How Can the U.S. Military Ensure that the speed of its decision making continues to keep pace with the accelerating speed of action on the battlefield due to artificial intelligence, automation, cyber weapons and high speed weapons?

The 5th Service for the 3rd Offset Strategy

Daniel L. Brown, Capt, USAF
E-3 Aircraft Commander
Daniel.brown.61@us.af.mil
323-459-7196

Byron K. Doan, Capt, USAF
Lead Fuse Design Engineer
Byron.doan.1@us.af.mil
850-883-0589

Michael T. Greer, Capt, USAF
ISR Instructor/Analyst
Michael.greer.12@us.af.mil
603-828-1879

Barron D. Stone, Capt, USAF
Branch Chief, Nuclear ISR Systems
Barron.stone@us.af.mil
321-494-0997

5 December 2016

How can the US military ensure the speed of it's decision making continues to keep pace with the accelerating speed of action on the battlefield due to 21st century technology?

Asking how C2 will change based on the 21st century battlefield technological improvements is an exercise in science fiction. We can list future technologies, such as hypersonic aircraft, railguns, artificial intelligence, and networked micro UAVs, but our assumptions about their capabilities and limitations may or may not be accurate. Assumptions about the functions of networked semi-autonomous sensor systems and AI are estimates at best. There were those who accurately predicted the capabilities of the 2016 internet in 1990, but who amongst them predicted the value of Twitter?

Because evolving C2 is iterative, this paper is not about the technology involved, but rather about the technological values that will guide development in the future. No matter how technology evolves, there are four things we can do to ensure that C2 remains able to remain relevant in the decades to come. They are:

1) Ensure the capability for **timely detection of new threats** through networked sensors which operate over a wider spectrum that we currently use
2) Use and trust **reliable artificial intelligence** for semi-autonomous data processing
3) Ensure that a **new generation of warfighters** is organized, trained, and equipped to interact with AI systems, commanding and controlling semi-autonomous operations faster than ever before
4) Have an **independent service branch** dedicated to maintaining an open flow of information across global networks and setting the pace for innovation

The rest of this paper will discuss some of the issues involved, but ultimately argue for DoD implementation of the above. Speculation is involved, but only to illustrate how the four basic ideas this paper proposes *could* apply to future scenarios.

Timely Detection of New Threats

In order for the C2 process to be effective, it first must continue to detect enemy intentions punctually and reliably. Airpower is proactive and not reactive. Nevertheless, the C2 process is an exercise in problem solving and thus first must observe and orient before it can and decide and act. Adversaries still have a vote on the most perfectly constructed and violently executed plan, and their reaction or capabilities should not be underestimated. DoD doctrine values detection capabilities and will continue to do so in the future, but to understand what detection capabilities the DoD should emphasize for future development it is important to understand 2 historical lessons.

First, detection of enemy intentions is not only decisive, it can literally counter other advantages in war. The significance of information superiority proving decisive in famous cases such as Midway are well known, but historical examples of information superiority offsetting force and material superiority in the past are not as well appreciated. The British ability to decipher German Enigma messages to their ships at sea included times and locations of attacks. This allowed the Royal Navy to dispatch their precious few destroyer squadrons wherever they were needed to protect the convoys and sink the U-boats. This helped break the Nazi blockade of England and turn the tide of WWII.

Second, the maximum time to detect enemy intentions will shorten as technology evolves. Cyber warfare and directed energy weapons will not only continue this trend, but completely destroy what we think to be an acceptable response time. Between the Civil War and

the Cold War, the necessary detection time shorted from days to minutes based on the critical threat being infantry columns and ICBMs respectively. The constant throughout was that the required detection time was known and based on the speed of the critical threat. Cyber warfare will decrease detection and response times by orders of magnitude. The US currently has no indications until the initial stages of a cyberattack. Creating time to warn the US government against an impending cyberattack should be a top national priority. Although it is uncomfortable to think about, the few minutes that the Cold War afforded its decision makers will be much longer than future commanders have.

Given the importance of detection and the short time for decision making in the future, the DoD must continue to improve both the bandwidth, resolution, and detail of its detection capabilities, which currently excel detecting in the electromagnetic, optical, and infrared spectrums. In the future it could be critical to our national security to detect the infinitesimal magnetic field created by the internal circuitry of a quadcopter, or a railgun electromagnetic pulse lasting less than a microsecond. The ability to deploy many networked microsensors close to a battlefield will aid in survivability and reliability.

However the next revolution in detection will be pattern recognition. It will aid networked sensors improving our ability to detect the signals we currently base our intelligence on and is the most likely base of a US cyberwarfare detection strategy in the immediate future. Even if the complete information about a program or file in a network cannot be determined in the available time, certain data about IP origin and previously seen subroutines and coding peculiarities within said file could be compiled quickly to identify a never-before-seen program as hostile. The fact that exponentially more data would have to be analyzed exponentially faster leads to the requirement for computer systems correspondingly faster.

Reliable Artificial Intelligence

The greater variety and growing number of sensors in the battlespace creates the opportunity to have greater situational awareness than ever before. But simply collecting huge amounts of data will not produce results - we need a way to way to quickly extract meaning. The overwhelming deluge of data will be impossibly large for humans to handle; artificial intelligence (AI) will be necessary to make sense of it. The AI will need to be context aware as it interprets and reacts to its surroundings.

Everyone that's ever interacted with Apple's 'Siri' knows conscious AI is decades away, however programs that do not even begin to approach the complexity and speed of a conscious AI can still incorporate information and recognize patterns from very diverse sources much faster than a human can. Today, financial traders exploit computer algorithms that make trades before a human can analyze the requisite data. These programs are iterative in nature, designed to make a good trade now rather than the perfect trade later, and have certain basic safeguards built in. Recognizing that Cyber Warfare has far greater consequences than high frequency trading and thus requires more robust safeguards, similar iterative programs will be required to analyze the diverse military situation and take basic defensive actions in air, space, and cyberspace, giving human operators the necessary time to strategize and win battles.

