makes management and upgrades of these more cumbersome and time intensive for humans.

### *Future Development*

When it comes to having multiple levels of security, the good news is that technological solutions exist or are in development that may not require huge shifts in policies about information-sharing and data access. However, adopting these solutions will require a new mindset in which decisionmakers are willing to accept a software-based solution to the problem rather than a hardware-based solution. Emerging solutions to multilevel data access build on developments in cloud infrastructure and specifically in how efficiently data centers are configured and used. The new model is about securing data, rather than securing networks. In this model, data with different access requirements reside on the same network and/or in the same data center infrastructure, and access is controlled by software. In one model being explored by both defense and commercial industries (sometimes in collaboration), users on multiple networks can access data in the same data center infrastructure. The network they are using for access delineates how much each user can see and have access to. A user with the greatest amount of access can see everything, and those with less access only see the portion they are allowed to see. When a user with high access manipulates data on the lower-access portion of the security spectrum, those data are then moved up in security to that user's access level.

The defense industry is now collaborating with open-source and other commercial entities to develop multilevel secure databases. For example, Lockheed Martin worked with several non–defense industry partners (including open-source partners) to create a new object-relational database to support the National Reconnaissance Office. This technology has been billed as secure and also as enabling effective data fusion capabilities that analysts can use to stream real-time data to their desktops.[153]

These types of software-defined solutions are useful in enabling more-flexible access in instances in which data currently trapped on a network do not all need to be at that level of security. However, it still does not solve the policy problem of data access if there are blanket policies (for example, about data coming off a specific collection platform) about who can access which data.

Better security is enabled in a cloud-based model because it better enables streamlined and rapidly updated security protocols. Furthermore, software-based access controls can operate at the level of a single data packet, which makes it more difficult for a bad actor to gain access to all the data on a server even if they are able to intrude.

The technology areas discussed in this chapter address three important pieces of the data management puzzle. Next, we turn to the important and related topic of containerized software.

[153] George Leopold, "NRO Jumps on Open Source Bandwagon," *Defense Systems*, June 26, 2015.

# Chapter 6. Flight Program Software and Containerized Microservices

One of the objectives of this study is to research various technologies and standards for the improvement of the EWIR process timelines, including those of software deployments. The goal is to achieve a continuous software integration and deployment pipeline using the concept of DevSecOps.[154, 155] In Figure 3.3, we identified this need as a part of the early wins and foundational changes. Some of these changes, including airborne, in-theater MDF updates, are less disruptive and more achievable as early-win solutions (as discussed later in this chapter). Software update processes, however, would require moving to newer architectural paradigms that support deployment time modularity[156] for rapid capability deployments and DevSecOps and to support algorithms for future autonomy (i.e., to provide the infrastructure support for fielding AI/ML and cognitive EW capabilities in the future).

Software is possibly the most prevalent, yet oftentimes the most overlooked, aspect of a weapon system. It is a critical technology and technology enabler in modern USAF platforms forming the core element of flight instrumentation, avionics, flight control systems (including pilot-vehicle interfaces), OFPs, and real-time operating systems (RTOSs). Software forms the brain of a platform and supports practically all capabilities that compose a system's avionics, including the central display units; radars; integrated core processor; weapons; communication, navigation, and identification systems; mission support, including the EW system; and simulation tools. The reliability and longevity of a weapon system depends on how well a weapon system's software is developed and integrated and how flexible is its design to support the addition of new capabilities.

[154] In this report and accompanying reports, we highlight the importance of DevSecOps as a shift in the culture of software development to enable integrating the various steps of development into a continuous and automated software delivery process, thus removing bottlenecks such as those related to timelines and to the deployment of capabilities. We recognize that DevSecOps and DevOps cannot be prescriptive and therefore cannot be mandated with a "one size fits all" approach across the USAF. DevSecOps is a process of including testing and security as a part of development, automation, and delivery cycles, and the USAF should strive to create the frameworks to enable this cultural change.

[155] Continuous integration, continuous delivery (CI/CD) is also part of DevSecOps. See DoD, "DoD Enterprise DevSecOps Reference Design, CNCF Kubernetes," Version 2.0, March 2021b; and DoD, *DevSecOps Fundamentals Playbook*, Version 2.0, March 2021a.

[156] Most platform software programs achieve runtime modularity, however, they may lack the design for deployment modularity—design of how software code is packaged that will enable decoupling of functions and faster deployments. Newer paradigms of software architectures advocate packaging of the deployment code that enables both run-time and deployment time modularity. See Paul Bakker and Bert Ertman, *Building Modular Cloud Apps with OSGi*, 1st ed., O'Reilly Media, 2013; and Gabriel Baptista and Francesco Abbruzzese, "Microservices and the Evolution of the Concept of Modules," *Hands-On Software Architecture with C# 8 and .NET Core 3*, Packt Publishing, 2019.

Weapon system software is a generic term used to describe an intricate set of embedded flight control programs that interact with the platform hardware, core avionics, and each other[157] and respond to various management, functional, and operational needs of the platform. These software programs differ significantly from other systems and applications, such as command, control, and communications systems and other defense ground applications. Typically, various flight and weapon controls have distinct avionics subsystems and related computers with dedicated embedded operational software,[158] or OFPs, programmed for mission support. However, the extent of this separation of subsystems and related software depends on the avionics architecture of the platform, as will be illustrated in the following sections.[159]

Almost all platforms supporting EW have an EW suite of avionics subsystems (Figure 6.1).[160] These EW subsystems are supported by the embedded software, which consists of the OFP and the MDF. The software processes the emission signals detected in the EMS and defines any related operations for the platform to take in response. For example, for a countermeasures dispenser EW subsystem, the input signal/EM emission data received is processed by the OFP, which uses the MDF to determine the mission parameters for the platform and calculates the optimal response based on the platform's speed and position. As mentioned earlier in this report, both the OFP and MDF are programmable components of a platform; the former determines the capabilities of the EW suite, and the latter determines its mission response based on theater data sets and extensive planning. Both OFP and MDF require reprogramming and updated software deployments based on new threat data and threat impact analysis and resolution (EWIR process[161]), new capability needs, and resolutions for existing deficiencies (bug fixes). These updates take a long time to field, with only specific exceptional cases, because of dispersed development (multiple vendors) and software release schedules, security and safety verifications, and DT&E and OT&E timelines.

A platform's software design depends on its underlying avionics architecture. Hence, the software design could vary between its subsystems and functions or could be more integrated across functions, depending on the avionics architecture. This applies to the OFP(s) of all of a platform's operational and mission functions, including its EW suite. To explore the solutions for faster software updates and deployments for EW, we will first take a deeper look at the current issues with these updates, particularly with respect to the EWIR process. We will then

[157] For example, they could interact via a 1553B data bus interface with other electronic countermeasure and avionics systems on the platform. See Raytheon Technologies, "AN/ALR-69A[V] Radar Warning Receiver," webpage, undated; and H. R. Schnelle, H. O. Sees, and D. P. Floyd, "Integration of the AN/ALQ-131(V) Electronic Countermeasures Pod on Tactical Aircraft Using a MIL-STD-1553B Interface," *Proceedings of National Aerospace and Electronics Conference (NAECON '94)*, Vol. 2, 1994.

[158] *Operational software* typically refers to both MDF and OFP. In this particular usage, we refer more specifically to the OFP.

[159] In this chapter, the use of the term *OFP* going forward refers to OFP software specifically related to the EW capability of the platform.

[160] Some subsystems may have multiple EW functions integrated within them.

[161] AFI 10-703, 2017.

briefly delve into the fundamental differences between platform OFP(s) and the two types of current avionics architectures that dictate their design. Next, we will look into the differences in fifth-generation and legacy platform software and their respective drawbacks. This will be followed by an analysis of the more recent open software architectures and software engineering practices followed by DoD, the USAF, and the suppliers to understand the reasons for delays in fielding updates despite these practices. Finally, this chapter will introduce a new pathway for the USAF in general, and the EWIR community in particular, to incorporate new agile software engineering practices, DevSecOps, and future ops support for AI/ML and cognitive EW capability development. The chapter provides an argument for the adoption of containerized microservices[162] for future weapon systems software; their advantages in terms of speed of deployment, stability, and long-term sustainability; and the process and cultural changes that such an adoption may entail.

## Current Issues Related to Software Updates and Deployments in the EWIR Process

Chapters One and Two illustrate the issues in the EWIR process, including those related to deployment of reprogrammed software. Here, we will investigate a few additional factors that contribute to the delays in the deployment of software updates in the EWIR process and, more generally, for the USAF platforms.

### *OFP and MDF Update Processes and Related Issues*

To reiterate the current issues with the EWIR process, the final step of the process[163] is to field reprogrammed software (and/or minor hardware upgrades) for new threat information (MDF) and capabilities (OFP)[164] and/or as fixes for deficiencies. Deployment of new software requires verification of security or, sometimes, post-production (software development and release) security hardening,[165] airworthiness recertification, and DT&E and OT&E end-to-end regression testing. These requirements add anywhere from months (for MDF) to almost two years (for OFP) to the process. MDF programmers sometimes have to resort to adding workarounds or stopgap solutions for OFP inadequacies within the mission data update to

[162] As noted above, this report does not prescribe the size or granularity of the microservices themselves. The sizes of microservices in the commercial industry, for example, vary from an entire application containerized with its dependencies to be deployed for a larger commercial enterprise platform—for example, a search engine or graph database application—to granular services and functions within a single application. This report uses the term *microservices* to advocate for the development of independent services within an application or platform with well-defined interfaces so as to enable independent deployment of service-specific or system-specific software.

[163] The unclassified name of the process is PACER WARE, as mentioned above.

[164] Once again, new capability developments are usually pushed back (i.e., downgraded in priority) to cater to bug fixes. Sometimes new capabilities take several iterations of the OFP update to be developed. This is more often true for newer, fifth-generation platforms than for legacy platforms (SME interview, March 11, 2021).

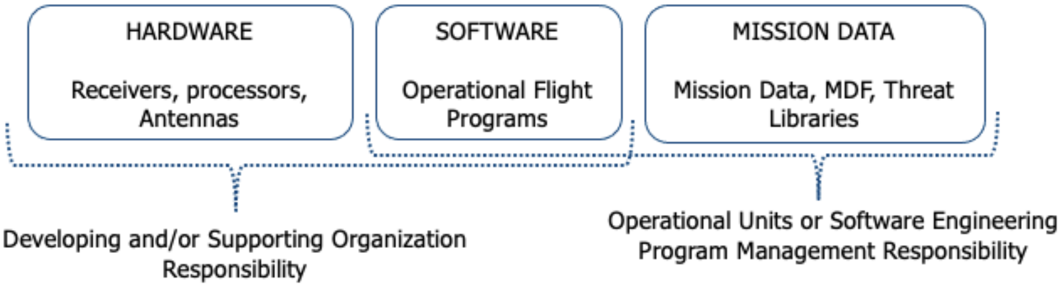
[165] SME interview, August 17, 2021.

circumvent these long deployment timelines. These stopgap solutions are used to trick the system into performing or responding in a particular way until a routine software change provides the necessary functionality.[166] These types of solutions might make the software inflexible to future software updates[167] and also affect the performance of the platform in the long run.

### *Fragmented Responsibilities for Software Updates*

OFP software programs are still largely proprietary (with a few exceptions of USAF-owned legacy software) and complicated, causing long fielding timelines due to the reasons mentioned above, along with code complexity and process requirements. To understand the reasons for the impediments and delays in EWIR software deployments, it would be useful to understand the separation of ownership, responsibilities, and management of hardware, OFP, and mission data. Figure 6.1 shows a generic division of responsibilities for an EW subsystem.

**Figure 6.1. Typical EW Subsystem Elements and Ownership/Responsibilities**


HARDWARE
Receivers, processors, Antennas
SOFTWARE
Operational Flight Programs
MISSION DATA
Mission Data, MDF, Threat Libraries
Developing and/or Supporting Organization Responsibility
Operational Units or Software Engineering Program Management Responsibility

SOURCE: RAND analysis, adapted from North Atlantic Treaty Organization Research and Technology Organisation, *Electronic Warfare Test and Evaluation*, AC/323(SCI-203)TP/471, RTO AGARDograph 300 Flight Test Technique Series, Vol. 28, 2012.

The subsystem hardware and OFP are generally provided by a vendor and are proprietary.[168] Mission data analysis, planning, and MDF programming is the responsibility of the USAF and the EWSs under the 350th SWW.[169] In an EW suite,[170] most of the subsystem OFP(s) are proprietary. Some of the OFP software, particularly in fifth-generation platforms, is developed

[166] SME interview, March 5, 2021.

[167] Any new OFP update might create a mismatch with the MDF stopgap solutions and require additional testing to ensure consistency.

[168] Even for legacy systems such as the F-16, while the core OFP suite is owned by the USAF, the related hardware can still have proprietary elements, and some subsystems, such as EW, are mostly proprietary. OFP development is owned by the program offices and is contracted out to the air frame prime contractor. See USAF, *Weapon Systems Software Management Guidebook*, 2008.

[169] The 53rd EWG under the SWW is the Operational Reprogramming Center for the CAF.

[170] This could refer to EW subsystems with multiple OFPs and provided by more than one vendor or even two separate OFPs or an OFP hosted on two processors in some cases. See Navy SBIR, "Future Airborne Capability Environment (FACE) Compliant ALE-47 Operational Flight Program Software Application," February 2018.

as computer software configuration items (CSCIs) for different subsystems by different vendors or suppliers that are then integrated before deploying the software. The prime system integrator is responsible for final system integration and testing before the software is released for deployment.[171] This splitting of responsibilities, compounded with the long requirements and development processes and other architectural issues (especially of older platforms), is part of the reason for delays.[172] Despite the adoption of newer software engineering practices and processes in fifth-generation platforms, the ownership and development of CSCI software by different vendors in different development environments adds to the delays in update timelines. Additionally, because of differences and inconsistencies in development, integration, and testing (including flight test) environments, the software sometimes reveals system stability issues and faults introduced by the software change only during DT&E and OT&E, thus slowing deployments.[173] The introduction of the agile defense acquisition model for software deployments (i.e., the DoD Continuous Capability, Development, and Delivery [C2D2] model detailed later in this chapter) has not managed to bring about significant changes in the timelines of software updates and the deployment of new capabilities.

### *Testing Bottlenecks*

The main bottlenecks for faster software deployments, however, are the testing, security hardening, and safety certification cycles. When a platform receives a new OFP update for a subsystem (from a vendor or the USAF[174]), it goes through testing phases, which include airworthiness,[175] DT&E, and OT&E.[176] Airworthiness is a safety certification process that can take several months to years, depending on the change.[177] The USAF airworthiness certification process for OFP or software changes and avionics follows software and hardware safety certification standards called DO-178B/C and DO-254,[178] respectively. If any enhancements or

[171] CSCI software is generally audited and tested individually and after all the subsystems are integrated in a process called the software functional configuration audit. See USAF, *Weapon Systems Software Management Guidebook*, 2008.

[172] SME interview, August 17, 2021.

[173] DoD, Director, Operational Test and Evaluation, *FY 2019 Annual Report*, December 2019, p. 19; and SME interview, March 11, 2021.

[174] Core OFP updates for the F-16 OFP suite, for example, are developed by the Air Force Software Engineering Group ((SME interview, August 17, 2021).

[175] Airworthiness approval is necessary for a new configuration or weapon system modification to a previous unfielded configuration. In such cases, airworthiness certification is required before test execution commences. See Air Combat Command, *Instruction 99-101: ACC Test and Evaluation*, August 24, 2020.

[176] OT&E includes initial operational testing and evaluation and other categories. See Air Combat Command, 2020.

[177] SME interview, October 2021.

[178] Vance Hilderman, "DO-178B and DO-254: A Unified Aerospace-Field Theory?" *Military Embedded Systems*, February 2009; Emma Helfrich, "DO-178 Continues to Adapt to Emerging Digital Technologies," *Military Embedded Systems*, March 2021; Department of the Air Force Headquarters, Air Force Life Cycle Management

new capabilities are added to the OFP software, the platform generally has to go through an airworthiness safety certification process.[179] Additionally, DT&E can take up to 18 months, and OT&E takes a minimum of six months.[180] DT&E and OT&E certify whether the OFP is production-ready for the USAF platform. Frequently, these phases would reveal new bugs or performance issues that have been introduced during the latest update.[181] These issues are then reported as deficiencies for the next update cycle, unless the weapon system does not perform according to the expected key performance requirements.[182] Because of the regularity of issues with system performance or the introduction of new issues with each update, the development and fielding of planned new capabilities are pushed into a backlog.[183]

Another process that adds to the time delays in OFP software deployments is security hardening. With every software update, regardless of the size or type of change (a bug fix or a new capability), the weapon system may become vulnerable to cyber threats.[184] Security verification is an important process to ensure that the software update does not leave the platform vulnerable. In many cases, the security hardening and verification process is completed after software development and release and could take up to three months of additional time.[185] Many of these efforts are splintered into cyber silos for different units and agencies.[186] Some of these efforts are closer to the mission or are part of the mission planning process, where OFP cyber vulnerabilities and threat surfaces are discovered and addressed prior to a mission. Security patches seem to be the best way to address many of the cybersecurity issues found in systems and software after development.[187]

Center (AFMC) Engineering Directorate, *Airworthiness Circular—Verification Expectations for Select Section 15 Criteria*, Wright-Patterson Air Force Base, March 2017; and Department of the Air Force, *Department of Defense Handbook: Airworthiness Certification Criteria*, Military Handbook MIL-HDBK-516C, December 2014.

[179] Airworthiness certification is required after any change in a platform's software, hardware, and other configurations, unless the change could be proven to be independent and to have no impact on the platform's performance and stability (Department of the Air Force, 2014).

[180] SME interview, March 11, 2021.

[181] Joint Strike Fighter, Block 4 (DoD, Director, Operational Test and Evaluation, 2019, p. 19; and SME interview, March 11, 2021).

[182] As a very rare case, an OFP update was rejected because it did not meet all the essential performance requirements (SME interview, March 11, 2021).

[183] DoD, 2019, p. 19.

[184] Kris Osborn, "Air Force Operationalizes New Cyber Security Plans," *Defense Systems*, June 2017.

[185] SME interview, August 17, 2021.

[186] Greg Hadley, "Air Force Leadership Needs to 'Walk the Walk' in Baking Security into Cyber, Software Boss Says," *Air Force Magazine*, August 12, 2021.

[187] Osborn, 2017.

### *OFP Architectural Disadvantages*

Several of the issues mentioned above are persistent even with some adoption of new software development methodologies.[188] Two key issues are (1) development and, in some cases, agile development, without the necessary production support, and (2) delayed or post-production security hardening. Another important reason for these delays in the timely deployment of OFP software is the architectural disadvantages of platform software, particularly legacy platform software, and the lack of a functional development and operations (DevOps) cycle with fully incorporated security testing and enhancement. Architectural disadvantages include the lack of decoupling and reducing the interdependencies of functional components. This leads to software changes or integration for one functionality affecting the performance or stability of another functionality or that of the platform.[189] Thus, most weapon systems software lacks the necessary decoupling for deployment time modularity (discussed below) and, hence, lacks support for faster development, testing, and deployment cycles.

The next section will address the architectural differences between different platforms and the reasons for issues with software deployments and testing for each.

## Avionics Architectures and Related OFP Design

Early OFPs had software for each embedded subsystem with sequential logic and Boolean decision trees. In other words, much of the logic was linear with multiple, conditional "if-else" type blocks of code defining the behavior of the system. For EW, mission data were hardwired into the OFP software.[190] This resulted in the addition of conditional logic for special cases with each update (new capability or mission requirement), creating monolithic software that is difficult to maintain and does not lend itself to redesign into logical components.[191] Even today's functional legacy platforms have monolithic OFPs with no clear design and are written in low-level or legacy languages such as ADA 95, low-level C,[192] and even machine-level functions.[193] OFP software, however, differs significantly between legacy and fifth-generation platforms. This is due to the underlying avionics architectures of these platforms. Avionics architectures essentially define the way in which the OFP for a platform is designed and how this design influences the development and testing processes for the platform. Thus, it is important to briefly look at the differences between these architectures. Overall, the underlying

[188] Lara Seligman, "What F-35 Can Learn From F-22 Upgrade Hiccups," *Aviation Week and Space Technology*, March 28, 2018.

[189] DoD, Director, Operational Test and Evaluation, 2019, p. 19; and SME interview, March 11, 2021.

[190] Neese, Brantley, and Pitarys, 1991.

[191] This difficulty persists even though new capabilities built for legacy systems have a more modular design with some promise of interoperability with other platforms (SME interview, August 17, 2021).

[192] Navy SBIR, "Future Airborne Capability Environment (FACE) Compliant ALE-47 Operational Flight Program Software Application," webpage, January 2018.

[193] SME interview, August 17, 2021.

architecture of a platform defines the avionics mission computers, hardware, and software requirements and their interactions and interoperability.[194] The two primary avionics architectures are federated avionics architecture and integrated modular avionics (IMA) architecture. The modularity and partitioning of software and hardware in platforms designed on both these architectures enable either separate OFPs for various subsystems or an integrated OFP based on various CSCIs.

### *Federated Avionics Architecture*

Federated avionics architectures have dedicated subsystems composed of avionics, mission computers or processing units, and related OFPs for various functions. Each of these subsystems, also called line replacement units or line replacement modules, are independent, partitioned systems with specialized hardware and software. Each subsystem has specific interfaces with its sensors and effectors. The interfaces between subsystems are defined by the interface control documents, which primarily define only the acceptable data and message structures, and not the implementation logic of the interface itself.[195] This type of architecture resulted in duplication of resources, both software and hardware, which are not generally open or reusable.[196] For legacy platforms with federated avionics architecture, many of the OFPs (in the OFP suite for various subsystems) have monolithic software with no specific core design.[197] New capabilities and enhancements result in additional layers of conditional software code and updates to interfaces between subsystems. Due to this lack of decoupling of deployable code, an OFP software deployment for even a single subsystem generally requires end-to-end platform testing for safety certification, DT&E, and OT&E. This results in long deployment timelines for OFP software despite the independent and partitioned design of federated subsystems.[198]

### *Integrated Modular Avionics Architecture*

IMA architecture was developed to create a more integrated platform with shared computing processors and optimized avionics functions, such that each processing unit on the platform supports shared apertures or a suite of various subsystems.[199] IMA was primarily designed to reduce airframe weight, power consumption, and maintenance costs. In addition to shared

[194] Cody Fleming and Nancy Leveson, "Improving Hazard Analysis and Certification of Integrated Modular Avionics," *Journal of Aerospace Information Systems*, Vol. 11, No. 6, 2014, p. 399.

[195] Fleming and Leveson, 2014, p. 399; and René L.C. Eveleens, *Open Systems Integrated Modular Avionics—The Real Thing*, National Aerospace Laboratory NLR, Amsterdam, North Atlantic Treaty Organization Research and Technology Organisation, RTO-EN-SCI-176, 2006.

[196] Christopher B. Watkins and Randy Walter, "Transitioning from Federated Avionics Architectures to Integrated Modular Avionics," IEEE/AIAA 26th Digital Avionics Systems Conference, 2007, pp. 2.A.1-1–2.A.1-10; Eveleens, 2006; and Fleming and Leveson, 2014, p. 399.

[197] SME interview, August 17, 2021.

[198] SME interview, multiple dates.

[199] Ian Moir and Allan Seabridge, "Military Avionics Systems," Wiley, 2006.

computing, IMA architecture also has shared communication and input/output resources.[200] The architecture requires the use of hardware partitioning and virtual machines to support the management of the allocation of time, memory, processing power, and other resources to various supported software applications.[201] The introduction of newer programming languages and software methodologies such as service-oriented architecture (SOA) and, more recently, open systems architecture (OSA)[202] has allowed the development of more modular software (e.g., components, subcomponents, and interfaces) primarily for IMA fifth-generation platforms.

Although IMA is supported by a more modular architecture as compared with federated legacy systems and reduces the number of avionics subsystems with dedicated communication, input/output, and other resources, many platforms based on IMA still have proprietary line replacement modules with specific functions, software, and hardware that are not reusable. Partitioning, high-speed buses, and module standards and designs are also proprietary even with the implementation of open IMA architecture.[203] Hardware partitioning and virtual machine–based applications in many IMA platform OFPs are built on the CSCI integration approach. Even with the level of partitioning provided, system integration and avionics software still face stability issues caused by different development and testing environments of various vendors. These issues, as mentioned above, are generally discovered during DT&E and OT&E phases, further delaying the deployment of software updates to the platforms.[204]

### *Open Avionics Architectures*

Open avionics architectures for a weapon system platform comprise various standards defined for software, hardware, network, and sensor and signal processing for safety-critical

[200] Watkins and Walter, 2007; Fleming and Leveson, 2014, p. 398.

[201] The shared resources include the RTOSs, central processing unit(s), memory management unit(s), and input/output handlers (Fleming and Leveson, 2014, p. 398). The IMA assumes that a set of time-critical and safety-critical real-time applications (avionics units) may be executed on one microprocessor module. To cope with this level of criticality, new RTOS architecture has been suggested. ARINC 653 defines generic structure of the system and the logical structure of RTOSs. See Slawomir Samolej, "ARINC Specification 653 Based Real-Time Software Engineering," *Informatica*, Vol. 5, No. 1, 2011.

[202] DoD, under the requirement of the National Defense Strategy, has been working to produce an OSA guideline for the modification of software for major weapon systems. The DoD Modular Open Systems Approach (MOSA) has been a standard for DoD for 20 years and has been formally mandated by recent legislation. Open Mission Systems (OMS) and Future Airborne Capabilities Environment (FACE) come under the umbrella of MOSA. While OMS has been implemented successfully to a certain extent in weapon systems for the standardization of interfaces, FACE, which is an important standard for developing portable and interoperable software components, has been difficult to mandate and so far lacks the necessary specifications to be effective. MOSA, more generally, has also been difficult to implement given the acquisition strategies and proprietary software of weapon systems. In this report, we will refer to OSA as a paradigm rather than a successful mandate.

