15th ICCRTS

"The Evolution of C2: Where Have We Been: Where Are We Going?"

"Who's got the grease pencil?!"
What Cyber Security can Learn from the Outer Air Battle

Topics: 1, 2, 3

Mark N. Clemente
Captain, U.S. Navy (Ret.)
The Boeing Company

1215 S Clark St MC 793C-G029
Arlington, VA 22202-4398
Phone: +1 703-872-4106
E-mail: mark.n.clemente@boeing.com

“Who’s got the grease pencil?!”

What Cyber Security can Learn from the Outer Air Battle

Abstract

When the lights go out and our networks grow dim, can we nonetheless operate successfully enough to achieve our objectives? Today – with government operations at all levels dependent on bits and bytes traversing ubiquitous cyberspace – cyber security, information assurance and protecting organizational electronic integrity from malicious intent have become increasingly critical. This is not the first time however, that we have found our organizations reliant on electromagnetic systems vulnerable to attack. During the Cold War, the Soviet Union had elaborate plans to foil U.S. Navy Carrier Battle Groups with bomber raids whose success depended on disrupting discrete segments of the electromagnetic spectrum. This was a comprehensive battle for information and communication, featuring both broadband noise and deception jamming. To counter a hostile electronic warfare (EW) environment, Carrier Battle Groups developed an operating concept that enabled long-range fighter patrols to coordinate and fight without traditional command and control. Fortunately, that preparation was for a battle never fought, but from it we can glean lessons about developing trust, promulgating and interpreting command intent, self-synchronization, adaptation and local networking that should help inform a more comprehensive approach to today’s challenges.

Introduction

The theme of the 15th ICCRTS “*The Evolution of C2: Where Have We Been? Where Are We Going?*” continues a tradition of focusing on how militaries might evolve traditional, mostly Industrial Age command and control processes and systems to better address Information Age challenges. And if Industrial Age processes were about centralizing production and closely controlling data and information, the Information Age calls for decentralizing production and getting information “to the edge”[1] – in order to enable self-synchronizing actors with deep understanding of enterprise (or command) intent to operate more effectively and efficiently. And the Information Age has matured to include new and innovative ways for users to participate in the creation as well as distribution of content. These are exciting developments and innovators will create many useful tools (and toys) that we cannot even imagine today. However, there is rising concern that, as essential processes are moved "on-line," we are unwittingly exposing ourselves to unknown vulnerabilities. How can we be sure that information we access has not been interrupted or doctored? We keep flashlights for when the lights go out, and candles for when the batteries run out – but what is our backup plan for the systems we rely on in today's cyber-centric world?

As George Santayana famously said, "Those who cannot remember the past are condemned to repeat it."[2] We have been here before, and this paper will use an historical example to explore parallels between then and now. During the Cold War, while the U.S. and U.S.S.R. were locked in an ideological, economic and military struggle, they were also waging a pitched battle for the tactically relevant segment of the electromagnetic spectrum.[3] The paper will recall the experiences of Cold War aircraft carrier crews preparing to defend themselves from Soviet attack in an attempt to extract lessons we might apply in dealing with our increasing reliance on connectivity.

A U.S. aircraft carrier conducting flight operations is a ballet of immense complexity that harmonizes advanced technological systems with human endurance and ingenuity. It also, at times, employs some very basic tools and procedures to keep track of highly dynamic events. For instance, while the Navy is in the midst of transitioning to a more technologically advanced system,[4] they still keep track of every aircraft's position on the flight and hangar decks on a table top board with to-scale aircraft silhouettes, using various push-pins, colored nuts and washers placed on top to signify different status conditions. And to keep track of the aircraft coming back to land, the Navy still trains sailors to write backwards on a glass panel with a grease pencil. As we evolve into our highly technological future, do we still own a flashlight? Can we find the candles if the lights go out? WHO'S GOT THE GREASE PENCIL?

In addition to needing to operate under degraded conditions, the ease of distributing available information under normal conditions invites micromanagement from higher level commands. The promise of the Information Age is total connectivity. And in this "flatter,"[5] more globalized world, we believe we can afford to let go of the "middle man," since data, information and intelligence are sent, pulled or gleaned at the points of action. Technological gains have given the world revolutions in communications technology and, for the military, the ability to conduct precision maneuver and engagement. We have wireless access to the world, and can put a guided weapon through an air duct. But precision geo-location does not guarantee a precision effect – especially as you are attempting to gage an operational or strategic level effect. Another caution of increased granular knowledge enabled through robust information technology, is the degree to which it lures higher level commanders into the tactical battle, causing them to neglect the “big picture.”

And while many may seek “black box” technological solutions to complex challenges, this paper examines how complexity theory and living systems theory helps us to better understand the true nature of these highly dynamic challenges and what this portends for human decision-making – at the edge – as well as in the command centers.

