SANDIA REPORT
SAND2015-1081
Unlimited Release
Printed February 2015

Radar Design to Protect Against Surprise

Armin W. Doerry

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2015-1081
Unlimited Release
Printed February 2015

Radar Design to Protect Against Surprise

Armin Doerry
ISR Mission Engineering
Sandia National Laboratories
P.O. Box 5800, MS 0519
Albuquerque, NM 87185

Abstract

Technological and doctrinal surprise is about rendering preparations for conflict as irrelevant or ineffective. For a sensor, this means essentially rendering the sensor as irrelevant or ineffective in its ability to help determine truth. Recovery from this sort of surprise is facilitated by flexibility in our own technology and doctrine. For a sensor, this means flexibility in its architecture, design, tactics, and the designing organizations' processes.

Acknowledgements

This report is the result of an unfunded research and development activity.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Contents

Foreword

This report details the results of an academic study. It does not presently exemplify any operational systems with respect to modes, methodologies, or techniques.

Classification

Any specific mathematics and algorithms presented herein do not bear any release restrictions or distribution limitations.

This distribution limitations of this report are in accordance with the classification guidance detailed in the memorandum “Classification Guidance Recommendations for Sandia Radar Testbed Research and Development”, DRAFT memorandum from Brett Remund (Deputy Director, RF Remote Sensing Systems, Electronic Systems Center) to Randy Bell (US Department of Energy, NA-22), February 23, 2004. Sandia has adopted this guidance where otherwise none has been given.

This report formalizes preexisting informal notes and other documentation on the subject matter herein.

1 Introduction

Intelligence, Surveillance, and Reconnaissance (ISR) has the singular purpose of determining "truth" with respect to relevant concerns. This is true for military sensing as well as law enforcement sensing, and civilian applications' sensing. Knowing truth may also go by the phrase "Situational Awareness (SA)." Short of determining truth outright, the purpose of ISR is to drive down uncertainty, i.e. susceptibility to "surprise."

An important distinction is that it is in fact "truth" that we seek, not merely information. Information that isn't relevant to the truth we seek is at best merely wasted effort, and at worst actually obfuscating of the truth. Quite simply, there is no point to information that doesn't matter, although we acknowledge that information that doesn't seem to matter now may in fact matter later in a forensic fashion. Alternatively, not actually using available 'useable' information is no different than not having it in the first place. Information must serve finding truth.

Although ISR is crucial to military, law enforcement, and many civilian applications, we will focus hereafter mainly on military applications, with occasional comments specifically addressing other uses.

It is instructive to ponder the question "Why do we need truth? and by extension ISR?"

We observe that military operations are essentially an extension of foreign policy. As such, it's about freedom and ability to exert political will in a favorable manner. By the time the military gets actively involved, we are often in a physical contest of incompatible inter-nation political wills, i.e. war.

We further observe that continual change is the natural order of war. Nothing in war remains static. Mobility and movement permeates conventional warfighting doctrines. At its core is that an adversary is always looking for advantage while blunting or mitigating your advantage. More generally, this is often termed "dislocation," rendering an adversary's advantage irrelevant.

Seemingly, there is nothing like an existential threat to spur innovation and development of all sorts. Accordingly, a period of war will naturally spur constant change, especially in technology, tactics, and procedures. It is natural for all belligerents to keep looking for something better and more effective to their cause. It is also natural for efforts to be constrained by limited resources, imposing a requirement for economy.

Knowing truth allows "economy of force" in achieving a political end between nations, and "economy of effort" overall. An appropriate adage is "getting a bigger bang for the buck." Consequently, the purpose of ISR is to facilitate economy in the sense of minimizing effort to achieve the desired end.

Situational Awareness adds (or should add) velocity to our movement. Velocity here means allowing quicker achievement of our desired end without hesitancy due to uncertainties. We don't need to worry about tactical surprise. Truth then provides

security. Our velocity can also aid in our own ability to achieve tactical surprise towards an adversary. The attribute of velocity also leads to an ability for preemption, which is more desirable than confrontation. A military thrives on order. Disruption is anathema to that order, thereby degrading a military's effectiveness. We wish to disrupt an adversary, while not suffering disruption ourselves.

Economy also leads to (in fact requires) precision, including the avoidance of wasted effects resulting in collateral damage. Precision weapons require precision ISR. In addition, precision ISR aids the difficult but necessary economical task of deciding "what not to do."

In today's warfare, the real battle is about detection and location. Actual destruction of the enemy becomes anti-climactic. However, to find it, you need to be able to detect it, and to deal with it you have to locate it. Nevertheless, it is critical to understand that it is not about the sensor itself, but rather it is about "sensing."

Modern military tactics require technology to work correctly. When technology works correctly, it becomes an incredible force multiplier. Consequently, technology development has become a major national security activity. However, in today's defense establishment, we have largely adopted a requirements-driven approach to technology development; a favorite dictum being "Doctrine drives technology." This means that we survey the threats, decide how to fight them, define needs for how we wish to fight the threats we see, and fund technology development accordingly. Less appreciated is that available technology inevitably does drive doctrine. These are the "disruptive" technologies that a doctrine must evolve to accommodate. Particularly annoying are an adversary's disruptive technologies, which may not always be all that sophisticated; just effective.