[203] Eveleens, 2006; Watkins and Walter, 2007; Michael J. Brown, Robert D. Fass, and Jonathan Ritschel, "A Case for Open Mission Systems in DOD Aircraft Avionics," *Air and Space Power Journal*, Vol. 33, No. 4, Winter 2019.

[204] DoD, Director, Operational Test and Evaluation, 2019, p. 19; SME interview, March 11, 2021; and DoD, Director, Operational Test and Evaluation, *FY 2016 Annual Report F-22A*, August 2016.

systems.[205] DoD and the USAF have recognized several different standards.[206] Here, we will concentrate on the software standards.

The concepts of open avionics and OSA have been around for over two decades. SOA and OSA have been applied to embedded weapon systems and avionics software design and implementation[207] for several years. SOA forms the primary concept for service-oriented subsystems and service-oriented avionics middleware for the OMS standard developed by the USAF.[208] SOA has been considered the base architecture to redesign a modular OFP for various tasks in an IMA platform.[209] Even in legacy platforms with federated architecture, SOA has been implemented in subsystem OFPs—for example, the OFP for the fire control computer of the Block 30 F-16 aircraft.[210] OSA was introduced as a part of DoD's acquisition strategy to enable cost-effective software development acquisitions that allow DoD to manage software intellectual property and competition for software upgrades, thereby removing vendor lock-ins, speeding deployment of new capabilities, reducing cost through competition, and enabling portable and interoperable software.[211]

OMS is a DoD and USAF OSA specification that primarily defines an open standard for interfaces between services and subsystems of a platform. OMS also specifies open data exchange standards. OMS was designed to enable reusability, extensibility,[212] interoperability of interfaces, and rapid integration of new subsystems or capabilities.[213] Many fifth-generation USAF platforms today are OMS compliant. While OMS is a standard for interfaces between subsystems, services, and sensors, DoD is working toward a technical standard for the

[205] Examples are FACE and OMS/UCI for software, VICTORY for Network, MORA for RF/Signal processing, and OpenVPX for hardware. See U.S. Department of Defense, Deputy Director for Engineering, *Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs*, May 2020; Chris Crook and Chip Downing, *System Architectures, MOSA and the FACE Technical Standard 2020*, The Open Group, December 2020; and Chris Garrett, "Open System Standards and Agile Acquisition," Air Force Life Cycle Management Center, 2018.

[206] Richard Kirk, "MOSA/SOSA: A New Dawn for Military Computing," *Abaco Systems*, June 12, 2019; John Keller, "SOSA Open-Systems Standard Gains Momentum for Embedded Computing; Snapshot 3 by April, 1.0 Later This Year," *Military and Aerospace Electronics*, February 3, 2020.

[207] Joyce L. Tokar, "A Comparison of Avionics Open System Architectures," ACM SIGAda, *Ada Letters*, Vol. 36, No. 2, December 2016, pp. 22–26.

[208] U.S. Air Force Life Cycle Management Center, "Open Mission Systems in a Nutshell," undated.

[209] Robert Bond, "Air Force Evolution to Open Avionics—HPEC 2010 Workshop," presentation, September 2010.

[210] Mitch Chan, *Applying a Service-Oriented Architecture to Operational Flight Program Development*, 309 Software Maintenance Group, Hill Air Force Base, Utah, 2007.

[211] DoD, *Operation of the Defense Acquisition System*, Instruction Number 5000.02, January 2015; and Tokar, 2016.

[212] Extensibility is considered one of the pillars of good modular software design, which allows the platform's software to support extension of existing capabilities, or the addition of new ones, without changing the underlying architecture or significant sections of the code.

[213] U.S. Air Force Life Cycle Management Center, undated.

development of safety-critical avionics components that have a software abstraction,[214] allowing them to be portable to other platforms or subsystems and making them reusable and interoperable.[215] This standard is aimed at a level of abstraction that would form the basis of acquiring and maintaining nonproprietary software.[216] While the number of systems implementing some form of portable modules is growing, weapon system software is very far from being platform agnostic, reusable, or extensible.[217] Platforms with complex avionics software systems with varied supply chains of modules that are developed on different architectures and standards are still the norm. Many platforms still have system integration issues with every release, as mentioned above.[218] Consequently, resolution of deficiencies takes precedence over fielding of new capabilities.[219] Modularity and architectural upgrades (e.g., design time, run time, and deployment time) to allow portability and reuse of software are put on the back burner, despite their potential to reduce proprietary software and costs and to help speed software deployment.

### *What the Issues Mean for the EW Suite*

Issues of stability, integration, and long testing timelines are persistent, despite the (1) differences in core avionics and software architectures between legacy and fifth-generation systems and (2) the introduction of open architectures. Focusing primarily on EW and EWIR, we attempt to highlight some of the current and emerging technological solutions that would provide a pathway to accomplishing future capabilities and implementations in the next section. Figure 6.2 shows the differences in how an EW suite would be designed under different avionics architectures. OFP and MDF reside in the subsystems and mission computer,[220] respectively, for the EW suite in federated systems. They reside in the common processor in

[214] While there may not be a single overarching definition of *software abstraction*, for the purposes of this report, we define it as designing modular software that supports decoupling of most of the implementation logic of the software from the underlying interfaces and hardware. This allows the software to be portable between different platforms with significantly lower numbers of software changes and configuration issues.

[215] As noted above, the FACE standard was developed by the Open Group, a consortium of industry, academia, and government experts, for this purpose. Although the conceptual standard is present, as of today, FACE still lacks the necessary specifications to be fully effective as a standard and a mandate. In this report, we refer primarily to the concepts of modularity and portability advocated by FACE and several previous standards that were developed by DoD (Tokar, 2016; Crook and Downing, 2020).

[216] Nicholas Kovach, Benjamin Natarian, and Kenneth Littlejohn, "The Rise of Open Architectures in the U.S. Department of Defense," Proc. SPIE 11753, *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2021*, April 2021.

[217] SME interviews, multiple dates.

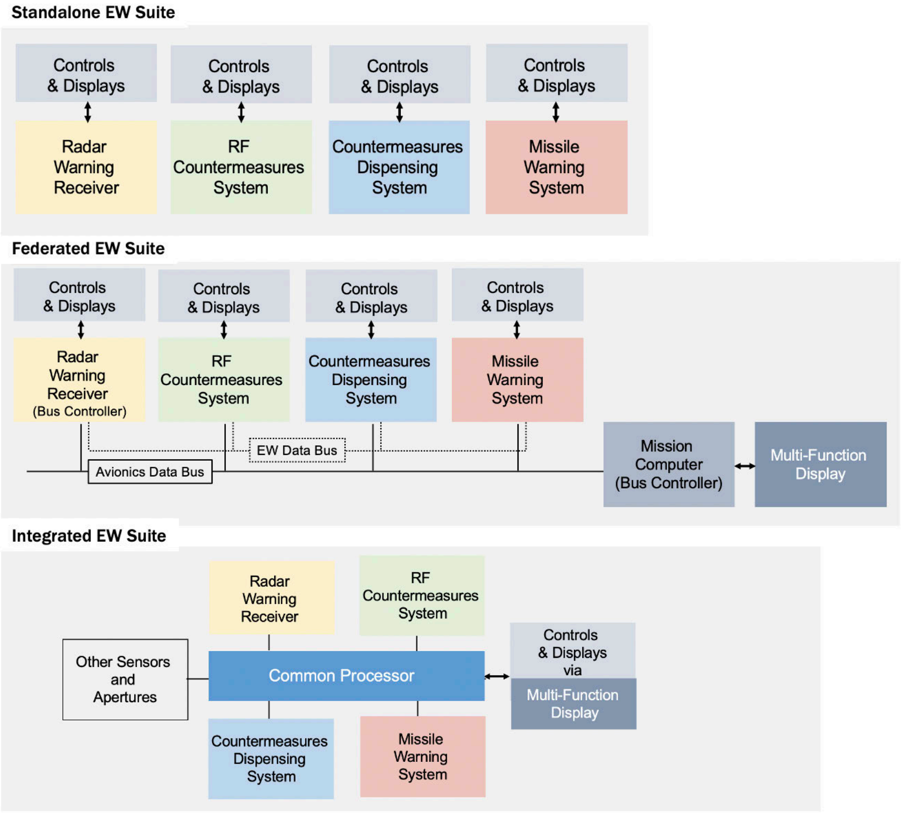
[218] SME interviews, multiple dates.

[219] SME interview, March 11, 2021.

[220] The exact location of the MDF for federated systems is unknown and out of the scope of this study. For federated architectures, each subsystem could have an OFP and the MDF could reside in a mission computer or in an EW controller (Terma, "Electronic Warfare Management Systems," webpage, undated; and Greg Waldron, "USAF Demonstrates Ability to Update F-16 EW Software in Flight," *FlightGlobal*, August 3, 2021).

integrated systems. For MDF, the vision could be an airborne, real-time reprogramming of the threat library in a platform—that is, the deployment of reprogrammed MDF (for known threats) in theater. This can be achieved by replacing the MDF residing in the mission computer or the common processor of a platform. The new MDF file would then be reread[221] into the memory in real time. For OFP, on the other hand, although an airborne reprogramming may seem ideal, what would initially be required is a software deployment paradigm in which an update to the RWR software, for example, does not affect the functionality of other subsystems and does not entail a long airworthiness verification process or an end-to-end testing cycle, thus reducing the deployment timelines. In addition, what is also required is a software paradigm that is applicable to an EW suite with any type of underlying avionics architecture.

**Figure 6.2. EW Suite Under Different Avionics Architectures**



SOURCE: Adapted from North Atlantic Treaty Organization Research and Technology Organisation, 2012.

[221] The technical details of how MDF data is read into memory are not covered here; however, once a parametric data file (in this case, the threat library) is read into the runtime memory, the lookup of information could be extremely fast.

## Redesign of Weapon Systems Software Deployment to Enable Integration Pipelines

Given the existing issues, what does the USAF require for faster and easier weapon systems software deployments for EWIR and for the USAF more generally? To enable faster software updates with new or upgraded capabilities, software needs to be redesigned to enable deployment time modularity.[222] Most weapon systems today have achieved runtime modularity, which ensures that a component's code and defined interfaces and dependencies are supported at run time for optimal use of the platform's and subsystems' central processing unit, memory, and resources and to avoid runtime errors.[223] For deploying new software updates and for supporting a future CI/CD and the DevSecOps software delivery paradigm, it is necessary to redesign how software components are packaged and how they are tested and delivered.

Redesign of embedded software for a platform's avionics suite, even to achieve deployment modularity (i.e., without changing the design of the platform at run time or how the platform should behave during operation) is certainly no small task. Having said that, "An important aspect of run time modularity is the packaging of the deployment artifact."[224] That is, the ability to update or upgrade functionalities affects the run time performance of a platform in the long run. Therefore, what is needed is to design how current software and future components are repackaged or packaged in such a way that there is minimal impact on the platform at run time and software updates for one or more components achieve a level of independence so as to reduce the need to recertify and test the platforms end to end for security, safety, and stability on every update.

Applying new OSA paradigms for the packaging of software to allow faster delivery also requires taking the number of vendors, suppliers, and system integration efforts into consideration. We recognize that this would necessitate changes in policies, technology, and culture. Given this, to achieve future modernization of weapon systems software, following DoD's OSA efforts and DevSecOps guidelines,[225] the requirements and standards for weapon systems software need to be iteratively developed and implemented. Here, it is also important to note that DevSecOps is not a prescriptive process from development to delivery but a shift in policies and culture to include testing and security efforts and teams in the development cycles, to remove silos of postproduction efforts that become bottlenecks to delivery, and to automate

[222] Baptista and Abbruzzese, 2019.

[223] *Runtime errors* are errors that occur due to various parameters that may change while a platform is in operation. These could be memory issues, resource issues, software dependency issues, or a combination of these. See Bakker and Ertman, 2013.

[224] Bakker and Ertman, 2013.

[225] These guidelines support reusable and extensible solutions and support for development and integration pipelines.

supporting processes.[226] Additionally, it must be recognized that in the long run, as seen in the commercial industry, OSAs contribute to significant cost savings by cutting down time and effort. In the next sections, we will look at how these changes will support the building of an ML infrastructure for future cognitive EW capabilities.

### *MDF or Threat Library Deployments*

An EWIR software deployment, as mentioned earlier, sometimes requires only an MDF update. Changes to the MDF define the way a platform behaves for a specific threat in a specific environment and, therefore, also require extensive performance testing.[227] MDF updates are then ready for in-theater platform download and deployment. Thus, regular MDF updates also take months to be deployed. For emergency and urgent MDF changes, and other future rapid reprogramming needs, an airborne deployment would reduce the time frames of MDF uploads, with minimal software development for pushing the upload.[228] Airborne deployments are not just an ideal near-term solution but something that has already been implemented and tested successfully in July 2021 on an F-16 (Block 50 Series[229]) aircraft. This upload was achieved even with different OFPs for the central display unit, digital video recorder, and EW controller (ALQ-213) communicating with each other. Even though several policy and infrastructure upgrade decisions are needed to support this capability in the future (including decisions related to network capabilities and speeds, as discussed in Chapter Five), this type of rapid reprogramming is already an achievable goalpost for known threats.

### *OFP Software Deployments*

The DoD C2D2 model is an attempt to increase parallel development of capabilities and the integrated deployments of new OFP software updates every six months.[230] The C2D2 model is not without problems, as the stability issues during regression testing mentioned earlier are still prevalent in fifth-generation systems today.[231] OFP software updates for many other platforms take more than two years to field, with some legacy systems taking four or five years of total

[226] A long-standing framework for assessing the need and the requirements for applying DevOps or DevSecOps is called CALMS (Culture, Automation, Lean, Measurement and Sharing). See Ian Buchanan, "CALMS Framework," webpage, undated.

[227] North Atlantic Treaty Organization Research and Technology Organisation, 2012. Testing of routine MDF updates is a part of the testing processes of DT&E and OT&E.

[228] This type of deployment would use satellite communications links or data links to send the MDF file directly to the EW controller onboard.

[229] F-16 System Program Office, "F-16 Roadmap to ABMS," presentation, undated; and USAF, F-16 System Program Office, Air Force Life Cycle Management Center, "F-16 Receives In-Flight Software Update During Recent Flight Test," July 31, 2021.

[230] In the case of fifth-generation platforms, CSCIs map to functional software built for various shared hardware. In this report, *OFP* is a generic term used for OFP in legacy platforms as well as for the aggregation of the CSCI software.

[231] DoD, Director, Operational Test and Evaluation, 2019, p. 19; and SME interview, March 11, 2021.

fielding time "for all aircrafts around the world."[232] Owning to stability issues and to the lack of new capability deployments in each release, the aim for C2D2 is to move to yearly updates to allow deployment of new capabilities and more testing time in the future. Legacy systems, as discussed earlier, have core suite OFPs that do not have an inherent design, and features are added on the existing monolithic code.[233] For EWIR and EW, as with any other mission function of a platform, continuous capability enhancement is the only way to remain competitive in an environment of changing threats and rapidly advancing capabilities of adversaries.

One of the focus areas of DoD's open standards, just to reiterate, is rapid fielding of capabilities with nonproprietary, reusable, and portable modules, interfaces, and other implementations. Although some of these goals are difficult to achieve simultaneously, owing to complexities inherent to acquisition strategies, rapid software deployments may be achieved with some level of portability and reusability by implementing new software deployment architectures. For an OFP[234] design, this requires a deployment architecture that supports the following four requirements.

### Timely and Cost-Effective Software Safety Certification

OFPs are typically designed, both in federated and IMA platforms, on a "fault containment and separation of concerns" model.[235] Some implementations of this, as stated above, are achieved through separate subsystems with separate OFPs, programmed in one or more submodules (federated). Other implementations use partitioning of memory, time management, and hosting of several software functions or applications on the same hardware (IMA).[236] This is enabled by the concept of hardware virtualization[237] supported by higher core processing power.[238] A partitioned OFP software design, as demonstrated by Lim et al., 2012, divided into

[232] SME interview, August 17, 2021.

[233] With some exceptions (for example, any new line replacement unit modules), for the latest or future block series, the development process follows agile methodology and modular design (SME interview, August 17, 2021).

[234] *OFP* here refers to both CSCI and multiple modules based OFP models.

[235] *Separation of concerns* is a software engineering design pattern for reducing complexity, improving reusability, and supporting improvements (Peri Tarr and Stanley M. Sutton, Jr., "N Degrees of Separation: Multi-Dimensional Separation of Concerns," *ICSE '99 Los Angeles, CA*, 1999; Sungshin Lim, Jongsoo Hyun, Sang Myun Shin, In Gyu Kim, Byung Moon Hwang, and Hyuk-Chul Kwon, "A Feasibility Study for ARINC 653 Based Operational Flight Program Development," IEEE/AIAA 31st Digital Avionics Systems Conference, 2012).

[236] Ananda CM, Sabitha Nair, and Mainak Ghoshhajra, "ARINC 653 API and Its Application—An Insight into Avionics System Case Study," *Defense Science Journal*, Vol. 63, No. 2, March 2013.

[237] *Hardware virtualization* is the process of using the same physical system to support multiple applications running on separate operating systems (virtual machines) simultaneously. This is achieved by specialized host software that creates and manages virtual machines and their resources. Figure 6.3 shows how a host software program, also called the hypervisor, is used to create a layer of interaction between the hardware and the applications using it through virtual machines.

[238] Luidi De Simone and Giovanni Mazzeo, "Isolating Real-Time Safety-Critical Embedded Systems via SGX-Based Lightweight Virtualization," *2019 IEEE International Symposium on Software Reliability Engineering Workshops*, 2019.

core hardware interface and application modules with submodules for various avionics functions, provides a "separation of concerns," where a fault in one partition does not affect the other. Lim et al., 2012, concludes that "robust partitioning of software can easily and cost-effectively obtain software safety assurance" (for the DO-178 B/C) "[and] each partition can be designed and developed by a specialized company reducing the cost."[239] This is true to a certain extent with CSCI and C2D2 in fifth-generation platforms, albeit with the aforementioned integration and stability issues. Additionally, time management and fault tolerance increasingly become a point of concern with greater complexity and with the addition of new capabilities. Finally, for a DO-178 safety (or airworthiness) certification process for a single isolated software component (or a small composite of software components) for this type of hardware partitioning, the developers have to demonstrate a level of partitioning for safety-critical functions that would be able to contain a failure without affecting other applications or functions.[240] What could be hypothesized is that a further separation of OFP core and individual applications, with minimum dependencies and supported by a management of processing time and resources, might allow the development of more-stable software, which would require much less time in a safety certification cycle. Later in this chapter, we will introduce the concept of containerization, which could provide this lightweight virtualization for embedded systems.[241]

### Secure, Reusable Modules

The second concern that the architecture should address is security verification and postproduction software security hardening timelines. The isolation of applications required for faster safety certification should also be able to provide an inherent protection from malicious attacks and the isolation of vulnerabilities from the host platforms. In addition, for safety-critical weapon systems, vulnerabilities in any component should be removed through incorporating security controls in the development and testing phases of software deployments—what has come to be called "shifting security left."[242] Additionally, security hardening policies should be designed and applied to portable, reusable software deployment modules to build secure, platform-agnostic, and maintainable software. The design of portable components should be able to support easy integration and automation of testing to reduce security verification timelines. In other words, shifting security left would not only reduce security verification timelines but would also allow the building of modular software deployment artifacts that are hardened, pretested, and certified for reuse.

[239] Lim et al., 2012.

[240] Simone and Mazzeo, 2019.

[241] Simone and Mazzeo, 2019.

[242] Rusty Sides, "DevSecOps and Security Automation—Making Application Security a Part of Development," webpage, May 2021.

### Development and Integration Pipeline for Rapid and Continuous Deployment

The DoD DevSecOps playbook[243] highlights the need for enabling DevSecOps. Rapid and continuous deployment of new or upgraded capabilities to weapon systems would require a software development and integration pipeline (CI/CD) specifically tailored to support DevSecOps for safety-critical systems. For breaking down silos of weapon system software development efforts, unifying production, and adopting a capability model for development, the playbook offers three important steps:

1. adopting infrastructure as code, which allows "virtualization of compute, network, and storage capabilities"[244] from traditional hardware installations
2. facilitating the delivery of cloud capabilities to the tactical edge, or the edge cloud (as mentioned in Chapter Five).[245] An edge cloud implementation would be able to deliver operational and mission-specific capabilities, including support for cognitive EW, as explained below. Additionally, the edge cloud would enable computing on the tactical edge, which would address any latency and network issues that new cloud-based software paradigms could introduce. This point will be elaborated later in this chapter.
3. shifting OT&E activities into the DevSecOps pipeline (in other words, shifting testing into an automated pipeline to reduce post-release deficiencies). This would address the primary goal of a DevSecOps pipeline, which is to reduce the time of software deployment from years to months to minutes.

### Integration Pipeline for Future ML Capability Development

Our case study analysis of the four technologies (cognitive EW, cloud integration and data engineering, flight program software and containerized microservices, and onboard high-performance computing) has concluded that for building, testing, training, and deploying (and updating) cognitive EW models, a robust infrastructure support would be required. This would enable a life cycle support for the testing and deployment of cognitive models on embedded systems, similar to that of a regular OFP software deployment.

## Microservices, Containers, and Orchestration

In this section, we look at a software deployment architecture that provides a lightweight virtualization[246] of OFP or weapon systems software applications or functions and addresses the four requirements mentioned in the previous section. Overall, there is a need for agile

[243] DoD, 2021a.

[244] Amazon Web Services, "Infrastructure as Code," white paper, July 2017.

[245] DoD, Office of the DoD Chief Information Officer, *Outside the Continental United States (OCONUS) Cloud Strategy*, April 2021.

[246] *Lightweight virtualization* is a process of using new software approaches to create and run multiple applications packaged with all their dependencies in the same operating system without the need to create virtual machines using hardware virtualization. Lightweight virtualization in the form of operating system virtualization and the use of containers will be discussed in this section.

methodologies for incremental capability development and a change from the fundamental commercial-off-the-shelf systems approach accompanied by tighter process requirements to a development and integration–focused capability development approach. As discussed in the previous sections, this can be achieved using a software paradigm that supports developing and packaging of software into portable, reusable modules and components that would allow easy integration, deployment, and maintenance.[247]

Containerization is a deployment architecture that provides lightweight virtualization and the design principles to package software and its dependencies into "containers" to allow software to execute consistently in any environment, platform, or system.[248] Containerization simplifies the deployment of capabilities and upgrades. It is also well suited to large-scale deployments onto dissimilar platforms (i.e., platforms that have widely different computing infrastructures, including operating systems and computing hardware). 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, including its own 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.

To understand how the concept of containerized microservices could improve the timelines of software deployments, we have to briefly look into the concept of *operating system (OS) virtualization*. OS virtualization is a higher level of abstraction than hardware virtualization used for application development today. Containerized microservices with OS virtualization enable applications to be developed and run consistently on any platform or a platform variation, allowing portability and application stability. Figure 6.3 shows how containers provide OS-level virtualization. Each container, from App A to App F, has a function or application, a microservice, enclosed within it, along with its dependencies.[249] Containers, or a composite of containers, can theoretically[250] support a self-contained capability that can be virtualized,[251] certified, tested, and deployed independently (i.e., without affecting the rest of the

[247] Nickolas Guertin and Douglas C. Schmidt, "Emerging Opportunities in Modularity and Open Systems Architectures," Software Engineering Institute, October 15, 2018.

[248] IBM Cloud Education, "Containerization," webpage, May 15, 2019.

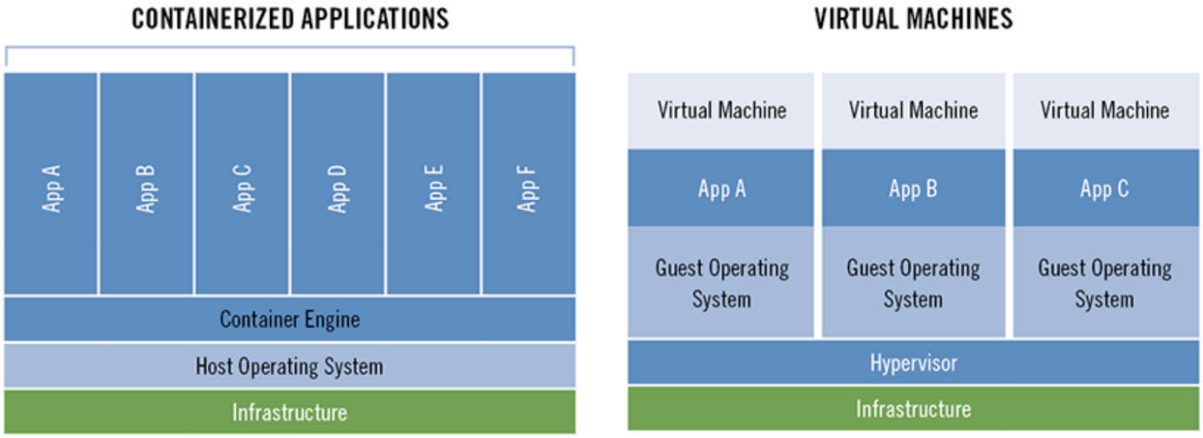
[249] Although there is another way of implementing containerization over hardware virtualization using virtual machines, for the purpose of explaining the concept of lightweight virtualization, we will only refer to pure containerization in this chapter, as shown in Figure 6.5. See Donald Firesmith, "Multicore Processing, Virtualization, and Containerization: Similarities, Differences, Challenges, and Recommendations," presentation, Software Engineering Institute, Carnegie Mellon University, 2019.

[250] This has already been tested successfully on a small, independent scale for noncritical OFP functions on the T-38 and U-2 in 2020. See Jill Pickett, "586 FLTS Testing Software Management Program for Aircraft," *Arnold Engineering Development Complex Public Affairs*, September 18, 2020; and Firesmith, 2019.

[251] Simone and Mazzeo, 2019.

OFP software, subsystem, or other subsystems).[252] Portability enabled by containers would allow reuse of software and interoperability between platforms. This, with the right policies, will support DoD's open avionics vision of removing vendor lock-ins on weapon systems software in the long run.[253] With the containerized microservices approach, CSCI and other OFP components can be developed by different suppliers or software groups and integrated for the platform without running into issues during testing caused by the inconsistencies related to different development, test, and integration environments and different dependencies.[254] This is vital for safety-critical software of weapon systems.