As AI progresses so will the required level of trust human users will need to have in AI systems to present them with the most accurate, relevant, and pertinent information for daily military operations. In the not too distant future, society will begin trusting lives to artificial

intelligence in the form of self-driving cars. Programmed values based on terabytes of information will make life or death split-second decisions that affect the lives of people both inside and outside the vehicle. The scale and level of reliability required for self-driving cars gives some idea of the complexity of a military AI. In the distant future, AI may progress to the point where it is able to make and act upon local decisions without operator intervention. High-speed threats may necessitate AI systems making decisions that result in kinetic and non-kinetic effects.

As this paradigm evolves, the human operators will no longer be the ones collecting information; they will define policies that direct how AI systems collect information and execute tasks. Cyberwarfare and C2 tactical operators will operate at what we now consider strategic levels to set those policies, requiring a change in the way our operators think. We will need to train our people to think in terms of computer based strategy and problem solving from the beginning rather than the current emphasis on learning unique tactical solutions first.

New Generation of Warfighters

Developing unique new sensors and integrating their information into a consolidated battle picture addresses one side of this issue: modernizing the systems and equipment used by our forces. The other component is modernizing organizations and individuals to harness the full potential of new systems and capabilities. The ultimate goal is optimizing human behaviors alongside automated AI data gathering and analysis systems. An ideal level of human-machine cooperation is one where each benefits from the other's strengths. Training operators to utilize AI problem solving tools will take time, but yield benefits.

The DoD will need to acknowledge the trend towards integration of AI systems, and understand that the relationship between operator and AI will require more complex coordination. Human decision makers will still factor into organizations, but improving AI systems will not only allow computers to compute the range of possible outcomes, but to facilitate the problem solving process. Operators will define an objective for computers to gather data, list solutions and run iterative simulations. The computer will gather its own inputs and present data to operators for further clarification. Highly evolved solutions will then be presented to operators for a decision requiring computer action. This process requires warfighters to focus brainpower on defining the problem rather than providing a solution. Ultimately, the critical decision point for operations will be shifted closer to the front than ever before.

Additionally, the DoD will need to recruit and train those to ask these crucial questions. Recruiting and training efforts should focus on cognitive ability, as decision speed will be limited by human response to machine inputs. Some may argue that certain cognitive skills cannot be taught, however we only know that there has not yet been a major impetus to teach those skills. Every improvement in aircraft performance in the 20th century has required operators to push past what was then considered to be the limits of human performance. Critical thinkers on every level will be a force multiplier in operations from the depths of the ocean to the edge of space.

By recruiting and developing individuals who understand the man-machine cooperation and forcing the critical decision point to be closer to the battlefield, the result will be an ultimately leaner military. A strategically trained warfighter will exert a span of control previously reserved for those in command of far more assets, in much the same way the British

codebreakers allowed the outsized Royal Navy to protect a far larger area of ocean. A force of strategically trained, AI assisted warfighters will react faster to changing scenarios than their adversaries, furnishing the ultimate advantage.

This highly technical and specialized force will look and think differently than the force today. Solving problems aided by artificial intelligence will be known as tactical thinking. Strategic thinking will generate new ideas on how to best use AI to develop new problem solving methods that will achieve a desired end-state. Just as aircraft technology and supporting doctrine grew to the point where a separate service was required, reliance on AI and cyber systems will require the creation of an organization designed to operate and dominate within the domain.

Independent Service Branch

In November of 2016 the DoD announced the impending creation of a new cyber-warfare joint command. The fact that worldwide network infrastructure is a domain over which the United States and its adversaries exert control is now universally recognized. The advantage the United States holds over its adversaries is primarily an informational one. The ability to drop a bomb within 18 inches of an aim-point is useless unless you know where to drop, when to drop, and precisely what type of kinetic effect you are trying to create. The US spends significant resources to guarantee information superiority. If the US loses that information superiority, the corresponding reduced efficiency of its limited stockpiles will be unable to create the desired effects.

For better or worse, DoD doctrine is as dependent on network superiority in 2016 as the doctrine of the Army and Navy was dependent on air superiority in 1946.

Additionally, US adversaries recognize this and see networks as a domain over which they can achieve parity with the US with the fewest resources expended. Adversary countries no longer have to build a squadron of aircraft or a destroyer to render the US impotent, when the necessary program can eliminate our ability to deliver ordinance at the necessary hour.
The main argument for an independent cyber service replacing a joint cyber command is doctrinal. Many statements about airpower are true when applied to the cyber domain. In particular the unique timescales over which a cyberwar would be fought *"necessitate that it be centrally controlled by [cyber operators]."*

To ensure our C2 is able to respond to the evolving pace of warfare, it must set the pace. The Air Force service traditions and organizational norms are optimized to spend decades and billions of dollars procuring weapons systems that require an hour from launch to delivery. Dominance over networks will be won or lost between the time the command is given for ICBM ignition and the time the ICBM clears the silo. A cyber MWS that takes even a year to implement could be useless, one that takes 5 years to implement would be laughable. A new service with new traditions and organizational norms is required.

Conclusion

In conclusion, this paper is not intended to be science fiction. Initial actions working towards timely detection of new threats, reliable artificial intelligence for data gathering, a new generation of warfighters using AI-assisted problem solving and an independent force can be implemented today. These ideas are not crafted to respond to any particular technology, but rather to utilize evolving technologies in a way to best fulfill US national security objectives.

Daniel L. Brown *daniel.brown.61@us.af.mil* *Comm:323-459-7196*