We observe that it is not reasonable to expect that we will always possess the initiative, despite our best efforts and most earnest wishes. An adversary will expend great effort to prevent this, and it is not reasonable to believe that an adversary will not at least occasionally succeed, requiring us to react to his own initiative. Consequently offence versus defense is almost never a commander's choice. It is thrust upon him by circumstance. The bottom line is that no matter how much we prepare, we will encounter surprise. Consequently we have the seemingly absurd task to prepare for surprise without knowing what the specific surprise is.

This is then the theme of this report; how to prepare for surprise. In particular, we concern ourselves with radar ISR sensors, although the principles espoused herein are much more broadly applicable.

1.1 Doctrine

We are a "doctrine-based" military. For the purposes of this report, doctrine is the set of principles by which our military undertakes their function. It is the bridge between theory and practice. It includes Tactics, Techniques, and Procedures (TTPs) with which our military wages war.

A discussion of military doctrine and arguments for/against its components is beyond the scope of this report. What has been written on military doctrine can itself fill a large library. An excellent treatment on military doctrine, principles of war, and how they relate to technology is given in a book by Leonhard.[1]

Relative to the following discussion, we observe that while doctrine is quite useful in adding structure to military affairs, it does come at a price of often constraining how we even perceive threats.

1.2 The Nature of Surprise

> *"It isn't what we don't know that gives us trouble, it's what we know that ain't so."*
> *-- Will Rogers*

When speaking of "surprise" in conjunction with our military, most will immediately center their thoughts on strategic, operational, or tactical surprise. Examples of these include Pearl Harbor and the Battle of the Bulge in World War II, and perhaps the Tet Offensive in Viet Nam. It is not hard to think of many other examples.

We will not concern ourselves in this report with strategic/operational/tactical surprise per se. Rather, herein and hereafter we will concern ourselves with surprise in technology and doctrine. The difference is that strategic/operational/tactical surprise is being unprepared for the attack, whereas doctrinal and/or technological surprise is being prepared for the attack, but with ineffective preparations. Sometimes doctrinal/technological surprise falls under the banner of technology "emerging threats." However, we stipulate that surprise is somewhat more urgent than merely "emerging."

That is not to say that strategic/operational/tactical surprise is entirely irrelevant to our interest herein. Certainly, with the benefit of hindsight we often find that strategic/operational/tactical surprise is often accompanied, and perhaps even facilitated by, doctrinal/technological surprise. Consequently, these are certainly worthy of study.

For example, Waters writes in his masters' thesis about operational surprise in the 1944 German Ardennes Offensive (Battle of the Bulge) in World War II, and in the Chinese Counteroffensive in the Korean War.[2] Keller also discusses the 1944 German Ardennes Offensive as well as the 1973 Yom Kippur War in a monograph.[3] O'Leary assesses a number of military operations, including the 1941 Japanese attack on Pearl Harbor, the 1941 German Operation Barbarossa, the 1990 Iraqi invasion of Kuwait, and the 1962 Cuban missile crisis.[4] Gray discusses strategic surprise in a monograph that relates warfare to geopolitical ends.[5] Peterson argues from history that surprise is inevitable and

unavoidable, and must be accommodated in doctrine.[6] A fairly common theme is that with hindsight analysis, surprise was routinely achieved in spite of intelligence warnings of impending attacks. That is, intel didn't quite work the way it might have. This theme is relevant to our subsequent discussion as well.

Regardless, our focus hereafter will remain on doctrinal/technological surprise. An excellent discussion of technological and doctrinal surprise in warfare, and how to recover from it, is given in a book by Finkel.[7] Much of the basic framework of this report follows Finkel's ideas and nomenclature. Surprise of this nature essentially renders previous training and doctrine irrelevant. There are a number of ways that we might encounter such surprise.

Conceptual surprise is the lack of understanding the nature of the conflict. This might be due to any of a number of reasons, including our over-reliance on preplanned solutions, or perhaps from intel that has been doctored to fit a pre-conceived narrative, say for political reasons. An appropriate metaphor for this is "Drinking our own bathwater." Doctrinal rigidity manifests as a "just do as you're told" mentality.

Surprise is not always intentional by the adversary. Self-surprise may result from ignoring available information, erroneous assessments of the available information, drawing wrong conclusions, learning wrong lessons, or self-delusion in spite of the evidence. The one constant in warfare is reliance on the frailty of human judgment.

Surprise might result from over-reliance on rigid conditions to implement your own doctrine, or an inability to implement your own doctrine due to an uncooperative environment, conditions, or adversary. This might occur due to an over-reliance on factors that are really beyond your control, e.g. weather, political factors, Rules-of-Engagement (ROE), etc. Alternatively, surprise might also result from failure to exploit superiority at critical moments.

Surprise might also result from temporal issues. For example, surprise might result from an adversary inside your decision-loop, what Boyd[8] calls the Observation, Orientation, Decision, Action (OODA) loop; adversarial events happening on a time-scale not consistent with your own doctrinal expectations.

We note that the more powerful/effective a weapon or capability, the greater effort an adversary will employ to circumvent or defeat it; leaving it ineffective in spite of its power. No weapon or technique is so powerful that it is immune to countermeasures (and sometimes rather simple ones), or ubiquitously applicable. Even the most awesome power of nuclear weapons has been mitigated by political pressures such that they are of no help in Counter-Insurgency (COIN) operations. They have become weapons of mass irrelevance. We note that the ultimate flank is a country's stomach for war (the attitudes of those that enable the warfighter).