**Figure 6.3. Containerized Applications Versus Partitioned Virtual Machines**



SOURCE: Keith Larson, "Containerization Meets Process Automation," Control Global, June 2020.

This level of virtualization also allows *orchestration*, an ability provided by supporting tools[255] for autoscaling and workload management services for containers when executed in a cloud computing environment.[256] Autoscaling is particularly powerful when a function or an

[252] Avionics International, "Using Containers for Avionics Applications," webinar, Wind River, June 3, 2021.

[253] The USAF already has software factories, such as Platform One, that are developing precertified hardened containerized software for reuse. Policies to allow Platform One and other software factories to integrate teams with platform program management to develop container services for weapon systems would be a great start for removing vendor lock-ins on specific software.

[254] Because of different development, test, and integration environments, software developed and tested in one environment might behave differently or reveal issues during integration or integration testing (Firesmith, 2019).

[255] One example of such a supporting tool is Kubernetes, an open-source, portable platform that can scale and roll back virtual instances of containers depending on the workload and processing needs. Kubernetes is now a part of the Cloud Native Computing Foundation and is the DoD-recommended orchestration tool for DevSecOps. See Kubernetes, "Production-Grade Container Orchestration," webpage, undated; and DoD, 2021b.

[256] Both containerization and the orchestration tools used for the resource management and autoscaling 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 reduce development and deployment times. Later in this section, we discuss how the edge cloud on platforms or the dispersed cloud

OFP software program has additional workload and requires additional time-managed processing power. These services allow computing resources to be optimally utilized based on need, which would be crucial for the deployment and high-speed processing of an adaptive or cognitive EW model. Containerization also supports the building and deployment of DevSecOps pipelines. To address the need for secure, reusable modules and DevSecOps, it is important to understand the differences in containerization for generic cloud-based ground applications and embedded avionics software.

Traditional embedded avionic software programs are generally written in Ada, C, C++, or lower-level languages and have a lower level of abstraction from the hardware, which is exposed to the code via the Board Support Package.[257] Containers, as mentioned above, create a higher level of abstraction and virtualization. They are thus considered more lightweight: Unlike virtual machines, they do not have direct dependence on the underlying hardware.[258] There are, however, certain important considerations for using containers for embedded software.

1. *Replacing proprietary software designs*: Proprietary embedded software packages (for example, for an EW subsystem[259]) control the behavior of the hardware and the interaction with an OFP. Containerization enables not only higher-level virtualization but also portability and reusability that could reduce proprietary software with proper management of resources.
2. *Management of resources*: For safety-critical systems, containerized OFP software running on the OS should be designed to follow the embedded workflow for time management, power consumption and management, etc., of the embedded system.[260]
3. *Security*: Since the containerized software would enable safety-critical systems, a major consideration is ensuring security from tampering, access control, management and sharing of code artifacts, and code traceability.[261]
4. *Integrated development pipelines*: Having established considerations 1 through 3, cloud-based pipelines, DevSecOps, will streamline the creation, maintenance, sharing, and reuse of containerized modules in repositories and their testing using virtualized hardware.[262]

(cloudlets or mini clouds) can provide storage and processing power required for containerized software while overcoming the limitations of latency and bandwidth.

[257] Wind River, “Board Support Packages (BSPs),” webpage, undated.

[258] Avionics International, 2021; Firesmith, 2019.

[259] Here an EW subsystem refers to both a federated subsystem and an IMA EW suite with shared processing.

[260] Avionics International, 2021.

[261] Twain Taylor, "Top 4 Open Source Tools for Observability of Containers and Microservices," webpage, May 2020. The DoD Platform One initiative provides certified containers and certification of containers to ensure that the chain of trust is preserved. See DoD, Platform One Software Factory, undated; Avionics International, 2021; and SME interview, August 17, 2021.

[262] Hasan Yasar, “Expanding DevSecOps to Embedded Systems; Is It Possible?” presentation, Software Engineering Institute, Carnegie Mellon University, 2020; Performance, “JETS, Virtualization for Embedded Software,” white paper, 2019.

5. *Performance, latency, and bandwidth*: Performance of embedded software is the most important consideration for a weapon system and forms the basis of all OT&E testing. Thus, it is worthwhile to note that the performance overheads of containerized embedded software are considered to be negligible.[263] Depending on the deployment stack, containers deployed on a cloud infrastructure could cause latency and bandwidth issues during processing and communication between containerized services due to issues with network traversal to a traditional cloud infrastructure.[264] Similar to performance, latency and bandwidth issues in mission support functions, such as EW, in safety-critical weapon systems would be unacceptable. Edge cloud, edge computing, and dispersed cloud computing paradigms (also called fog computing[265]) enabled by cloudlets[266] are viable solutions to these issues. Edge cloud computing would solve storage, data processing, and service and communication latency and bandwidth issues by providing processing on the edge and limiting the traffic to data centers.[267] Edge computing devices within a platform, which the USAF and the commercial industry are already developing, would be vital for optimum performance of cognitive EW algorithms.
6. *Automation and orchestration* for management of containers and resources (e.g., processing power), using onboard orchestration tools:[268] Orchestration tools have processing overheads.[269] Most platforms would require hardware upgrades for dedicated processing power to support orchestration. However, it might be possible to use scaled-down versions of these tools or leaner commercially available versions with limited required functionality.[270] Additionally, edge cloud solutions would provide the processing power required for container orchestration tools onboard platforms or in cloudlets or dispersed cloud solutions discussed above.

[263] Studies have shown that "in general, the execution time, CPU [central processing unit], memory usage, and power consumption of containers are better than those of virtual machines" (Ching-Han Chen and Chao-Tsu Liu, "A 3.5-Tier Container-Based Edge Computing Architecture," *Computers and Electrical Engineering*, Vol. 93, 2021; Avionics International, 2021).

[264] Yu Liu Dapeng Lan, Zhibo Pang, Magnus Karlsson, and Shaofang Gong, "Performance Evaluation of Containerization in Edge-Cloud Computing Stacks for Industrial Applications: A Client Perspective," *IEEE Open Journal of the Industrial Electronics Society*, Vol. 2, 2021.

[265] Tina Francis and Madhiajagan Muthiya, "A Comparison of Execution Mechanisms: Fog and Edge Cloud Computing," EECSI 2017, Yogyakarta, Indonesia, September 2017.

[266] Mahadev Satyanarayanan, "The Emergence of Edge Computing," *Computer*, Vol. 50, No. 1, January 2017.

[267] Chen and Liu, 2021.

[268] Kubernetes, undated.

[269] Legacy platforms have processing power constraints and cannot support the hosting of an orchestration tool along with the OFP (SME interview, March 2021).

[270] This was used for the flight test of U-2 with Kubernetes (U.S. Air Force, "U-2 Federal Lab Achieves Flight with Kubernetes," October 7, 2020c; SME interview, July 30, 2021).

Prototyped deployments of containerization on USAF platform-embedded systems OFP have already been tested for noncritical OFP functions on the T-38 and for a pilot mission test for the U-2, and more developmental programs are underway.[271]

## Future Machine Learning Support and Infrastructure

Modeling, training, testing, and fielding of AI/ML or future cognitive EW capabilities would require several steps: requirements and problem definition, definition of key performance indicators to enable future monitoring of the model, data collection, preparation and analyses, modeling, evaluation and optimization, and deployment.[272] AI or deep learning packages require a complex set of dependencies and a specific environment to run. The user of AI packages (platform program management, in the case of EW) should not have to build and compile the AI packages and should not be expected to have the computing environment needed to run and test the packages. Additionally, and more importantly, the introduction of a cognitive EW model on a platform's EW OFP should have the same considerations of fault tolerance[273] and self-contained capability that can be virtualized,[274] certified, tested, and deployed independently (i.e., without affecting the rest of the OFP software, subsystem, or other subsystems) as any other OFP software functionality or application on a platform. Containerization allows the development of an AI/ML or cognitive EW model that can be self-contained, with all its dependencies and common environment or operating system bundled together.[275] This would mean that, similar to any other function or application module within an EW subsystem, cognitive EW (or other adaptive or AI models) could be made portable and interoperable using containerization.[276] Containerization also allows independent updates of modules, which would include updated and retrained cognitive models.

For any AI/ML model to be developed, trained, tested, and validated (particularly for a mission-critical and safety-critical capability), supporting infrastructure with automated pipelines is required for data engineering and modeling teams, as shown in Figure 6.4. With continuously changing data profiles, the models need to be continuously updated and trained. Thus, these automated pipelines would provide an integrated life cycle of various steps, from data ingestion to the training and deployment process.[277] In other words, an automated

[271] Pickett, 2020; USAF, 2020c; and SME interview, July 30, 2021.

[272] Alaa Khamis, "The 7-Step Procedure of Machine Learning," *Towards Data Science*, March 30, 2019.

[273] Firesmith, 2019.

[274] Simone and Mazzeo, 2019.

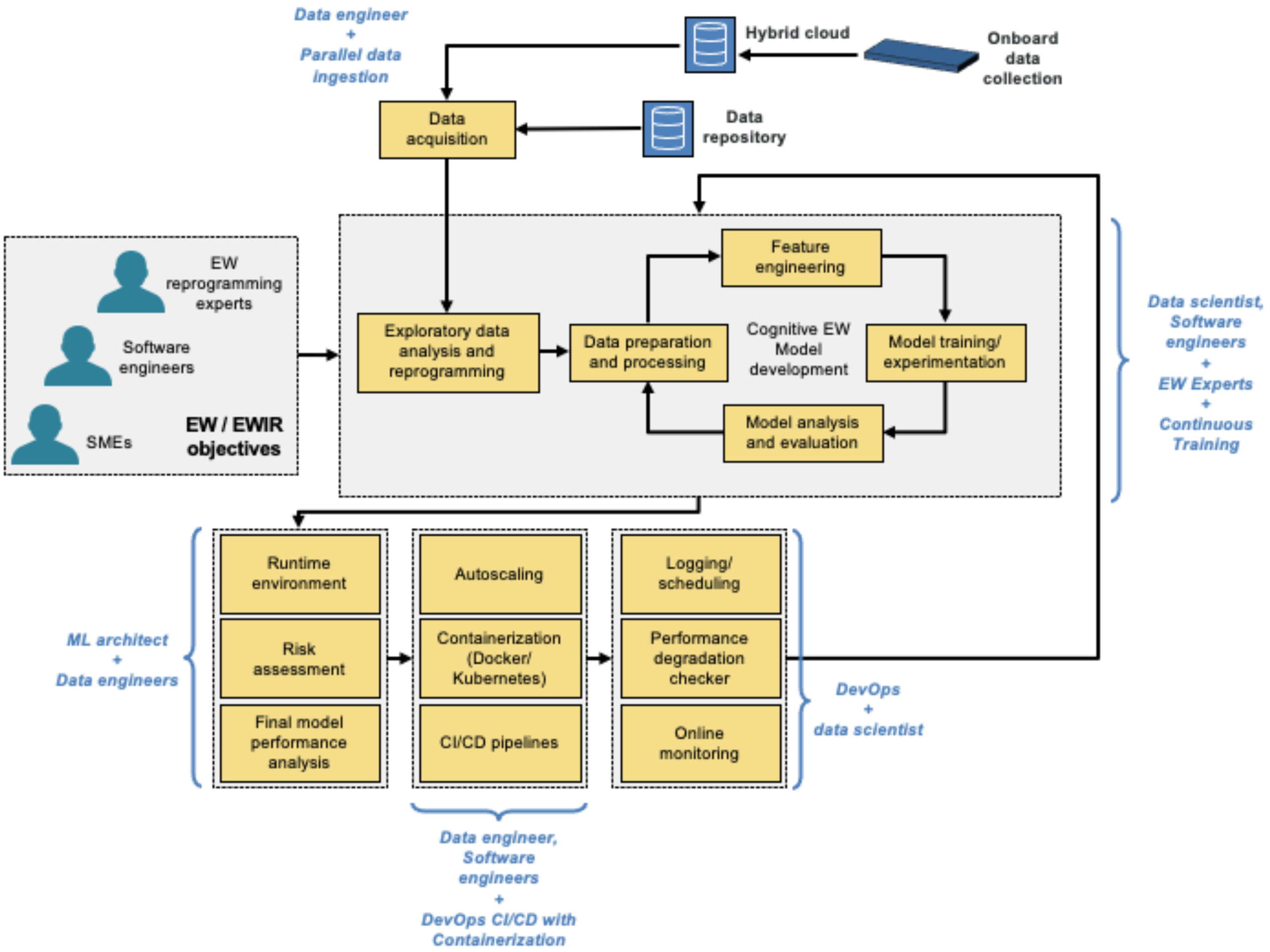
[275] Rachel McDowell, *Containers Provide Access to Deep Learning Frameworks*, Oak Ridge National Laboratory, 2017.

[276] Janakiram MSV, "Google Just Made Machine Learning More Accessible and Portable with Containers," *Forbes*, July 1, 2019.

[277] Tapasvi Kaza, "MLOps Lifecycle," *VivoSoft*, blog, updated December 6, 2020; Harshit Tyagi, "What Is MLOps—Everything You Must Know to Get Started," *Towards Data Science*, March 25, 2021.

DevSecOps pipeline would add continuous training of AI/ML models to its continuous integration and continuous delivery process. Such a pipeline is also called MLOps, as illustrated in Figure 6.4. Containers not only support the development of portable, reusable ML models but also help sustain these pipelines by enabling rapid deployment of new models as threat data profiles change. Containers also increase the ease of verification and testing in these environments. Additionally, newer ML and data management tools that work seamlessly with orchestration tools for container management are being developed to automate these pipelines and support reuse even further.[278] See Figure 6.5.

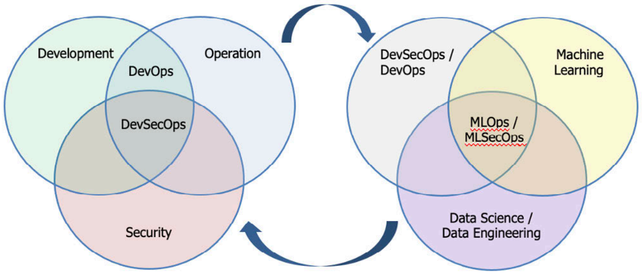
**Figure 6.4. Machine Learning and Engineering Operations**


Data engineer
+
Parallel data ingestion
Hybrid cloud
Onboard data collection
Data acquisition
Data repository
EW reprogramming experts
Software engineers
SMEs
EW / EWIR objectives
Exploratory data analysis and reprogramming
Data preparation and processing
Feature engineering
Cognitive EW Model development
Model training/ experimentation
Model analysis and evaluation
Data scientist, Software engineers
+
EW Experts
+
Continuous Training
ML architect
+
Data engineers
Runtime environment
Risk assessment
Final model performance analysis
Autoscaling
Containerization (Docker/ Kubernetes)
CI/CD pipelines
Logging/ scheduling
Performance degradation checker
Online monitoring
DevOps
+
data scientist
Data engineer, Software engineers
+
DevOps CI/CD with Containerization

SOURCE: Adapted from Tyagi, 2021.

[278] Kubeflow, homepage, undated.

**Figure 6.5. Continuous Training, Continuous Integration, and Continuous Testing**



The USAF has several current ongoing pilot efforts for building cognitive and adaptive EW capabilities. However, for a sustained future life cycle in which DoD engineers, EWIR engineers and analysts, and other supporting teams could contribute to preparing data and developing, training, and testing cognitive models, the USAF should support the building of a MLOps infrastructure with a supporting simulation environment.

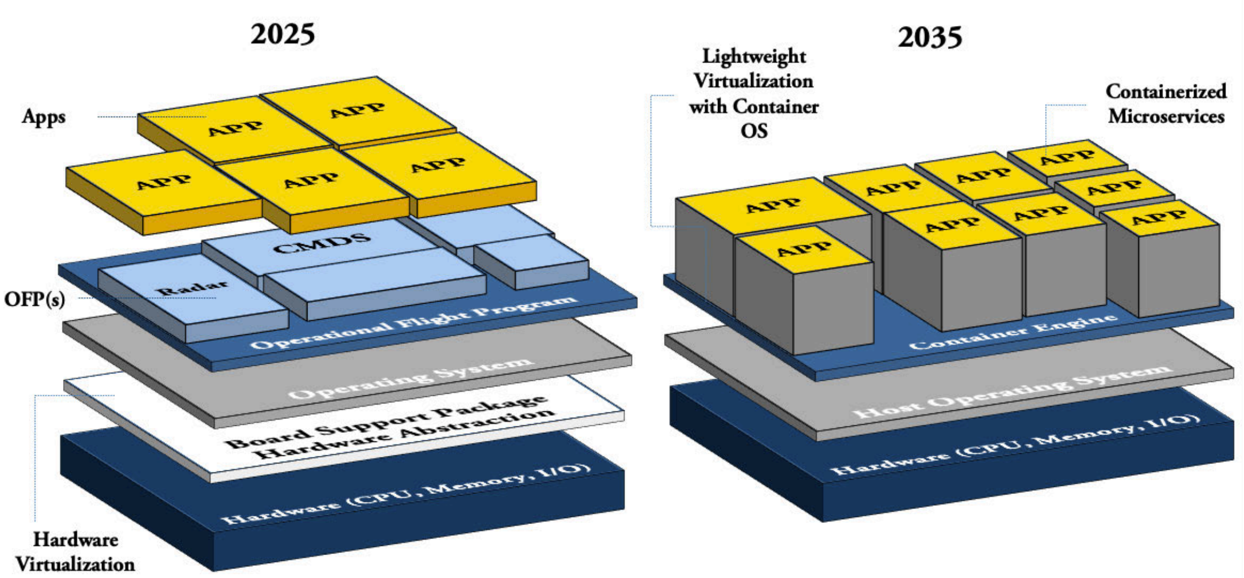
## Conclusion and Next Steps

To support the demands of advancements in EW and EWIR capabilities, the USAF must consider a more agile, integrated, and streamlined approach to the development of weapon system software. The OFPs in embedded avionics software today are platform and subsystem specific and are rarely designed with a modular approach. Furthermore, they are proprietary for many mission systems, such as EW. As has been illustrated in this chapter, this kind of design does not lend itself to component- or module-based safety certifications for changes to a capability configuration or for the addition of a new capability. Additionally, with both legacy and fifth-generation platforms (some of which do follow some form of agile process), DT&E and OT&E testing take a very long time because of rigorous end-to-end testing, stability issues introduced by new OFP integrations that require immediate fixes, and additional deficiencies with new updates that need to be documented and assessed. The other drawbacks are that (1) current weapon system software design does not support faster deployments, (2) ownership of the software is primarily proprietary, and (3) there is a lack of a consistent software development and deployment approach that enables faster deployments of new capabilities, including those supporting EWIR.

DoD's attempts to implement and mandate OSAs have been only partially successful. Several fifth-generation platforms are OMS compliant. Since OMS is a standard for interfaces and data exchange between platform services and subsystems, it was easier to standardize as the services and subsystem software remained largely proprietary. For portable and reusable module development for weapon systems software, standards are hard to enforce. However, new deployment architectures such as containerization would allow the decoupling of OFP and avionics software functions and modules. Though initially disruptive because of the process and cultural changes needed along with the redesign of the deployment architecture, containerization allows for a lightweight virtualization and partitioning of OFP modules at a higher level than current hardware partitioning technologies. Such a partitioning would support component-based safety certification and testing, drastically reducing the time for fielding new safety-critical capabilities. Containerization will also support fielding cognitive EW capabilities, with all the dependencies in a self-contained module keeping the system's integrity and fault tolerance intact.

We noted in Chapter Four that there are current initiatives for the development of lightweight, service-specific apps that will interact with the existing OFP using new software interfaces without requiring any changes to the OFP software itself. These initiatives will enable rapid fielding of new EMS capabilities and will deliver modular, reusable, open-standard software in the near term. However, in the long term, this type of layered design might lead to brittle architecture, where any changes to the OFP will require updates to the apps, interfaces, or both. This will cause maintenance and performance issues in the long run. Thus, the long-term vision requires a shift in the architectural design of weapon system software, as described in this chapter, to support seamless, sustainable, and maintainable software that provides apps-based solutions with a higher level of abstraction, stability, fault tolerance, and fidelity. Figure 6.6 illustrates the differences between apps-based and containerized microservices frameworks.

**Figure 6.6. Comparison of Apps-Based Framework (left) and Next-Generation Flight Software with Microservices (right)**



Going forward, the USAF should invest in the design and development of modular embedded software for both legacy[279] and fifth-generation platforms. This would allow the platforms to share resources, set up DevSecOps pipelines, and accelerate software updates and

[279] Some legacy platforms would require support for the rearchitecture and porting of OFP software to a high-level language, such as C++ , in order to be able to utilize and support common, reusable containerized modules (SME interview, August 17, 2021).

security testing along with continuous integration. DoD Platform One, Cloud One, and other software factories have the tools to provide this infrastructure support. However, the efforts of platform program offices, engineering groups, and software factories are still in silos and not fully integrated. To make full use of these software factories to support embedded avionics software pipelines, DoD and the USAF have to authorize more seamless integration between these efforts. Additionally, DoD should mandate the use and maintenance of common core functions[280] to enable portable, interoperable modules among all platforms. This might be possible through a consortium or a secure community of interest among DoD, the USAF, and vendor engineering groups. As a starting point for building nonproprietary software, such a community of interest would be able to develop and maintain core components in a common repository.

For cognitive EW and advanced reprogramming capability development, the USAF should consider setting up an engineering unit for the development and testing of cognitive AI/ML models. This integrated unit should consist of EWIR, platform OFP, and other supporting teams to set up a cloud-based development and testing pipeline for data engineering, modeling, and testing capabilities. Cognitive EW capability would require iterative development and testing and the skill set of varied EW teams. Finally, these advanced, and somewhat disruptive, technological changes would require training for teams and enhancements of legacy computer systems, along with changes to policies, processes, and culture.

[280] Common core functions could be platform-agnostic core software, such as weapons control software or messaging services.

# Chapter 7. Onboard High-Performance Computing

In this chapter, we focus on bringing advances in HPC onboard aircraft that rely on EWIR. Enhanced OBP is essential for achieving the goal of rapid, in-flight reprogramming. It could also support automated, in-flight MDF updates in the near term, assuming that the requisite satellite communications and high-speed data links are also available. OBP is necessary for incorporating the ML capabilities required for cognitive EW in the future.

This chapter lays out the basic components of OBP, along with some of the problems that need to be resolved to make software updates much faster and more capable based on available hardware. It then describes the types of hardware-based technologies that are available (at least commercially) in the near term that are worth investments to achieve in-flight reprogramming goals. We assess that the basic advances in hardware required for cognitive EW already exist commercially, albeit in the context of very different applications, such as natural language processing. That said, we offer a perspective on what additional hardware advances might offer (or not) to further enable rapid reprogramming onboard in the future. At the end of the chapter, we also briefly reflect on additional applications for EWIR-relevant hardware upgrades, including cloud computing capabilities at the edge, along with modeling and simulation for rapid threat model and software testing.[281]

## Defining Onboard Processing

### *Process Summary*

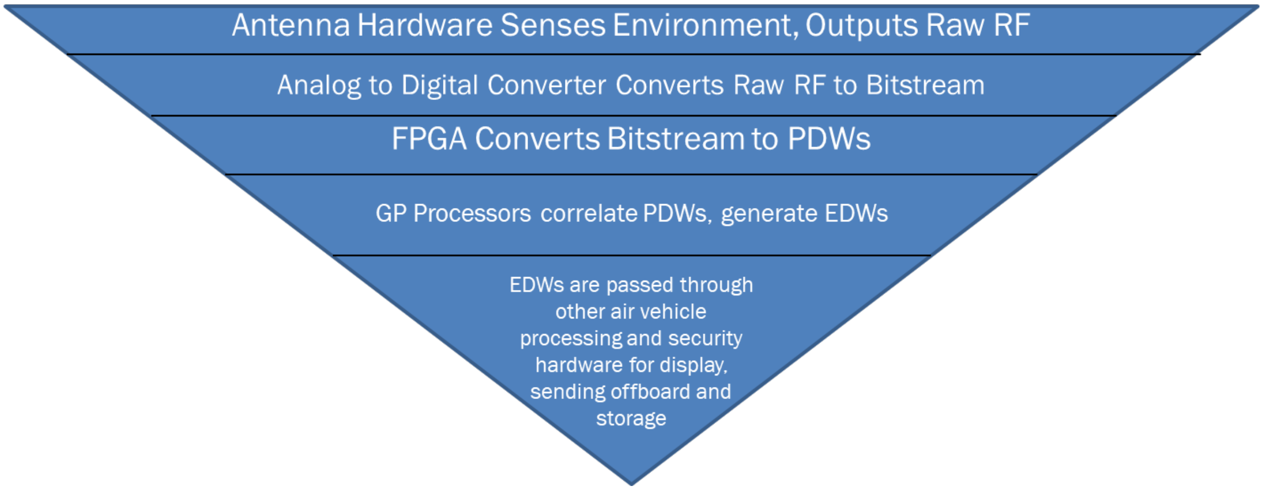
Without sufficient OBP, sensors and platforms would be unable to digest and make sense of activity detected by their RWRs and unable to run any number of other onboard components. There is a growing need for military platforms to follow the commercial industry trend of miniaturization, as demonstrated by highly capable wearable and pocket-sized devices. Packing more processing power into smaller, lighter components could support additional OBP capacity.

As argued elsewhere in this report, advanced threats will increasingly require platforms to respond more quickly to changing activity in the EMS. Timelines between the sensing of new information in the EMS and the need to process, analyze, and react to that information will shorten to such an extent that raw data reflecting a change in the EMS environment will need to be processed and understood onboard the platform during the mission. In other words, centralized, ground-based data processing facilities can no longer be the sole option in this type of threat future. Both legacy and future systems will need to do more of this work onboard.

[281] Although these limitations are relevant to multiple aspects of the topics we focus on in this report, we include them here because they were not individual areas of focus for our research and the relevant issues are particularly hardware-driven.