The Outer Air Battle

During the Cold War, the U.S.S.R was considered an existential threat to the West. While the geographic focal point might have been in Germany, the U.S. Navy developed a “Maritime Strategy” that included a plan to open up a northern front. It began operating aircraft carrier operations in the “GIUK”[6] gap and the fjords of Norway in preparation for offensive action against the Soviets in their own backyard. The Soviets, the ultimate land power, saw the U.S. Navy as a direct threat to their plans. They developed an impressive Navy of their own and devised a multi-prong plan to attack and negate the U.S. Navy -- in particular, the U.S. aircraft carriers. While the Soviet submarine force garnered a lot of attention from the U.S. Navy and national intelligence agencies[7], this paper focuses on the narrower aerospace dimension of Soviet plans to challenge U.S. Carrier Battle Groups with large Badger or Backfire bomber raids armed with very fast anti-ship cruise missiles[8].

Shoot the Archer, not the Arrows

Meeting Art Cebrowski for the first time was quite an experience. We met in early 1982 while embarked in USS Nimitz deployed to the Mediterranean Sea when then Commander Cebrowski was the air wing commander. This was well before Cebrowski had earned a reputation as the “father of network centric warfare” and as Donald Rumsfeld’s Director of Force Transformation.

Even back then, Cebrowski thought differently about challenges than most of his fellow fighter pilots.

He approached a couple of junior officers one afternoon in a fighter squadron ready room and started questioning us about Soviet bomber tactics. “Where are the Backfires based?” “What is their maximum fueled and unrefueled range?” After answering some basic questions, he asked us, “so if you are correct, and our Battle Group is located ‘here’ … what would be the threat axis?” Using a push pin and a string normally used to calculate time/distance information for long duration flights, we started to posit threat arcs around our Battle Group – that were dependent on the carrier’s distance from the bomber bases. Then he asked the group what would change if the carrier pulled back another 100, 200, 300 miles? Theoretically, if we backed up the carrier to the maximum range of the threat aircraft– and if we knew their launch point – we could determine with precision the attack bearing of an inbound threat.

Cebrowski also asked about Soviet anti-carrier missiles, the AS-4 and AS-6.[9] “At what range would the Backfires release these Mach 3+ missiles?”[10] As we knew intercepting supersonic missiles would be a challenge, it was imperative that we engage the “archer” well before he was in range to release his “arrows.”

Cebrowski seeded ideas by asking pregnant questions and allowing his interlocutors to believe they had given birth to the solutions themselves. In this case, he eventually asked if we would build him a brief that described our “discovery.” Built on butcher-block paper, we built Commander Cebrowski one of the first briefs that became the basis for a new carrier tactic dubbed “chain-saw.”

Chain-Saw

We needed to intercept the Soviet bombers as far from the defended point as possible and before the bombers reached their weapons release point. This required both a good cueing system to direct our fighters to the Soviet bombers and a “chain” of aircraft sent down a pre-selected axis to replace aircraft coming off station because of weapons expenditure or aircrew fatigue. Aerial refueling was also used to keep the chain manned as long as necessary. Usually, one carrier could keep the chain going for about 12 hours, so around-the-clock coverage required multiple carriers. The F-14 Tomcat equipped with the AIM-54 Phoenix missile was designed specifically for this Soviet bomber threat. The Tomcat radar could simultaneously support multiple bomber / AIM-54 engagements while continuing to scan for additional targets. This capability would be critical when combating the large anticipated Backfire raids.

Electrons on the Attack

The Soviets knew this, of course. In addition to long-range bombers and fast anti-ship missiles, they relied on extensive electronic attack and electronic countermeasures to thwart the U.S. Carrier Battle Groups' defensive screen. To make it more difficult for the battle group to target them, Soviet bombers were planning to deliver their weapons through a cloud of chaff[11] and would also employ broadband noise, communication and deception jamming.[12]   F-14 aircrew spent a fair amount of time training against these electronic countermeasures. In addition, radar and missile engineers were constantly adapting U.S. weapons systems to better counter this threat by fighting through, working around, or – in the case of "home-on-jam"[13]– acting like an eastern martial artist and turning the threat against itself.

The Soviets used surveillance and signals intelligence equipment to help track the aircraft carriers, as well as a fleet of auxiliary vessels which would often tail Carrier Battle Groups. To counter the signals intelligence, carriers often trained by "pulling the plug" on their own transmissions, operating under what was called "EMCON" (or emissions control) conditions. But doing this also meant that the people operating and conducting flight operations on the carrier had to learn how to conduct business without all the high-tech electronic aids built over the decades. During takeoff, aircraft would stay low over the water and fly a pre-determined route while keeping all systems off or in standby and forgoing all transmissions. At a pre-determined location, the aircraft would climb to higher altitude and only then be allowed to start radiating.