For a sensor, "surprise" is not just encountering jamming, spoofing, or other countermeasures, but also results from encountering unanticipated adversarial doctrine and/or technology, unanticipated targets, target characteristics and/or phenomenology,

unanticipated relevant environmental factors, and unanticipated changes in friendly doctrines and/or procedures that prohibit operational methods and modes of the radar. Surprise happens when an adversary by design or by accident "just doesn't care to be compatible with your ISR equipment and techniques."

Even designing a sensor system that does everything we can think of today can't foresee adversarial surprises in technology and doctrine. This is why every conflict has Joint Urgent Operational Needs Statements (JUONS), Quick Reaction Capability (QRC) projects, or equivalent. In fact, sensor advances will net new sensor denial TTPs by an adversary. The greater the success of a sensor, the quicker will be the adaptation to mitigate its capability. Consequently, your sensor capabilities will influence adversarial behavior. We opine that success of a particular sensor mode would include the effect of causing an adversary to move in a direction less advantageous to them, or causing them to move in a direction to be more observable by other sensors.

The bottom line is that we need to expect, and to accommodate, inevitable "surprise."

1.3 Mitigating Surprise with Prediction and Intelligence

> *"[N]o plan of operations extends with any certainty beyond the first contact with the main hostile force." -- Field Marshall Helmuth von Moltke the Elder, Chief of Staff of the Prussian General Staff from 1857 to 1871 and then of the Great General Staff (GGS) from 1871 to 1888.*

The obvious mitigation technique for surprise is to avoid it. Consequently, prediction and intelligence has been the predominant approach to dealing with surprise. Unfortunately, this approach by itself, although clearly useful, has generally failed to eliminate surprise. For example, during the US involvement in Iraq and Afghanistan, between 2001 and 2009, more than 7000 needs statements for urgent solutions were submitted through command channels to the Joint Staff and Services.[9] These represent an unpreparedness for what was encountered by the warfighter, in essence "surprise." Note that these conflicts were COIN operations against a relatively unsophisticated adversary while we possessed arguably the most capable intelligence capabilities in the world. This is not a sign of intelligence failure so much as an indication of what intelligence can practically achieve.

That is not to say that intelligence collection is bad or of little value. Quite the opposite is true. There is great value in studying friend and foe alike if for no other reason than to broaden the range of options with which to advance national policy in general, and military effectiveness in particular.

It must be appreciated, however, that more data does not equate to more information, and more information does not equate to more 'useful' information, or a better understanding of truth. Furthermore, massive infusions of information can actually *increase* the fog and friction of war, as noted by Baker.[10]

The point here is that we cannot rely on intelligence and prediction for always picking the right sensor or sensor characteristics, because often enough we will get it wrong, and encounter surprise in spite of our best efforts.

1.4 Preparing for Surprise with Flexibility

> *"He will win who, prepared himself, waits to take the enemy unprepared."*
> *— Sun Tzu, The Art of War*

Our recovery from surprise is precisely our ability to react constructively to surprise. Optimally, this means quick adaptation to mitigate the new threat. Consequently, preparation for surprise means that a sensor needs to be adaptable and flexible, and quickly so. We must be able to quickly answer the question "What do you do if the adversary doesn't behave according to your expectations?" Flexibility means "You need to be able to quickly implement 'plan B'" when "plan A" doesn't work or becomes obsolete. The abilities for adaptation and flexibility have indeed shaped history.[11]

Warfare is and will remain a time-based competition. Recent history suggests that the tempo of future wars and conflicts will not allow responding to urgent needs by ramping up to a lengthy wartime production procurement process. Rather, the future is trending to rapid fielding of essentially prototype systems to meet QRC timelines. Sometimes this is referred to as "embracing change."

Finally, we observe that a small force structure (toward which our military is trending) coupled with requisite economics makes flexibility even more important.

Figure 1. The appearance of the first tanks at the Battle of Flers-Courcelette (part of the Battle of the Somme) on 15 September 1916, represents a technological surprise. (Image courtesy of Imperial War Museums)

2 The Nature of Flexibility

Recall that the aim of flexibility is to ensure a quick recovery from doctrinal or technological surprise. To preface the following discussion, we suggest that it might be useful to present synonyms and antonyms to the word "flexibility."

> Synonyms include adaptable, compliant, resilient, versatile, adjustable, alterable, changeable, convertible, ductile, modifiable, pliable, pliant, supple, variable, and mobile.
>
> Antonyms include rigid, strict, stiff, uniform, constrained, intractable, uncompromising, static, adamant, set-in-stone, single-minded, hard-line, fixed, and lock-step.

We now examine several flavors of flexibility.

2.1 Conceptual and Doctrinal Flexibility

> *"If everyone is thinking alike, then somebody isn't thinking."*
> *– Gen. George S. Patton*

This is about flexibility in the overall conduct of the warfighting organization, that is, flexibility in what it means to "fight" the war.

Flexibility in doctrine embodies the following three elements,

1. Openness to new ideas versus dogmatism,
2. Tolerance to different views, and
3. Multi-dimensional versus one-dimensional doctrines.

An organization's TTPs need to reflect this flexibility. In other organizations TTPs are otherwise called processes. This means that dogma in processes, that is strict adherence to processes, is inherently inflexible.

Furthermore, training itself needs to allow the exercise of flexibility by embodying surprise. Consider training that doesn't anticipate the surprise. Training that doesn't expose the trainee to surprise will ultimately build an inflexible organization regardless of "what the book says."

Relatedly, flexibility in concept means allowing for consideration a different understanding of the evidence at hand. This means collecting a staff of Subject Matter Experts (SMEs), and using them. We emphasize that the key is in using SMEs as opposed to high titles and ranks.

