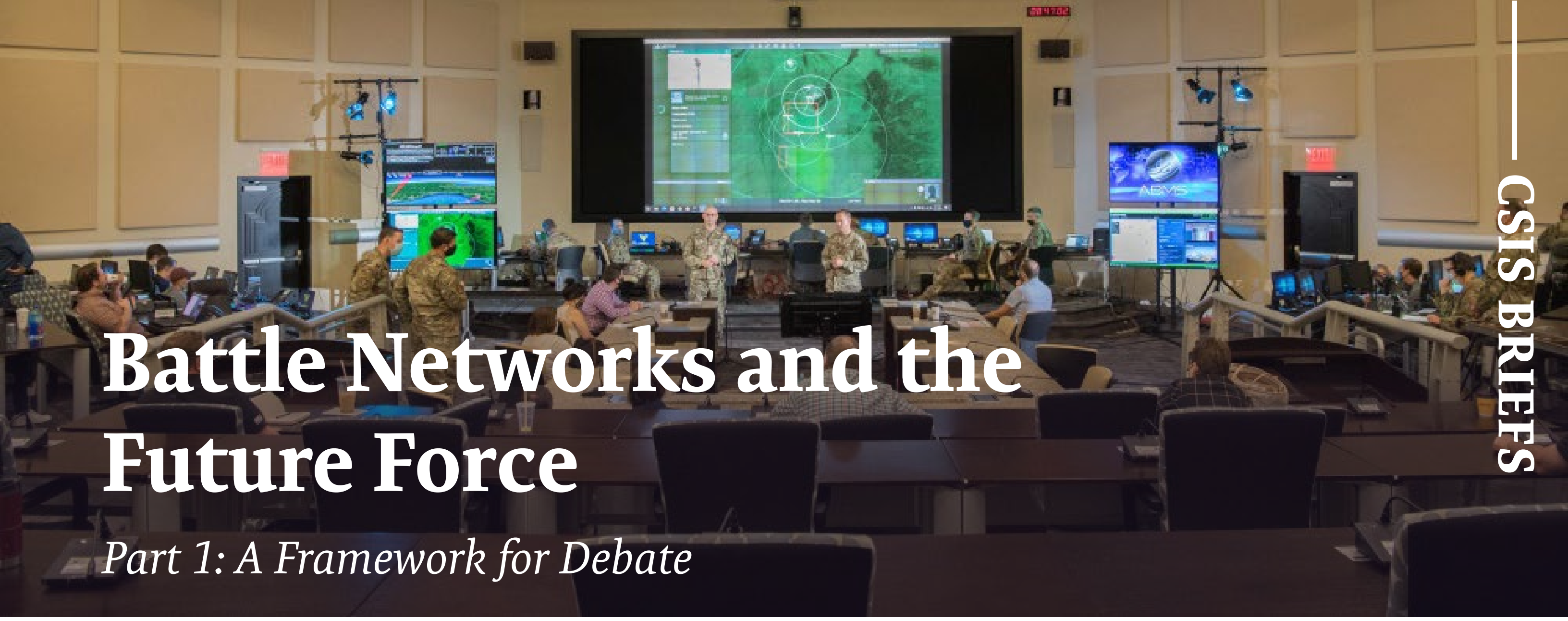


CSIS BRIEFS

Battle Networks and the Future Force

Part 1: A Framework for Debate

By Todd Harrison

AUGUST 2021

THE ISSUE

As the first in a two-part series that explores the future of battle networks in the U.S. military—what has become known as Joint All-Domain Command and Control (JADC2)—this paper examines the importance of battle networks to modern military operations and presents a framework of five functional elements that make up a battle network. This framework provides a common basis for conceptualizing and comparing existing systems and proposed new capabilities in terms of how they contribute to JADC2. The second brief in the series explores factors the Department of Defense (DoD) must contemplate in designing battle networks for the future force, including operational constraints, strategy and policy issues, and alternative acquisition approaches.

DEFINING THE CHALLENGE

Militaries use battle networks to detect what is happening on the battlefield, process that data into actionable information, decide on a course of action, communicate decisions among forces, act on those decisions, and assess the effectiveness of the actions taken. Battle networks are sometimes referred to as the "sensor-to-shooter kill chain" (or just the "**kill chain**"), and they are widely acknowledged as an increasingly important element of modern warfare.

While the importance of battle networks has garnered more attention in recent years, battle networks themselves are not new. Early battle networks used scouts, couriers, flags, telegraphs, and wired field telephones to transmit information and decisions among forces on the battlefield. More advanced battle networks began to emerge in World War II with the widespread adoption of technologies such as radar, sonar, radio communications, and aerial reconnaissance. As battle networks became faster, longer range, and more advantageous to militaries, the networks themselves also became an attractive target. As **John Stillion and Bryan Clark** have noted, the competition between battle networks was a key element of World War II, particularly in submarine and anti-submarine warfare.

What has changed in recent decades is the *amount of information* produced by sensors, the *speed and ubiquity* of communications, and the *magnitude* of tactical advantage possible from processing that information and making decisions faster than one's adversary—what some have called "**informationized**" warfare. In this "new way of war," advantage accrues to those that can see farther and clearer and act faster and at greater range—and **deny the other side** the ability to do the same.

