MITRE CENTER FOR TECHNOLOGY AND NATIONAL SECURITY

BATTLE NETWORKS: INNOVATION AND KILL CHAINS FOR THE FUTURE FIGHT

by Eliahu Niewood and Greg Grant

What do hypersonics, 5G, quantum computing, data analytics, and artificial intelligence have in common? They are all examples of the Department of Defense creating organizations or appointing leaders around exciting technologies rather than starting with tactical and operational kill chains and identifying the right technologies to close gaps.

Talking about kill chains isn't the same as building them.

Former Senate staffer Christian Brose, in his book "The Kill Chain: Defending America in the Future of High Tech Warfare," rightly points out that great power rivals like China and Russia do a much better job building kill chains of their own and developing advanced capabilities to disrupt our traditional ways of operating. Brose provides a number of reasons for that, but one he doesn't discuss is that nobody in the vast defense enterprise is actually responsible for building the kind of cross-domain, cross-Service, mission-oriented kill chains that our potential adversaries are rolling out. Brose describes China's development of a "carrier killer" concept built around its very long-range DF-21 and DF-26 precision guided missiles.

It merits asking: Who would be responsible inside DoD for creating such a kill chain? The Army might get tasked to build the missile itself, since it is fired from land. The Air Force or maybe even the new Space Force might be asked to build the sensors to track enemy ships, if those sensors happened to be airborne or space based. The need for the kill chain itself and the writing of elaborate (and ultimately constraining) requirements might come from the Navy. If we wanted to put artificial intelligence in the sensors, or in the weapon's seekers, maybe the Joint Artificial Intelligence Center (JAIC) would get involved. At the end of the day, though, it is no one person's job to get all that to work together. Traditionally, the approach is to just give a handful of capabilities to the combatant commander and hope that they're able to kludge the various systems together into something useful.

SEPTEMBER 2020

If we want to make progress building more effective kill chains we should stop devoting time, money, and energy into standing up offices organized around a specific technology or focusing senior leadership on developing a specific technology. Don't spend time and resources building "Communities of Interest." We need to either create organizational structures that are focused on developing kill chains with specific missions in mind, or we need to fix our existing organizational structures so they have the responsibility and freedom to do so.

One potential model is a capability-centric portfolio management approach. Under this model, the Department would bring together requirements definition, technology development, engineering capability, business management, and the necessary resources, all under a single, empowered leader who is then responsible for delivering an operationally impactful solution to a specific problem. For some problems, this could all be done within an individual service. For other kill chains and problem areas, this portfolio management might be better done through a joint organization. We have done this in the past.

At its best, particularly before bureaucracy started to become more prevalent, the Missile Defense Agency had the necessary focus and drive. For kill chains that fit wholly within its purview, the Navy has demonstrated the ability to do this kind of work with things like Naval Integrated Fire Control—Counter Air (NIF-CA). In its early days, the National Reconnaissance Office (NRO) operated in this way. We need leaders and offices around DoD empowered to do the same things.

Innovation doesn't happen in Innovation Offices

In 2016, DoD launched the Defense Innovation Initiative (DII) to help spur the Department to develop innovative response options to reverse an eroding military advantage relative to our great power rivals China and Russia. Since then, we've seen that many of DoD's innovation hubs haven't proven all that innovative, yielding little in the way of game-changing capabilities. Real innovation comes from the close collaboration between the operators who bring deep understanding of the mission problems facing troops in the field and the engineers and technology developers who build new systems. It doesn't come from military officers taking VIPs on day tours of Silicon Valley start-ups. It doesn't come from staging "pitch days" where small companies pitch their wares that more often than not have little or nothing to do with user problems to judges who don't really understand the technology. Too often, there is an impedance mismatch between the users and the developers. Moreover, these initiatives typically solve for micro-level problems but don't provide solutions for the big operational challenges facing DoD. And they rarely, if ever, provide the kind of capability the Joint Force needs to counter the advanced weapons our great power rivals are fielding at a rapid pace.

WE NEED TO EITHER CREATE ORGANIZATIONAL STRUCTURES THAT ARE FOCUSED ON DEVELOPING KILL CHAINS WITH SPECIFIC MISSIONS IN MIND OR FIX OUR EXISTING ORGANIZATIONAL STRUCTURES SO THEY HAVE THE RESPONSIBILITY AND FREEDOM TO DO SO.

Look at those places that have been truly innovative and that provided real solutions to the most challenging problems and you'll see operators and technology developers who have been working together for long periods of time designing and executing programs.