To be flexible, an organization must avoid the suppression of thinking that deviates from doctrine. An inflexible organization will often be hostile to innovative thinkers; calling

them alarmists, non-team-players, defeatists, rogues, renegades, possessing questionable loyalties, having "gone native," etc. This hostility can severely diminish flexibility.

To be flexible, doctrines need to be multi-dimensional. That is we must avoid the "one size fits all" mentality. We have to allow responses that fit the circumstance, and not believe that circumstances will always favor our preferred doctrine.

Finally, we must acknowledge that information comes with a cost. Knowledge needs to be balanced against tolerable ignorance. The value of timeliness requires us to be wary of "paralysis by analysis."

2.2 Organizational and Technological Flexibility

> *"The most important thing is to have a flexible approach.... The truth is no one knows exactly what air fighting will be like in the future. We can't say anything will stay as it is, but we also can't be certain the future will conform to particular theories, which so often, between the wars, have proved wrong." – Brigadier General Robin Olds*

This is about ensuring the warfighter (including his support organizations) has tools that allow for flexible response.

We examine several components of this genre of flexibility in the following subsections.

2.2.1 Balance

The flexible organization or system apportions resources across a set of capabilities. In a warfighting organization this means for example balance between the executive function and the supply function, also known as logistics balance.

Similarly, a flexible sensor needs to facilitate ISR as well as perhaps target prosecution. That is, for example, a flexible ISR sensor should have an answer to "What will I do *after* I find the target?"

Balance also means supporting multiple modes of operation for different missions. Generally it is preferable to do multiple tasks acceptably well rather than a single task exquisitely well and others not at all. A sensor (or sensor system) that facilitates only one mission is inherently inflexible, and is in fact wasteful.

2.2.2 Diversity

Diversity in weapons is about employing different weapons with different but supporting effects. This supports a combined-arms approach to warfare.

Diversity in sensors is about using different sensors that complement each other, bringing different but supporting information to the analyst. This supports a sensor-suite approach to sensing.

Using variety in your own capabilities allows you to probe for weakness in an adversary. Furthermore, integrated effects facilitate economy. Consequently, the value of a system in not in its singular capability, but rather it is in how it combines with other systems. It is the sensor suite that is important, not the individual sensor. With a sensor suite, we don't necessarily mind an adversary adapting with a countermeasure to any one measure. In fact we may even desire an adversary adapting, since it tends to make him become more vulnerable to other detection methods. Of course all this presupposes that the sensor suite is in fact operated as an integrated suite, and not in an exclusive-or fashion.[12]

Single system approaches, as with single-capability systems, are inherently wasteful. They are inherently inflexible. Furthermore, such systems are vulnerable to single-system countermeasures. Essentially, technology patterns invite an adversary to predict our tactics and then defeat them. The more narrow the pattern, as with a single sensor, the more apt they are to be defeated. The bottom line is that overreliance on a single capability virtually guarantees ultimate failure and defeat.

Succinctly put, diversity is the opposite of commonality, and common means vulnerable to the same surprise.

2.2.3 Redundancy

Redundancy in weapons means different weapons intended to cause the same effect but by different means. Although perhaps subtle, there is a difference between redundancy and diversity.

Redundancy in sensors means sensing the same phenomena, but doing so with different specific sensors. An example might be both space-borne and airborne radar systems.

Most importantly, redundancy is about embodying similar utility, and does not necessarily imply similar performance capability. Utility is not the same as performance. Even otherwise antiquated systems may retain their utility in environments were higher-performance systems might be vulnerable to a surprise development by an adversary.

We note that an important relative of utility is reliability. We opine that twice the performance with half the instrument availability is not necessarily a good deal.

2.2.4 Technological Flexibility

Technological flexibility in a weapon or sensor embodies the following basic characteristics.

1. Versatility – the ability to use the weapon or sensor for multiple purposes. This includes multiple sensor modes to broaden its utility.

2. Changeability – the ability to be easily updated with new features.

In general, maintaining options is a good thing. In fact, providing more options allows for tailoring a response to surprise. Mission/feature creep, while denigrated by

conventional wisdom, actually equates to “option acceleration,” which is arguably a good thing. This allows flexibility to respond to opportunity.

This does not mean that a system be designed as broadly multi-functional from the outset, but rather that the system be designed in a manner to not prohibit adaptation to changing operational needs. Technological flexibility is not the same as complexity.

Sensor systems need to be able to serve JUONS and QRC requests with short-term enhancements and modifications. In particular, ISR systems do need to consider that they might eventually be opposed by countermeasures.

2.2.5 Flexibility in Development

This is about developmental agility, i.e. the ability to adjust the development and/or acquisition process to gain a new or enhanced capability.

We observe that the conventional acquisition process begins with identifying a current or anticipated need, generating requirements for the solution system, and awarding a contract to provide that system with great consideration to minimizing the cost of the system. Consequently, a supplier builds the system that typically just barely meets the requirements and rarely more. Later, this same model is applied to any upgrades.

An alternative is to specify the system architecture in a manner that allows easy enhancement from the outset. Often this entails modularity. In some systems, modularity allows swapping “mission packages” which may be designed on a separate time-line from the host system, often delaying commitment to specific equipment allowing for taking advantage of more recent advances in equipment performance. We note that building this kind of flexibility into new system designs has found traction in naval warship engineering.[13] This flexibility is facilitated by design methodologies such as Set-Based Design (SBD).[14]

2.3 Cognitive and Command & Control (C2) Flexibility

“Flexibility Masters Hardness" – Japanese / Judo proverb

This is about allowing for flexible behaviors at various levels in the warfighting organization. Generally, the hierarchy may include human as well as machine nodes. As such, an ISR sensor system is just a bottom node in the hierarchy.