The technological advances that have enabled this new way of operating are driven in part by commercial developments: lighter, cheaper, and higher fidelity sensors; increases in data throughput capacity and coverage from cellular, fiber, and satellite communications networks; massive cloud computing and data storage centers; and big data analytics, machine learning (ML), and artificial intelligence (AI) systems. The application of these commercial technologies to military battle networks has been widely acknowledged for more than three decades and has manifested itself in whole or in part in many different concepts, initiatives, strategies, and buzzwords over the years. This long line of thinking includes the ***Revolution in Military Affairs*** and what the Soviet's termed the ***Long-Range Reconnaissance-Strike Complex*** in the 1980s and 1990s; the ***Transformation Initiative, Network-Centric Warfare,*** and the ***Global Information Grid*** of the 1990s and 2000s; and the ***Third Offset Strategy*** of the 2010s (to name a few examples).

Despite the abundance of thinking and strategizing about the need to modernize the U.S. military's battle networks to increase speed, resilience, and interoperability, progress has been slow. As Chris Brose notes in his book ***Kill Chain***, "Rather than thinking in terms of buying new battle networks that could close the kill chain faster than ever, they [the U.S. military] thought in terms of buying incrementally better versions of the same platforms they had relied upon for decades—tanks, manned short-range aircraft, big satellites, and bigger ships." As Brose goes on to discuss, the focus on buying next-generation platforms rather than the sensors, payloads, and communications systems needed to make both existing and next-generation platforms work together more effectively is a deep cultural limitation of the military. It is the root cause of many interoperability limitations present in the force today, such as the inability of the U.S. Air Force's two fifth-generation fighters (the F-22 and F-35) to communicate directly with one another.

To address some interoperability issues, DoD is using workarounds, such as **U-2s** equipped with a communications payload that connects F-22s and F-35s with each other and with units on the ground. Similarly, the **Battlefield Airborne Communication Node** (BACN) can be flown on platforms such as the RQ-4 and E-11 to act as a communications gateway to connect aircraft and users on the ground using various tactical data links, such as Link 16 and the Situational Awareness Data Link (SADL). Workarounds such as these are a necessary first step, but they fall short of achieving the full vision of a mesh network that allows dynamic and resilient interoperability across military services, domains, and allied and partner forces.

CURRENT EFFORTS

The military is now at a critical point in architecting the battle networks of the future. DoD's overarching concept for this is known as Joint All Domain Command and Control (JADC2), and on May 13, 2021, Defense Secretary Lloyd Austin **officially signed** the military's JADC2 implementation strategy. Within the JADC2 concept, however, are multiple overlapping and sometimes contradictory efforts. The Air Force is pursuing the Advanced Battle Management System (ABMS), which started out as a replacement for the aging fleet of **E-8C Joint Surveillance Target Attack Radar System** (JSTARS) aircraft and morphed into a program to develop a "**secure, military digital network environment,**" but the program remains **ill-defined** in terms of which elements of the battle network it is building. For several years, the U.S. Navy has been developing and expanding its **Naval Integrated Fire Control-Counter Air (NIFC-CA)** architecture to integrate more platforms, sensors, and weapons, including the F-35, Aegis ships, and SM-6 anti-aircraft missiles. The Navy is also exploring its own future network architecture through Project Overmatch, which is intended "**to enable a Navy that swarms the sea, delivering synchronized lethal and nonlethal effects from near-and-far, every axis, and every domain**." The U.S. Army is taking a more incremental approach through its Project Convergence, which it bills as a "**campaign of learning organized around a continuous, structured series of demonstrations and experiments.**" The Army is also experimenting with the **Terrestrial Layer System**, which is intended to network a range of sensors—including intelligence agency sensors—to enable precision kinetic, electronic, and cyberattacks, and the service has begun initial production of its **Integrated Battle Command System (IBCS)**.

Beyond the military departments, the Joint Staff, the Office of the Under Secretary of Defense for Research and Engineering (OSD/R&E), Special Operations Command (SOCOM), and the Defense Advanced Research Projects Agency (DARPA) each have ongoing initiatives related to JADC2. The Joint Staff is tasked with developing an overall **strategy for JADC2** and leading a joint cross-functional team on the subject. OSD/R&E has a research effort known as **Fully Networked Command, Control, and Communications** (FNC3) that is initially focused on developing resilient and diversified communication paths for future battle networks. SOCOM is working on multiple initiatives to increase interoperability among forces, such as a **data fabric** and data management environment for special operations forces. DARPA has developed a concept known as **Mosaic Warfare** that aims "to turn complexity into a powerful new asymmetric weapon via rapidly composable networks of low-cost sensors, multi-domain command and control nodes, and cooperative manned and unmanned systems." As part of this effort, DARPA has **sponsored a series of projects** that use AI to turn raw sensor data into actionable information, to connect radios that otherwise are not compatible, and to perform airspace deconfliction.

COMPLICATING FACTORS

While many programs and activities are simultaneously underway across DoD, a major impediment to making meaningful progress is that **no one "owns" the overall JADC2 mission area**. Each of the military services owns their respective programs, platforms, and battle networks (and the budgets that fund them), but there is no effective forcing function that ensures the services' systems will be able to work together. For example, in ABMS, the Air Force is developing a system that may work well for connecting a few thousand aircraft, but the same system **may not work well** for connecting hundreds of thousands of soldiers (and their equipment) on the ground. And if the Army and Navy develop their own independent battle networks, connecting them to ABMS may end up being an afterthought or, worse, an unfunded requirement. The risk in the current approach is that each service, COCOM, or agency goes in its own direction and develops multiple stove-piped networks that do not allow the kind of interoperability and resilience that would be possible with a more coordinated approach.