Before discussing how to increase OBP, we must first discuss the enabling hardware. All platforms that can sense and respond to the EMS have some degree of OBP, and all the components on the aircraft (or other platform) that process data from the EMS compose OBP from an EWIR perspective. There are a few major technology types that are most relevant for understanding the scope of OBP and thus may need to be manipulated or replaced to increase processing capacity using a relatively small amount of space. These are summarized in Figure 7.1 and include the antenna or sensor that receives raw data, analog-to-digital converters (ADCs) and digital-to-analog converters (DACs), FPGAs, general-purpose processors, and security-related hardware, such as encryptors and guards.[282]

**Figure 7.1. Hardware Data Flow and Formats**


Antenna Hardware Senses Environment, Outputs Raw RF
Analog to Digital Converter Converts Raw RF to Bitstream
FPGA Converts Bitstream to PDWs
GP Processors correlate PDWs, generate EDWs
EDWs are passed through other air vehicle processing and security hardware for display, sending offboard and storage

NOTE: EDW = emitter descriptor word; FPGA = field-programmable gate array; GP = general purpose.

The purpose of each layer of OBP is to distill significant amounts of raw RF data into tracks and to enable the identification of individual emitters in the EMS environment (particularly threats or friendly/partner systems). OBP is like a funnel or a sieve, converting data into a form that the system will understand and weeding out what is not needed. At every level of the processing chain, less data are used to represent the environment, which saves storage space and processing power further down the chain. As a result, there are data lost at every step in the process. Thus, there is an important trade-off between the speed of processing and the amount and richness of data available for understanding the EMS environment. Richer data means slower processing, given a fixed amount of capacity.

[282] Although the information we cover here could be relevant to other hardware-based technologies important for EWIR, the basic process for how this works is most pertinent to OBP in the context of this report, and so we include it here.

### *Components That Process Data*

A platform's antennas that sense the EMS environment and capture data are the first part of any processing chain. Key antenna performance parameters include peak gain (tied to the distance from which a threat can be seen), frequency response (how well threats can be detected over the entire relevant frequency band), directivity (measure of gain in certain directions), and aperture[283] size and shape. While this discussion is focused on the processing hardware after the antennas, it should be noted that EW system performance can be severely limited based on the key performance parameters of the antenna system.

The first funnel summarized in Figure 7.1 is the ADC. An ADC converts unprocessed RF data into bits. The main key performance parameters for ADCs are dynamic range as driven by effective number of bits (ENOB) and sampling frequency. The more bits an ADC can use to represent the analog signal, the higher the dynamic range. *Dynamic range* is a measure of the strongest to the weakest signal a system can detect. For example, if a system has a 40-decibel (dB) dynamic range centered at 0 dB, it could not detect signals below –20dB, and signals above +20 would be capped at +20 dB as far as the ADC could detect.

The ADC processing component has physical limitations related to the ENOB and *sampling frequency*, which means that it cannot perfectly represent the physical environment. ENOB for ADCs and DACs would ideally be one to one; for example, a 12-bit ADC/DAC would have an ENOB of 12. This does not happen in reality, however, because of noise, distortion, and other errors. For example, the 12-bit ADC/DAC could have an ENOB of 10. Put another way, limitations in how often the environment is sampled and the resolution of that representation result in an inexact proxy, much the way a photocopy of a document does not look exactly like the original.

The sampling frequency of an ADC/DAC in an EMS sensing system limits the resolution of the data. The frequency is tied to the distortion and other errors present in the ENOB. Frequency and sampling time errors affect ENOB. Thus, the design of these converters must balance among sampling frequency, ENOB, and potential errors. Design compromises present another opportunity for data loss and distortion that can ultimately impact a system's ability to utilize the information resident in the MDF to correctly distinguish and identify activity in the EMS.

Once a signal is converted into bits (referred to by practitioners as "raw" or "I/Q"), it is generally passed to an FPGA to convert it into a PDW. This step represents the largest distillation of the data in processing. A PDW distills the raw RF data down further into pulse trains. Pulse trains can be described by frequency, pulse width, pulse repetition interval, amplitude, phase, direction, and other characteristics.

In converting from raw bits into a PDW, the system can only parametrize what it knows to be present. If an adversary platform changes a parameter not measured by the EW system firmware, the threat could be identified incorrectly. Indeed, sensors can vary by an order of

[283] This is important to mention because an antenna can add to the radar cross-section of the host platform, increasing its visibility to threats.

magnitude in how many parameters they can sense and use to identify threats, and they will use different parameters. This is one of the principal challenges of using data from one sensor for reprogramming of a different sensor, as described elsewhere in the report.

FPGAs are reprogrammable devices that allow system developers to write custom algorithms to process the bitstream. The predecessors to FPGAs in EW systems were application-specific integrated circuits (ASICs). ASICs are custom-fabricated parts that cannot be changed once fabricated. Some legacy systems still have ASICs for EW processing, but they have largely been phased out. FPGAs are the main component of modern EW systems because of the speed at which they operate and how close to the ADC they are in the chain. Some modern EW systems have processing paths entirely in FPGAs to respond to select high-priority threats. Programming FPGAs can become a bottleneck because much of the work is still done manually in hardware description languages such as Verilog. FPGA upgrades for existing platforms take a long time for a number of reasons, including the time it takes to conduct the appropriate modeling and simulation.

The next batch of processing groups PDWs into EDWs, which are sometimes referred to as *tracks*. EDWs are the most minimized or tailored representation of what a sensor detects in the EMS. This is the first explicit use of EWIR in most EW systems, as platform MDFs are derived from the EWIR database. The EDW is often what drives the display of threats to the platform operator and to a platform's fusion engine and are the data reported offboard using the Electronic Intelligence Notation format to other platforms or other entities (such as an AOC) that are monitoring the COP. Information includes threat identification based on the MDF present on the platform. The EDW will be incorrect if the wrong MDF is loaded, if the MDF does not contain a proper entry, or if the threat has changed such that it is unrecognizable to the sensor.

As discussed above, much like a lossy compression algorithm, relevant information can be lost as data move from RF to EDW. If more storage and processing power are available to a system, less data are lost that may help to differentiate similar targets or identify unknown targets based on previously unseen metrics. SIGINT systems employ more-advanced signal processing and EMS sensing technologies than tactical RWR/ES systems as a means of addressing the timing requirements and SWaP limitations of the latter.

The conversion of PDWs into EDWs typically happens in general purpose processing. General purpose processors are what most people consider when they think of processors. These are analogous to what is found in a typical laptop or desktop computer. They are able to perform a large number of tasks on varied data sets, whereas FPGAs are programmed for a single task or purpose. The sorting and conversion of PDWs into EDWs is a process called *de-interleaving*. This process usually consists of picking a few key metrics to sort on and then combing pulses detected from emitters based on what is known about certain emitters in the MDF. Internally, many EW systems assign a confidence value or error percentage to the identification they give, because even without multiple possible matches, this kind of statistical analysis carries error, which is compounded by the error inherent in the sensors and processors upstream, such as the ADCs.

The final piece of the OBP data funnel is security hardware, such as encryptors and guards. In a multilevel security architecture, these devices, along with best practices for software interfaces and data tagging, are essential to ensuring system security when using less-trusted devices and parts and operating in environments where the security of the technology is very important.

## Problems

Although all platforms that sense data and do something with it have OBP for this purpose, not all USAF platforms have sufficient OBP to support cognitive EW or even automated MDF updates. Increasing OBP using the legacy hardware that tends to be immediately compatible with legacy systems is generally untenable given the SWaP constraints. Large servers will weigh the aircraft down and use too much of its power supply. The exception might be transport aircraft such as the C-130 and larger ISR aircraft such as the RC-135 that already devote a lot of space and power to computers by design. For any aircraft, however, whether new or legacy, more processing power is better in a voluminous data environment, and every airframe will meet its physical limitations to hold heavy, power-hungry hardware before an end to the data is found.

In addition to needing more OBP to process more data, there could be much utility in losing fewer data characteristics by having to use the sieves described above to make the volume of data tenable for processing onboard. Thus, improving OBP would enhance both timeliness and quality in the context of EWIR.

The bottom line is this: Modernizing hardware is needed to enable better performance, and the way to do this for both legacy and new platforms is through miniaturization. *Hardware miniaturization* refers to a broad suite of technological advances that significantly reduce the SWaP needed for processing in numerous applications. These interrelated advances are at the heart, for example, of why the incredible computing power of smartphones can fit into a pocket. There are numerous applications within the defense industry as well, in particular for enabling more computing to happen on platforms themselves rather than at a centralized facility with the associated significant delays in developing a COP or responding to threats.

Sensing and adapting to threats in the EMS is a good example of a prime application for hardware miniaturization to help substantially improve speed by increasing OBP. The process outlined in Figure 7.1 and described above currently requires a significant amount of SWaP to do basic processing and still relies heavily on centralized, ground-based computing for software updates. Reducing SWaP limitations for OBP would not only enable more capability on increasingly smaller platforms (such as small unmanned aircraft) but would also enable larger platforms to do more processing—something required for in-flight software reprogramming. There are also relevant policy issues; for example, vendor lock-in is an issue that can prevent easy transition of technologies to enable more processing power on legacy platforms. This being said, some legacy platforms have more potential processing power available than commonly thought; for example, the U-2 was able to fly with Kubernetes,[284] a container orchestration tool that (as described in Chapter Six) takes substantial processing power, because engineers discovered some spare processing power on part of the aircraft that was not being used for other critical purposes.

## Nearer-Term Solutions

Four near-term approaches can enhance OBP using existing technological and policy tools and will make the introduction of advanced EW software features available to more platforms.

The first approach is **better utilization of commercially designed tools and parts**. Many specialized electronic circuits or "cards" are still custom-made for DoD vendors because of military standards requirements levied on the hardware. Adapting policies and processes to enable use of wider industry standards will generate a larger array of cheaper options for necessary upgrades. It could also help reduce upgrade timelines by limiting design, test, and evaluation time; existing products have already been tested, and using industry standards when possible reduces testing required for unique requirements. The performance history of existing equipment should be considered when using this approach with legacy systems.

The second approach, building from the first, is to **require the inclusion of specialized processing units for AI/ML acceleration** as part of regular hardware upgrades. Tensor Cores[285] and other specialized ML hardware accelerate computer operations, which is meant to speed the training of NNs. Adding AI/ML acceleration will be a win-win for EWIR: Not only will these specialized processing units enable training and execution of the algorithms at the heart of cognitive EW, but they can also support the complex math needed to manage OBP itself efficiently in real time.

The third approach would be to **invest in model-based system engineering (MBSE)** tools for FPGA development to shorten the timeline to deploy new firmware. Firmware is essential to the capabilities of EW systems, and updating it can take a significant amount of time and cost. MSBE shortens the time between systems engineering activities (requirements) and implementation on the FPGA (firmware).

A final approach would be to **create standard MDF formats** and to better document platform-specific offsets and accommodations that are needed for modifying a baseline digital description of a threat so that each particular platform's sensors can recognize it. Although this approach would more generally help EWIR from a process perspective, it would also help OBP by speeding new procurement and upgrades—including those related to HPC—by introducing more consistency between platforms. Furthermore, identifying which systems currently need more major workarounds to get EWIR to work could also help prioritize future system investment toward designs that require less-intensive work for updates.

[284] USAF, 2020c.

[285] NVIDIA, "NVIDIA Tensor Cores: Unprecedented Acceleration for HPC and AI," webpage, undated.

Looking at the macro level, another difficulty comes with fielding new and advanced capabilities at scale. Traditional platforms take significant time and budget to upgrade. Depending on the time and scope of the upgrades, by the time they are fielded, they could already be irrelevant. This is a significant issue with a field that moves as quickly as EW. This is why hardware upgrades need to be considered as a stressing requirement when a new EW system is being procured. Leaving space for new cards in a box and using standard interfaces should be strictly enforced, even to the slight potential degradation of current performance. This concept is similar in principle to the ability in cloud computing to quickly ramp up power when needed.[286]

Threat agility is driving requirements for ML and cognitive processing. In the near term, upgrading to more-capable hardware will enable more-agile software development practices, such as the use of containers to enable a faster software update process. In addition to this, specialized hardware for ML applications, such as Tensor Cores, should be utilized to enable increased use of AI/ML algorithms onboard the aircraft.

## The Quantum Future

Quantum computing, or leveraging the quantum principle of superposition for the purposes of exponentially faster computation, is the technological paradigm from which the next major advances in computing capacity are expected to come. Put another way, quantum computing enables the employment of outcomes defined by a probability distribution as opposed to either a 1 or a 0 (“on” or “off”) familiar from classical computing.

Quantum computing is currently being utilized only in the cloud and for specific research purposes. Like all other revolutions in computing, it will get smaller and cheaper over time and should thus eventually be ready for a flight system. (Consider, for example, that the first device considered to be a modern computer was released in the 1930s, but there was no desktop equivalent until the 1970s.[287]) In late 2019, DARPA solicited proposals to create an industry consortium around quantum computing development.[288] The USAF should be working with DARPA on what this means for EW and the radar systems they are trying to detect. As the USAF investigates the potential for embedded (on-aircraft) quantum computing in the coming years, it should also consider how quantum computing might revolutionize OBP and what algorithms would need to be developed to leverage quantum computing technology for EW processing needs.

[286] Azure, “What Is Elastic Computing or Cloud Elasticity?” webpage, undated.

[287] Britannica, “Personal Computer,” webpage, May 21, 2020.

[288] DARPA, “DARPA Quantum Hardware Request for Information (RFI),” Notice ID DARPA-SN-20-21, December 24, 2019.

## Other Hardware Applications

### *Edge Cloud Computing*

Chapter Five and Chapter Six discussed the role that cloud computing, including edge cloud and dispersed cloud design, could play to support robust future reprogramming and cognitive EW. An important aspect of cloud computing is the physical points of presence—the hardware. Miniaturization, or the increase in processing and storage in smaller and smaller spaces, will particularly support the development of edge clouds.[289] In the context of the OBP discussion above, this same miniaturization could ultimately help groups of aircraft become their own edge cloud, processing and storing data temporarily until it can be sent to centralized cloud infrastructure. This application would also reduce network traffic by retaining the data and processing power for cognitive algorithms, thus enabling low-latency applications at the edge,[290] which is critical for weapon systems and mission support functions, such as EW. The types of hardware in question include different data recorders, processors, datalinks, and hardware connections.

### *Test Infrastructure*

As part of the description of current EWIR problems, Chapter Two raised the problem of prolonged software testing and certification cycles. The long pole in that tent is the current requirement to test all the software, as opposed to a single container of software. However, we also mentioned limited computing for running simulations as an issue. Limitations on hardware updates and the amount of hardware processing available is an issue for testing software and also for developing and conducting initial simulations of the threat models used to create the MDF of OFP updates. Thus, hardware updates impact several parts of the current EWIR process, and there are therefore multiple reasons to address this as a priority issue.

## Next Steps

The physical limitations of each platform often end up driving the design decisions for the EW system. If a system cannot receive low-frequency data, the EW system does not need hardware and software to process it. Trade-offs like this need to be considered in the earliest requirement phases of a program. If a system is specified too ambitiously, it may never meet the operational objectives for which it was intended. This is a known issue in system procurement, and the lessons learned from other platforms may be applied to the EW space as well.

In this chapter, we have argued that hardware miniaturization—in particular, increasing the amount of processing available across smaller areas—is very important to support the goal of rapid in-flight reprogramming. This means designing new systems with smaller components in

[289] Liu et al., 2021; Mahadev Satyanarayanan, Nathan Beckmann, Grace A. Lewis, and Brandon Lucia, "The Role of Edge Offload for Hardware-Accelerated Mobile Devices," HotMobile '21, February 2021.

[290] Chen and Liu, 2021.

mind and potentially opting for more-specialized chips or accelerators that can pack more processing power into less space and with less power for given applications such as ML. For legacy systems, this entails a somewhat different approach, first determining whether there is unrecognized spare processing onboard and, if not, determining the requirements needed to add more processing in the context of obstacles such as much older programming languages used to support their OFPs.

# Chapter 8. Envisioning a Future EW Capability: Vignette Analysis

In this chapter, we explore the implications of a dramatically faster EWIR process in operational contexts. For this, we use vignettes depicting an operational setting and problem to illustrate what the current role and process for EWIR would look like and how future changes would cause this to evolve. These insights connect the technologies discussed in the previous four chapters—cognitive EW, data pipelines, software architecture, and hardware miniaturization—to impacts on significant military problems. We begin with a discussion of scope and methodology and then discuss two vignettes before sharing some conclusions.

## Vignette Approach

While it is impossible to view EWIR and future advancements in rapid reprogramming through every relevant operational lens, we selected two vignettes that illustrate the software reprogramming challenge in different EW-relevant ways. Both vignettes reflect conditions that are imaginable in the 2021 present. We use them to provide use cases for faster reprogramming in an operational setting. They reflect technological and policy changes discussed earlier in this report that may be realized between 2025 and 2035.

The first vignette focuses on the suppression of enemy air defenses (SEAD) in the vicinity of Kaliningrad. The second vignette concerns tracing potential EW threats in a competitive Arctic. In the first vignette, sensing and operations in the EMS are supporting a typical kinetic operation. In the second, the EMS is the sole focus of the vignette with no kinetic warfighting activity, thus presenting a different set of operational and rapid reprogramming challenges.

For each vignette, we consider several key operational questions: What is the operational problem for the USAF and for the Joint or Coalition force as a whole? What is the nature of the EMOE (e.g., permissive versus contested, sparse versus congested)? What are the specific threats, and how must they be addressed (e.g., avoid, suppress, or destroy)? How does EWIR support EMS awareness and EW capabilities in this vignette? And how would an improved near-term edge capability and a future cognitive EW capability affect these operations, compared with the status quo?

Vignette analysis was informed by reviews of the relevant literature, interviews with SMEs, and two relevant USAF exercises: a United States Air Forces Europe training event that took place in late June 2021 at Ramstein Air Base and a Headquarters Air Force (HAF) Plan Blue Arctic wargame that took place August 9–13, 2021, at the RAND Corporation’s Arlington, Virginia, offices.

The vignettes examine three key metrics for the EWIR process: speed, accuracy, and security. We estimate speed based on the specific historical EWIR steps that would be cut out of the process as a result of improvements and the estimated time from threat sensing to software reprogramming completion based on our understanding of technological specifications and knowledge of EWIR procedures. We discuss accuracy qualitatively in terms of the risk of disruption to the find, fix, track, and target process. Finally, we assess security qualitatively in terms of high-level vulnerabilities that an adversary might exploit.

## Vignette 1: Suppressing Enemy Air Defenses in Kaliningrad

SEAD is a key aspect of offensive counterair essential for gaining and maintaining air superiority. This is a Joint mission, but the USAF has a particularly important stake in it given the need to conduct SEAD to ensure aircraft survivability. Historically, air defense threats could reasonably be detected readily through unique radar emissions. As we addressed in the report introduction and in further detail below, this has become quite a bit more complicated, making rapid reprogramming even more relevant.

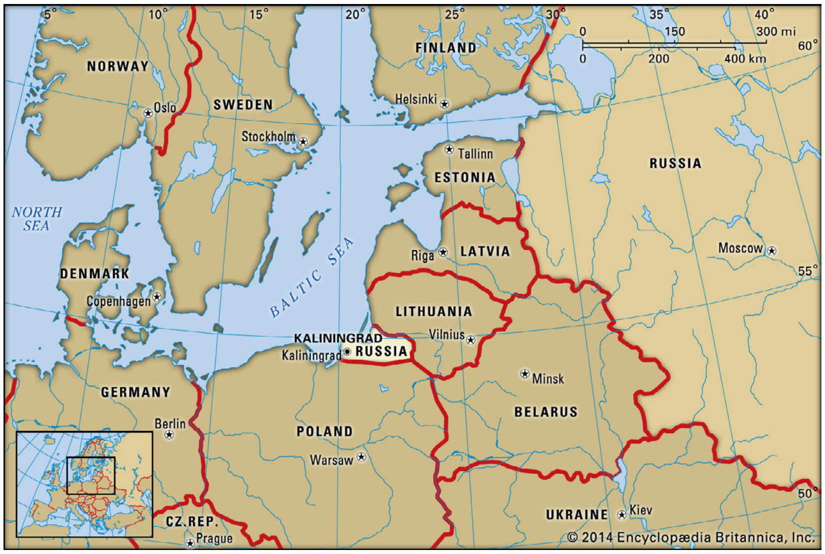
### *Stage Setting*

Kaliningrad (Figure 8.1) is located between Poland and Lithuania and was geographically isolated from the rest of Russia following the collapse of the Soviet Union. This strategic bastion in the Baltic region is defended from air threats by both longer-range and shorter-range missile defenses. Russia has long maintained an air defense cordon in this area and has expanded its reach considerably in recent years.[291] As such, it is important to both Russian and North Atlantic Treaty Organization (NATO) strategy in any scenario involving a conflict between these two parties in the Baltic region. In theory, defending the Baltic capitals of Vilnius, Riga, and Talinn would require NATO forces to access a narrow corridor between Kaliningrad and Belarus (not a NATO member), making them quite vulnerable to long-range artillery and other attacks.[292]

[291] Improved missiles have recently pushed the range out to at least 400 kilometers. See Andrew Radin, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long, *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition—Appendixes*, Santa Monica, Calif.: RAND Corporation, RR-3099-A, 2019.

[292] See, for example, David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*, Santa Monica, Calif.: RAND Corporation, RR-1253-A, 2016.

Figure 8.1. Location of Kaliningrad



SOURCE: Encyclopedia Britannica.

To secure this maneuvering space, NATO forces would need to first render Kaliningrad's air defenses inoperable. The potential density of both long- and short-range air defenses in Kaliningrad would seriously obstruct NATO forces' airspace access. Gaining this access would be necessary not only to clear a land corridor from Poland to the Baltic states but also to conduct the day-to-day aspects of running a war: C2, ISR, and logistics.

Looking at Figure 8.1, Kaliningrad's location is in a dense part of Europe. This is quite unlike the next vignette, which focuses on the sparsely populated Arctic. From an EMS perspective, this means that it is a data-heavy environment with a lot of activity. For example, there are dozens of civilian radio towers and masts in the countries immediately surrounding Kaliningrad, transmitting on numerous frequencies.[293]

From a NATO perspective, this level of background or benign activity in the EMS compounds the challenges of contending with Russia's air defenses. In this context, we characterize these air defense threats to NATO forces as being problematic both in the sense of having ranges that could hold critical assets at risk and increasingly having the potential to evade detection in the EMS.

### *Approach to the Operational Problem*

In this vignette, NATO has formed a Combined Joint Task Force (CJTF), making air, maritime, ground, and other forces available from member countries. Here, we look only at the problem of neutralizing the integrated air defense systems in Kaliningrad and not a complete wartime scenario (e.g., moving ground forces toward Baltic capitals). To achieve this objective, the CJTF would employ long-range fires such as the Joint Air-to-Surface Standoff Missile from

[293] See, for example, European Radio Map, "European Radio Map: Central Europe," webpage, undated.

a platform such as the F-15E, the Tomahawk Land Attack Missile from a Ticonderoga-class guided missile cruiser, and stand-off jamming from an EA-18G or similar[294] to first neutralize longer-range surface-to-air missiles (SAMs). Then, with long-range SAMs neutralized, Army ground fires (e.g., the Army Tactical Missile System), tactical airpower (e.g., F-15E or F-16C/D), and stand-in jamming from an EA-18G could help eliminate the shorter-range SAM threat.

Having a clear COP is critical to this vignette, both for achieving the mission at hand and for avoiding unintended consequences, such as damage to critical CJTF or civilian infrastructure. This is complicated in the vignette by the presence of a potentially overwhelmingly capable adversary[295] and the density of activity in both physical domains and the EMS. An AOC, for example, would be watching the COP carefully to ensure robust target prioritization against capabilities appropriate for the task, without duplication of effort. The AOC would also monitor for dynamic targeting opportunities. Individual platforms involved would need to maintain situational awareness to ensure accurate targeting (and not be spoofed by decoys or endure dilemmas caused by ambiguous signals) and ensure protection for themselves and other CJTF assets operating around them.

EWIR is one of the capabilities that will ultimately help decide whether the CJTF is successful. Without recent software updates to reflect the best information available about the threat environment, the CJTF capabilities would be operating with potentially large blind spots because the threat can change so quickly. Sensing the EMOE is key; theoretical intelligence alternatives such as using still imagery (from a satellite or overhead aircraft) alone would require a substantial improvement in the speed and accuracy of automated target recognition and an incredibly robust network of communications systems to transmit high data volumes quickly.

Furthermore, in this vignette, the initial long-range strikes could, in theory, be the first time that the CJTF observes new threat behaviors that systems may not yet be able to recognize. This implies the need for something other than a long-term, centralized EWIR process, as we discuss next.

[294] Steve Trimble, “House Panel Backs Airborne Electronic Warfare Upgrades,” *Aviation Week Intelligence Network*, July 28, 2021.

[295] See, e.g., Shlapak and Johnson, 2016.

## *EWIR's Evolving Role*

In this section, we compare the status quo EWIR process, a rapid MDF update, and a cognitive EW capability in the context of this vignette. This is meant to illustrate and explain potential differences in mission impact.

### Status Quo

If we freeze the EWIR process as it generally operates today and apply it to this vignette, an argument can be made that it would be very unlikely that any reprogramming would happen within this type of "kick down the door" vignette. Consider the best case, in which the CJTF is alerted to an MDF update right before operations commence. Intelligence is available and fortuitously had already undergone the modeling, testing, and programming required. (We also assume here that there is perfect sharing of information among partners.) Under present doctrine, it would still take up to 72 hours to update the MDF for one type of platform. During this time, each individual platform would need to be grounded for several hours, placing NATO's objective at risk because the platforms are unavailable for operations and potentially endangering the maintenance and logistics enterprise (which may have since become a Red target).