2.3.1 Decision Authority

If we believe that information is useful to make a decision, then optimal decision making should happen at the level of most information. Essentially, authority must follow information. Equivalently, the decision maker needs both the authority and the information on which to base a decision. A commander cut off from information is not in a good position to make an optimum decision. However, he also needs the capacity (aptitude) to process the information into a decision, and in a timely manner.

2.3.2 Decentralized Command

If a centralized authority were also the centralized collection point for information, then a centralized C2 would be optimum… almost. The velocity with which information can be assembled and processed, and a decision distributed, is also a factor. For a centralized C2 to be truly optimum, we would need infinite bandwidth to transmit/receive the information and decision, and infinitely fast processing speed. This is problematic. We cannot allow resources to be avatars waiting around to receive a decision. This is wasteful. It is the same as disabling those resources.

It is the limitations of the decision makers that limits a centralized C2. Communication and decision latency (a.k.a. "bandwidth") makes centralized command inherently inflexible, thereby limiting recovery from surprise. This also drives us towards objective-based actions, enabling and in fact requiring a decentralized C2. This facilitates autonomy and consequently drives us towards simplicity of overall plans. The down-side is that this ultimately limits options.

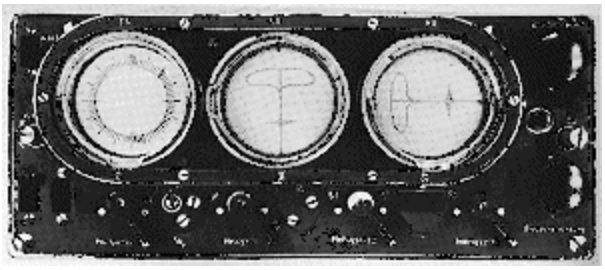

Figure 2. In response to the German surprise by British use of chaff (window) in July 1943, Germany embarked on a crash effort to neutralize this development. By October 1943, the chaff-immune Telefunken FuG 220 Lichtenstein SN-2 airborne radar operating in the VHF band was being installed on operational night-fighters. Its effectiveness provided in turn a surprise to Allied forces, who took until the summer of 1944 to develop effective jamming techniques for this radar. The display contained three indicators, one each for range, azimuth, and elevation of target echoes. (Images courtesy of GMT Games, and Stefano Pasini)

To summarize, more information communication and processing bandwidth gives us more options and allows a more centralized C2 to be optimum. Less information communication or processing bandwidth limits our overall options and begs a more decentralized C2 to be optimum. As bandwidth changes, so too does the optimum decision authority. Since dealing with surprise often requires quick assessment and response, this drives us to a flexible C2 doctrine.

The antithesis of a flexible C2 doctrine is one of a rigid centralized command. A rigid centralized command is often advocated under the maxim of needing "unity of command." However, we stipulate that unity of command is really more about ensuring integrated efforts, and opine that integrated efforts are better served by a flexible C2 doctrine. We note that a rigid centralized command, especially in a practical limited bandwidth environment, is often derided as "micro-management."

As a final note, we observe that a flexible C2 doctrine encourages low-level initiative, innovation, and initiative. Furthermore, a flexible C2 doctrine rewards these attributes.

2.4 Dealing with Lessons Learned and Rapid Dissemination

> *"Experience is a hard teacher because she gives the test first, the lesson afterward."* ─ *Vernon Law*

This is about maximizing profit from flexibility. Once a surprise has been encountered, the question becomes "How do we go about developing a solution and quickly fielding it so that friendlies will no longer be surprised?"

Historical recovery from surprise has entailed the following three elements

1. A culture that encourages learning and drawing lessons,
2. A mechanism for rapidly conveying lessons, and
3. A mechanism for rapid linkage between the warfighter and the defense industry.

Clearly, if past practices resulted in our surprise, then we need to alter those practices in order to recover and better prepare us for future surprises. This is learning. We need to be willing to change for the better, and facilitate those that can help us do so. This especially applies to encouraging real-time learning by the warfighters themselves.

Additionally, if we develop a solution for our surprise, we need to rapidly share it with others to mitigate its effect on our larger warfighting capability. Unit "A" having a solution and not sharing with unit "B" is inherently uneconomical and counterproductive to the larger effort.

Similarly, those that encounter the surprise may not themselves be the most efficient at developing a solution to the surprise. Consequently we need high-bandwidth communication between warfighter and solution developers, e.g. research laboratories and industry. This suggests meaningful networking between warfighter and industry/laboratories.

3 Discussion

What follows below is a discussion of means of incorporating flexibility to prepare for surprise, limited to the realm of ISR radar systems. We begin with some general comments.

It's not about pretty pictures, color renderings, or fancy displays per se. It's about target detection, discrimination, and location presented effectively to an information analyst, often a tactical sensor operator, but sometimes a machine. Tactical sensors need to be speedy, real-time, with real-time exploitation and information dissemination to the decision makers. Sensor improvements need to be capable of adding to our understanding of truth in a timely manner.

Economy demands low-cost enhancements to meet future needs. Cost will always be a factor, but cost is more than development dollars. Cost also includes life-cycle costs such as operation, maintenance, and training. It also includes non-monetary expenditure such as development times and schedules. Low-cost enhancement capability is a competitive advantage, with all adversaries and competitors, state and industrial.