Further complicating matters, the debate over JADC2 is obscured in the generic language used to describe the vision, the technologies being developed, and the programs executing the services' plans. While the need for JADC2 is well established and articulated, in many cases, the military services and Congress appear to be talking past each other when it comes to specific programs and activities.

The following sections provide a framework for discussing battle networks and the various payloads, platforms, and other components that comprise them. This framework is intended to provide a common lexicon for comparing and evaluating different concepts and programs, and it provides an overview of the various options available in each functional element. It does not provide specific recommendations on which options should be pursued. Many competing ideas already exist for how to build the battle networks of the future and what technologies should or should not be incorporated. This paper aims to raise the level of debate by offering a framework by which competing ideas can be compared, and roles and missions can be more precisely and deliberately articulated. The second paper in this series explores the operational, strategy and policy, and acquisition approaches senior leaders should consider when designing and building battle networks for the future force.

DEFINING A BATTLE NETWORK: FIVE FUNCTIONAL ELEMENTS

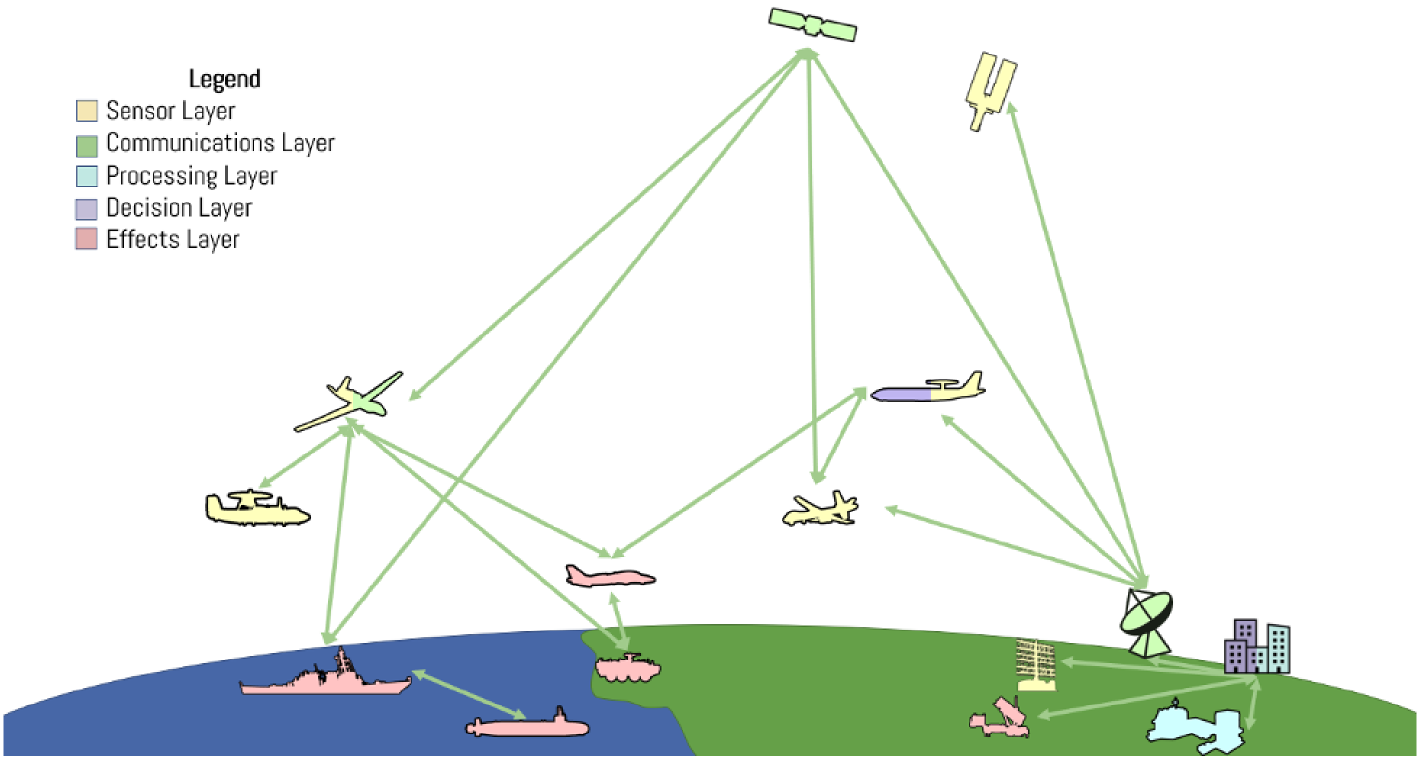
The framework proposed in this paper divides the component parts of a battle network into five functional elements, shown in Figure 1. Within each functional element, a combination of people, processes, and tools (i.e., technology) govern how the element works and the capabilities it can provide in the overall battle network. Each element of the network can include multiple types of platforms and payloads, and some of these platforms and payloads can be part of multiple functional elements simultaneously. For example, an E-3 AWACS aircraft can be part of the sensor and processing functional elements in a battle network because it houses a powerful radar used to detect and track aircraft and the computer systems and personnel needed to process and analyze that data in real time.