As a result, we suggest that the CJTF would be more likely to adopt a contingency plan for finding, fixing, and tracking targets. In theory, this would probably involve the provisioning of more ISR assets (potentially including other types of assets in a surveillance role) and even heavier reliance on platform-to-platform communications to organically build a COP quite literally on the fly. This raises the potential risk of miscommunication or misunderstanding, which could degrade the accuracy of effects delivered by kinetic and nonkinetic means and could place into question some platforms' abilities to adequately protect themselves from threats. Manned ES platforms such as the RC-135V/W Rivet Joint would need either to operate at standoff range or to place themselves in vulnerable positions. Given the extended reach of Russian air defenses in the environs of Kaliningrad, operating at standoff range would be a significant or even mission-fatal disadvantage.

### Automated MDF Update

Now imagine an automated MDF update capability assigned to the CJTF. This would consist of a data recording and offloading capability on platforms, high-speed data links and good satellite communications access, and hardware on the ground or as a hybrid ground-air-maritime architecture forming an edge data processing and storage capability that would ultimately be part of the cloud used to support combat operations. Consider a modified threat behavior that is detected by, for example, an F-15E that is then able to immediately cue an exquisite ISR asset to sleuth out more information. All assets that detected the new behavior would send data to be processed at the edge. A series of automated tools, overseen by personnel in theater (or with good communications outside of theater), would generate an MDF update for each platform, which would be wirelessly transmitted on the ground at rest or even potentially during the mission.

The result would be a complete run-through of the EWIR process, albeit for a very small update task, in a matter of minutes or hours. Although the current EWIR process would remain intact at the macro level, several current substeps would be circumvented. In particular, the use of containerized software would be a strong step toward minimizing the time it takes to conduct testing and airworthiness certification. Another significant change would be the lack of a multistep intelligence vetting process. Instead, the new intelligence data would ultimately be sent back into the centralized cloud for longer-term analysis and consideration, after vetting, for inclusion in key intelligence databases.

An automated MDF update capability could enable an incremental improvement in accuracy, resulting in fewer effects expended compared to the status quo. There could also be second-order impacts to accuracy. For example, more-tailored jamming could result in less activity in the EMS and thus a less cluttered and ambiguous operating environment.

### Cognitive EW

Finally, how would cognitive EW affect the operation? In addition to containerized software and some minimal separate edge computing infrastructure, every platform would be enabled by HPC tailored to ML needs and preprogrammed and primed algorithms. With more OBP capacity, platforms might be able to retain more of the raw data collected by their sensors, thus potentially making their organically collected data more useful to other platforms that have different sensing capabilities. In this “every asset is a sensor” model, there might be a possibility of somewhat reducing redundant ISR platforms. Because ML algorithms would be continuously running in response to new information gathered from the environment, software updates would be made during the mission, in a handful of seconds to minutes, depending on how long the update-learning-update cycle would need to be in response to a change in the threat environment. There would no longer need to be a clear distinction between MDF and OFP updates; the more extensive the change in the threat environment or the more rapidly those changes are happening, the longer it would take to make the update. The only human in the loop would be the platform operator. As in the case of automated MDF updates, data would ultimately be shared with a centralized system for future storage and study.

The end result would enable the CJTF to dynamically target novel systems and would provide much-improved self-protection for personnel and platforms. This is because the cognitive system would learn from threat responses in real time and would adapt to improve countermeasures if or when an initial effort fails. Alongside these operational benefits would also be a new vulnerability to an adversary system designed to target AI. This is something that the USAF would need to detect and neutralize using new tools.

In summary, Table 8.1 highlights some key differences from the comparisons made above. Note that, for this vignette, there is some benefit from even relatively small changes to the EWIR process, but the most substantial impact is clearly made through cognitive EW.

**Table 8.1. Comparison of Status Quo, Rapid MDF Update, and Cognitive EW in the Context of the SEAD Vignette**

| EWIR Process | Key Changes Versus Baseline | Speed (best) | Accuracy | Security |
|---|---|---|---|---|
| Status quo | None for EWIR; more ISR for workaround | Days | Low, because updates are not happening; workaround risks accuracy | Baseline level for software, potential increase in physical risk |
| Rapid or airborne MDF update or airborne software update | Automation with humans in the loop; containerized software, edge computing architecture | Minutes | Limited to small changes in threat behavior (OFP updates not possible) | Improved due to containerization of software |
| Cognitive EW | HPC and algorithms onboard, less redundancy in ISR assets | Seconds | Continuous improvement | Much improved because algorithms can detect intrusions; some risk from adversarial AI |

## Vignette 2: Operating in a Competitive Arctic

In June 2020, the USAF released its first Arctic Strategy.[296] The Arctic has received increasing attention related to military security issues over recent years with the growth in climate change impacts and growing global interest in economic and strategic aspects. The Arctic has been a strategic location for U.S. air power since the Cold War. Though the United States and Russia have historically partnered in this region of mutual interest and responsibility, Russia's ramp-up of military capability, including EW assets, in the far north could present the United States and regional NATO allies and partners with dilemmas about whether and how to act in an ambiguous, information domain–focused environment. Here, we explore a fictional vignette in which reprogramming could play an important role in navigating competition and an apparent Russian EW-based anti-access strategy in this region of vast distances, harsh environmental conditions, and sparse infrastructure.

### *Stage Setting*

Besides Russia, seven other countries have land territory in the vicinity of the Arctic Circle: the United States, Canada, Greenland (Realm of Denmark), Iceland, Norway, Sweden, and Finland.[297] Russia has by far the largest amount of land territory in the Arctic, followed by Canada. It is inhabited, but sparsely so compared with many other parts of the world. There are several substantial settlements across the region (e.g., Murmansk, Russia; Fairbanks, Alaska;

[296] U.S. Air Force, *Arctic Strategy*, July 21, 2020a.

[297] For more information, a good place to begin is the Arctic Council's website. The Arctic Council enables dialogue and decisionmaking among the Arctic states but does not address military affairs (Arctic Council, homepage, undated).

Yellowknife, Canada; Nuuk, Greenland; Reykjavík, Iceland; Tromsø, Norway; Umeå, Sweden; and Oulu, Finland), and it is home to several indigenous groups. Generally speaking, the availability of all forms of infrastructure is very uneven, with many areas lacking consistent access to transportation and communications. The Arctic contains many natural resources, including hydrocarbons, minerals, timber, and fish. Russia, in particular, has been rebuilding post–Cold War military capability in the region,[298] though all Arctic countries are actively considering their needs for military presence as the physical and strategic environments continue to change.

Despite Cold War tensions and more-recent competitiveness, this region has remained one of the most peaceful in the world. This is largely because there are relatively few active disputes, and Arctic countries have thus far sought international rules–based approaches to resolving them or have otherwise limited the fallout from these disputes to the diplomatic arena.

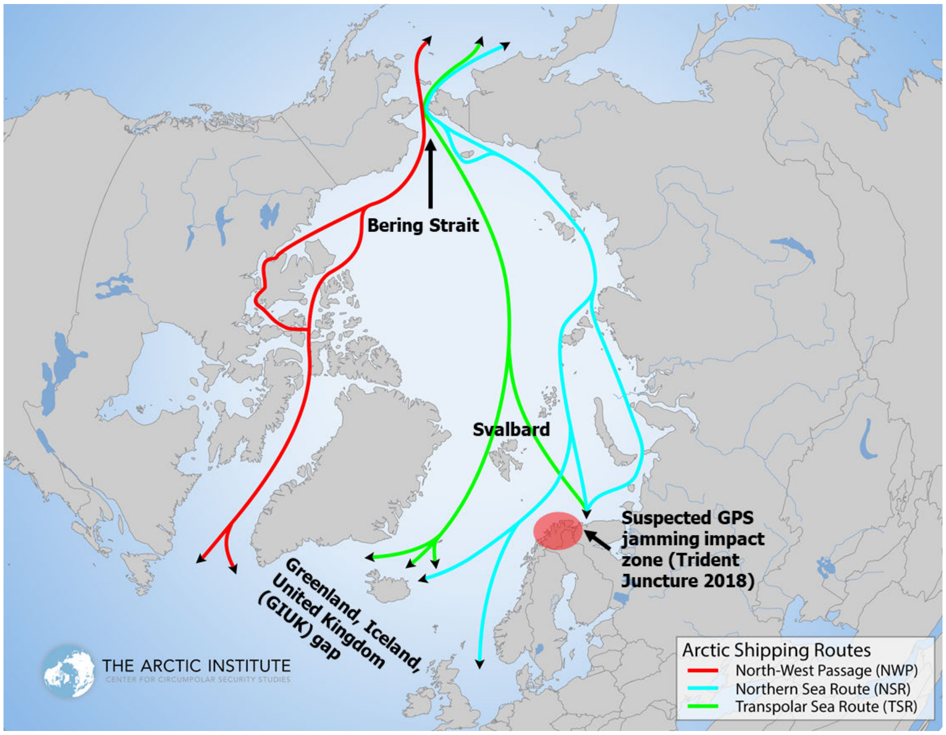
There are three exceptions, which have seen the initial signs of growing military attention to the region. The first has to do with the boundaries of acceptable steady-state military behavior, which we do not focus on in this vignette except to note that, in some cases, growing military presence can serve to increase tensions, encouraging different sides to build up in kind to match the perceived threat from others. The second is about the legal status of the Northeast Passage, also known as the Northern Sea Route, which runs along Russia's Arctic coastline (see Figure 8.2). Russia claims control over this sea route on the basis of guidelines written about ice-covered waters in the United Nations Convention on the Law of the Sea,[299] among other legal arguments, and has established infrastructure and a management system to support commercial traffic along the route—for a fee and with a Russian icebreaker escort.[300] (Canada also claims legal control over the sea route along its northern coast, the Northwest Passage, and has based this argument on international norms concerning historic internal waters.) The third is less frequently discussed but very much pertinent to the subject of this report: Russia has substantial EW capabilities in the Arctic. For example, during the 2018 NATO Trident Juncture Exercise in northern Norway, Russia was suspected of jamming GPS, resulting in substantial disruptions to both military and commercial air traffic.

[298] See, e.g., Eugene Rumer, Richard Sokolsky, and Paul Stronski, "Russia in the Arctic—A Critical Examination," *The Return of Global Russia*, Carnegie Endowment for International Peace, March 2021; and Rebecca Hersman and Eric Brewer, "Deep Dive Debrief: Strategic Stability and Competition in the Arctic," *CSIS Briefs*, January 6, 2021.

[299] United Nations Convention on the Law of the Sea, December 10, 1982.

[300] An argument can be made that an icebreaker escort is a necessary and desirable safety measure for transit of nonicebreaking vessels anywhere in the Arctic, but the fact that Russia has made this a requirement has raised concerns from other countries.

**Figure 8.2. Selected Key Arctic Locations**


Bering Strait
Svalbard
Suspected GPS jamming impact zone (Trident Juncture 2018)
Greenland, Iceland, United Kingdom (GIUK) gap
THE ARCTIC INSTITUTE
CENTER FOR CIRCUMPOLAR SECURITY STUDIES
Arctic Shipping Routes
🟥 North-West Passage (NWP)
🟦 Northern Sea Route (NSR)
🟩 Transpolar Sea Route (TSR)

SOURCE: Malte Humpert, “Arctic Shipping Routes,” Arctic Institute, July 2016.

As a point of departure for this vignette, we pose the fictitious situation in which commercial vessels transiting the Northern Sea Route early in the warm season, when ice conditions can be very unpredictable, refuse to pay Russian tariffs or accept other terms of passage, such as a Russian icebreaker escort. They ultimately find themselves stranded in frigid Arctic Ocean waters at either end of the route, south of Svalbard and just past the Bering Strait, respectively. This is because their navigation, communication, and sensing systems are experiencing intense interference and they cannot safely resume transit. Russia is suspected of initiating this interference as a way of demonstrating control over the route and displeasure with the commercial companies’ assertion that they do not need to accept Russian laws and policies about the route.

Norwegian and U.S. forces begin low-level surface presence and airborne reconnaissance missions in their respective areas of responsibility to prepare for possible escort and/or search and rescue (SAR) needs. Any mission to get to the stranded vessels would be within the boundaries of the disputed Northern Sea Route waters. Norwegian and U.S forces report concerns to their National Command Authorities regarding erratic behavior of Russian anti-ship and anti-aircraft capabilities. National intelligence authorities are unable to confirm these observations, and confusion ensues about whether Russia is planning to take kinetic defensive or offensive actions or whether its actions are a massive deception attempt. It does not appear that sensors onboard relevant platforms are able to easily distinguish real from potentially false signals intended to deceive. This confusion is compounded by the fact that Norwegian and U.S. forces are also somewhat impacted by the interference that is stranding the commercial vessels.

### *Approach to the Operational Problem*

Following brief diplomatic discussions, the UK stands up a Joint Expeditionary Force (JEF), which at the time is believed to be a less provocative option than a U.S.- or NATO-led effort. The JEF also enables more-seamless cooperation with non-NATO members Sweden and Finland, as well as the Baltic countries, should tensions spill over or the Arctic crisis be a military feint in order to create more favorable conditions for Russia to conduct operations further south. In addition, both the United States and Norway activate national incident teams to address issues specific to their respective countries alone. The JEF coordinates with NATO to increase air policing missions over Iceland and begins a separate SAR exercise in the Greenland, Iceland, and United Kingdom Gap as a means to move more capabilities into the region without overtly provoking Russia. The JEF focuses on three lines of effort:

1. Support civil authorities in planning and preparing for SAR or escort missions to preserve life and property.
2. Protect military and other assets from anti-ship and anti-air threats.
3. Prepare information to support information warfare and diplomatic discussions, as needed.

There are a number of air-, sea-, and land-based capabilities involved. In this context, the USAF would be involved on both ends of the Arctic. Starting with the European theater, the USAF might support NATO air policing missions (e.g., F-15C),[301] provide airborne surveillance (e.g., RC-135, RQ-4), enhance logistics and supply lines (e.g., C-17, KC-10),[302] support readiness for air-to-air or air-to-ground missions (e.g., F-16),[303] and even prepare to execute a long-range bomber flight to emphasize NATO strategic intentions.[304] For this, the USAF might deploy some assets in Germany, the UK, and Italy further north temporarily—for example, to northern Norway or to Iceland. The exception would be the B-52, which would remain based in the continental United States.

The USAF already bases assets in Alaska, and these would undoubtedly remain or go on high alert. There might be preparations to conduct rescue and air-drop supplies (e.g., 176th Wing with specialized personnel, HC-130J, and HH-60G), and as in the European theater, there would be a need to support readiness for air-to-air, air-to-ground, or show-of-force (e.g., F-35) operations. The USAF supports early warning through the Distant Early Warning line, which

[301] Allied Air Command, "US F-15s Complete NATO Air Policing Deployment to Iceland," Ramstein, Germany, August 3, 2021.

[302] Douglas Ellis, "Linking Continents Through Refueling," *Aerotech News*, November 10, 2015.

[303] Kenya Shiloh, "U.S. Solidifies NATO, Allied Partnership at Trident Juncture 2015," 52nd Fighter Wing Public Affairs, U.S. Air Force, October 30, 2015.

[304] Charles Ramey, "Global Strike Airmen Support Largest NATO Exercise in 20 Years," Air Force Global Strike Command Public Affairs, November 6, 2015.

we assume has had some upgrades by 2025, and through capabilities at Thule Airbase in northwestern Greenland. Finally, some additional airborne surveillance (e.g., U-2, RQ-4) might be sent to monitor conditions in the vicinity of the Bering Strait. We assume that Norway and other partners are monitoring the situation on the other side of the Arctic, south of Svalbard.

These USAF capabilities would be employed alongside Joint and Coalition assets. A full detailing is beyond the scope of this vignette, but, generally speaking, we can imagine the presence of various nations' Coast Guard and Navy surface vessels, including for icebreaking, rescue and law enforcement, reconnaissance, and resupply. Canada, the UK, and the Nordic countries all have fighter aircraft, including the F-18 and F-35. The United States and some foreign partners would also contribute maritime patrol aircraft, potentially including EW-capable aircraft (e.g., EA-18G, UK Eurofighter Typhoon) in this role given the nature of the crisis, and the United States Army might deploy one or more Multidomain Task Forces[305] and aid in logistics. There are also relevant subsurface and foreign land force capabilities.

Having a good COP in this context is important for numerous reasons. First, there is a great deal of ambiguity in the general situation and in the EMS specifically. Second, the crisis is spread over different parts of the Arctic with some concern and need to watch the Baltic region at the same time. Third, there are many partners involved—Joint and Coalition—because no single country or military unit has sufficient capability to resolve this type of crisis in the Arctic alone, and there will be difficulty in planning and C2.

Software reprogramming of aircraft sensing in the EMS is critical in this vignette, not only because potential threats are capable and evasive, but principally due to the highly ambiguous environment in which it is difficult to discern whether the unusual activity in the EMS is related to real threats or false indicators devised to deceive. In addition to trying to avoid areas of suspected interference, any operations to conduct the three lines of effort outlined above would need to be able to detect and respond to real or false threats, and in different ways. Responding to real threats would involve typical options ranging from avoidance to a kinetic action. Responding to false threats may be much more complicated, since the intent of the deception could be to send a Coalition asset directly into harm's way.

### *EWIR's Evolving Role*

Due to the complexities of this situation, it is unlikely that conventional, heavily human-dependent reprogramming could play an active role in this vignette. Unlike the SEAD vignette, this is less due to timeliness (though that would also be a potential problem) and more about accuracy. With weeks or months of time and upgraded hardware and software to enable fine-tuning of RWR components, it might be possible to achieve more accuracy. Certainly, the deep expertise throughout the EWIR enterprise would contribute heavily to a win in this situation. However, many systems that would require a software update because of a shifting threat environment would struggle with the complexity of data needed to distinguish real from false

[305] Thomas Brading, "First Multi-Domain Task Force Plans to Be Centerpiece of Army Modernization," *Army News Service*, February 1, 2021.

threats in this circumstance (made worse in some areas by interference) and to determine how to respond to them. Rather than reprogram software or even elevate the level of intelligence support, the United States and its partners would likely contemplate a range of options, from simply trying to avoid areas of interference (which may prevent any rescue or effective show of force) to contemplating some sort of response in kind through the EMS, which would potentially result in escalation. The most likely outcome would be continued diplomatic talks without a strong, in-region NATO rescue and military option to back these up.

This vignette also lacks a compelling concept for establishing an in-theater MDF update. Once again, the complexity of the EMS activity is beyond a software tweak. Furthermore, the lack of infrastructure in the region could hinder the rapid establishment of edge processing and other necessary capabilities in the Arctic theater itself. Something could be done at existing bases further south, perhaps.

However, the cognitive EW concept could prove quite useful. The ML algorithms, if designed to do so, could have the capacity to distinguish threat behavior from that of false threats or EMS actors that are not threats at all. Indeed, we have discussed the possibility that cognitive EW would rely in some cases on recognizing threat behavior, rather than seeking to identify each individual threat. That approach could prove quite useful in a situation such as that outlined in this vignette.

Table 8.2 summarizes the speed, accuracy, and security implications of this vignette, assuming status quo EWIR, MDF updates at the edge, and a cognitive EW future. While there is a role for EWIR to play in this type of scenario, current and even moderately improved EW capabilities would not help. Only cognitive EW would likely enable sufficient ability to distinguish threats because it could pick up, based on machine-to-machine interactions, very subtle nuances that distinguish real from mock threats based on responses to attempted countermeasures. As before, there would also be a new vulnerability to an adversary system designed to target AI.

**Table 8.2. Comparison of Status Quo, Rapid MDF Update, and Cognitive EW in the Context of the Arctic Vignette**

| EWIR Process | Key Changes Versus Baseline | Speed (best) | Accuracy | Security |
|---|---|---|---|---|
| Status quo | None | Not applicable | Only as good as the going-in software (no updates) | Possible risk to nonhardened software |
| Rapid MDF update | Not supported by Arctic environment | Not applicable | Not applicable | Not applicable |
| Cognitive EW | HPC and algorithms onboard | Seconds | Continuous improvement | Much improved because algorithms can detect intrusions; some risk from adversarial AI |

## Conclusions

Both vignettes highlight the limitations of the current EWIR process for addressing hard operational problems. In each case, current EWIR capability is useful up to the point of crisis, after which an updated concept would be needed to conduct timely and accurate reprogramming. Although these vignettes are not representative of all possible competition and conflict scenarios, we selected them because they do cover relevant, hard problems. They also highlight two important problems with the current EWIR process: speed and accuracy.[306] Furthermore, they both illustrate the broader point that the limitations articulated in Chapter Two have real operational drawbacks that make the United States less competitive against highly capable adversaries. In the next chapter, we discuss recommendations for revitalizing EWIR to be relevant in contexts such as those described herein.

[306] Neither vignette strongly addresses the security of the EWIR process, although we do point out its relevance.

# Chapter 9. Recommendations

U.S. adversaries are looking to offset the United States' historical capabilities in the EMS 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. Adversaries may also cause dilemmas for the United States and its allies by taking actions in the EMS without initiating a kinetic war.

Software reprogramming—from data collection to coding, testing, uploading, and using updates—is necessary against an adaptive adversary, whether that adversary is simply seeking to evade detection or using the EMS in novel ways during competition to confuse decisionmaking. As discussed in Chapter Two, the current EWIR process is not designed to respond adaptably to complex, fast-changing, and evasive EMS threats of the future. 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. This situation is not unusual; processes are often designed with the past, present, and near-term future in mind and have limited flexibility to adapt to total regime or paradigm shifts such as are emerging in the EMS.

We have highlighted a variety of obstacles that limit the current process. These include a large number of steps, many of them manual; problems with data capture and sharing; lack of sufficient manpower and resources; issues with requirements communication; long security hardening and certification timelines; and persistence of legacy software and hardware.

Fixing problems that slow the existing EWIR process is a necessary step to keeping the United States competitive in the EMS; but the USAF should be thinking much further ahead about the kind of EWIR capability it will need to meet the most challenging adversaries in the future—and it should start investing now in the enabling technologies required to realize that vision. In our estimation, the key technologies to enabling an ultimate vision of cognitive EW would include the development of a capability and process for generating and seeding ML algorithms, enabling advanced data engineering and cloud computing, containerizing software, and taking advantage of miniaturized hardware, especially in the area of HPC.

To that end, we introduce a series of recommendations in Tables 9.1 and 9.2. Some of our recommended investments will have immediate benefits for the existing EWIR process, but all will move the USAF toward the autonomous, onboard reprogramming capability necessary to survive in future denied and congested EMS environments. These are derived from selected portions of our DOTMLPF-P matrix in Chapter Three and are informed by the research presented in Chapters Four through Seven (technology case studies). Table 9.1 includes recommendations that we call "fundamental," which focus on generating faster and more-accurate reprogramming in the next two to five years while also preparing for cognitive EW. Table 9.2 includes recommendations that we call "visionary," which focus on accelerating and integrating technology development and adoption in order to support the cognitive EW vision over the longer term. Within the fundamental recommendations are two main thrusts: (1) changing how software is architected and (2) enabling rapid[307] MDF updates in theater. Within the visionary recommendations are two additional thrusts: (1) accelerating the development and adoption of key technologies and (2) integrating these into a cohesive core to better enable cognitive EW. For each recommendation, we include a specific action and organizations that we believe would play a critical role in executing them.

[307] Here we define *rapid* as within seconds to a few hours (at least an order-of-magnitude faster than "emergency" updates, which doctrinally take place within 24 hours), leveraging computing and communications capabilities that enable lookup table updates after landing but before the next mission (perhaps with a different aircraft tail and crew) or even in-flight updates during a mission.

**Table 9.1. Summary of Fundamental Recommendations**

| | | |
|---|---|---|
| *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<br>HAF A5<br>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<br>ACC A3<br>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), OBP, 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<br>ACC A3<br>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<br>NASIC<br>Air components |
| 10 | Update AFI 10-703 to clarify under which circumstances MDF updates can be conducted in-theater | HAF A5 |
| 11 | Update data QA/QC processes for intelligence to facilitate more-rapid data use at the edge | HAF A2/6<br>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 |

**Table 9.2. Summary of Visionary Recommendations**

| | | |
|---|---|---|
| *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<br>350th SWW |
| 15 | Gather and write requirements for increasing onboard HPC, use of dedicated ML accelerators (e.g., Tensor Cores), development of data warehouses, and real-time data fusion | ACC A5/8/9<br>ACC A3<br>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<br>USAF Life Cycle Management Center Big Safari<br>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<br>350th SWW<br>(Air Force Research Laboratory)<br>(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<br>HAF A3<br>HAF A5 |
| *Integrate technologies to enable cognitive EW vision* | | |
| 19 | Develop integrated enterprise strategy of investments and employment related to cognitive and adaptive EW algorithms, data engineering and cloud integration, software containerization and orchestration, and hardware miniaturization | HAF A5<br>ACC A5/8/9<br>USAF digital executive |
| 20 | Organize, train, equip, and provide EMS operations-capable forces that<br>i. employ interoperable and extensible software components and microservices across platforms<br>ii. analyze real-world data sets necessary to train cognitive EW systems<br>iii. develop ML algorithms to facilitate cross-correlation of data from multiple sources<br>iv. marry data to miniaturized hardware and containerized software<br>v. enable access to high-speed datalinks to prime algorithms with the most recent data pre-mission<br>vi. facilitate data extraction post-mission to share with other aircraft before their missions<br>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) |

## Fundamental Recommendations

### *Alter How Software Is Architected and Supported*

Our first set of recommendations on rearchitecting software are intended to serve the dual purpose of jump-starting rapid reprogramming in the next two to five years and also setting the stage for cognitive EW.

Recommendation 1 calls for coordination to move toward containerized software. It is important to emphasize that without containerized deployment architecture for faster deployments of software, there is no digital basis upon which to truly modernize what has for decades been the most capable air force in the world. This will also involve coordination at the DoD level. DoD recently released its "DevSecOps Reference Design" for Kubernetes,[308] which the USAF is coordinating through Platform One.[309] The USAF also has similar ideas in its Science and Technology[310] and AI Strategy[311] documents. However, we have not observed documentation of policy-level activities intended to specifically meet the software containerization and orchestration needs of intelligence and EW aircraft, data, and organizations. Some of the Advanced Battle Management System on-ramp activities may provide opportunities to learn more about intelligence and EW needs when it comes to software;[312] however, recommendation 1 is directed toward developing a firm commitment toward modernization, as well as more focused and purposeful inclusion of the needs of the intelligence and EW communities in the broader DoD and USAF software containerization initiatives. For example, aircraft with intelligence capabilities may carry multiple sensors of interest that already take up considerable processing power aboard (generally speaking) legacy platforms or those that are rapidly approaching legacy status, and it is not clear how they will be able to also enable sufficient OBP to support orchestration software. In another example, there are several platforms that are not focused on EW but carry RWRs for self-protection; the USAF will need to decide whether these should also be prioritized for containerized software.