3.1 Radar/System Architecture Definition

> *"We are called to be architects of the future, not its victims."*
> *— R. Buckminster Fuller*

The design of a specific sensor begins with its architecture. This is the framework into which technology components are inserted to build the system. Its architecture typically bounds the eventual capabilities of the system.

A system architecture needs to consider and allow for efficient future modifications and enhancements to address new and changing requirements, ultimately to also accommodate JUONS and QRC needs. This is sometimes called "Designing for Modernization." This means that an architecture must insist on useful "hooks" for enhancements, even if a capability isn't implemented 'yet.'

Similarly, an architecture must readily allow for alternatives. This means we must rid an architecture of choke points; vulnerabilities to single points-of-failure. Lack of an efficient ability for alternatives is an inhibition to flexibility. Furthermore, a flexible architecture will facilitate a breadth of capabilities, for real sustained utility, else it isn't particularly flexible by definition.

Furthermore, an ISR system's architecture must ultimately serve finding truth. Its output products are not an end unto themselves. Consequently an architecture must facilitate integration with other sensors and relevant systems.[12] A sensor that isn't employed is simply ballast.

We do note, however, that sometimes otherwise seemingly desirable features may actually inhibit flexibility. Even features ostensibly meant to enhance flexibility may in fact inhibit the very thing they purport to enhance. Implementing these features requires informed debate during the architecture design process. Furthermore, flexibility also entails recognizing that a feature that must be implemented at any cost may in fact be too expensive and ultimately be prohibitive.

We acknowledge that flexibility may come at a price, at least initially, although this too is quite arguable. However, it doesn't take very many enhancements to recoup any initial cost of flexibility, and in fact reap substantial dividends.

3.1.1 Comments on Common Architecture

One area that has unappreciated flexibility-limiting side effects is the popular notion of forcing commonality across multiple systems.

Forcing a common architecture is about centralized design and control, and initially sounds like a great idea. The usual advertised benefits include economy of scale, commonality itself, and the promise of faster, better, and cheaper system development. However, often overlooked is that forcing a common architecture exhibits all the usual problems of centralized planning and control including bloated bureaucracy to administer, lack of efficiency in program execution, lack of benefits of competition, difficulty with flexibility, common vulnerabilities, and disturbingly often delivering slower, worse, and more expensive system development.

Commonality entails overhead as it forces the constraint of similarity onto otherwise diverse systems. At the same time commonality in and of itself is 'not' a performance measure, and doesn't contribute to sensor performance. Insisting on one-size-fits-all ultimately fits nobody very well, as it is a constraint that ultimately restricts the flexibility of a unique solution. It therefor limits options. For example, insisting on a single software code branch (or limited number of code branches) across multiple systems is inherently inflexible.

For a common architecture to be flexible, it must

1. Allow un-common features, including special code branches,
2. Allow low-level external control of data collection parameters, and
3. Allow pass-through of raw data to external un-common processors.

This, of course, makes the common architecture decidedly un-common. We adduce that the test for how well a common architecture serves flexibility is how quickly and how inexpensively a new specialized experimental mode may be inserted into the system.

We advocate that what the sensor system really needs is a 'modular' architecture, not necessarily a common one. We do note that modularity may require some degree of commonality of module interfaces, but this is a far lower bar than commonality of all components themselves.

3.1.2 Comments on Open Architecture

The concept of "open architecture" has gained substantial traction in the military acquisition community. Its attractiveness is in facilitating easy addition, upgrading, and swapping of components, especially by third parties. This applies to both hardware and to software. This is expected to contain costs for sensor modifications especially after initial manufacture. Oft-cited as example is the personal computer. Furthermore, even during initial development, an open architecture is expected to facilitate "concurrent design" and "concurrent engineering" with the subsequent expectation of expediting the design and development process. These are all good things… to a point.

However, less appreciated is that an open architecture is no panacea; that it comes with opportunity for all sorts of surprises by itself; that it comes with inherent flaws. For example, for an open architecture to achieve its intended benefits, interfaces between modules must be well-defined, indeed quite rigidly so. Making everything compatible with other compartmentalized modules presumes that we know the bounds of required new innovations, and of course we may be surprised to learn that we don't. This is especially problematic when the open architecture extends to a too-low level.

Openness requires to some degree a more rigid definition of the system. Basically, the more we rigidly define the system, the more we constrain the system, and the less flexible the system becomes.

One might question why modularity was adjudged good in the previous discussion on common architecture, and is approached with warnings in this section on open architecture. The difference is in where the authority lies in which modules may be enhanced or otherwise modified, indeed when module interfaces themselves may be touched. Openness generally requires a higher level of oversight than architectural modularity. It is a C2 function in the system design process. Inherent communication bandwidth in the acquisition chain, especially with respect to technical matters, simply favors a lower level authority for module-related technical decisions. Essentially, modularity is good, but not when the module definitions are controlled too far up the chain of authority.

Nevertheless, for an open architecture to be successful and yet allow flexibility, its modules must minimally

1. Exhibit standard hardware interfaces for control, status, and data output, for standard products,
2. Mirror a well-defined Interface Control Document (ICD), for standard products,
3. Provide standard data output formats, with adequate metadata, for standard products,
4. Provide documented data characteristics, including high-level models for the data and perhaps for any processing employed, for standard products, and

5. Provide a low-level system control and raw data output capability, for nonstandard processing by external auxiliary processors, including non-standard processors. This might be data pass-through, or bypass modes.