SENSOR ELEMENT

The functional purpose of the sensor element is to collect data on what is happening in the battlespace. This data can be used to detect and geolocate forces, identify who or what is involved, characterize the activities or types of forces being used, and track forces as they move around the battlespace. The sensor element can also be used to assess the effectiveness of actions taken—what is commonly known as battle damage assessment. The targets for data collection can include adversary forces, friendly forces, and non-combatants, and one of the most important roles of the sensor element is to distinguish among these.

Operators can use a variety of sensor technologies to acquire the desired data. Active sensors, such as active

Figure 1: Example Diagram of the Five Functional Elements of a Battle Network



Source: Based on author's own creation.

scanning radar and sonar, emit a source of energy and measure the reflected returns of that energy from an object to determine its location, size, relative motion, or other characteristics. Passive sensors, such as optical and infrared cameras or passive radar and sonar, rely on the collection of energy emitted by an object or reflected from natural sources. Active sensors can potentially be detected by an adversary and give away the location of the sensor and how it is being used, whereas passive sensors can operate with a lower probability of detection.

Sensors can be used in-domain or cross-domain depending on their capabilities and the needs of the user. Table 1 provides a crosswalk with some examples of specific sensor platforms, including both military and commercial systems. For example, tracking moving targets on the ground can be accomplished by many different types of sensors. Ground-based sensors can detect some movements, but they are limited in range to a relatively small area around the sensor itself. Airborne sensors can monitor a much broader area and provide persistent tracking of ground targets, but their use can be limited by weather conditions, aircraft flight duration, adversary air defenses, and the maximum effective range of the sensors, which scales with altitude. Synthetic aperture radar (SAR) satellites can also detect and track moving targets on the ground without the same range, weather, overflight, or flight duration limitations as aircraft, but continuous coverage of an area from space requires a large constellation of satellites in low Earth orbit (LEO) because satellites in LEO are in constant motion relative to the surface of the Earth.

COMMUNICATIONS ELEMENT

The communications element of battle networks often receives the most attention because it provides the data links that pass information among systems and operators. The information transmitted can include voice, video, one-way data broadcasts, or two-way data links. Raw data from high-fidelity sensors often requires high data rate communication links, whereas compressed data, processed data, or telemetry can use significantly lower data rates.

The physical means of communication can be through wired (copper or fiber), radio frequency (RF), or free-space laser communication (i.e., lasercom). Wired links can only connect fixed sites within the ground domain, whereas mobile and cross-domain data links require RF or lasercom. Communication systems use a wide range of encryption and waveforms, which can be unique to a

Table 1: Examples of In-Domain and Cross-Domain Sensor Applications

		SENSING FROM:				
		MARITIME (SUBSURFACE)	MARITIME (SURFACE)	GROUND	AIRBORNE	SPACE
SENSING TO:	MARITIME (SUBSURFACE)	Towed Array Sonar (TB-29X)	Hull-Mounted Sonar (AN/SQS-53C)		Maritime Patrol Aircraft with Sonobuoys (P-3, P-8)	
	MARITIME (SURFACE)	Towed Array Sonar (TB-29X)	Hull-Mounted Sonar (AN/SQS-53C)	Over-the-Horizon Radar (Jindalee Radar Network)	Maritime Patrol Aircraft (P-3, P-8)	Synthetic Aperture Radar (SAR) Satellites (Umbra, Orbital Effects, Capella)
	GROUND			Acoustic, Seismic, Optical, and Infrared (Unattended Ground Sensor)	Optical, Infrared, and Radar ISR Aircraft (E-8C, MQ-9, U-2, RQ-4)	SAR, Electro Optical, and RF Monitoring Satellites (Digital Globe, Planet, Hawkeye360**)**
	AIRBORNE		Ship-Mounted Radar (AN/SPY-1)	Surface-to-Air radar systems (AN/MPQ-65 passive radar, AN/TPY-2)	Airborne Warning and Control Aircraft (E-2D, E-3)	Missile Warning Satellites (SBIRS)
	SPACE		Ship-Mounted Radar (AN/SPY-1)	Radar and Optical Telescopes for Space Domain Awareness (Space Fence, LeoLabs)		Space Domain Awareness Satellites (GSSAP**,** SBSS)

Source: Author's own research and analysis.

particular mission area or system. Previous efforts, such as the **Joint Tactical Radio System** (JTRS) and the related Software Communications Architecture (SCA), attempted to mandate compatibility across communications systems with **limited success**. Gateways (or teleports) can be used to connect systems across a variety of protocols and standards and act as translators between otherwise incompatible radios. For example, the Air Force envisions aerial refueling aircraft such as the **KC-46 serving as flying gateways** that connect aircraft inside adversary air defenses with other parts of the battle network.

The military must weigh several factors when selecting the best types of communication links to use for a particular mission, including: latency; probability of detection and intercept; and resilience to jamming, spoofing, and weather disruptions. Latency is the roundtrip time it takes for data to travel between systems, and this can be a factor for missions where real-time data is critical, such as passing tracking and targeting data for air and missile defense. While RF, fiber, and lasercom links operate at near the speed of light, transit times can start to add up over long distances. The transit time to a satellite in geostationary orbit (GEO) and back to Earth, for example, is roughly 0.25 seconds. If multiple hops between satellites in GEO are needed to close a link, the total round trip latency can rise above 0.5 seconds—a noticeable delay for applications such as voice or video communications. The roundtrip time to satellites in LEO, however, is on the order of 0.01 seconds, depending on the altitude of the satellite and the look angle of the user.