Returning to the carrier was even more challenging. The E-2 Hawkeye airborne early warning aircraft would take the place of the carrier's air traffic control center, and would gather up the air wing far away from the carrier and then direct each aircraft to the carrier in a coded update of the carrier's expected recovery position. And nearly all day-time landings were conducted "zip-lip" (without radio communications) even when not in EMCON conditions. Talking on the radio was reserved for emergencies only. Because radio failures happen in all aircraft from time to time, knowing how to land safely without the benefit of a radio is something all pilots have to know. Expanding these procedures to operate sans electronic systems – making it more difficult for the Soviets to track our fleet – seemed only natural. Obviously, it is less useful to jam someone's communication when they are used to operating without.

A Solution: Vector Logic

Practicing to operate under reduced communications was beneficial, but aircrew fighting the outer-air-battle also needed a way to build and share situational awareness. The dynamics and speed of air warfare have historically led airmen to seek better ways to push more decision-making to "the edge"[14]. This could be accomplished through (1) defining more explicit rules of engagement (ROE) that codify the commander's intent, or (2) technically verifying an unknown target as hostile, or (3) through data links that allow aircraft to share situational awareness. "Power to the edge" could also be accomplished by training elite crews, trusting them to make the right decision in the absence of authoritative guidance. The dynamic nature of tactics at the point of contact, combined in this case with jet aircraft closure speeds, made it nearly impossible to centrally control outcomes, even when the Soviets were not trying to make it more difficult through electronic attack.

For this reason, the Navy fighter community developed "vector logic" – a tactic that helped outer-air-battle aircrew self-synchronize actions, communicating through data links and localized broadcast radio transmissions to help build and maintain situational awareness.

The AIM-54 Phoenix missile may have been built for this threat, but the system still needed cueing to be in position in time to challenge the bomber raids. The "Chain Saw" tactic relied on aerial refueling and knowledge of the adversary to intercept the threat at the greatest distance from the carrier. While Chain Saw was good in theory and did help change the battle group's mindset from point defense to a more extended defense, in reality, the situations were more complex. Intelligence is always imperfect, and while defending the carrier was important, in order to accomplish other assigned missions, carriers often found themselves operating well inside the adversary's threat ring. This meant that instead of a narrow threat axis, a carrier battle group would have to defend a threat sector resembling more a slice of pie. Assuming the threat would do all in its power (communications, chaff, barrage noise and smart jamming) to make that defense more difficult, fighter aircrew devised a self-synchronization communication strategy.

Accustomed to operating with minimal communications and assuming that it might be difficult to transmit back to the ship due to long range and enemy intrusion, fighter crews thought that they might at least be able to communicate locally – at short range – between themselves even while under attack. Each combat air patrol (CAP) would identify its station and targets with a bearing and range from the defended point (in this case, the carrier). If a fighter picked up an inbound bandit,[15] he would immediately commence an attack, declaring in a broadcast to all within range "33 DELTA IS HOT FOR FOUR IN 33 GOLF."[16] Other fighter aircrew in the vicinity would then build a mental model of the attack based on these broadcasts and flow to areas where needed. Aircraft would also report in a broadcast manner their weapons expenditure and successes, in addition to any "leakers," aircraft that got through and would therefore need to be addressed by assets closer to the carrier. These simple procedures allowed self-synchronization, under attack, taking into account the expected lack of a direct controlling authority.

Opportunity Cost of Super-Connectivity

Vector logic was developed to enable continued outer-air-battle operations under degraded conditions. While over reliance on unbroken and untarnished connectivity is subject to a lot of well-deserved worry these days, there is another caution: does the connectivity of senior leadership to the tactical battlefield invite micromanagement? Or, more importantly, does increased tactical level visibility lure senior leaders away from their primary role, managing operational and strategic level effects?

The military describes its planning and thought processes in three related, but distinct levels of war: strategic, operational, and tactical. In analogous terms, consider building a home. At the strategic level is the developer or architect with a vision and access to resources to execute that vision. The operational level would be the general contractor. He is responsible for bringing in the right players to execute the blueprint and synchronizing their efforts. Tactical level carpenters, plumbers, and electricians, actually build the home.

In warfare, since a tactical action can have strategic effect, (especially in our YouTube Age where video feed of an incident spreads like a virus within hours), some may be inclined to think that the three levels no longer apply, or at least that the dividing lines have blurred beyond distinction. While tactical actions can and will have effects at multiple levels, operational and strategic functions are still necessary. The architects' role, and that of the general contractor have not gone away.

The military is very adept at the operational level. This is why the U.S. government often defaults to the military when disaster (manmade or natural) strikes. That said, most military tools are built to address tactical level problems. We design better hammers, saws, wiring and pipes – and even promote our best carpenters to become general contractors (and even architects) – sometimes giving scant additional training and resources to those assuming the new role. But the more serious concern is the opportunity cost of allowing information technology to entice higher command to micromanage the tactical battle. What important and emergent functions of the higher command are no longer being performed when it focuses overly on the tactical level?