Recommendations 2 and 3 focus on better understanding what platforms need in terms of OBP in order to enable containerized software and support orchestration of those containers. We discovered during the course of our interviews that the capacity of current hardware and requirements for avionics that use containerized software are unknowns for many platforms.

Recommendation 4 addresses the fact that the USAF's software factories, while conducting important work, generally develop tools that assume a prevalence of ground-based computing capacity to support processing and storage. However, as we have pointed out, in-flight reprogramming will require processing and some storage to be enabled onboard. This will necessitate changing the model for software factory customer service, in which the factories pull needs from flying units, as opposed to flying units being invited to participate in software factory initiatives.

[308] DoD, 2021b.

[309] U.S. Air Force Chief Software Office, "Platform One Products and Services: Customer DevSecOps Platform (DSOP)," webpage, undated-b.

[310] U.S. Air Force, *Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*, April 2019b.

[311] U.S. Air Force, *The United States Air Force Artificial Intelligence Annex to the Department of Defense Artificial Intelligence Strategy*, 2019a.

[312] Brian W. Everstine, "USAFE's ABMS On-Ramp Included Partner Nations, Base Defense Scenario," *Air Force Magazine*, March 1, 2021.

Recommendation 5 is about helping to break platform-based stovepipes in the reprogramming community. As discussed in this report, personnel are assigned to platforms because of the uniqueness of each RWR and broader system. However, this model inhibits learning and agility, so we recommend that personnel gain experience across at least two platforms. This will specifically increase agility for supporting near-term improvements in reprogramming and readying the force for containerized software, which will help further automation. In the near future, personnel may be needed to monitor automated reprogramming across platforms, so this cross-platform familiarization will be an important first step.

### *Enable Rapid MDF Updates in Theater*

We now move to discussing our second series of recommendations regarding rapid in-theater MDF updates. These correspond with recommendations 6 through 12 and assume that recommendations 1 through 5 are also moving forward in parallel. In-theater MDF updates would ideally be done in flight, but even a ground-based capability (i.e., after an aircraft has landed) would be valuable. It is possible that a hybrid approach will be used; aircraft with sufficient OBP can have minor MDF updates done in flight. Enhanced ground-based computing closer to the combat edge can be leveraged for aircraft with less OBP and/or for less urgent MDF updates.

Recommendation 6 is about getting the hardware and tools ready for edge operations. This will include ensuring that platform data are recorded and made available (e.g., via QRIP and KM/RAPIDS), that there is a hybrid edge cloud with urgent processing and storage at the edge and a central repository for longer-term data management, and that existing tools like SPECTRE are considered for further improvement toward automating some MDF updates.

These technology-focused changes would need to be accompanied by the development of edge-based tactics (recommendation 7) and the potential alignment of some reprogramming personnel from a platform-centric approach to a theater-based one, following a recent series of changes in how intelligence supports theater ISR (recommendation 8).[313] Such changes would also necessitate exercises at the edge (recommendation 9), something that might be enabled by regularly occurring mini-exercises that are already happening within air components.

Two additional policy recommendations are needed to support these changes. Recommendation 10 focuses on the need to rewrite AFI 10-703, focused on the EWIR process, roles, and responsibilities, to clarify under which conditions automated MDF updates should be attempted at the edge. Recommendation 11 acknowledges that, in order to rapidly update MDFs at the edge, there will need to be additional flexibility in how intelligence data and products receive QA and QC, at least for the individualized purpose of MDF updates at the edge. Intelligence data used for these rapid MDF updates, once in a centralized database, might undergo the standard QA/QC before heading to a permanent repository.

[313] Menthe et al., 2021a.

Our final fundamental recommendations consider personnel experience. Increasingly, airmen who are not formally trained in software development and coding are receiving exposure to these fields on the job. Some become quite adept in manipulating software and even doing some of their own coding. In rare cases, airmen from nonsoftware fields have coded prototype tools that have then been further developed. At the very least, airmen in the intelligence, EW, and reprogramming communities are increasingly capable of articulating their requirements in ways that software and data engineers can take action on. Thus, recommendation 12 suggests developing a way to track software-savvy airmen, such as through the use of a special experience identifier.

Recommendation 13 is about elevating the depth of EW experience among the elite but small cadre of Electronic Warfare Officers. At present, these officers receive a platform assignment early in their careers. However, experience across platforms would benefit those who end up in an AOC, for example. Thus, we recommend the USAF explore development of a subset of EW officers who would ultimately serve as theater EW coordinators within the AOCs and thus require some hands-on experience with more than one platform. This would indirectly benefit the development of rapid MDF updates at the edge because EW officers would be needed to help manage the process in theater.

## Visionary Recommendations

### *Accelerate Technological Development*

Recommendations 14 through 18 address the need to accelerate technology development toward a cognitive EW future. Recommendation 14 recognizes that an applications-based approach provides a near-term opportunity for enhancing capabilities, especially at the edge. However, we argue that the USAF must go beyond achieving additional automation and an adaptive (i.e., via complex, preprogrammed rules) EW capability through any use of an applications layer built on top of existing OFPs. An applications-based approach should not replace a longer-term goal to redesign flight software to enable lightweight virtualization and containerized microservices, which will ultimately provide the seamless software environment in which to operate cognitive EW. This will be much more difficult to achieve than less-invasive options, such as an applications-based approach or (at a more basic level) in-flight MDF updates, that involve many fewer organizations. Ultimately, the USAF must recognize that significant modernization is required to counter threats that may also leverage ML to evade detection or recognition—and perhaps even to counter those that do not, given the complexity of the EMS and the difficulty of operating within it.

Recommendation 15 calls upon the USAF to write requirements for the longer term, specifically in the areas of HPC and the use of ML accelerators, data warehouses, and real-time data fusion. Hardware is a critical component of software- and data-driven operations, and the USAF must account at the enterprise level for the needs required across platforms to achieve advanced EW concepts in order to take advantage of advances in hardware capacity and specialization.

Next, we introduce two ways to expand the testing and operational use of advanced EW concepts. Recommendation 16 focuses on using ES, mobility, and tanker aircraft to move the state of the science forward. These platforms can become early adopters of EMSO-relevant smart systems and ML-driven algorithms, additional HPC, changes to software architecture and orchestration, cloud integration, and advanced data fusion. Although these platforms lack stealth, they have extremely favorable SWaP and, in some cases, have existing sensors and communications systems that could demonstrate autonomous reprogramming concepts using native sensing capabilities and an airborne cloud environment. Upgrades and flying time will not come for free, but we argue that much could be achieved within the context of missions or exercises that these platforms would participate in anyway.

Recommendation 17 is to create a service-owned reprogramming and cognitive EW development and testing activity ("EWIR-X"). This will also necessitate the establishment of an integrated team of EWIR engineers, data engineers, and software engineers to build the developmental pipeline and testing environment. Creating adaptive and cognitive EW algorithms and conducting the necessary data analysis, development, and testing will not happen overnight and will require much trial and error. This could be done by commercial organizations, by existing software factories, and/or as distributed activities across many service organizations. However, we believe that this type of experimentation would best be endemic to the 350th SWW itself as the locus of subject-matter expertise on EMS operational needs, tactics, and platforms. The research outcomes will be much more tailored to specific needs, and can evolve with wing efforts to organize, train, and equip, if software and data engineering, ML, and other skills are brought *in* rather than contracted *out*. This will also better ensure that the resource remains available to the wing, as forward movement cannot be sustained with interrupted progress in research and experimentation because (for example) another mission is deemed a higher priority for a shared resource.

Finally, recommendation 18 acknowledges the need for a change to data classification and access policies to create a healthy data pipeline. Newer data warehouses (called for by recommendation 15) could expand accessibility using software-defined security practices. However, this still does not solve the policy problem of data classification. Some data will likely continue to be highly classified; however, this recommendation aims to make as much data available as possible. This will also require establishing policies and architectures for moving data incidental to Title 10 (military) operations to use for Title 50 (intelligence) purposes.

### *Integrate Technologies to Enable Cognitive EW Vision*

We end with two recommendations on integrating technologies and approaches to achieve cognitive EW. Recommendation 19 is about strategy: There is a need to develop an adaptive strategy (updated regularly, perhaps even in a living, DevSecOps sense) to ensure that efforts within the USAF and DoD are coordinated. This is especially true of the key pillars we discussed in this report: containerization, data engineering and cloud computing, hardware miniaturization for OBP, and cognitive EW algorithms.

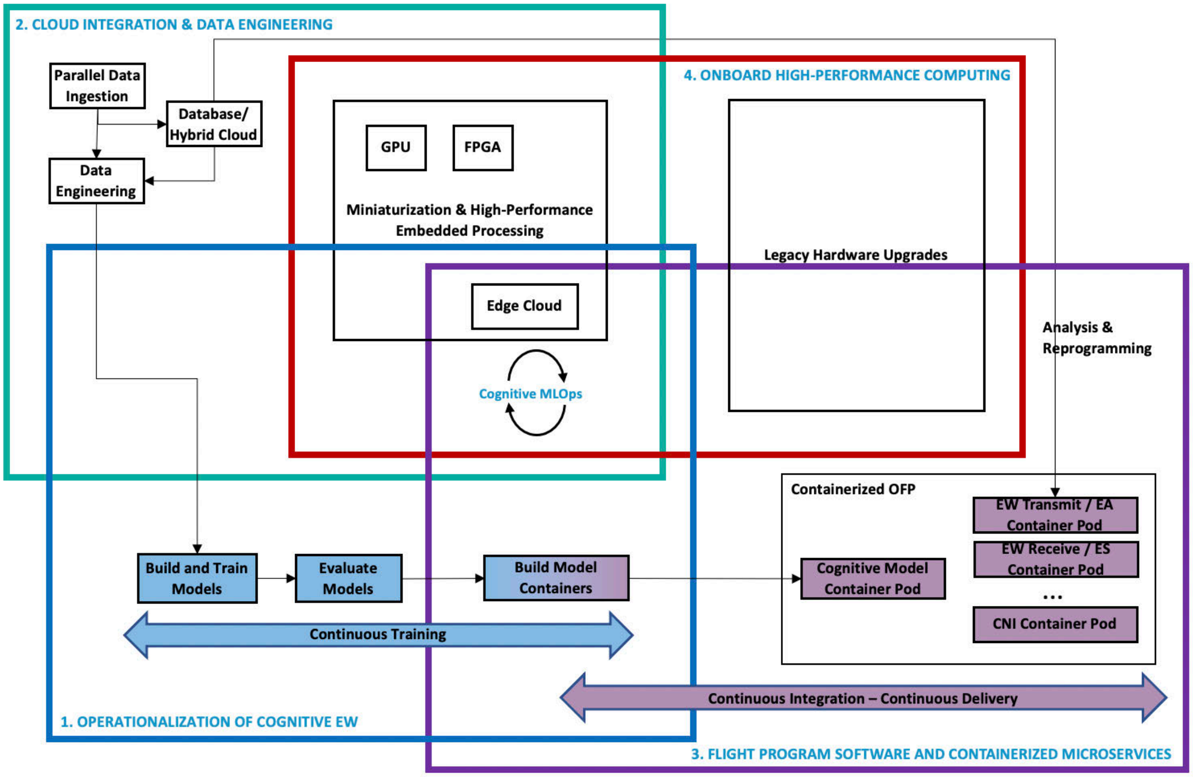
Recommendation 20 speaks to the types of activities that operational wings, together with partners such as software factories, will need to be able to routinely do as part of implementing a cognitive EW strategy. Key activities that are necessary for enabling cognitive EW include having interoperable and extensible software components and microservices across platforms, training cognitive EW systems using real-world data sets, developing ML algorithms that can help cross-correlate data from multiple sources, joining data to high-performance hardware and containerized software, using high-speed datalinks to inject cognitive EW systems with the most recent data to "prime" them with the latest threat information pre-mission, facilitating the extraction of data post-mission to be added to cognitive EW algorithm training data sets, and allowing more personnel to develop knowledge of software and associated services across platforms to ensure more-holistic perspectives on implementation and operationalization across the fleet. These activities will need to be explored and used at scale on a day-to-day basis.

## Conclusion

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 most capable of evading conventional tracking and countermeasures.

Though disruptive, many of the changes on the path toward cognitive EW described in this report could be incrementally achieved to enable some early capabilities, which could then support the next steps as illustrated in Figure 9.1. Figure 9.1 depicts the four technologies discussed in this report and how they support various requirements for the development of future autonomous reprogramming capabilities. The USAF can and should make use of these developments to advance toward a future EWIR capability. For this reason, PAF recommends *continuous investment* in enabling technologies, starting now. Though separate in terms of individual development and evolution, the four technologies have several interdependencies for collectively supporting the incremental enhancements of the EWIR process. In other words, these technologies will evolve to support the USAF in several ways and are needed to operationalize benefits resident in each for achieving autonomous reprogramming.

**Figure 9.1. Interdependencies of Key Technologies**


2. CLOUD INTEGRATION & DATA ENGINEERING
Parallel Data Ingestion
Database/ Hybrid Cloud
Data Engineering
4. ONBOARD HIGH-PERFORMANCE COMPUTING
GPU
FPGA
Miniaturization & High-Performance Embedded Processing
Edge Cloud
Legacy Hardware Upgrades
Cognitive MLOps
Analysis & Reprogramming
Containerized OFP
EW Transmit / EA Container Pod
EW Receive / ES Container Pod
...
CNI Container Pod
Cognitive Model Container Pod
Build and Train Models
Evaluate Models
Build Model Containers
Continuous Training
Continuous Integration – Continuous Delivery
1. OPERATIONALIZATION OF COGNITIVE EW
3. FLIGHT PROGRAM SOFTWARE AND CONTAINERIZED MICROSERVICES

We note, too, that beginning investments in the near term will have immediate benefits for the existing EWIR process, even as the USAF proceeds toward the autonomous, onboard reprogramming capability that will be necessary to survive in future denied and disrupted EMS environments. In addition, the advent of adaptive and ultimately cognitive capabilities does not render the current EWIR process unusable. During the transition toward and even with cognitive capabilities, the current EWIR process, organizations, people, and materiel—in some form—will continue to be needed to maintain routine changes that do not require cognitive capabilities to counter an advanced threat operating at the top of its capability. Indeed, as more and more systems become connected and pool processing power and communications bandwidth, it will likely be necessary for systems to *not* operate in cognitive mode as a default in order to reserve these resources for when they are most needed. Furthermore, even if cognitive capabilities were adopted to counter less advanced threats (which would inefficiently utilize resources), the need for foundational intelligence, threat modeling, and testing activities still remains because the cognitive algorithms must be trained and maintained. In other words, we envision the EWIR status quo and the road to a cognitive future coevolving because both are in fact needed and are not mutually exclusive in gaining traction in an increasingly complex EMOE.

On a final note, the changes described in this report—though articulated in the context of reprogramming for EMSO—are 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 about how all players are connected and must pool information between them to outsmart an adversary.

# Appendix A. Research Tasks and Methodology

This appendix provides additional detail about the tasks and methodologies employed in this research project. It also includes a full list of interviews conducted for the project.

At the outset, this work was organized into four tasks, beginning with defining problems with the status quo and associated lessons that were articulated in Chapter Two and identifying potentially promising technologies for overcoming them. The work then compared the foundations required for inflight rapid reprogramming (through adaptive and cognitive EW) with the status quo and summarized some important changes needed to make this shift using a DOTMLPF-P framing. Finally, the project team identified specific areas for improvement, focusing on materiel needs related to software but also considering related policy issues related to organizations and training.

Overall, the project team followed an exploratory mixed methods approach for several corresponding steps in each research phase described in Table A.1. The outcome of research in earlier phases informed the subsequent steps. In this way, the research was highly iterative.

**Table A.1. Research Methodology**

| Phase | Methods |
|---|---|
| Phase 1 | • Document review<br>• Semistructured interviews<br>• Process overview and identification of process impediments<br>• Lessons and DOTMLPF-P needs assessment<br>o Identification of capability needs, technologies, and timelines |
| Phase 2 | • Selection of technology case studies for long-term technology solutions<br>• Vignette development |
| Phase 3 | • Selected technology case studies<br>o Document review<br>o Semistructured interviews<br>o Technology deep dives<br>o Writeup<br>• Mapping interdependencies of technologies<br>• Vignette analysis<br>• Recommendations development |

Phase 1 included several qualitative analysis methods to define the scope and needs of the study for determining the current EWIR processes, issues, and future requirements. This was followed by process mapping, identification of process impediments using the information from the interviews and RAND expertise, followed by DOTMLPF-P framework-based needs assessment and lessons analysis (Chapter Two).

Based on the results of the interviews, status quo lessons identification, and DOTMLPF-P needs assessment, we created a time-based framework to link near-term needs and the long-term vision for speeding up reprogramming and ultimately moving to cognitive EW over a 15-year time horizon. The supporting software, hardware, and intelligence foundations required to develop these capabilities at each of these timelines were identified based on various current and emerging technologies, both in software and hardware, as well as intelligence and data collection, classification, access, and storage requirements. Figure 3.3 summarizes this framework. Another parallel step that was initiated in this phase was the development of an early solution for edge processing of intelligence data (Appendix B).

In Phase 2, we had two parallel approaches: (1) selection of case studies for long-term technology solutions and (2) vignette development for illustrating potential implications of improved reprogramming timelines using the technologies highlighted in this report.

We selected four technologies to focus on as case studies for deeper analysis based on interviews with RAND and external experts:

- cognitive EW
- cloud integration and data engineering
- flight program software and containerized microservices
- onboard HPC.

For each case study, we then identified five major questions:

- How do we define the technology?
- What is the current status of this technology?
- What are its projected near-term EWIR applications?
- What longer-term developments appear likely or possible?
- What are the potential implications for EWIR within each vignette?

Vignette development drew upon observation of relevant real-time planning exercises along with supplemental interviews and the reading of documents for context. More information on the approach is available in Chapter Eight.

Phase 3 involved three different parallel steps:

1. a deeper analysis of each of the four selected technology case studies. Each involved semistructured interviews, site visits, and literature reviews and technology assessments. Chapters Four through Seven summarize the results of these analyses.
2. vignette analysis, to examine how changes to EWIR might enable future operations in these contexts (Chapter Eight)
3. mapping the interdependencies between these technologies to highlight the influence of the development of one technology on the others. This enabled us to map the requirements and risks to achieve the vision (Figure 9.1).

The steps in Phase 3 helped finalize our findings and informed our recommendations (Chapter Nine).

Table A.2 contains a complete documentation of the interviews conducted for this research. We do not include interviewee names per human subjects protection guidelines. Furthermore, we do not directly quote any interviewees in this document, though we do use some specific interviews (as listed below) as citations for some of the information contained in this report.

**Table A.2. Interviews Conducted by Organization**

**USAF**

- Group interview with ACC Intelligence Directorate and Directorate of Air and Space Operations staff members, October 8, 2020
- Interview with 53rd EWG staff member, October 30, 2020
- Interview with 772 Test Squadron staff members, November 4, 2020
- Interview with Air Force Research Laboratory staff member, November 13, 2020
- Interview with HAF, Plans and Requirements Directorate staff members, December 9, 2020
- Interview with United States Air Forces Europe, Operations Directorate staff members, January 19, 2021
- Interview with 36th EWS staff member, January 22, 2021
- Interview with NASIC staff member, January 26, 2021
- Interview with EW expert, United States Air Forces Europe, February 4, 2021
- Interview with Intelligence Directorate staff member, United States Air Forces Europe, March 2, 2021
- Interview with F-16 maintenance staff member, United States Air Forces Europe, March 3, 2021
- Interview with 603rd AOC staff member, March 4, 2021
- Interview with Operations Directorate staff members, United States Air Forces Europe, March 5, 2021
- Interview with 36th EWS staff members, March 5, 2021
- Interview with 453rd EWS staff members, March 24, 2021
- Interview with F-16 System Program Office, March 26, 2021
- Interview with Air Force Research Laboratory staff members, April 20, 2021
- Interview with 453rd EWS staff members, April 30, 2021
- Interview with 36th and 87th EWS staff members, April 30, 2021
- Interview with 59th Test and Evaluation Squadron staff members, April 30, 2021
- Interview with Operations Directorate staff member, Air Combat Command, May 3, 2021
- Interview with F-16 System Program Office, May 3, 2021
- Interview with NASIC staff members, May 24, 2021
- Interview with Air Combat Command Operations Directorate staff members, June 2, 2021
- Interview with Air Force Cloud One staff members, June 28, 2021
- Mission observation at United States Air Forces Europe, June 28–29, 2021
- Interview with U-2 Federal Laboratory staff members, July 30, 2021
- Interview with 36th EWS staff members, August 6, 2021
- Interview with Air Force Platform One staff members, August 10, 2021
- Interview with 453rd EWS staff members, August 11, 2021
- Interview with F-16 System Program Office, August 17, 2021
- Interview with HAF, Intelligence Directorate staff members, September 23, 2021
- Interview with Joint EMSO Core Function Team, April 30, 2021
- Participation in Plan Blue wargame, RAND Corporation, Arlington, Va., August 9–13, 2021

**Other DoD**

- Interview with U.S. Navy Electronic Warfare Data Systems staff member, November 19, 2020
- Interview with Joint EMSO Core Function Team, January 26, 2021
- Interview with DARPA expert, February 8, 2021
- Interview with Joint EMSO Core Function Team, April 30, 2021
- Participation in Plan Blue wargame, RAND Corporation, Arlington, Va., August 9–13, 2021

**Commercial**

- Interview with L3 Communications staff members, October 13, 2020
- Interview with SRC staff member, November 6, 2020
- Interview with SRC staff members, January 26, 2021
- Interview with Lockheed Martin staff members, February 11, 2021
- Interview with Mercury Systems staff members, April 21, 2021
- Interview with Vadum, Inc., and Mercury Systems staff members, May 4, 2021
- Interview with Lockheed Martin staff members, May 17, 2021

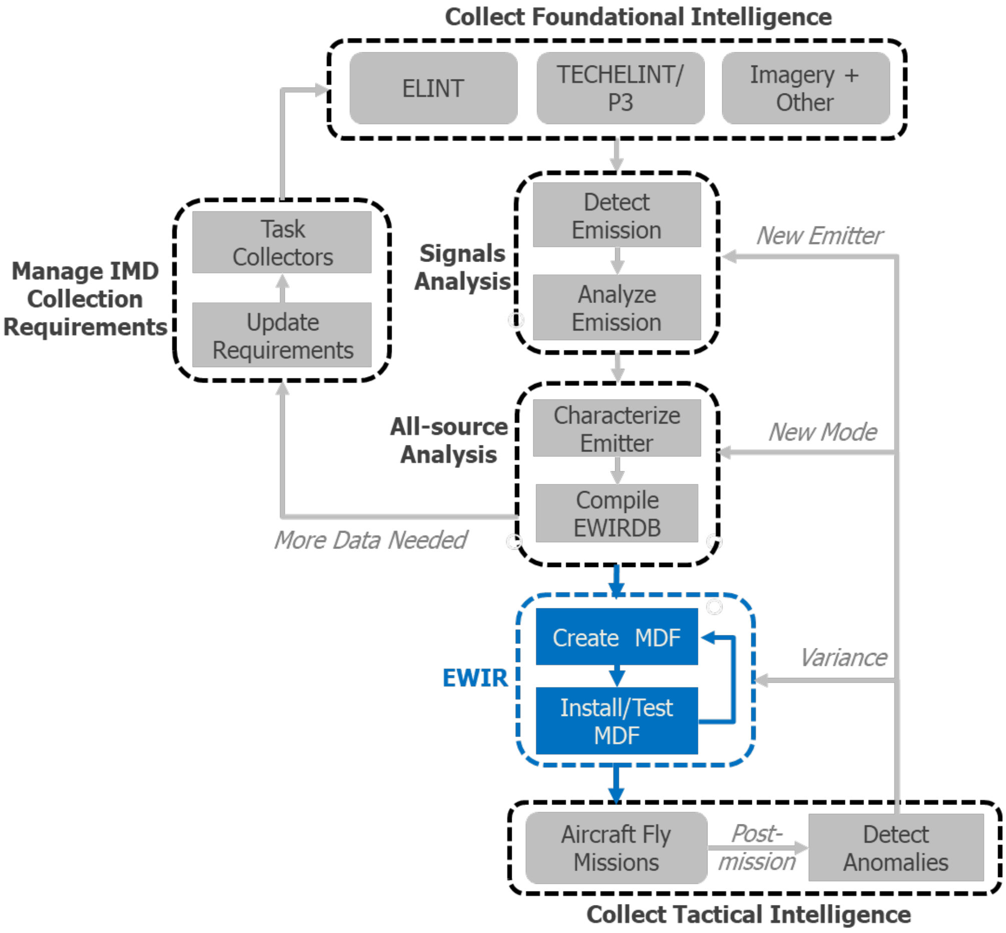
**Other**

- Interview with MITRE Corporation staff members, February 8, 2021
- Interview with Georgia Research Tech Institute staff members, April 29, 2021

# Appendix B. Additional Information on Intelligence Challenges

EWIR is not a standalone process but instead lives within a larger ecosystem of analysis, testing, and development processes involving many Joint and IC partners. The transformational changes to the EWIR process described in this report are supported by—and must support—the related processes shown (loosely) in Figure B.1. In this appendix, we describe investments and workflow improvements in five areas that will be needed in the future for the transformed EWIR process to succeed: *collect foundational intelligence*, *perform signals analysis*, *perform all-source analysis*, *manage IMD collection requirements*, and *collect tactical intelligence.*

**Figure B.1. Larger Ecosystem**



## Collect Foundational Intelligence

To recognize U.S., allied, neutral, commercial, and adversary emitters of all kinds—or to train AI applications to recognize these systems—it is necessary to collect foundational intelligence on their design and capabilities, such as their waveforms, signal parameters, power and sensitivity, vulnerabilities, functions, and associated threats (e.g., SAMs). The increasing sophistication of radars has elevated the importance of TECHELINT[314] for the development of IMD for EWIR. TECHELINT collection is a wide-ranging effort that spans the IC, and other intelligence disciplines also make critical contributions to IMD.