RF communication links, whether direct between users or relayed through airborne or satellite communications systems, are vulnerable to detection, interception, and interference. **Various methods** are available to make RF signals more protected from these threats, such as using frequency-hopping spread spectrum waveforms, antenna nulling, adaptive filtering, and high-gain/narrow beamwidth antennas. RF signals are also bandwidth limited by the range of frequencies allocated for their use to help avoid interference with other military and civilian signals. Depending on the frequency band being used, **atmospheric attenuation**, **weather conditions**, **solar flares**, or other natural forms of interference can degrade communications. Wired communications systems, including fiberoptic cables, do not have the same bandwidth limitations as RF signals because more lines can often be run along the same path as needed, but wired communications remain vulnerable to detection, interception, and interference through physical tampering along cable routes or cyberattacks that target routers or terminals in the network.

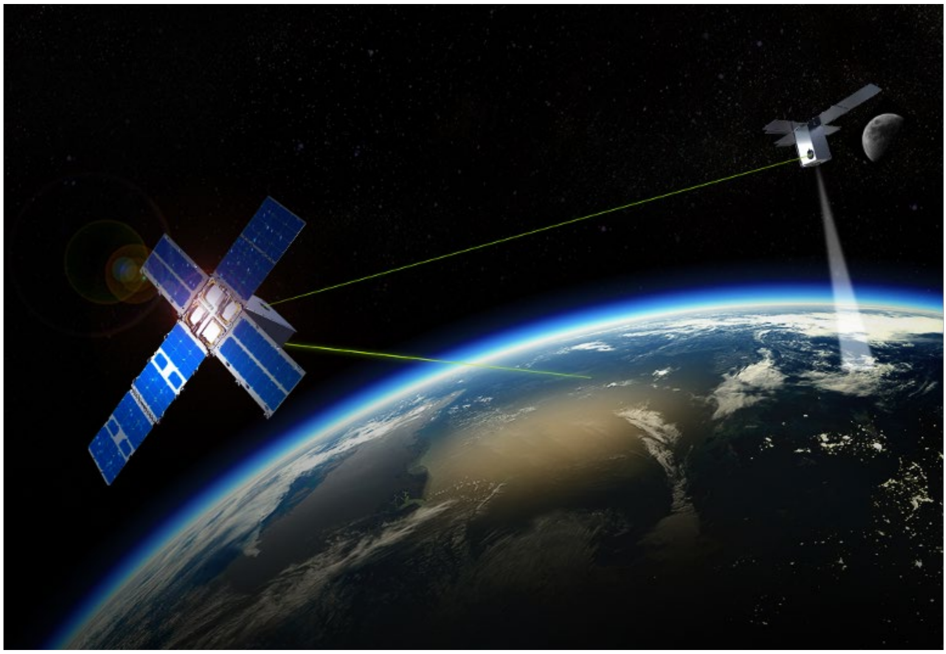
Lasercom systems can overcome many of the limitations of RF and wired communications. Lasercom links are inherently protected from detection, interception, and interference because of the extremely **narrow beamwidth** of the laser and the narrow field of view of the receiver. This limits an adversary from being able to detect, intercept, jam, or otherwise interfere with a transmission unless it is physically located within the beam. However, the extremely narrow beamwidth of lasercom links also means that they are not ideal for broadcast communications. Whereas an RF link can be transmitted across a broad area for many users simultaneously, lasercom links are best suited for point-to-point communications that require dedicated high data rate links. Lasercom links that transit through the atmosphere (as opposed to space-to-space lasercom links) are subject to atmosphere distortion and weather disruptions, but lasercom links between space and airborne platforms can avoid much of the atmosphere, depending on the altitude of the aircraft involved.

Space-based lasercom was a key component of the Air Force's Transformational Satellite Communications (TSAT) program that began in 2003, but that program was **canceled in 2009** without fielding any satellites. Despite this setback, progress on space-based lasercom continued in the decade that followed both within and outside of government programs, such as the **2020 demonstration** by General Atomics and Tesat-Spacecom of an airborne lasercom communications system. This demonstration connected an MQ-9 Reaper with a satellite in geostationary orbit using a lasercom link. The latest generation of **SpaceX's Starlink communications satellites** is equipped with lasercom crosslinks for passing data directly between satellites. The Space Development Agency (SDA) initiated development of a constellation of satellites in LEO that plan to use lasercom for high data rate links, and it funded **a pair of satellites** with infrared and lasercom payloads to demonstrate the technology, shown in Figure 2. **DARPA's Blackjack program** separately funded a lasercom demonstration on its Mandrake 2 mission. Both sets of satellites launched together as part of a ridesharing mission on June 30, 2021 and, as of this writing, are undergoing initial testing and assessment.

PROCESSING ELEMENT

Perhaps one of the most overlooked but critically important functional elements of a battle network is the processing element. The processing element is used to analyze, aggregate, and synthesize data from a variety of sensor sources to inform decisions. For example, raw data from SAR systems must be processed to produce radar images and to identify objects or movements of interest in the battlespace. Processing can also be used to compress data before transmission, to filter or flag data of potential interest to decisionmakers, and to produce specific intelligence products. Commercial companies, for example, have developed **algorithms** that analyze satellite imagery to count the number of cars in a parking lot or the number of ships in an area. Importantly, the output of

Figure 2: Rendering of the General Atomics and Space Development Agency Lasercom Demonstration Mission



Source: General Atomics Electromagnetic Systems.

the processing element can sometimes be a set of numbers (with statistical confidence parameters) rather than an image or qualitative assessment.