While vector logic was devised for a particular threat, the underlying idea was not foreign to naval practitioners who had grown up using "command by negation" C2 for their entire careers. Vector logic was just an extension of a familiar concept. In command by negation, a battle group commander established intent, and then delegated execution to sub-commanders for various functional missions such as: undersea warfare, air warfare, surface warfare, strike warfare etc. The battle group assumed the role of composite warfare commander (CWC), and after providing general guidance and mission objectives, monitored the execution flow and intervened only when and where he sensed the mission were going awry. These situations were rare and usually occurred when the CWC realized he had some information that his warfare commander did not, or when there was a conflicting interpretation of the tactical picture.

The proliferation of more precise and timely tactical-level situational awareness tools, all excellent in their own right, could cause operational level commanders not only to second guess subordinates (and thereby suppress initiative), but to be drawn into the tactical battle themselves, causing them to perhaps lose site of the big picture. This begs several questions. Are operational level commanders provided tools appropriate to the operational level mission? What are the operational and strategic effects sought? Do we have the means to address and measure these effects? These questions are particularly apt in today's operations, where disparate interagency, non-governmental and military groups find themselves together on a common "battlefield" with limited tools, metrics, and inevitable cultural barriers that challenge collaboration. This begs more questions. When dealing with disparate elements and differing scales, how do we determine what is essential for success? How do we train and educate our personnel to prevail in degraded conditions? How do we get to ground truth?

Seeking Ground Truth

Some leaders venture to the front to ascertain what's really going on with soldiers who have "boots on the ground." Other leaders step back to better take in the "big picture" … so they don't miss the forest for the trees. Which leader comes closer to the truth?

It is instructive to look at military insignia as a metaphor. Junior officers wear gold and silver bars, precious metals are found in the ground, and this is their focus, close to the ground. When they are promoted to "field grade," their bars are exchanged for oak leaves – found in tall trees – representing a more elevated view of the tactical picture. While still focused on the tactical battle, perhaps they're now able to see around corners. Colonels wear eagles, which fly well above the tree line, gaining perhaps a campaign-level perspective where several battles can be monitored simultaneously and – if need be – constrained resources can be appropriately parsed out. Finally, general and flag officers wear stars, representing the broadest view of all – perhaps even global.

For those who find themselves with "boots on the ground," calling for fires, there is nothing more important than completing the mission and surviving -- to either fight another day or return home. But when resources are constrained, an operational level commander may have to make hard decisions that prioritize one effort over another – euphemistically called risk management. In addition, an operational level commander may choose to halt or accelerate an effort on witnessing operational or strategic effects that may or may not be obvious at the lower scales of operation. The operational level of war is not merely the aggregation of tactical level actions, and this makes an operational level perspective different, often dramatically so, from the perspective needed at the tactical level. Let me explain with an analogy.

SCOOOOORREEEE!!

Similar to the outer air battle, association football (soccer in the U.S.) is fluid, dynamic, and success comes to those who better adapt on the fly. It's less about diagramming and executing the perfect play and more about self synchronized movement towards a common goal. It requires stamina and endurance, in addition to numerous ball handling and team skills. In other words, success requires tacticians who can adapt, modify, and execute at the point of action.

But what skill sets are required at the next higher level? To be a successful coach, additional knowledge, skills and abilities are needed. While players are immersed in the rhythm of the game, coaches are concerned with harnessing resources to win over time – to not only win a particular game, but have a successful season. And what about team owners or league officials? While an appreciation of the game itself is certainly desirable, different expertise needed at the enterprise level might include marketers, accountants, physicians, travel agents … people with business acumen, financiers. At this level, the actual play of the game is less important than television contracts, sponsorship, which jerseys to market and which cities to open up or close down based on potential support base or tax incentives.

Of course, one big difference between the sports example and the outer air battle is that the military DOES care who "wins the games" and the state of play on the field. But that doesn't mean that at the operational and strategic levels there aren't different effects that need to be assessed, requiring different tools and expertise. Unfortunately, our personnel plans often groom expert tacticians with “strong legs and lungs” for higher command, giving minimal attention to the skill sets needed to succeed at the operational and strategic levels.

Operational and strategic commanders do need a sense of the fight at the point of action, but even more, they need a sense of the battle at their own level; monitoring operational and strategic effects and providing value-added input – whether it’s proactive or by negation. Moreover, commanders must avoid the temptation to micromanage tactical-level actions just because information technology has provided them visibility to that level.

This caution applies in both directions. With the ability to network and move massive amounts of data, there’s an increased tendency to push more tactical data up to senior leadership for either background or decision making. Not only may this overload the higher-level commander, but allowing – or worse, demanding – it will act as a disincentive to subordinate level commanders who may become inclined to seek “mother may I” and lose the audacity required to take appropriate initiative. As stated previously, this loss will be starkly revealed when communications have been degraded or negated, most likely by electronic or cyber attack.