USAF manned airborne collectors are an important part of this effort because they can achieve otherwise difficult-to-attain geometries and persistence against sensitive targets. However, aircraft equipped with exquisite sensing capabilities of this type remain very limited. The USAF lists 17 operational RC-135 V/W Rivet Joint and two RC-135U Combat Sent platforms—the latter being the most capable.[315] These manned aircraft are nearly 60 years old, although key equipment has been upgraded and refreshed over time.

The scarcity of these resources remains a bottleneck to collecting certain foundational intelligence on certain systems. While SDR and related technologies may one day render it impossible to collect meaningful parametric data on certain adversary systems in advance—which would thereby moot the purpose of IMD—the vast majority of emitters are more conventional and are likely to remain so for years to come. Furthermore, the search for unintentional modulations that may allow the USAF to “fingerprint” even such SDR-enabled emitters is more reason to aggressively collect TECHELINT data now.

We also note that, for obvious reasons, collection to support the development of foundational intelligence must often yield to higher-priority collection tasks requiring more urgent analysis. High-demand, low-density collection platforms therefore often “bump” requests for foundational intelligence from the collection deck, if they were admitted at all. While this is unavoidable, it implies that the bottleneck is stiffer than may be commonly thought.

## Signals Analysis

Despite the relative scarcity of airborne collectors, the IC still collects a tremendous amount of TECHELINT data that requires processing and analysis, in part because TECHELINT almost by definition involves collecting orders of magnitude more data—both in quantity and quality—for each signal than a typical EW platform or RWR might collect. Analyzing this data is an effort that spans many intelligence centers. NASIC is the technical manager for processing all airborne TECHELINT in support of EW,[316] and it works with several other intelligence centers, such as

[314] This is also referred to as technical signals intelligence (TECHSIGINT).

[315] This platform collects pattern, power, and polarization information (P3).

[316] “NASIC is the Air Force Technical Manager for Tech ELINT and all processing of Air Force airborne Tech ELINT processing in support of EW. Additionally, they will coordinate with all SPCs and ensure the EWIRDB is updated online with validated threat changes” (AFI 10-703; U.S. Air Force, 2017, p. 29).

the NGIC and the MSIC, to analyze these data.[317] Meanwhile, the "center of gravity" for TECHELINT efforts in general is the NSA, including the related signals analysis tradecraft.[318]

As the USAF moves to improve EWIR processes and tighten the cycle to be more responsive, the ELINT analysis process in general needs to keep pace. The chain of steps in the EWIR process is only as strong as its weakest link; for improvements in throughput later in the process to pay the dividends expected, the earlier parts of the pipeline must also be enhanced. One path to doing so, which will pay dividends in other areas as well, is to automate common signals analysis tasks to make better use of experienced TECHELINT analysts and to allow less experienced analysts to do more.

The process of analyzing an unknown signal may be thought of as applying various decryption schemes to a mystery text until the message is revealed. The tests for simple modulation—such as standard frequency, amplitude, and phase modulation—are easy to apply, and such demodulation techniques have long been automated in commercial radio systems.[319] If the signal does not yield to easy processing, however, one must then test for more complicated families of modulation, such as frequency- and high-order phase-shift schemes in which the waveform jumps and twists across the EM spectrum following a hidden key. To decipher the signal, a series of complicated filters must be applied to test for different families of codes, with many options and variations. Moreover, learning other salient features of the emission, such as geolocating its source, may require complex "what if" analysis of the relative motion between the collecting platform and the unknown emitter.

As the sophistication of radars has increased, the number of potential processing filters that might be brought to bear has grown exponentially as well. Where this proliferation outpaces the development of automated software capabilities, much of the TECHELINT analysis may need to be done manually. Indeed, much of the skill of an experienced TECHELINT analyst involves working with spectral analysis programs that represent different aspects of an unknown signal visually and allow the analyst to manipulate the signal manually, searching for any pattern thus revealed that might hint at the nature of the underlying waveform. As NSA seeks to revitalize its TECHSIGINT capabilities, it is imperative to continue to include more filters and algorithms that will allow the processing programs to recognize advanced waveforms more easily.[320] We note

[317] "Scientific and technical intelligence and other centers (including NASIC, NGIC, NMIC [National Maritime Intelligence Center], MSIC, 453 EWS, and NSA) provide the data to NASIC for inclusion in the database" (USAF, 2019c, p. 58).

[318] "NSA/CSS-Colorado . . . is the enterprise center for overhead technical signals intelligence (TECHSIGINT) collection and processing the hub for management of the global overhead SIGINT mission, is a corporate leader in innovative cryptologic discovery, and is the focal point for ELINT analysis and tradecraft development. [It is] the center-of-gravity for the cryptologic sub-discipline of TECHSIGINT" (NSA, "About NSA/CSS," webpage, 2021).

[319] For example, automobile radio systems have for decades been able to scan very high frequency bands and lock onto frequency modulated (FM) signals, processing them automatically for their audio content in real time.

[320] For example, Kubilay Savci, Gaspare Galati, and Gabriele Pavan, "Low-PAPR Waveforms with Shaped Spectrum for Enhanced Low Probability of Intercept Noise Radars," *Remote Sensing*, Vol. 13, No. 2372, 2021, notes: "Modern [electronic support] systems are capable of generating time–frequency analysis maps apart from

that new algorithms appear regularly in the academic literature and should be gathered for this purpose, as appropriate.[321] Workflow enhancements that enable these filters to run in automated sequence, following the appropriate decision tree, are essential parts of making these algorithms practical.

Finally, we note that the U.S. Government Accountability Office found that DoD has a "shortage of staff with EMS expertise" in general,[322] let alone for a highly skilled subdiscipline such as TECHELINT. While such shortages may remain, the development of new algorithms and the workflow enhancements to support their automation is not only vital to ensure the best use of TECHELINT talent but also will allow forensic analysis of data that currently goes unanalyzed. For example, these algorithms may be used to process RWR returns post-mission, data that may otherwise be tossed aside for lack of skilled analysts capable of performing detailed analysis at the fighter intelligence squadron.

## All-Source Analysis

Despite the difficulties described in the previous sections, the longest pole in the tent in the traditional EWIR cycle is neither the collection nor the analysis of specific emissions, but rather the need for comprehensive, all-source analysis of the emitters that produced them. Building the picture of an emitter not only requires understanding as many waveforms as possible—which often requires analyzing many intercepts—but also modeling the capabilities and limitations of the radar, understanding how it fits into the enemy's electronic order of battle, and understanding with which threats it is associated. This is a difficult intelligence task requiring an experienced hand that may take months or years to fully complete, depending on the uniqueness of the emitter and its sensitivity.

Some parts of this timeline depend on other processes. In particular, as noted in Figure B.1, there may be a loop back to the collection stage, if the accumulated data are deemed insufficient to make the necessary determinations. Clearly, no amount of automation can speed up the processing of data if the data do not yet exist. However, other parts of the all-source analysis process are amenable to workflow enhancements and other improvements. In particular, the art of all-source intelligence involves searching for data in different formats from across the IC: databases of geospatial intelligence to obtain reconnaissance imagery; the Modernized Integrated

traditional spectral analysis methods. . . . Some methods used in time–frequency domain signal analysis are based on: Short Time Fourier Transform (STFT), Wigner-Ville Distribution (WVD), and Choi-Williams Distribution (CWD)."

[321] For example, Jen-Yu Gau, "Analysis of LPI Radar Signals Using the Wigner Distribution," thesis, Monterey, Calif.: Naval Postgraduate School, 2002; F. Taboada, "Detection and Classification of LPI Radar Signals Using Parallel Filter Arrays and Higher Order Statistics," thesis, Monterey, Calif.: Naval Postgraduate School, September 2002; M. Song, "Characterizing Cyclostationary Features of Digital Modulated Signals with Empirical Measurements Using Spectral Correlation Function," thesis, Wright-Patterson Air Force Base, Ohio: Air Force Institute of Technology, November 2009.

[322] U.S. Government Accountability Office, *Electromagnetic Spectrum Operations: DoD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64, December 2020c.

Database (MIDB), and its successor-to-be, Machine-Assisted Analysis Rapid-Repository System (MARS),[323] to obtain order-of-battle information on known adversary systems; and other key repositories of data. Assuring continued access to this data, and compatible machine-to-machine pathways for this data to flow to the all-source analysts who need it for this purpose, remains critical to this process.

When completed, the fruits of the analysis reside in the EWIR database maintained by NASIC. A new version of the EWIR database was created over the past several years to be the next-generation database, with a number of improvements, including a shift away from the old "flat file" format to make a complex relational database with state modeling and the ability to represent a broader array of parameters.[324] However, while more powerful, the complicated format also makes it more difficult for automated tools to pull from it. As a result, improvements to tools that can translate such data into other formats or compare them with sensor intercepts are of greater importance. We emphasize that solving these translation and data cleaning issues now is an important precursor to more-advanced technologies such as cognitive EW, which must be trained on such data.

## Manage IMD Collection Requirements

Collection and re-collection on emitters do not occur in a vacuum but require the partners in the IMD enterprise to agree on priorities and to have internal visibility as to who is working on analyzing which emissions or emitters, which assets have been tasked to collect on what targets, whether the various taskings have been completed successfully, and what was collected. Annual working groups are an important part of this process, as are spreadsheets and databases. As emitters proliferate and requirements grow, this back end of tracking collection requirements must also be managed properly. It is important to remember that IMD processes and the TECHELINT enterprise in general are not self-executing but must instead be actively managed.

## Collect Tactical Intelligence

In addition to the electronic support aircraft previously mentioned, aircraft flying in theater can, in principle at least, also help collect tactical intelligence on adversary emitters that can feed the IMD development process—and the EWIR process—by sharing data from electronic support systems. Unmanned vehicles can collect such data: For example, some variants of the RQ-4 Global Hawk carry SIGINT sensors,[325] and the MQ-9 Reaper is also capable of carrying

[323] For information on MIDB/MARS, see U.S. Government Accountability Office, *Defense Intelligence: Comprehensive Plan Needed to Improve Stakeholder Engagement in the Development of New Military Intelligence System*, GAO-21-57, November 2020b.

[324] It was initially called NGES but now is just EWIRDB (the old system is now commonly called the legacy version). "Next Generation EWIRDB System (NGES) [is a] follow-on database for EWIRDB, incorporating improved relational database scheme, better modeling of signals, and other improvements" (USAF, 2019c).

[325] U.S. Air Force, "RQ-4 Global Hawk," webpage, October 27, 2014.

electronic support systems.[326] Manned platforms flown by other services, such as the Army's Guardrail Common Sensor,[327] also collect such data.

Furthermore, the same RWRs that the EWIR process seeks to reprogram also collect valuable data on signals that they do not recognize or cannot classify with high confidence. Getting this operational reconnaissance data back from the edge to be processed is difficult, but the more data that can be retrieved and stored in this manner, the more data are available to search for new systems or to train advanced cognitive EW algorithms. Currently, there is no requirement in place to ingest these data into a common database in an automated fashion. The infrastructure to do so at scale is also lacking.

One approach is referred to as "crowd-sourcing data," which uses extra hardware on these platforms (and on the ground) to capture and process these data. The 59th Test and Evaluation Squadron has developed the QRIP program to accomplish this.[328] QRIP has the potential to significantly improve the offboarding of data from many USAF aircraft. However, policies and appropriate security infrastructure must be in place to leverage these data, and to do so in a timely fashion. It is also necessary that whatever solution is chosen can capture this data when the ground crew that downloads it has cloud access and also when they do not.

Finally, there is also room for aircrews themselves to support this process: "In addition, EW equipment anomalies reported by aircrew in post mission reports (MISREPs) and/or Joint Spectrum Interference Reports (JSIRs) may also start this process."[329] Ensuring that these MISREPs and the associated debriefing outcomes are available for AI algorithms to peruse could also provide a mine of data.

[326] General Atomics Aeronautical Systems, Inc., "GA-ASI Further Expands MQ-9 Mission Capability: 26th WPS Flies Reaper Defense Electronic Support System; High-Def Recording Supports AI/ML Development," San Diego, April 22, 2021.

[327] U.S. Army, "Guardrail Common Sensor (GRCS)," webpage, PEO Aviation, September 24, 2020.

[328] BusinessWire, "Intelligent Waves Awarded $89 Million Contract for Crowd-Sourced Data Support," October 8, 2019.

[329] AFI 10-703, 2017.

## Abbreviations

| | |
|---|---|
| ACC | Air Combat Command |
| ADC | analog-to-digital converter |
| AFI | Air Force Instruction |
| AI | artificial intelligence |
| AOC | Air and Space Operations Center |
| ASIC | application-specific integrated circuit |
| C2 | command and control |
| C2D2 | Continuous Capability, Development, and Delivery |
| CI/CD | continuous integration, continuous delivery |
| CJTF | Combined Joint Task Force |
| COP | common operating picture |
| CSCI | computer software configuration item |
| DAC | digital-to-analog converter |
| DAF | Department of the Air Force |
| DARPA | Defense Advanced Research Projects Agency |
| DevSecOps | development, security, and operations |
| DoD | U.S. Department of Defense |
| DOTMLPF-P | doctrine, organization, training, materiel, leadership, personnel, facilities, and policies |
| DT&E | developmental testing and evaluation |
| EA | electromagnetic attack |
| EDW | emitter descriptor word |
| ELINT | electronic intelligence |
| EMOE | electromagnetic operating environment |
| EMS | electromagnetic spectrum |
| EMSO | electromagnetic spectrum operations |
| ENOB | effective number of bits |

| | |
|---|---|
| EP | electromagnetic protection |
| ES | electromagnetic support |
| EW | electronic warfare |
| EWG | Electronic Warfare Group |
| EWIR | electronic warfare integrated reprogramming |
| EWIRDB | electronic warfare integrated reprogramming database |
| EWS | Electronic Warfare Squadron |
| FACE | Future Airborne Capabilities Environment |
| FPGA | field-programmable gate array |
| FY | fiscal year |
| GPU | graphics processing unit |
| HAF | Headquarters Air Force |
| HPC | high-performance computing |
| IC | intelligence community |
| IMA | integrated modular avionics |
| IMD | intelligence mission data |
| ISR | intelligence, surveillance, and reconnaissance |
| JADC2 | Joint All Domain Command and Control |
| JEF | Joint Expeditionary Force |
| KM/RAPIDS | Knowledge Management/Rapid Analysis Processing Independent Deployable System |
| LPI | low probability of intercept |
| MARS | Machine-Assisted Analysis Rapid-Repository System |
| MDF | mission data file |
| MIDB | Modernized Integrated Database |
| MISREP | mission report |
| ML | machine learning |
| MOSA | Modular Open Systems Approach |
| MSIC | Missile and Space Intelligence Center |
| NASIC | National Air and Space Intelligence Center |

| | |
|---|---|
| NATO | North Atlantic Treaty Organization |
| NGES | Next-Generation EW Integrated Reprogramming Database System |
| NGIC | National Ground Intelligence Center |
| NN | neural network |
| NSA | National Security Agency |
| OBP | onboard processing |
| OFP | operational flight program |
| OMS | Open Mission Systems |
| OSA | open systems architecture |
| OT&E | operational testing and evaluation |
| PAF | Project AIR FORCE |
| PDW | pulse descriptor word |
| QA | quality assurance |
| QC | quality control |
| QRIP | Quick-Reaction Instrumentation Package |
| RF | radio frequency |
| RTOS | real-time operating system |
| RWR | radar warning receiver |
| SAM | surface-to-air missile |
| SAR | search and rescue |
| SDR | software-defined radar |
| SEAD | suppression of enemy air defenses |
| SIGINT | signals intelligence |
| SME | subject-matter expert |
| SOA | service-oriented architecture |
| SPECTRE | Specialized Electromagnetic Combat Tools and Reprogramming Environment |
| SRC | Syracuse Research Corporation |
| SWaP | size, weight, and power |
| SWW | Spectrum Warfare Wing |

| | |
|---|---|
| T&E | testing and evaluation |
| TECHELINT | technical electronic intelligence |
| TECHSIGINT | technical signals intelligence |
| USAF | U.S. Air Force |
| VIPR | Vigilant Protector |

# References

5th Combat Communications Group, *5 CCG Planners Guide*, May 30, 2018.

36th Electronic Warfare Squadron Mission Briefing, February 5, 2021.

87th Electronic Warfare Squadron Mission Briefing, April 29, 2021.

Adams, Charlotte, "Cognitive Electronic Warfare: Radio Frequency Spectrum Meets Machine Learning: A Look at the Technologies That Will Power the Aircraft of Tomorrow," *Avionics International*, August-September 2018.

AFI 10-703—See U.S. Air Force, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming*, February 22, 2017.

Air Combat Command, *Instruction 99-101: ACC Test and Evaluation*, August 24, 2020.

Air Force Chief Data Office (SAF/CO), *Data Services Reference Architecture*, USAF, March 2019.

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/

Alkire, Brien, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Elena Danescu, William Fry, D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie Riposo, Timothy William James Smith, and Alexander Stephenson, *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, Santa Monica, Calif.: RAND Corporation, RR-1330-AF, 2016. As of November 1, 2021: https://www.rand.org/pubs/research_reports/RR1330.html

Allied Air Command, "US F-15s Complete NATO Air Policing Deployment to Iceland," Ramstein, Germany, August 3, 2021.

Amazon Web Services, "Infrastructure as Code," white paper, July 2017.

Arctic Council, homepage, undated. As of August 27, 2021: https://arctic-council.org/en/

Assistant Secretary of Defense for Research and Engineering, *Technology Readiness Assessment (TRA) Guidance*, Washington, D.C.: U.S. Department of Defense, April 2011.

Avionics International, "Using Containers for Avionics Applications," webinar, Wind River, June 3, 2021. As of August 31, 2021: https://www.bigmarker.com/access-intelligence3/Using-containers-for-avionics-applications/

AWS, "Explore AWS Partner Profiles, Solutions, Case Studies, and Locations," webpage, undated. As of August 27, 2021: https://partners.amazonaws.com/search/partners?facets=Industry%20%3A%20Government%20%3A%20National%20Security%20%26%20Defense&page=1

Azure, “What Is Elastic Computing or Cloud Elasticity?” webpage, undated. As of September 3, 2021:
https://azure.microsoft.com/en-us/overview/what-is-elastic-computing/

Bakker, Paul, and Bert Ertman, *Building Modular Cloud Apps with OSGi*, 1st ed., O’Reilly Media, 2013.

Baptista, Gabriel, and Francesco Abbruzzese, “Microservices and the Evolution of the Concept of Modules,” *Hands-On Software Architecture with C# 8 and .NET Core 3*, Packt Publishing, 2019.

Beckers, Jacques M., “Adaptive Optics for Astronomy: Principles, Performance, and Applications,” *Annual Review of Astronomy and Astrophysics*, Vol. 31, 1993, pp. 13–62.

Ben-David, Arie, and Eibe Frank, “Accuracy of Machine Learning Models Versus ‘Hand Crafted’ Expert Systems—A Credit Scoring Case Study,” *Expert Systems with Applications*, Vol. 31, No. 3, Part 1, April 2009, pp. 5264–5271.

Bond, Robert, “Air Force Evolution to Open Avionics—HPEC 2010 Workshop,” presentation, September 2010.

Brading, Thomas, “First Multi-Domain Task Force Plans to Be Centerpiece of Army Modernization,” *Army News Service*, February 1, 2021.

Britannica, “Personal Computer,” webpage, May 21, 2020. As of September 3, 2021:
https://www.britannica.com/technology/personal-computer

Brown, Michael J., Robert D. Fass, and Jonathan Ritschel, "A Case for Open Mission Systems in DOD Aircraft Avionics," *Air and Space Power Journal*, Vol. 33, No. 4, Winter 2019.

Browne, Jack, “Digital Techniques Train Cognitive EW Systems,” *Microwaves and RF,* August 12, 2020.

Bruce, James B., Sina Beaghley, and W. George Jameson, *Secrecy in U.S. National Security: Why a Paradigm Shift Is Needed*, Santa Monica, Calif.: RAND Corporation, PE-305-OSD, 2018. As of September 1, 2022:
https://www.rand.org/pubs/perspectives/PE305.html

Buchanan, Ian, “CALMS Framework”, webpage, undated. As of December 1, 2021:
https://www.atlassian.com/devops/frameworks/calms-framework

Bukhary, Ikhwan Ismail, Ehsan Mostajeran Goortani, Mohd Bazli Ab Karim, Wong Ming Tat, Sharipah Setapa, Jing Yuan Luke, and Ong Hong Hoe, “Evaluation of Docker as Edge Computing Platform,” *IEEE Conference on Open Systems*, 2015.

BusinessWire, “Intelligent Waves Awarded $89 Million Contract for Crowd-Sourced Data Support,” October 8, 2019.

Casey, John G., "Cognitive Electronic Warfare: A Move Towards EMS Maneuver Warfare," *Over the Horizon*, July 3, 2020.

Chairman of the Joint Chiefs of Staff, *Joint Lessons Learned Program*, Manual 3150.25B, October 12, 2018.

Chan, Mitch, *Applying a Service-Oriented Architecture to Operational Flight Program Development*, 309 Software Maintenance Group, Hill Air Force Base, Utah, 2007.

Chen, Ching-Han, and Chao-Tsu Liu, "A 3.5-Tier Container-Based Edge Computing Architecture," *Computers and Electrical Engineering*, Vol. 93, 2021.

CM, Ananda, Sabitha Nair, and Mainak Goshjara, "ARINC 653 API and Its Application—An Insight into Avionics System Case Study," *Defense Science Journal*, Vol. 63, No. 2, March 2013, pp. 223–229.

Cook, Cynthia R., David Luckey, Bradley Knopp, Yuliya Shokh, Karen M. Sudkamp, Don Casler, Yousuf Abdelfatah, and Hilary Reininger, *Improving Intelligence Support to the Future Warfighter: Acquisition for the Contested Environment*, Santa Monica, Calif.: RAND Corporation, RR-A537-1, 2021. As of November 4, 2021:
https://www.rand.org/pubs/research_reports/RRA537-1.html

Crook, Chris, and Chip Downing, *System Architectures, MOSA and the FACE Technical Standard* 2020, The Open Group, December 2020. As of August 25, 2021:
https://www.youtube.com/watch?v=J7DD4yBCEL8

Curtis E. LeMay Center for Doctrine Development and Education, *Annex 2-0 Global Integrated Intelligence, Surveillance & Reconnaissance Operations*, undated.

Curtis E. LeMay Center for Doctrine Development and Education, "Electromagnetic Spectrum Support Activities," Air Force Doctrine Publication 3-51, Electromagnetic Warfare and Electromagnetic Spectrum Operations, last updated July 30, 2019.

DARPA—*See* Defense Advanced Research Projects Agency.

Defense Acquisition University, "DOTmLPF-P Analysis," webpage, undated. As of November 29, 2021:
https://www.dau.edu/acquipedia/pages/ArticleContent.aspx?itemid=457

Defense Advanced Research Projects Agency, "DARPA Quantum Hardware Request for Information (RFI)," Notice ID DARPA-SN-20-21, December 24, 2019. As of September 3, 2021:
https://sam.gov/opp/01a65dd69a8444b2ba0b9f09bfd85981/view?keywords=&sort=-modifiedDate&index=&is_active=true&page=1&organization_id=300000412

Debatty, Thibault, "Software Defined RADAR a State of the Art," *2nd International Workshop on Cognitive Information Processing*, 2010, pp. 253–257.

De Palo, Francesco, Gaspare Galati, Gabriele Pavan, Christoph Wasserzier, and Kubilay Savci, "Introduction to Noise Radar and Its Waveforms," *Sensors*, Vol. 20, No. 18, Article 5187, 2020.

Department of Defense, *Operation of the Defense Acquisition System*, Instruction Number 5000.02, January 2015.

Department of the Air Force, *Department of Defense Handbook: Airworthiness Certification Criteria*, Military Handbook MIL-HDBK-516C, December 2014.

Department of the Air Force Headquarters, Air Force Life Cycle Management Center (AFMC) Engineering Directorate, *Airworthiness Circular—Verification Expectations for Select Section 15 Criteria*, Wright-Patterson Air Force Base, March 2017.

Deputy Under Secretary of Defense for Science and Technology, *Technology Readiness Assessment (TRA) Deskbook*, Washington, D.C.: U.S. Department of Defense, May 2005.

DoD—*See* U.S. Department of Defense.

Elgazar, Ali, and Khaled. A. Harras, "Enabling Seamless Container Migration in Edge Platforms," *CHANTS: Challenged Networks*, Los Cabos, Mexico, October 25, 2019.

Ellis, Douglas, "Linking Continents Through Refueling," *Aerotech News*, November 10, 2015.

European Radio Map, "European Radio Map: Central Europe," webpage, undated. As of August 30, 2021:
https://radiomap.eu/map

Eveleens, René L.C., *Open Systems Integrated Modular Avionics—The Real Thing*, National Aerospace Laboratory NLR, Amsterdam, North Atlantic Treaty Organization Research and Technology Organisation, RTO-EN-SCI-176, 2006.

Everstine, Brian W., "USAFE's ABMS On-Ramp Included Partner Nations, Base Defense Scenario," *Air Force Magazine*, March 1, 2021.

F-16 System Program Office, "F-16 Roadmap to ABMS," presentation, undated.

F-16 System Program Office, "F-16 Receives In-Flight Software Update During Recent Flight Test," Air Force Life Cycle Management Center, July 31, 2021.

Firesmith, Donald, "Multicore Processing, Virtualization, and Containerization: Similarities, Differences, Challenges, and Recommendations," presentation, Software Engineering Institute, Carnegie Mellon University, 2019.