A key discriminator in the processing element is where the processing occurs: on-board the sensor, in the cloud, or at the tactical edge. The platforms that carry some sensors may also have sufficient size, weight, and power (SWAP) to carry the computational components needed to process the data they produce before transmitting it. For example, imagers may have the processing capacity to compress data (and greatly reduce communications requirements), and radars may have on-board processors to filter and compute initial products from the raw data they produce. On-board processing has many advantages in terms of increasing the speed of analysis, automating some sensor cueing and tracking functions, and reducing communications requirements. But for some platforms, particularly smaller aircraft and satellites, SWAP is highly limited, and it may make more operational and economic sense to perform the processing separate from the sensing platform.

Cloud-based processing offers the advantage of essentially unlimited processing and data storage capacity without the SWAP limitations of many platforms. Sensors can transmit raw or partially processed information to data centers on the ground for final processing and analysis. In the past two decades, commercial firms have built **massive data centers around the globe** with processing, storage capacity, and (in some cases) reliability far beyond the scope of the **data centers owned and operated** by the U.S. military and intelligence agencies. DoD's **Cloud Strategy**, released in December 2018, notes the importance of cloud computing as a key differentiator of mission success. However, the main contract to build a common cloud computing environment for DoD, known as the Joint Enterprise Defense Infrastructure (JEDI), was **mired in legal disputes** for years and ultimately **canceled**.

Some military missions require high-frequency or low-latency processed data that the communication links to and from cloud computing centers may not be able to support. Moreover, in a contested communications environment, these long-haul data links may be degraded or disrupted, especially for forces operating at the edge or within the contested battlespace. These forces may need sensors that link directly to other platforms in-theater with sufficient processing capacity to close the sensor-to-shooter kill chain quickly and reliably. Airborne or satellite sensors can downlink their data directly to user terminals on the ground that process the data onsite without relying on other data links. Stealthy aircraft in contested airspace can relay their sensor data to non-stealthy aircraft operating just outside the threat area for processing and dissemination, leveraging systems such as the **Open Mission Systems** computer on the U-2 or the **Advanced Display Core Processor (ADCP) II** being fielded in the new F-15EX. And aerial refueling aircraft can double as communication gateways and data processing and distribution centers at the tactical edge, given their size and power generation capacity.

DECISION ELEMENT

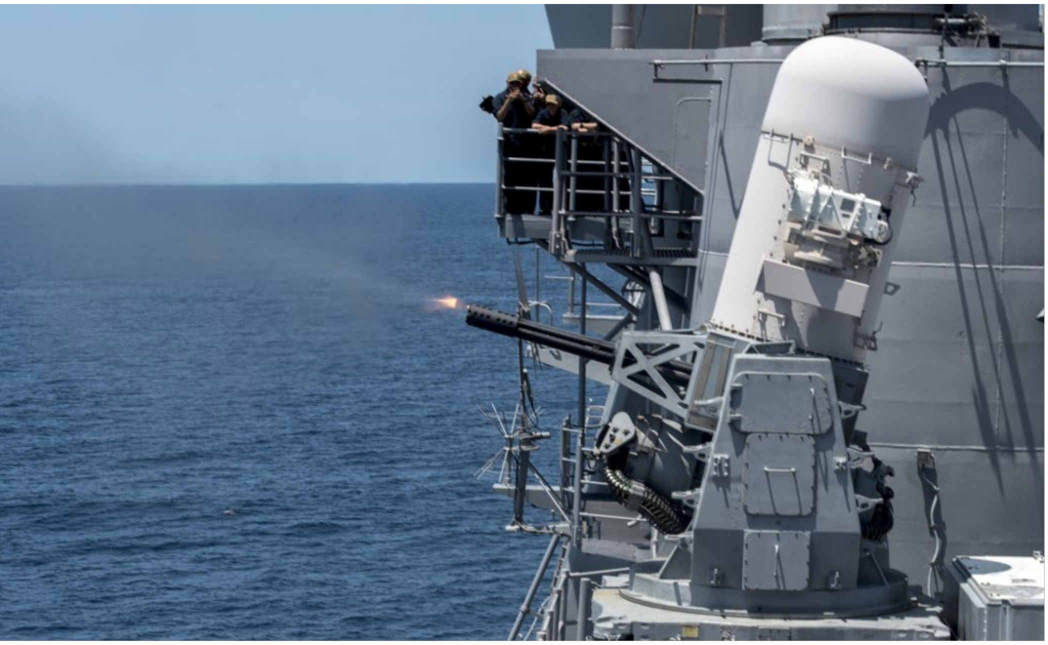
The decision element is perhaps the most important part of the battle network because it is where information is translated into action. Where the decision occurs, how it is made, and who is involved depends on what types of actions are being considered. For the foreseeable future, major decisions, such as the use of lethal force, will likely involve a human-in-the-loop at some level, and historically this has been the default for most decisions in battle networks. Human-in-the-loop decisionmaking can still involve many forms of computer-assisted or artificial intelligence and machine learning (AI/ML) augmented processes to better inform decisions and accelerate the process.