Mutual trust enables higher-level commanders to allow lower-level commanders to execute without detailed central control, and that allows lower-level commanders to operate autonomously in degraded conditions. And it is also imperative that we trust in the technology and systems that provide information both up and down chains of command – especially in a more dispersed force. Building and maintaining trust is crucial to success.

Building Trust

On a human level, militaries build trust by promoting a common culture. U.S. Marines do this better than most. They shepherd people from disparate backgrounds and through an intense bonding experience to make Marines. Knowing that all Marines share a common history and have all been through a similar crucible fosters an ensuring atmosphere of mutual trust within that fighting force.

In carrier aviation, trust is critical. A pilot has to trust that the aircraft has been maintained properly and is safe for flight. Aviators must also trust that the targets they are being asked to engage have been appropriately scrubbed by intelligence and higher authority as both fruitful and legitimate military targets. Building trust through the nurturing of common culture works at the human level, but how can we build trust in our systems and information sources? And if precision weapons and increased connectivity make it less useful to mass force elements, how will we nurture trust within a force that is by design more distributed or dispersed?

An interesting combination of human and technological trust takes place when an aircraft, cocked and ready on a carrier catapult, has to abort the launch late in the sequence. The aircraft is initially taxied into the catapult shuttle which will fling the aircraft from a dead start to about 150 knots in a few seconds. Physical linking to the shuttle takes place near the nose landing gear, out of the pilot's line-of-sight. So he or she must rely on people underneath the aircraft to ensure the aircraft is properly situated for launch. Once attached, the aircraft is put under tension, not unlike a sling shot being pulled back and held prior to release. The aircraft actually lurches forward – and is held back only by a small fitting that will soon be released. Before that happens, the pilot must bring the aircraft engines to full power so the plane will fly away safely upon catapult release. At this point, there is one final check of flight controls (rudders, spoilers etc); and if a problem is found during this final check, the launch must be aborted. Because the aircraft is figuratively sitting on the end of a lit fuse, the pilot who is trying to abort his launch cannot risk coming back on the throttles until he is sure he is no longer attached to the catapult – something he can not see – in case the holdback should fail and the aircraft inadvertently launches. The catapult officer, a fellow aviator, is charged to ensure the aircraft is released from the catapult. Once he has done so, that officer smartly walks directly in front of the aircraft – still at full power – before giving the pilot the signal to pull back on his throttles. This lets the pilot know that his fellow aviator is putting his own life on the line – to give the now apprehensive pilot the assurance that he is clear of the shuttle and it is safe to reduce power.

Humans tend to trust other humans who are willing to place their life on the line to save a friend or shipmate. This is perhaps why warriors who go to battle together form bonds not easily replicated elsewhere in society. Building on the human ability to deal with complexity and trust issues will be crucial to success in future warfare, especially when it comes to command, control and decision making. Trying to engineer the human out of the loop is a mistake.

Complexity and Living Systems

A carrier battle group conducting flight operations is like any other system made up of human decision makers – it’s a complex and adaptive living system. And challenges to living systems cannot be “solved” in the classic sense of the scientific method, but they can be bounded, that is, reduced to a core of more likely responses that are useful for planning and execution. We can explain this process in terms of Complexity Theory and Living Systems Theory. The first helps describe the nature of the challenge and the limits of what we can know or measure; while the second provides us a framework of how living systems deal with complexity, adapting their behavior to better their fitness for success.

Complexity

Complex systems are characterized by the on-going interaction of many continually changing interdependent variables. We can never fully know all of the variables nor how they will interact and, as a result, cannot precisely predict their behavior. Furthermore, these changing constellations of variables are interconnected in time, space and function, are shaped by what has gone before, and influence what follows. They can affect other systems in their geographic area – or in other areas that may appear far removed. Small actions in one system can produce disproportionately large effects in others, and vice versa. Finally, as this interconnectedness implies, elements of complex systems cannot be separated from the system as a whole without changing the character both of the element itself and of the system.