Fleming, Cody, and Nancy Leveson, "Improving Hazard Analysis and Certification of Integrated Modular Avionics," *Journal of Aerospace Information Systems*, Vol. 11, No. 6, 2014, pp. 397–411.

FlightAware, "FlightAware's Data Sources," webpage, undated. As of August 18, 2021:
https://flightaware.com/about/datasources/

Fortunato, Evan, "Stitches: SoS Technology Integration Tool Chain for Heterogeneous Electronic Systems," Apogee Research, Abstract #18869, undated. As of December 2, 2021:
https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2016/systems/18869_Fortunato_SoSITE_STITCHES_Overview_Long_9Sep2016_.pdf

Francis, Tina, and Madhiajagan Muthiya, "A Comparison of Execution Mechanisms: Fog and Edge Cloud Computing," EECSI 2017, Yogyakarta, Indonesia, September 2017.

Garrett, Chris, "Open System Standards and Agile Acquisition," Air Force Life Cycle Management Center, 2018.

Gau, Jen-Yu, "Analysis of LPI Radar Signals Using the Wigner Distribution," thesis, Monterey, Calif.: Naval Postgraduate School, 2002.

General Atomics Aeronautical Systems, Inc., "GA-ASI Further Expands MQ-9 Mission Capability: 26th WPS Flies Reaper Defense Electronic Support System; High-Def Recording Supports AI/ML Development," San Diego, April 22, 2021.

Gilmore, Michael J., “Key Issues with Airborne Electronic Attack (AEA) Test and Evaluation,” Director, Operational Test and Evaluation, presentation to the 2011 Association of Old Crows, AEA Symposium, 2011. As of September 1, 2021: https://www.dote.osd.mil/Portals/97/pub/presentations/2011/AOC%20AEA%20Symposium.pdf?ver=2019-09-03-104633-353

Greco, Maria S., Fulvio Gini, Pietro Stinco, and Kristine Bell, “Cognitive Radars: On the Road to Reality: Progress Thus Far and Possibilities for the Future,” *IEEE Signal Processing Magazine*, Vol. 35, No. 4, July 2018, pp. 112–125.

Griffiths, Hugh, and Chris J. Baker, “Towards the Intelligent Adaptive Radar Network,” *2013 IEEE Radar Conference (RadarCon13)*, 2013, pp. 1–5.

Guertin, Nickolas, and Douglas C. Schmidt, “Emerging Opportunities in Modularity and Open Systems Architectures,” Software Engineering Institute, October 15, 2018.

Hadley, Greg, “Air Force Leadership Needs to ‘Walk the Walk’ in Baking Security into Cyber, Software Boss Says,” *Air Force Magazine*, August 12, 2021.

Harms, Brent N., *Data Fusion as Software Solution for 2018 OIR Lessons Learned and JADC2*, Air War College, Air University, March 27, 2020.

Haigh, Karen, and Julia Andrusenko, *Cognitive Electronic Warfare: An Artificial Intelligence Approach*, Boston, Mass.: Artech House, 2021.

Haykin, Simon, “Cognitive Radar: A Way of the Future,” *IEEE Signal Processing Magazine*, Vol. 23, No. 1, January 2006, pp. 30–40.

Helfrich, Emma, “DO-178 Continues to Adapt to Emerging Digital Technologies,” *Military Embedded Systems*, March 2021.

Hersman, Rebecca, and Eric Brewer, “Deep Dive Debrief: Strategic Stability and Competition in the Arctic,” *CSIS Briefs*, January 6, 2021.

Hilderman, Vance, "DO-178B and DO-254: A Unified Aerospace-Field Theory?" *Military Embedded Systems*, February 2009.

Humpert, Malte, “Arctic Shipping Routes,” Arctic Institute, July 2016. As of December 14, 2022: https://www.thearcticinstitute.org/wp-content/uploads/2016/07/Arctic-Shipping-Routes-Map-legend-1.png

IBM Cloud Education, “Containerization,” webpage, May 15, 2019. As of November 27, 2020: https://www.ibm.com/uk-en/cloud/learn/containerization

Intel, “FPGA vs. GPU for Deep Learning,” webpage, undated. As of May 12, 2022: https://www.intel.com/content/www/us/en/artificial-intelligence/programmable/fpga-gpu.html

Kaza, Tapasvi, “MLOps Lifecycle,” *VivoSoft*, blog, updated December 6, 2020. As of August 31, 2021: https://www.vivsoft.io/post/mlops

Keller, John, "SOSA Open-Systems Standard Gains Momentum for Embedded Computing; Snapshot 3 by April, 1.0 Later This Year," *Military and Aerospace Electronics*, February 3, 2020.

Keller, John, “Air Force Asks Industry for Artificial Intelligence (AI) Cognitive Electronic Warfare (EW) for F-15 Jets,” *Military & Aerospace Electronics*, March 15, 2021.

Kellett, Daniel, Dmitriy Garmatyuk, Saba Mudaliar, Nahlah Condict, and Isaiah Qualls, “Random Sequence Encoded Waveforms for Covert Asynchronous Communications and Radar,” *The Institution of Engineering and Technology Radar, Sonar & Navigation*, Vol. 13, No. 10, 2019, pp. 1713–1720.

Khamis, Alaa, “The 7-Step Procedure of Machine Learning," *Towards Data Science*, March 30, 2019.

Kirk, Richard, “MOSA/SOSA: A New Dawn for Military Computing,” *Abaco Systems*, June 12, 2019.

Knopp, Bradley, David Luckey, and Yuliya Shokh, *Documenting Intelligence Mission-Data Production Requirements: How the U.S. Department of Defense Can Improve Efficiency and Effectiveness by Streamlining the Production Requirement Process*, Santa Monica, Calif.: RAND Corporation, RR-A241-1, 2021. As of November 1, 2021:
https://www.rand.org/pubs/research_reports/RRA241-1.html

Kocić, J., N. Jovičić and V. Drndarević, “Sensors and Sensor Fusion in Autonomous Vehicles,” 2018 26th Telecommunications Forum (TELFOR), 2018, pp. 420–425.

Kovach, Nicholas, Benjamin Natarian, and Kenneth Littlejohn, “The Rise of Open Architectures in the U.S. Department of Defense,” Proc. SPIE 11753, *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2021*, April 2021.

Kubeflow, homepage, undated. As of August 31, 2021:
https://www.kubeflow.org

Kubernetes, “Production-Grade Container Orchestration,” webpage, undated. As of August 25, 2021:
https://kubernetes.io

Langley, Lawrence E., “Specific Emitter Identification (SEI) and Classical Parameter Fusion Technology,” *Proceedings of WESCON ’93*, 1993, pp. 377–381.

Larson, Keith, “Containerization Meets Process Automation,” *Control Global*, June 2020.

Leopold, George, “NRO Jumps on Open Source Bandwagon,” *Defense Systems*, June 26, 2015.

Lim, Sungshin, Jongsoo Hyun, Sang Myun Shin, In Gyu Kim, Byung Moon Hwang, and Hyuk-Chul Kwon, "A Feasibility Study for ARINC 653 Based Operational Flight Program Development," IEEE/AIAA 31st Digital Avionics Systems Conference, 2012, pp. 6C2-1–6C2-7.

Liu, Yu, Dapeng Lan, Zhibo Pang, Magnus Karlsson, and Shaofang Gong, “Performance Evaluation of Containerization in Edge-Cloud Computing Stacks for Industrial Applications: A Client Perspective,” *IEEE Open Journal of the Industrial Electronics Society*, Vol. 2, 2021, pp. 153–168.

Mankins, John C., “Technology Readiness Assessments: A Retrospective,” *Acta Astronautica*, Vol. 65, 2009, pp. 1216–1223.

McDowell, Rachel, *Containers Provide Access to Deep Learning Frameworks*, Oak Ridge National Laboratory, 2017.

Menthe, Lance, Dahlia Anne Goldfeld, Abbie Tingstad, Sherrill Lingel, Edward Geist, Donald Brunk, Amanda Wicker, Sarah Soliman, Balys Gintautas, Anne Stickells, and Amado Cordova, *Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 1, Findings and Recommendations*, Santa Monica, Calif.: RAND Corporation, RR-A341-1, 2021a. As of September 6, 2022:
https://www.rand.org/pubs/research_reports/RRA341-1.html

Menthe, Lance, Dahlia Anne Goldfeld, Abbie Tingstad, Sherrill Lingel, Edward Geist, Donald Brunk, Amanda Wicker, Sarah Soliman, Balys Gintautas, Anne Stickells, and Amado Cordova, *Technology Innovation and the Future of Air Force Intelligence Analysis: Volume 2, Technical Supporting Analysis*, Santa Monica, Calif.: RAND Corporation, RR-A341-2, 2021b. As of September 6, 2022:
https://www.rand.org/pubs/research_reports/RRA341-2.html

Metcalf, Justin, Shannon D. Blunt, and Braham Himed, “A Machine Learning Approach to Cognitive Radar Detection,” *Proceedings of the 2015 IEEE Radar Conference*, 2015, pp. 1405–1411.

Minsky, Marvin, ed., *Semantic Information Processing*, Cambridge, Mass.: MIT Press, 1968.

Mitola, Joseph, “Software Radios: Survey, Critical Evaluation and Future Directions,” *Proceedings of NTC-92: National Telesystems Conference*, 1992, pp. 13–23.

Moir, Ian, and Allan Seabridge, *Military Avionics Systems*, Wiley, 2006.

MSV, Janakiram, “Google Just Made Machine Learning More Accessible and Portable with Containers,” *Forbes*, July 1, 2019.

National Security Agency, “About NSA/CSS,” webpage, 2021. As of August 19, 2021:
https://www.nsa.gov/about/cryptologic-centers/colorado/

Navy SBIR, “Future Airborne Capability Environment (FACE) Compliant ALE-47 Operational Flight Program Software Application,” webpage, January 2018. As of November 28, 2022:
https://www.navysbir.com/n18_1/N181-024.htm

Neale, B. T., “Chain Home—The First Operational Radar,” *GEC Journal of Research*, Vol. 3, No. 2, 1985, pp. 73–83.

Neese, Richard E., Scott A. Brantley, and Marc J. Pitarys, “Partitioned Software Support for Modular Embedded Computer Software,” *Proceedings of the IEEE 1991 National Aerospace and Electronics Conference NAECON 1991*, Vol. 12, 1991, pp. 709–716.

North Atlantic Treaty Organization Research and Technology Organisation, *Electronic Warfare Test and Evaluation*, AC/323(SCI-203)TP/471, RTO AGARDograph 300 Flight Test Technique Series, Vol. 28, 2012.

NSA—*See* National Security Agency.

NVIDIA, "NVIDIA Tensor Cores: Unprecedented Acceleration for HPC and AI," webpage, undated. As of September 3, 2021:
https://www.nvidia.com/en-us/data-center/tensor-cores

Office of the Under Secretary of Defense for Acquisition and Sustainment, *Report to Congress on FY20 NDAA Section 862(b)(1)(B) Software Development and Software Acquisition Training and Management Programs*, January 2021.

Office of the Under Secretary of Defense for Research and Engineering, "DoD Launches Center of Excellence in Artificial Intelligence and Machine Learning at Howard University," January 28, 2021.

Osborn, Kris, "Air Force Operationalizes New Cyber Security Plans," *Defense Systems*, June 2017.

Paxson, E. W., *Detection by Airborne Intercept Radar*, Santa Monica, Calif.: RAND Corporation, RM-256, 1949.

Performance, "JETS, Virtualization for Embedded Software," white paper, 2019.

Pickett, Jill, "586 FLTS Testing Software Management Program for Aircraft," *Arnold Engineering Development Complex Public Affairs*, September 18, 2020.

Pomerleau, Mark, "What Is the Difference Between Adaptive and Cognitive Electronic Warfare?" *C4ISRNet*, December 16, 2016.

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

Pomerleau, Mark, "DoD Unveils Electromagnetic Spectrum Superiority Strategy," *C4ISRNet*, October 29, 2020b.

Radin, Andrew, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long, *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition—Appendixes*, Santa Monica, Calif.: RAND Corporation, RR-3099-A, 2019. As of August 31, 2021:
https://www.rand.org/pubs/research_reports/RR3099.html

Ramey, Charles, "Global Strike Airmen Support Largest NATO Exercise in 20 Years," Air Force Global Strike Command Public Affairs, November 6, 2015.

Raytheon Technologies, "AN/ALR-69A[V] Radar Warning Receiver," webpage, undated. As of August 22, 2021:
https://www.raytheon.com/capabilities/products/alr69

Rigault, François, "Astronomical Adaptive Optics," *Publications of the Astronomical Society of the Pacific*, Vol. 127, No. 958, 2015, pp. 1197–1203.

Rumer, Eugene, Richard Sokolsky, and Paul Stronski, "Russia in the Arctic—A Critical Examination," *The Return of Global Russia*, Carnegie Endowment for International Peace, March 2021.

Samolej, Slawomir, "ARINC Specification 653 Based Real-Time Software Engineering," *Informatica*, Vol. 5, No. 1, 2011, pp. 39–49.

Satyanarayanan, Mahadev, "The Emergence of Edge Computing," *Computer*, Vol. 50, No. 1, January 2017, pp. 30–39.

Satyanarayanan, Mahadev, Nathan Beckmann, Grace A. Lewis, and Brandon Lucia, “The Role of Edge Offload for Hardware-Accelerated Mobile Devices,” HotMobile ’21, February 2021, pp. 22–29.

Satyanarayanan, Mahadev, Wei Gao, and Brandon Lucia, “The Computing Landscape of the 21st Century,” *Ideas of the Future*, HotMobile ’19, Santa Cruz, Calif., February 2019, pp. 45–50.

Savci, Kubilay, Gaspare Galati, and Gabriele Pavan, “Low-PAPR Waveforms with Shaped Spectrum for Enhanced Low Probability of Intercept Noise Radars,” *Remote Sensing*, Vol. 13, No. 2372, 2021.

Savci, Kubilay, Andrew G. Stove, Francesco De Palo, Ahmet Yasin Erdogan, Gaspare Galati, Konstantin A. Lukin, Sergii Lukin, Paulo Marques, Gabriele Pavan, and Christoph Wasserzier, et al. “Noise Radar—Overview and Recent Developments,” *IEEE Aerospace and Electronic Systems Magazine*, Vol. 35, No. 9, September 1, 2020, pp. 8–20.

Schmidhuber, Jürgen, “Deep Learning in Neural Networks: An Overview,” *Neural Networks*, Vol. 61, January 2015, pp. 85–118.

Schleher, D. C., “LPI Radar: Fact or Fiction,” *IEEE Aerospace and Electronic Systems Magazine*, Vol. 21, No. 5, May 2006, pp. 3–6.

Schnelle, H. R., H. O. Sees, and D. P. Floyd, "Integration of the AN/ALQ-131(V) Electronic Countermeasures Pod on Tactical Aircraft Using a MIL-STD-1553B Interface," *Proceedings of National Aerospace and Electronics Conference (NAECON ’94)*, Vol. 2, 1994, pp. 1150–1157.

Seligman, Lara, “What F-35 Can Learn From F-22 Upgrade Hiccups,” *Aviation Week and Space Technology*, March 28, 2018.

Shiloh, Kenya, “U.S. Solidifies NATO, Allied Partnership at Trident Juncture 2015,” 52nd Fighter Wing Public Affairs, U.S. Air Force, October 30, 2015.

Shlapak, David A., and Michael Johnson, *Reinforcing Deterrence on NATO’s Eastern Flank: Wargaming the Defense of the Baltics*, Santa Monica, Calif.: RAND Corporation, RR-1253-A, 2016. As of November 12, 2022: https://www.rand.org/pubs/research_reports/RR1253.html

Sides, Rusty, “DevSecOps and Security Automation—Making Application Security a Part of Development,” webpage, May 2021. As of November 12, 2021: https://govdevsecopshub.com/2021/05/13/making-application-security-a-part-of-development/#.Yatd1C-cZN0

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.

Simone, Luidi De, and Giovanni Mazzeo, "Isolating Real-Time Safety-Critical Embedded Systems via SGX-Based Lightweight Virtualization," *2019 IEEE International Symposium on Software Reliability Engineering Workshops*, 2019, pp. 308–313.

Song, M., “Characterizing Cyclostationary Features of Digital Modulated Signals with Empirical Measurements Using Spectral Correlation Function,” thesis, Wright-Patterson Air Force Base, Ohio: Air Force Institute of Technology, November 2009.

SRC, Inc., “Electronic Warfare Intelligence Production & Programming,” webpage, undated. As of August 27, 2021: https://www.srcinc.com/services/intel-analysis-and-production/ew-intel-production-and-reprogramming.html

Taboada, F., “Detection and Classification of LPI Radar Signals Using Parallel Filter Arrays and Higher Order Statistics,” thesis, Monterey, Calif.: Naval Postgraduate School, September 2002.

Tarr, Peri, and Stanley M. Sutton, Jr., “N Degrees of Separation: Multi-Dimensional Separation of Concerns,” *ICSE ’99 Los Angeles, CA*, 1999.

Taylor, Twain, “Top 4 Open Source Tools for Observability of Containers and Microservices,” webpage, May 2020. As of November 20, 2021: https://www.conjur.org/blog/top-4-open-source-tools-for-observability-of-containers-and-microservices/

Tedesso, Thomas W., and Ric Romero, “Code Shift Keying Based Joint Radar and Communications for EMCON Applications,” *Digital Signal Processing*, Vol. 80, September 2018, pp. 48–56.

Terma, “Electronic Warfare Management Systems,” webpage, undated. As of August 31, 2021: https://www.terma.com/markets/air/electronic-warfare/selfprotection/

Thales Group, “A War to Win the Airwaves—The History of UK Electronic Warfare,” September 27, 2020.

Tingstad, Abbie, Dahlia Anne Goldfeld, Lance Menthe, Robert A. Guffey, Zachary Haldeman, Krista Langeland, Amado Cordova, Elizabeth M. Waina, and Balys Gintautas, *Assessing the Value of Intelligence Collected by U.S. Air Force Airborne Intelligence, Surveillance, and Reconnaissance Platforms*, Santa Monica, Calif.: RAND Corporation, RR-2742-AF, 2021. As of August 25, 2022: https://www.rand.org/pubs/research_reports/RR2742.html

Tingstad, Abbie, Padmaja Vedula, Robert A. Guffey, Karishma R. Mehta, Lance Menthe, and Jonathan Roberts, *Outsmarting Agile Adversaries in the Electromagnetic Spectrum: Executive Summary*, Santa Monica, Calif.: RAND Corporation, RR-A981-2, 2023. As of January 19, 2023: https://www.rand.org/pubs/research_reports/RRA981-2.html

Tokar, Joyce L., “A Comparison of Avionics Open System Architectures,” ACM SIGAda, *Ada Letters*, Vol. 36, No. 2, December 2016, pp. 22–26.

Trimble, Steve, “House Panel Backs Airborne Electronic Warfare Upgrades,” *Aviation Week Intelligence Network*, July 28, 2021.

Tyagi, Harshit, “What Is MLOps—Everything You Must Know to Get Started,” *Towards Data Science*, March 25, 2021.

United Nations Convention on the Law of the Sea, December 10, 1982. As of August 27, 2021: https://www.un.org/Depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm

USAF—*See* U.S. Air Force.

U.S. Air Force, *Weapon Systems Software Management Guidebook*, 2008.

U.S. Air Force, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming*, *Aviano Supplement*, August 20, 2013. As of December 1, 2021: https://static.e-publishing.af.mil/production/1/avianoab/publication/avianoabi10-703/avianoabi10-703.pdf

U.S. Air Force, "RQ-4 Global Hawk," webpage, October 27, 2014. As of August 20, 2021: https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/

U.S. Air Force, *Air Force Instruction 63-131, Modification Management*, 2015.

U.S. Air Force, *Air Force Instruction 10-703: Electronic Warfare Integrated Reprogramming: Ellsworth Supplement,* October 19, 2010, Supplement January 5, 2016. As of December 1, 2021: https://static.e-publishing.af.mil/production/1/ellsworthafb/publication/afi10-703_ellsworthafbsup/afi_0-703_ellsworthafbsup.pdf

U.S. Air Force, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming*, February 22, 2017.

U.S. Air Force, *The United States Air Force Artificial Intelligence Annex to The Department of Defense Artificial Intelligence Strategy*, 2019a.

U.S. Air Force, *Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*, April 2019b.

U.S. Air Force, *Air Force Instruction 10-703: Electronic Warfare (EW) Integrated Reprogramming: Beale Supplement*, April 3, 2019c. As of August 12, 2021: https://static.e-publishing.af.mil/production/1/bealeafb/publication/afi10-703_bealeafbsup_i/afi10-703_bealeafbsup_i.pdf

U.S. Air Force, *Air Force Doctrine Publication (AFDP) 3-51: Electromagnetic Spectrum Support Activities*, July 30, 2019d. As of August 27, 2021: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-51/3-51-D08-EW-EMS-Support.pdf

U.S. Air Force, *Air Force Doctrine Publication (AFDP) 3-51: Electromagnetic Warfare and Electromagnetic Spectrum Operations*, July 30, 2019e. 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, *Arctic Strategy*, July 21, 2020a. As of August 27, 2021: https://www.af.mil/Portals/1/documents/2020SAF/July/ArcticStrategy.pdf

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

U.S. Air Force, "U-2 Federal Lab Achieves Flight with Kubernetes," October 7, 2020c.

U.S. Air Force Chief Software Office, "Department of the Air Force Software Ecosystem," webpage, undated-a. As of August 27, 2021: https://software.af.mil/software-factories/

U.S. Air Force Chief Software Office, "Platform One Products and Services: Customer DevSecOps Platform (DSOP)," webpage, undated-b. As of August 30, 2021: https://software.af.mil/dsop/services/

U.S. Air Force, Det 8, ACC TRSS, "Electronic Warfare Fundamentals," Las Vegas, Nev.: Nellis Air Force Base, 2000.

U.S. Air Force, Headquarters Air Force Materiel Command, "Memorandum for F16SG/PM—F-16 M-Series Core Operational Flight Programs (OFPs) SORAP (02-043b)," October 2005.

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

U.S. Air Force, Office of the Chief Software Officer, "Software Ecosystem Innovation Hubs—One Platform," webpage, undated-b. As of December 2, 2021: https://software.af.mil/team/platformone/

U.S. Air Force Life Cycle Management Center, "Open Mission Systems in a Nutshell," undated.

U.S. Army, "Guardrail Common Sensor (GRCS)," webpage, PEO Aviation, September 24, 2020. As of August 20, 2021: https://www.army.mil/article/239338/guardrail_common_sensor_grcs

U.S. Code, Title 10, Armed Forces, 1956.

U.S. Code, Title 50, War and National Defense, 1947.

U.S. Department of Defense, "Platform One Software Factory," undated.

U.S. Department of Defense, *DoD Digital Modernization Strategy*, July 12, 2019.

U.S. Department of Defense, "Data Strategy, Unleashing Data to Advance the National Defense Strategy," September 30, 2020a.

U.S. Department of Defense, *Electromagnetic Spectrum Superiority Strategy*, October 2020a.

U.S. Department of Defense, *DevSecOps Fundamentals Playbook*, Version 2.0, March 2021a.

U.S. Department of Defense, "DoD Enterprise DevSecOps Reference Design: CNCF Kubernetes," Version 2.0, March 2021b. As of August 30, 2021: https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOpsReferenceDesign.pdf

U.S. Department of Defense, "Future of the Joint Enterprise Defense Infrastructure Cloud Contract," July 6, 2021c.

U.S. Department of Defense, Chief Information Officer, *Outside the Continental United States (OCONUS) Cloud Strategy*, April 2021.

U.S. Department of Defense, Deputy Director for Engineering, *Modular Open Systems Approach (MOSA) Reference Frameworks in Defense Acquisition Programs*, May 2020.

U.S. Department of Defense, Director, Operational Test and Evaluation*, FY 2016 Annual Report F-22A*, August 2016.

U.S. Department of Defense, Director, Operational Test and Evaluation, *FY 2019 Annual Report*, December 2019.

U.S. Government Accountability Office, *Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects*, GAO-20-48G, January 2020a.

U.S. Government Accountability Office, *Defense Intelligence: Comprehensive Plan Needed to Improve Stakeholder Engagement in the Development of New Military Intelligence System*, GAO-21-57, November 2020b.

U.S. Government Accountability Office, *Electromagnetic Spectrum Operations: DoD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64, December 2020c.

U.S. Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations*, Joint Publication 3-85, Washington, D.C., May 22, 2020.

Waldron, Greg, "USAF Demonstrates Ability to Update F-16 EW Software in Flight," *FlightGlobal*, August 3, 2021.

Watkins, Christopher B., and Randy Walter, "Transitioning from Federated Avionics Architectures to Integrated Modular Avionics," *IEEE/AIAA 26th Digital Avionics Systems Conference*, 2007, pp. 2.A.1-1–2.A.1-10.

Wilson, J. R., “Adaptive and Bistatic Electronic Warfare,” *Military & Aerospace Electronics*, February 1, 2018.

Wind River, “Board Support Packages (BSPs),” webpage, undated. As of August 31, 2021: https://www.windriver.com/products/board-support-packages

Xiong, Yung, Yulin Sun, Li Xing, and Ying Huang, “Extend Cloud to Edge with KubeEdge,” *2018 IEEE/ACM Symposium on Edge Computing (SEC)*, October 25–27, 2018. As of August 27, 2021:
https://ieeexplore.ieee.org/abstract/document/8567693

Yasar, Hasan, “Expanding DevSecOps to Embedded Systems; Is It Possible?” presentation, Software Engineering Institute, Carnegie Mellon University, 2020.

Youssef, Hanan, “Compute Engine Explained: Choosing the Right Machine Family and Type,” Google Cloud blog post, July 9, 2020. As of August 27, 2021:
https://cloud.google.com/blog/products/compute/choose-the-right-google-compute-engine-machine-type-for-you

RAND 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.

$49.95

ISBN-10 1-9774-1057-X
ISBN-13 978-1-9774-1057-3

54995

9 781977 410573

www.rand.org