Virtually all engagements **beyond visual range** already use computer-assisted decisionmaking. The human eye can only detect objects at roughly two miles or less in distance, and beyond this range, operators must rely on electronic sensors of some form. For example, a fighter jet in contested airspace will seek to engage adversary aircraft at the maximum range possible—well beyond two miles. The aircraft's radar will detect other aircraft in the area and compare their signatures to others in its database to determine the types of aircraft involved and whether they are friend, foe, or non-combatant. This information is displayed on the fighter jet's cockpit display, and it can be corroborated with data from other sensors to increase the confidence of the operator in the result. But ultimately, the pilot can decide to fire weapons based solely on the recommendations provided by its computer systems without direct confirmation.

AI/ML systems go a step further to assist decisionmaking and automate some decisions that do not necessarily require a human-in-the-loop. AI/ML systems can be used in the decision element to rapidly analyze data to find information or patterns of interest—and they can dynamically evolve the way they analyze and interpret data as more information is gathered. In the fighter jet example above, an AI/ML algorithm running on the radar data could detect new signatures or patterns in the data not already cataloged in its databases, such as aircraft using electronic countermeasures not seen before, and update its algorithms during flight based on this new information. The advantage of AI/ML systems is the ability to form connections in data that humans may miss and to analyze large volumes of data in a fraction of the time it would take humans to accomplish the same task. For relatively benign decisions, such as redirecting sensors to look for something or reallocating bandwidth in a jamming environment, AI/ML systems can be used to make decisions without human input. This helps off-load work from human operators so that they can focus their mental energies on the processes and decisions where humans are most needed.

For many types of military missions, the slowest part of the battle network can be the decision element, and for some applications it may not be feasible to have a human-in-the-loop because of the rapid response time required to be effective. This is already the case with many **close-in air and missile defenses**, such as the Close-In Weapons System (CWIS) shown in Figure 3. This raises several important policy issues about the role of AI/ML systems in future battle networks and the levels of automation that policymakers are comfortable with in different situations.

Figure 3: USS Vella Gulf (CG 72) Fires Its Close-In Weapons System (CWIS), July 10, 2019



Source: U.S. Navy photo by Mass Communication Specialist/Petty Officer 3rd Class Gian Prabhudas via Defense Visual Information Distribution Service.

The quality and confidence of decisions made by AI/ML systems—and humans as well—can be improved by increasing connectivity to additional sensors and data processing capacity. This higher level of connectivity may shift the balance in favor of automating more decisions and higher-level decisions in future battle networks. The strategic and policy implications of using AI/ML systems in decisionmaking are discussed in more detail in the second paper of this series.

EFFECTS ELEMENT

The fifth and final element of a battle network is where information is turned into effects in the battlespace. These effects include both kinetic fires, which physically damage or destroy adversary forces, and non-kinetic fires, such as electronic warfare, directed energy weapons, or cyberattacks. A key part of joint operations is the ability to coordinate these effects across domains in time and location to generate the desired effects against an adversary at minimal risk to friendly forces and non-combatants. Battle networks are how this coordination occurs. Cross-domain effects—where forces in one domain launch attacks against forces in another domain—are a particularly effective way to leverage asymmetric advantages and keep an adversary off balance. The **air campaign in the opening days of the First Gulf War in 1991** is a classic example where the U.S. military leveraged its advantages in air and space to achieve greater effects on the ground than ground forces alone.

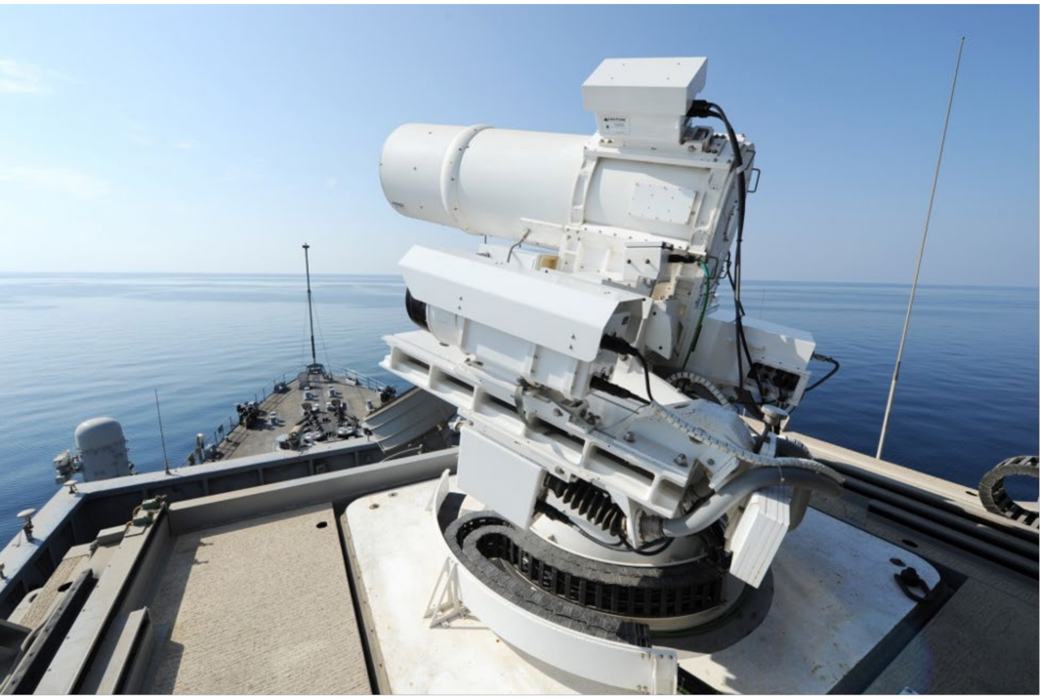
When selecting the best method to generate effects in an engagement, several factors must be considered, including: the range and number of targets, the threat environment, the potential for collateral damage, the need for post-attack damage assessment, and whether public visibility, reversibility, and attribution are a concern. Short-range kinetic weapons, such as the **Joint Direct Attack Munition** (JDAM), are ideal when a large volume of low-cost fires is needed and targets may be highly mobile. Long-range and stand-off kinetic weapons, such as the **Long Range**