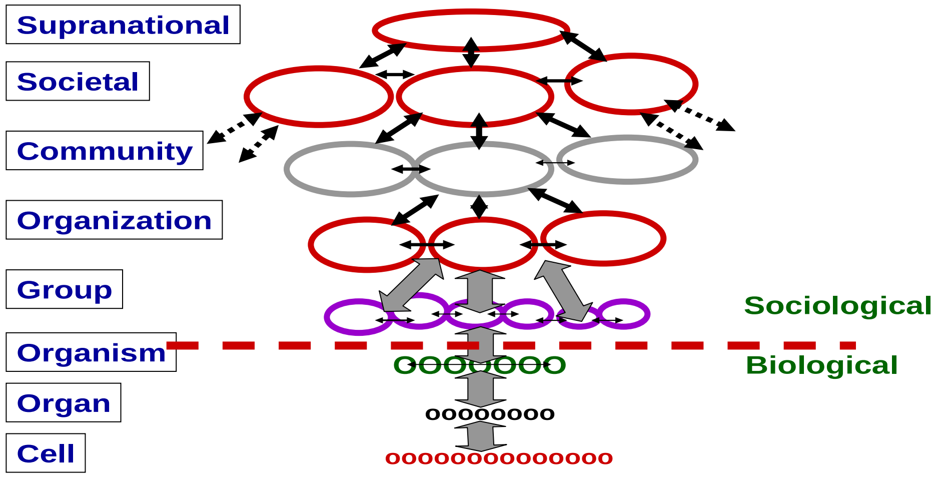
This complex “mess” can perhaps best be illustrated by the distinction between the English words “complicated” and “complex.” To use an example, a jet aircraft is complicated. Operators may understand every part of the cause and effect chain between advancing the throttle and the aircraft moving, but they know that advancing the throttle produces a predictable outcome. They also know from experience that output is proportional to input: the more power added, the more thrust is produced. The predictability and proportionality of input and output derive from the fact that the aircraft contains a series of known constants and linear cause and effect chains. It is complicated but not complex.

A piloted aircraft pitted against another piloted aircraft introduces “complexity.” We cannot know precisely what will happen in such an engagement because we cannot know all of the interdependent variables involved nor how they interact. What are the skills, psychological states, and experience levels of the pilots? What are the mission assignments and success metrics? Flight characteristics might be know, but what about the materiel condition of the aircraft and its systems. Is one pilot perhaps a new parent and therefore flying more conservatively? Is one flying with abandon after receiving a “Dear John” letter? We can never know all the permutations of complex systems nor be able to predict outcomes, but that does not mean the situation cannot be bounded.

And the piloted aircraft are not only complex but adaptive. They are continually absorbing new inputs and adapting their actions during the engagement. In brief, systems that involve people act more like living systems than mechanical systems.

Living Systems[17]

Efforts to try to treat or control people like mechanical systems will eventually fail. This is because human beings, human organizations and the security environment writ large are living, co-evolving complex adaptive systems. And all living systems are the current survivors of a Darwinian selection, products of a continuing, interlocking co-evolutionary process, that has taken two distinct forms: the biological evolution of cells, organs, animals and man; and the sociological evolution of groups, organizations, communities, societies, states, and the international security environment as a whole (Figure 1).



Based on James Grier Miller, Living Systems

Figure 1

The latter – the evolution of human organizations – is purposeful in that it is the aggregated fruit of human assessments, opinions and decisions, for better or worse. In essence, these living human systems learn and adapt as they deal with their changing human and physical environment. Paradoxically, this implies that the "stability" of any human system actually derives from a dynamic ability to learn, adapt and change. In fact, because the environment is always changing, stasis or the failure to evolve would signal a system's eventual demise. Because evolution implies "survival of the fittest," we should be able to understand why certain systems, organizations and societies survived or failed and identify the processes and capabilities that were critical to their survival, e.g., learning and adaptation. James Miller, in his book "Living Systems," identified 20 such "essential processes" common to all complex adaptive living systems.[18] These processes are reflected in the nature and actions of all human organizations and provide a starting point for any analysis of the systems or their actions.

Learning and Adaptation

The living systems theory highlights the need for all actors to adapt to a continually changing constellation of variables and in turn the need for a continuous process of learning – from the pilot in the outer air battle to national leaders – in fact, everywhere human decisions are required. Indeed, it is the ability to learn and adapt that is central both to the process of sociological evolution and in the way that humans cope with more immediate dangers. We can break this process down into five levels of adaptation:

1. Adaptive Action
2. Learning
3. Learning to learn
4. Defining/ redefining success, and
5. Co-adaptation.[19]

Adaptive action is the immediate tactical action and reaction as one actor, our fighter in the outer air battle, for example, observed change and adapted to the actions of others. Learning implies a process of evaluating this interaction for lessons to be learned and disseminating those lessons, for example debriefing the flight to intelligence officers who then synthesized the information to pass to follow-on aircrew. Learning to learn takes this the next step to address how we adapt the ongoing process of learning to better capture and disseminate the lessons learned; as in creating "Topgun" (Navy Fighter Weapons School) to provide an intense training course that simulated combat and helped accelerate experience. Defining or redefining "success" involves a higher level adaptation in which the original objectives, risk versus gains calculus, capabilities applied and approaches to achieving those objectives are reassessed and adapted to changing circumstances. For instance, at the end of the Cold War with the outer air battle threat to the aircraft carriers reduced, the U.S. Navy fighter community evolved their fighters to precision bombers to become more relevant to the new security situation. Finally, co-adaptation is the process of translating lessons learned from a set of external interactions into organizational and institutional changes to better deal with change. An example of this might be adversaries of the West building an anti-access capability to challenge a perceived power projection advantage, while Western forces adapt by building an emergent fleet of unmanned systems. Together, these overlapping levels of adaptation outline a process that occurs through multiple layers and many individual actors in the living system.

