Congressional Research Service
Informing the legislative debate since 1914

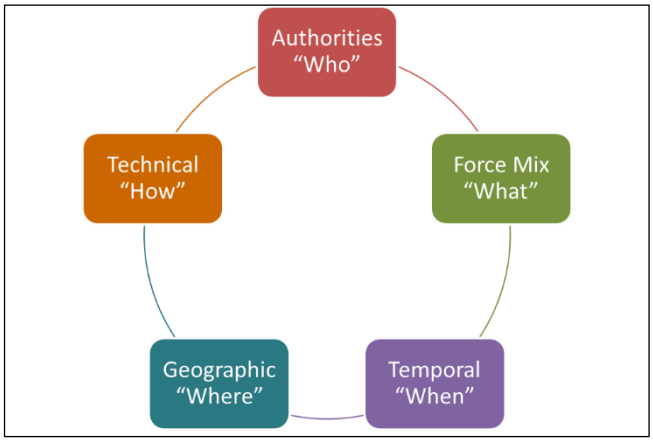
IN FOCUS

Updated November 14, 2022

Defense Primer: What Is Command and Control?

The Department of Defense (DOD) defines command and control (C2) as "[t]he exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission." At its most fundamental level, C2 represents how DOD makes operational decisions. One can view C2 through the context of five variables: who, what, when, where, and how (see **Figure 1**). Traditionally, Congress has focused on the authorities (the "who") and technology (the "how") variables, and less so on the force mix ("what"), temporal ("when"), and geographic ("where"). China and Russia have developed strategies to disrupt or potentially deny DOD its ability to make decisions; as a result, DOD is modernizing systems and processes to command and control military forces.

Figure 1. C2 Conceptual Model



Source: Congressional Research Service

The first variable that Congress has traditionally focused on reflects the authority a commander has to execute an operation. This line of discussion focuses on the chain of command, reflecting the differences between the military services—charged with organizing, training, and equipping U.S. forces (e.g., the Army provides infantry battalions and the Air Force creates fighter squadrons)—and the combatant commands who decide what those units should do and give them orders. This variable can be summarized by the question: "who commands forces?"

The second variable represents the hardware and systems that enable commanders to make these decisions and transmit them to the field. Terms like *command, control, communications* (C3), C3 *plus computers* (C4), and *intelligence, surveillance, and reconnaissance* (ISR) enter the discussion. This technical dimension of command and control looks at the data (and method of collection) that commanders use to make decisions (i.e., ISR is the data to enable decisionmaking), the processing power to transform data into information (the computer element), and the systems that enable commanders to communicate their decisions to geographically distributed forces. This technical approach to command and control can be summarized as, "how do you command forces?"

Other variables of command and control answer separate questions: which systems and units are being commanded ("what"), the temporal aspect ("when"), and geography ("where"). Congress has historically expressed interest in each of these variables in the context of specific, rather than general, issues. For example, rather than considering general purpose forces, Congress has focused on issues regarding nuclear forces and authorities associated with special operations ("What forces are being commanded?").

Regarding the "when," Congress has expressed interest in command and control associated with quick response to nuclear and cyber operations, and to a limited extent in terms of electromagnetic spectrum operations. However, a sensitivity on "when" generally is more tactically focused (e.g., when to have aircraft on target, when an assault on a building should begin); these decisions are often delegated to operational commanders.

The geographic component ("where") presents unique challenges for commanding U.S. forces. Congress and the executive branch traditionally explore and debate these issues through the lens of the National Security Strategy. This debate focuses on the U.S. role in the world and the locations and interests of its rivals, as well as potentially discussing authorization of the use of military forces.

What are strategic competitors doing?

Key strategic competitors identified in the 2022 National Defense Strategy (NDS), like China and Russia, have observed U.S. military operations for the past 30 years, noting that disrupting C2 systems could be one cost-effective solution to mitigating U.S. military advantages. As a result, potential adversaries have developed systems and strategies to reduce the effectiveness of U.S. command and control systems.

China's military strategy has been informed by the concept of "systems confrontation," which is similar to the U.S. concepts of sharing information with multiple systems. The systems confrontation concept assumes that victory in modern warfare does not necessarily require annihilation of adversary forces on the battlefield, but instead can be achieved by paralyzing major operational systems, such as command and control or logistics. To this end, China's military modernization has emphasized developing—for example—the ability to reduce the effectiveness of adversary satellites and communications systems and thus prevent adversary forces from connecting weapons systems

and sharing data and information. To facilitate this, China's military in 2015 established the Strategic Support Force (SSF), which combines cyber, space, and electronic warfare functions into a unified effort and supports the use of these capabilities by the military's ground, air, naval, and missile forces.