The fact is, innovation doesn't happen in a day; it happens over time as people take on big problems, develop potential solutions, see what works, see what doesn't work, and are forced to iterate and adapt. It comes from a deep knowledge of technology and mission needs. A good example of how this works is the Air Force's Rapid Capability Office (RCO)—which chooses people with operational experience, flight test engineers, and technology experts from research labs, and couples them with the best and brightest in the FFRDCs and industry. The Air Force's Big Safari special projects office has done this in the past as have other classified program offices.

Those organizations all have the ability to experiment and prototype within their development programs. They don't get locked into a Joint Requirements Oversight Council-blessed set of detailed requirements. Rather, they start with a high-level goal, build something or prototype something (depending on the scale), then iterate, adapt, etc. Consumer companies have a huge advantage when it comes to innovation in that they are typically users themselves and they have giant user bases that will take a first product, use it, break it, provide feedback, and then buy it again. DoD needs to find a way to capture the key elements of that process without that user base or daily operational opportunities. We do know that having a modern-looking office with foosball tables is not the answer.

Battle networks can't destroy targets on their own

A number of authors have recently highlighted the challenges posed to US power projection by advanced integrated air defense systems, counter-space systems, and long-range, precision-guided, ballistic and cruise missiles. Invariably, the discussion then shifts to the need to build a better battle network to address the growing threat. What such discussions frequently ignore is that it isn't the Chinese or Russian networks we are worried about or the threat's ability to move information that causes us so much concern. Rather, it is the range, speed, and coverage area of Chinese and Russian sensors and weapons that are most troubling and pose the greatest challenge to the Joint Force. If China's DF-21 kill chain was a little slower, or even required a human in the loop at some point, that wouldn't enable our aircraft carriers to get closer to China or make our airfields and installations in the Pacific more survivable. It is actually the sensors and the weapons, not the networks, that have outpaced and outmaneuvered us. Better battle networks can help and are certainly critical to the kill chains we need. But in and of themselves they are not enough. No battle network will provide the F-22 the fuel it requires to stay in the fight longer in the Western Pacific. No battle network will change the scarcity of sensing resources we possess that are able to look deep into an adversary's territory or survive in the face of the Kaliningrad integrated air defense system.

We need to come up with new approaches for developing sensors, weapons, battle networks, and decision-making systems and better understand how they come together in an integrated architecture. We need to do trades on those architectures to understand how capability and unit cost scale with each other. We need to develop the systems defined by those architectures and then build them and acquire them in sufficient numbers. It won't be cheap to do so. And it will require

DOD REQUIRES NEW APPROACHES FOR DEVELOPING SENSORS, WEAPONS, BATTLE NETWORKS, AND DECISION-MAKING SYSTEMS AND BETTER UNDERSTAND HOW TO INTEGRATE THEM.

making some hard choices about what legacy platforms and systems we're willing to do without.

More effective battle networks will be essential to fully enable better and more numerous platforms and capabilities. If we don't build new battle networks we won't be able to use all the other advanced capabilities in the development pipeline. Still, we need to remember that even if we could move all the data we have to everyone instantaneously it won't solve our power projection, cyber superiority, or space control problems. Even if we more rapidly move the right data to the right people and give them decision tools to process that data more quickly, it still won't solve those problems. However, if we develop better collection capabilities, move the right information (not data) to decision makers, and give them faster, longer-range weapons, then we can get there. But we need to move out now.

ABOUT THE AUTHORS

Eliahu Niewood, Ph.D. is vice president, intelligence programs and cross-cutting capabilities at MITRE. In this role, Niewood leads MITRE's efforts to identify national security problems that require joint and multi-agency solutions and shape MITRE and the nation's response to those problems. He also leads MITRE in applying systems engineering, technology expertise, and innovation to help the intelligence and federal law enforcement communities leverage cutting-edge technology for mission success, integrate across agencies, and operate effectively in a dynamic environment.

Greg Grant is director of MITRE's Center for Technology and National Security (CTNS) and is the senior principal of integration and plans for MITRE's National Security Sector. Previously, he was senior director of strategy at Defense Innovation Unit (DIU). During his tenure with DoD, he also served as special assistant to Deputy Secretary of Defense Robert Work, helping to develop the "Third Offset Strategy."

About the Center for Technology & National Security

MITRE launched the Center for Technology and National Security (CTNS) to provide national security leaders with the data-driven analysis and technologically informed insights needed to succeed in today's hyper-competitive strategic environment.

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | Center for Technology & National Security