It is this final feature that facilitates the greatest degree of flexibility.

Finally, while we don't dispute the benefits of an open architecture, we remain mindful of the limitations of insisting on formal 'openness' at too low a level in the system. We opine that optimum with respect to flexibility is with relatively few and larger open architecture modules. This applies to both hardware and to software.

While we have discussed open architecture in the context of flexibility, we note that other issues also really need to be addressed, such as "Who 'owns' the integration and testing of new modules into the open architecture?" and the resulting "Who owns the problem of two modules independently meeting all specifications, but nevertheless not working properly together?" Yup, it happens.

3.1.3 Comments on Fault Tolerance

Fault tolerance is the property of a system to continue useful operation in spite of failure or degradation of one or more of its constituent components or other resources.

A fault-tolerant architecture seeks to avoid system failure due to single-point faults. It must overcome non-functional modes regardless of the reason or source of the fault. This would include internal system faults as well as external faults in supporting equipment, e.g. GPS, etc. Fault tolerance means that we have a useful answer to the question "What do we do when…?" In particular, with today's advocacy of net-centric warfare, we need to also consider the potential of the network "going down."

The essence of fault-tolerance is to retain utility. Recall that utility is not the same as performance. Consequently, a fault-tolerant system might allow degraded operation modes in the presence of faults.

We might expect that an adversary would attempt to induce faults into our sensor system. Such hostile activity falls under the banner of countermeasures including jamming, spoofing, and/or other interference to our sensor system.[15] It might also generally include activities of cover and/or concealment. With respect to jamming/spoofing/interference, flexibility must allow for some degree of system self-reliance, indeed autonomy, consistent with a flexible C2 doctrine.

3.2 Radar Instrument Implementation

> *"Stay committed to your decisions, but stay flexible in your approach."*
> *— Tony Robbins*

Once an architecture is in place, the detailed design of the specific sensor may commence. This activity also must consider flexibility when making specific design choices.

Prudent design features would include allowing for easy expansion and modification. This includes incorporating spare circuit card slots, spare sense and control lines (including with interfaces), and generally excess capability. It would also facilitate easy reprogramming of any firmware and software.

Flexibility also includes planning for component obsolescence. Designs should consider second source procurement.

We note that faster processors and communications allow more complexity, which generally enhances performance and capabilities. This in turn provides more options for tailoring a recovery from surprise, which is good. However, we must be mindful that complexity also comes with its own vulnerability to surprise, which is bad. Basically it is often easier to mess up something complicated than something simple. This generally speaks to allowing simpler operation modes at least as backup capabilities.

All else equal, smaller Size, Weight, and Power (SWAP) is better than bigger SWAP. Sensor real estate on ISR platform aircraft will always be precious, and become more so. This will also allow the sensor to be installed on more platforms, thereby supporting economy. The same is true of cost. The metric will be capability per dollar per cubic foot. Requiring that the sensor installation displaces weapons will be a hindrance, and only be acceptable if it makes the remaining weapons more effective commensurately.

Data standards are good, and facilitate velocity of dissemination, but need to retain the flexibility to easily add new user defined metadata, and perhaps even new products.

3.3 Radar Design Practices

> *"While some see them as the crazy ones, we see genius. Because the people who are crazy enough to think they can change the world, are the ones who do." — Apple Commercial*

We assert here that an otherwise flexible sensor instrument, coupled with a rigid inflexible organizational doctrine with respect to design, will essentially negate the sensor instrument's flexibility. Rigid mechanization of the design "process" inhibits, and in fact destroys initiative, innovation, improvisation; the very qualities necessary to create the optimum recovery response to a surprise. There is not much difference in the outcome from between "can't" and "won't." Furthermore, "too late" is just another manifestation of "failure."

Related to this, as with lack of options in technology, a lack of options with respect to designers constitutes choke points in the response to surprise, and is inherently inflexible and thereby unhealthy to the ability to respond to surprise.

We further assert that an ISR sensor design cannot be purely [operational] requirements driven, because requirements cannot prepare for "surprise" by definition. The requirements are essentially a definition of the necessary end-state for a design. The more rigidly that the end-state is defined up front, the less will we be able to capitalize on opportunity, that which we learn along the way, or the ability to adapt to new needs. In spite of requirements, a sensor needs to incorporate flexibility, sometimes called "hooks," or growth-paths.

Furthermore yet, consistent with a multidimensional doctrine, the design process must avoid employing a single preeminent measure of goodness, such as resolution, or range. We must guard against falling prey to a "cult of performance" that may not add significantly to sensor utility, but does enhance vulnerability to single-point failure mechanisms. Recall that performance at any cost might be too expensive by introducing vulnerabilities. It remains a truism that reliable adequacy is better than unreliable/vulnerable stellar performance.

In addition, during the design process, dissenting comments and viewpoints should be encouraged, not punished. All too frequently an organization's analysis of alternatives and subsequent project reviews are incestuous, inbred, or too narrow in scope, ultimately being criticism-averse and exhibiting fear or even contempt for dissent. This leads to the false positive-feedback of "drinking your own bathwater." A design process' concept reviews, architectural reviews, and system design reviews need to optimally include a broad spectrum of SMEs, else options can be expected to be overlooked. Overlooked options limit flexibility and ability to respond to surprise.