Similarly, Russian military strategists and planners focus on countering adversaries' command, control, communications, computers, intelligence, surveillance, and reconnaissance capabilities. A central focus is striking critical targets to paralyze an adversary's military ability and political willingness to sustain a fight. Russian strategists take a holistic approach, often referred to as "disorganization" in Russian military doctrine, to disrupting an adversary's command and control capabilities through the integrated use of all available systems (including information, cyber, electronic, air defense, air, and missile strike forces). To do so, Russia combines defensive and offensive capabilities to target an adversary's ability to conduct and sustain operations by deflecting attacks on key Russian systems, while disrupting an adversary's command, control, and communications systems. Russian strategists view the initial period of war as decisive and believe that deflecting attacks while simultaneously degrading an enemy's capabilities will allow Russia to win a conflict through attrition. Like China, Russia focuses on destroying the ability of adversary forces to operate effectively rather than physically eliminating them.

What is DOD doing to modernize C2?

DOD officials have argued that future conflicts may require decisions to be made within hours, minutes, or potentially seconds compared with the current multiday process to analyze the operating environment and issue commands. They have also stated that the department's existing command and control architecture is insufficient to meet the demands of the NDS. DOD proposes the Joint All-Domain Command and Control (JADC2) concept as a method to counter potential adversaries' ability to disrupt U.S. forces' combat operations. The JADC2 concept envisions connecting sensors from all of the military services—Air Force, Army, Marine Corps, Navy, and Space Force—into a single network, thus eliminating the possibility that an adversary could cripple a U.S. force by taking out a single, key sensor. This contrasts with the tradition of each of the military services developing its own tactical network that was incompatible with those of other services (e.g., Army networks were unable to interface with Navy or Air Force networks).

DOD uses ride-sharing service Uber as an analogy to describe its desired end state for JADC2. Uber combines two different applications—one for riders and a second for drivers. Using the respective users' position, the Uber algorithm determines the optimal match based on distance, travel time, and passengers (among other variables). Uber then provides directions for the driver to follow, delivering the passenger to their destination. Uber relies on cellular and Wi-Fi networks to transmit data to match riders and provide driving instructions.

Proponents of JADC2 claim that it will provide a cloud-like environment for the joint force to share intelligence, surveillance, and reconnaissance data, transmitting across many communications networks, to enable faster decisionmaking (see **Figure 2**). JADC2 is intended to enable commanders to make better decisions by collecting data from numerous sensors, processing the data using artificial intelligence algorithms to identify targets, then recommending the optimal weapons—both kinetic and nonkinetic (e.g., cyber or electronic weapons)—to engage the target.

Figure 2. Visualization of JADC2 Vision

Source: https://www.monch.com/mpg/news/ew-c4i-channel/7334-saic-and-usaf-partner-for-jadc2.html.

Some analysts take a more skeptical approach to JADC2. They raise questions about its technical maturity and affordability, and whether it is even possible to field a network that can securely and reliably connect sensors to shooters and support command and control in a lethal, electronic warfare-rich environment. Analysts also ask who would have decisionmaking authority across air, land, sea, space, and cyberspace given that, traditionally, command authorities are delegated in each domain rather than from an overall campaign perspective. Some also question how much a human would be needed for JADC2 to make decisions in real time, and whether it is appropriate to reduce the amount of human involvement in military-related decisions.

CRS Products

CRS In Focus IF10542, *Defense Primer: Commanding U.S. Military Operations*, coordinated by Nathan J. Lucas

CRS In Focus IF10521, *Defense Primer: Command and Control of Nuclear Forces*, by Amy F. Woolf

CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary

CRS Report RS21048, *U.S. Special Operations Forces (SOF): Background and Issues for Congress*, by Andrew Feickert

CRS Report R44891, *U.S. Role in the World: Background and Issues for Congress*, by Ronald O'Rourke

CRS In Focus IF11493, *Joint All-Domain Command and Control (JADC2)*, by John R. Hoehn

John R. Hoehn, Coordinator, Analyst in Military Capabilities and Programs
Caitlin Campbell, Analyst in Asian Affairs

IF11805

Andrew S. Bowen, Analyst in Russian and European Affairs

Disclaimer