Anti-Surface Cruise Missile (LRASM) and the **Joint Air-to-Surface Standoff Missile** (JASSM), are better suited for small numbers of high-value targets and more contested environments where not all delivery platforms may be able to penetrate adversary defenses. **Precision-guided weapons** are used to reduce the number of weapons and delivery platforms required and the risks of collateral damage, especially for targets in dense urban areas. Kinetic weapons generally produce visible and permanent effects that allow for battle damage assessment using the sensor element of a battle network.

Non-kinetic methods of attack, such as cyberattacks, directed energy weapons, and electronic warfare, can achieve some of the same effects as kinetic weapons through different means. For example, instead of attacking a threatening drone or small ship with guns or missiles, operators could target it with a **high-powered laser**, such as the system shown in Figure 4. For some non-kinetic forms of attack, such as jamming, the effects can be reversible, creating temporary effects at the time and place they are needed. For some types of non-kinetic attack, third parties may not be able to see that an attack has occurred, or the party being attacked may not know right away who is attacking. For these reasons, non-kinetic attacks may be perceived as less escalatory in some situations, although this remains **a point of debate**. It can be difficult to determine if some non-kinetic forms of attack are effective, particularly if the effects are not publicly visible. And some methods of attack—such as exploiting **zero-day vulnerabilities** in a cyberattack—may have a limited period of effectiveness before an adversary develops defenses against them. For these reasons, operators may be reluctant to rely on non-kinetic effects that cannot be verified when kinetic effects can achieve the same results.

An important consideration when building and integrating the effects element of a battle network is the dynamic process of matching weapons to targets in an evolving battlespace. This requires close integration among the sensor, decision, and effects elements to optimize how targets are selected and prioritized based on the types of effects desired and the delivery methods available. In the battle networks of the future, this process could be much faster and more dynamic than it is today, with targets being identified and prosecuted on a rolling basis by swarms of crewed and remotely crewed systems across all domains. **As some have postulated**, it could be more like a commercial ride-sharing service (e.g., Uber or Lyft) that continually matches riders with drivers based on their relative locations, projected paths, and number of people and seats available. But this vision of a highly optimized and rapidly adapting effects element cannot be achieved without resilient and interoperable battle networks.

Figure 4: Laser Weapon System (LaWS) Undergoing Testing on the USS Ponce, November 17, 2014



Source: U.S. Navy photo by John F. Williams via Defense Visual Information Distribution Service.

FINAL THOUGHTS

The above sections provide a framework for defining the five functional elements that make up a battle network and the various payloads, platforms, and other components that comprise them. The sensor element collects data on what is happening in the battlespace and passes it to the processing element, where it analyzes, aggregates, and synthesizes data from a variety of sources. The decision element then uses data products to inform decisions and translate information into action in the effects element of the battle network. And the communications element allows all the other elements to pass data and decisions freely across the battlespace.

Perhaps the most important insight this framework yields is that the battle network of the future is not one network—it is a network of networks. Rather than using a traditional hub-and-spoke network architecture, the battle networks of the future should be dynamically reconfigurable mesh networks that are better capable of adapting to threats and disruptions. These networks can split into tactical sub-networks as necessary, reroute data through different systems and alternative pathways in unpredictable ways, and reconnect into larger networks as opportunities emerge. The communications element is the essential component that makes this higher level of interoperability and resilience possible, but the other elements of the battle network must also be adapted to pass data seamlessly across multiple levels of security using compatible data standards and protocols.

The battle networks of the future are also not composed exclusively of new systems built to a new set of standards. While new systems and new standards are an important part of enabling new capabilities, the vast majority of the platforms, sensors, radios, and other payloads that will comprise future battle networks are already in service—and these existing systems will continue to be a significant part of the force for decades to come. Existing systems must be integrated into the same networks as future systems to achieve the full potential of Joint All-Domain Operations. Moreover, DoD already owns or has access to a variety of U.S. government, commercial, allied, and partner systems across each of the functional elements. Building the battle networks of the future is as much about integrating existing systems to connect with one another to perform new missions in new ways as it is about fielding entirely new systems and capabilities. As the military pursues the vision set forth in its Joint Warfighting Concept, it raises several operational, strategic, and acquisition issues for policymakers. The second paper in this series addresses these issues and the key factors policymakers should consider when charting a way forward. ›

Todd Harrison *is the director of Defense Budget Analysis and director of the Aerospace Security Project at the Center for Strategic and International Studies in Washington, D.C.*

This brief is made possible by support from General Atomics and general support to CSIS.

Cover Photo: U.S. Air Force photo by Senior Airman Daniel Hernandez