Conclusion

Most of this is not new. Warfare is complex; requiring humans to innovatively combine disparate elements to solve uncommon challenges. Ongoing complex, cross-domain action on the ground in Iraq, Afghanistan, and even Haiti has shattered any false hope that information technology alone will "solve" today's security challenges. There is no "black box" solution to complex problems, and the notion of removing imperfect humans from the loop and replacing them with robots, processors and better algorithms has been discredited as security experts now cast about for cultural experts and other social scientists to augment advanced technological systems. War still is and always will be a human endeavor, a battle of wills – and the adversary gets a vote.

We have also sobered up some from the notion that all hierarchy is bad, and that simply flattening an organizational chart will increase productivity at the tactical level, be that aircraft at the edge of the outer air battle or a commercial company bringing products to market. Speed may indeed be increased by flattening, but without good enterprise governance, sub-systems may sub-optimize to their own benefit and the overall system's demise. And if everyone is engaged in the tactical battle, who is monitoring the operational and strategic level battle – and do they have the tools and experience to succeed? There needs to be balance.

What may be new is the recognition that all these challenges are complex. The outer air battle informed us that in a dynamic living system, we must be prepared to learn and adapt to evolving circumstances. We must plan for graceful degradation as our systems and people are challenged by other peoples and systems.

Sometime after the implosion of the Soviet Union, U.S. defense switched from threat-based to capability-based analysis to justify defense acquisition programs. The intent was to take a more systems-based approach to functionally allocating requirements generation and solutions – and to find and reduce redundancy and overlap. An unfortunate byproduct of this approach was the notion that we could engineer systems in a threat vacuum. We developed capabilities and assumed that because we were at the top of a unipolar world, our only limitations were our own ingenuity and imagination. But no system stands alone, and warfare is defined through interactions with other complex adaptive humans and systems attempting to thwart any perceived advantages.

In the Cold War, both sides knew they were fighting a chess game. They understood they had a formidable adversary who was working to gain advantage. Neither side sought perfection, the situation was too dynamic, just a timely advantage. And we should never assume that systems will always work. We must have a plan for graceful degradation, both in peacetime and when directly challenged. We must keep the flashlight and candles near, for when the lights go out. And while we should embrace and champion advancements in technology that help better illuminate truth as our world shrinks, we should never forget that this is, ultimately, a human endeavor.

Of course, human roles will change and adapt, and technology may continue to drive human labor and services higher up the value chain. But if I was still flying, and had to return home on a dark night to the pitching deck of an aircraft carrier at sea, it would be comforting to know that there was still a sailor on board who could find the grease pencil, and who was trained to write backwards on glass -- even if just as a backup. We must expect and anticipate disruption and, in the end, rely on people – connected through social as well as physical networks – to properly address and bound our most dynamic challenges. We must engineer our people in, not out of our solutions.

[1] "Power to the Edge" David S. Albert & Richard E. Hayes. CCRP, June 2003.

[2] From , http://en.wikiquote.org/wiki/George_Santayana accessed 5 January 2010

[3] The author was an F-14 Tomcat radar intercept officer from 1981-2006 and these ideas are wholly his own and based primarily on personal experience.

[4] Aviation Data Management and Control System (ADMACS): ADMACS will use state-of-the-art information technology and decision support systems to automate collection and distribution of information, enabling aviation operations on board aircraft carriers to be accomplished in a more efficient manner.
(a). ADMACS Block 2: Is a shipboard aviation information management system providing carrier aviation planning, execution & readiness assessment using integrated decision aids and supporting systems built into a highly adaptive Net-Centric comprehensive system for sea & land. ADMACS Block 2 provides real time, fault tolerant (redundant), tactical information management system.
(b). ADMACS Block 3: This is new start for FY 2010. ADMACS Block 3 begins to automate data input through various system interfaces. It also adds intelligent agent and decision aides. These are added to the Block 2 architecture established during the development and installation. From http://www.dtic.mil/descriptivesum/Y2010/Navy/0604512N.pdf accessed 5 January 2010

[5] Thomas L. Friedman, The World Is Flat: A Brief History of the Twenty-First Century (Farrar, Straus, and Giroux, 2005)

[6] Greenland Iceland United Kingdom

[7] Because the U.S. SSBN force was the most survivable leg of the Nuclear Triad and , therefore, a war terminating core value to hold at risk

[8] Without air superiority to enable the conduct of multi-dimensional strategic ASW north of the GIUK Gap, there would have been no teeth in the Maritime Strategy that threatened Soviet core values like the submarine "bastions" and the defense infrastructure made vulnerable by all-weather medium attack strikes well behind the Central Front.