As a side note, the key here is using SMEs in these reviews, not just titles and ranks. Furthermore, we caution to beware of the myth that "You need new [inexperienced] people for new ideas." Ample scholarly evidence suggests that creativity peaks after significant experience in a field.[16]

A completed design process would include rapidly documenting *and disseminating* lessons learned. Without dissemination, the documentation has little value. When considering modifications to address a surprise, we need to understand the starting point for the technology in question. Absence of a well-documented description of sensor operation is a failure to prepare for future surprises, and thus inherently inflexible.

3.4 Tactics

We mention without further elaboration that sensor flexibility might include flexibility in tactics, that is, how the sensor is specifically employed. This suggests that a flexible sensor needs a large performance envelope for operating parameters.

4 Summary & Conclusions

We repeat the following key observations.

- It is the purpose of war to exert political will to yield a favorable outcome. The purpose of a sensor is to aid in finding "truth" so that efforts to exert political will are economical with respect to effort. It is reasonable to expect an adversary to impede such efforts.

- It is the normal course of conflict to encounter technological and/or doctrinal surprise. Such surprise can be purposefully created by an adversary, or it can be self-generated, by essentially misjudging circumstances and/or events.

- The best mitigation or recovery strategy for encountering surprise is to retain flexibility in our own doctrine and technologies.

- Flexibility requires that a sensor exhibits flexibility features in its architecture. A flexible architecture is not identically a common architecture, nor is identically an open architecture. It does generally facilitate fault tolerance.

- Flexibility requires that a sensor exhibits flexibility features in its implementation. This includes easy expansion and modification, as well as foresight with respect to dealing with component obsolescence.

- Furthermore, flexibility requires that the sensor design practices of an organization facilitate timely consideration of a multitude of options from a broad base of SMEs. To do otherwise equates to "drinking your own bathwater."

Figure 3. Al Qaeda in the Arabian Peninsula is reported to have produced a 16-minute video titled "Combating Spy Airplanes" to teach their insurgent fighters that to avoid detection by drone infrared sensors, they should wrap themselves with insulation and aluminum foil.[17] This is an example of how the efficacy of a sensor system is causing an adversary to adapt their behavior in a manner that might actually make them more detectable by other sensors, e.g. radar.

References

[1] Robert R. Leonhard, *The Principles of War for the Information Age*, ISBN 0-89141-713-3, Ballantine Books, Presidio Press, 1998.

[2] Lonn Augustine Waters, *Secrecy, Deception, and Intelligence Failure: Explaining Operational Surprise in War*, Masters Thesis, Massachussettes Institute of Technology, September 2005.

[3] Major Brian A. Keller, *Avoiding Surprise: The Role of Intelligene Collection and Analysis At the Operational Level of War*, Monograph, AD-A258 103, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 28 April 1992.

[4] Major Jeffrey O'Leary USAF, *Surprise and Intelligence Towards a Clearer Understanding*, USAF Air War College, 15 September 1997.

[5] Colin S. Gray, *Transformation and Strategic Surprise*, Strategic Studies Institute, US Army War College, April 2005.

[6] LTC (P). Craig A. Peterson US Army, *Surprise: Get Used to it*, AD-A266 732, Department of Military Operations, US Naval War College, 17 May 1993.

[7] Meir Finkel, *On Flexibility – Recovery from Technological and Doctrinal Surprise on the Batlefield*, ISBN 978-0-8047-7489-5, Stanford University Press, 2011.

[8] John Boyd, *The Essence of Winning & Losing*, 5 slide presentation, 28 June 1995 (revised January 1996).

[9] Defense Science Board Task Force, *Fulfillment of Urgent Operational Needs*, Office of the Under Secratery of Defense For Acquisition, Technology, and Logistics, Washington, DC, July 2009.

[10] Lt. Col. Virginia E. Baker USAF, *Reexamining the Principles of Surprise in 21st Century Warfare*, Joint Military Operations Department, Naval War College, 16 June 1996.

[11] Victor Davis Hanson, *Carnage and Culture – Landmark Battles in the Rise of Western Power*, ISBN 0-385-50052-1, Doubleday, a division of Random House, Inc., 2001.

[12] Armin W. Doerry, *Improving ISR Radar Utilization (How I quit blaming the user, and made the radar easier to use)*, Sandia Report SAND2014-16616, Unlimited Release, August 2014.

[13] Shawna Garver, Jack Abbott, "Embracing Change," *Marine Technology*, Society of Naval Architects and Marine Engineers, pp. 22-28, July 2014.

[14] Thomas McKenney, David Singer, "Set-Based Design," *Marine Technology*, Society of Naval Architects and Marine Engineers, pp. 51-55, July 2014.

[15] Armin W. Doerry, "Comments on radar interference sources and mitigation techniques," SPIE 2015 Defense & Security Symposium, Radar Sensor Technology XIX, Vol. 9461, Baltimore, MD, 20-24 April 2015.

[16] Dean Keith Simonton, "Creative Productivity: A Predictive and Explanatory Model of Career Trajectories and Landmarks," *Psychological Review*, Vol. 104, No. 1, pp. 66-89, 1997.

[17] Rowan Scarborough, "Terrorists adapting to avoid U.S. drones," *The Washington Times*, Sunday, January 4, 2015.

Distribution

Unlimited Release

1	MS 0519	J. A. Ruffner	5349	
1	MS 0519	A. W. Doerry	5349	
1	MS 0519	L. Klein	5349	
1	MS 0532	J. J. Hudgens	5240	
1	MS 0899	Technical Library	9536	(electronic copy)


Sandia National Laboratories