[9] NATO Air to Surface designations: AS-4 Kitchen and AS - 6 Kingfish

[10] Both systems are believed capable of attaining Mach 2.5-3.5 speeds (Mach equals the speed of sound at sea level), with an operational range of 150 nautical miles, although absolute maximum ranges are purportedly substantially greater. From "The Soviet Backfire Bomber: Capabilities and SALT Complications," dtd 4 Apr 1978. http://www.heritage.org/Research/RussiaandEurasia/upload/86857_1.pdf accessed 11 Jan 2010

[11] Chaff is a radar countermeasure in which aircraft or other targets spread a cloud of small, thin pieces of aluminum, metalized glass fiber or plastic, which either appears as a cluster of secondary targets on radar screens or swamps the screen with multiple returns. From http://en.wikipedia.org/wiki/Chaff_(countermeasure) accessed 11 January 2010.

[12] "Jammers can be broadly divided into two categories, noise jammers and deception jammers. In either instance the jammer comprises a receiver which listens for threat radars, a processor to make decisions and a tunable transmitter. The transmitter is automatically tuned to the frequency of the hostile transmission and jams it by transmitting a commanded signal.

A noise jammer will transmit a signal much like electrical noise which results in the radar return (echo) from the aircraft being obscured and at range may cause the aircraft to disappear from the threat operator's scope. At closer range however considerable power is required to outshout the return from the jamming aircraft and distinct radial lines termed strobes will appear on the victim's scope. The operator will know he is being jammed and may attempt to tune the radar to a slightly different frequency which may or may not defeat the jammer (a technique used to defeat an ECM system is termed an Electronic Counter Counter Measure or ECCM).

At some even closer range the victim radar will 'burn through' the jamming as the return becomes more powerful than the jamming transmission, the aircraft will then become distinguishable from the jamming.

A deception jammer doesn't attempt to conceal the presence of the aircraft but rather transmits signals very much like the real return to deceive the radar or its operator.

The number of deception jamming techniques is immense and every type of radar and specific design of a radar has some exploitable vulnerability.

Broadly, deception jammers can be divided into false target generators and track breakers."
From http://www.ausairpower.net/TE-RWR-ECM.html accessed 25 January 2010.

[13] Home-on-jam: (electronics) A feature that permits radar to track a jamming source in angle. From http://www.answers.com/topic/home-on-jam accessed 11 January 2010. "An anti-radiation missile (ARM) is a missile which is designed to detect and home in on an enemy radio emission source. Typically these are designed for use against an enemy radar, although jammers and even radios used for communication can also be targeted in this manner." From http://en.wikipedia.org/wiki/Anti-radiation_missile accessed 26 January 2010.

[14] "The duty of the fighter pilot is to patrol his area of the sky, and shoot down any enemy fighters in that area. Anything else is rubbish." Baron Manfred von Richthofen, 1917 from http://www.skygod.com/quotes/combat.html accessed 18 January 2010.

[15] An aircraft positively identified as hostile – the enemy.

[16] Translation: the CAP aircraft at bearing 330 at the 4th range ring has picked up and is prosecuting 4 inbound targets on the same bearing at the 7th range ring.

[17] Based on James Grier Miller, Living Systems, Denver, University of Colorado, 1995. pp. xix-xxv.

[18] The 20 essential processes or critical subsystems of a Living System are: the *boundary* which maintains the identity and culture of the system or organization, and protects it from the outside environment; the *reproducer* which ensures the system's continuation, the *ingestor* which brings matter-energy across the boundary for system sustenance, e.g. revenue and budget; the *distributor* which allocates the matter-energy throughout the system; the *converter* which adapts the matter-energy to the needs of the parts; the *producer* which generates the matter-energy; the *storager* which maintains and operating stock of matter-energy; and the *supporter* which takes care of housekeeping functions; the *extruder* which eliminates system waste products; the *motor* which moves the system

with relation to its environment; the *input transducer* which senses outside information and brings it into the system; *internal transducer* which senses internal system information and readies it for transmission within the system; *channel and net* which is the architecture that transfers signals between systems; *timer* which helps the decider with any time related actions; *decoder* which takes information from the input transducer and gives it a private code for the internal system; *associator* which helps the system learn by forming enduring associations among items of information in the system; *memory* which stores information in the system and retrieves it; *decider* which gives guidance, coordination, and control of the system; *encoder* which turns private code to external code for communicating outside the system; *output transducer* which transmits information from the system to the outside environment. Miller, p. xix.

[19] See Anne-Marie Grisogono and Edward Smith, "Warfighters to Coalitions: A Case Study in Multi-level Adaptation," Paper presented at the 11th ICCRTS, Cambridge, United Kingdom, 2006, and Anne-Marie Grisogono, Edward Smith and Mark Clemente, "Cajole and Coordinate? C2 in Whole of --Government, --Nation, and -Coalition Action," Paper for the 13th ICCRTS, Seattle, Washington, 2007.