Booz | Allen | Hamilton

THINKING DIFFERENTLY ABOUT NETWORK RESILIENCE

Felix Yao
Distinguished Engineer
yao_felix@bah.com

Patrick Ward
Chief Technologist
ward_patrick@bah.com

THINKING DIFFERENTLY ABOUT NETWORK RESILIENCE

THE CHALLENGE: TODAY'S NETWORKS ARE COMPLEX, FRAGILE AND VULNERABLE

Department of Defense (DoD) networks are not what they need to be. Technology, governance, and operational issues have made them vulnerable to outages, component failure and intentional disruption. While all these things are true throughout DoD's network infrastructure, they are particularly problematic when it comes to supporting expeditionary operations.

These deficiencies have been acknowledged throughout the military, civilian government, and by numerous third parties who report and comment on military technology. These concerns are by no means new. A Defense Science Board study released nearly five years ago warned about the inability of military networks to withstand a full scale cyberattack, "Military Commanders may rapidly lose trust in the information and ability to control U.S. systems and forces" in such a case, the report stated.[1]

Senior military commanders do, in fact, share these concerns, as Army Chief of Staff General Mark Milley made clear in testimony last spring about the survivability of networks and command systems as lessons learned from recent operations in Eastern Europe.

"Frankly, my concern is these systems may or may not work in the conditions of combat that I envision in the future with the changing character of warfare because of issues with line of sight, electromagnetic spectrum, the inability to operate on the move, the inability to operate in large, dense complex urban areas or complex terrain."[2]

General Milley's comments are in line with those of other DoD leaders, and are echoed in statements from Defense Secretary James Mattis and, going back to 2015, in cybersecurity analyses from the Congressional Research Service.

All that being said, there are a number of efforts taking place aimed at improving the reliability of military networks. The Defense Advanced Research Projects Agency (DARPA) is reaching out to defense contractors to develop new algorithms and protocols for networks in large, forward-deployed areas. DoD and the Defense Information Systems Agency (DISA) are working to improve secure wireless access to classified networks for deployed warfighters, as well as enabling them to interoperate with coalition partners without having to provide those partners with classified equipment. Other, similar, technology-focused solution efforts are taking place as well.

However, technology is just part of the root cause of the resilience issues facing military networks, as General Milley also declared in his testimony.

DoD's network is a system built out of small pieces, (unique systems, applications and tools with service- and agency-specific requirements, access, interfaces, etc.) all of which are reasonable and understandable in isolation. But, together, becomes a system so large and complex that no single entity can appreciate or control it and it can therefore be very sensitive to unexpected shocks or "emergent behavior" (the way that large numbers of small elements can develop behaviors that are not simple, straightforward aggregations of the individual parts). With so many variables, making changes to these networks can be expensive or, worse, unreliable. The problem seems intractable.

Addressing the overall governance, loci of control, and real-world operations of military networks are just as critical to improving resiliency as are technological enhancements. Without taking these factors into account, all the hardware and software available can only provide point solutions to some of the specific

"We believe that combating fragility and improving resilience is dependent on addressing not just technology gaps, but in coming to grips with the pertinent organizational dynamics of military networks as well."

deficiencies General Milley and others have called out – not systemic improvements.

Overall guidance from cybersecurity executive orders during the Trump and Obama administrations has been too broad-based to be of effective use in these systemic concerns. While they provide useful underpinnings to critical infrastructure risk management, particularly the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as an overall assessment mechanism, these executive orders are too high-level to be of specific value in addressing the overall issue of military network resilience.

A NEW PERSPECTIVE: NETWORK RESILIENCE DEPENDS ON MORE THAN JUST TECHNOLOGY

We believe that combating fragility and improving resilience is dependent on addressing not just technology gaps, but in coming to grips with the pertinent organizational dynamics of military networks as well. There is resilience already built into military networks; improvements of governance, control, and operational factors can result in more effective leveraging of the technology which already exists, as well as making the most of new technological enhancements.

Resilience and Technology Today

There is no doubt that the lack of robustness of military networks is, in part, a function of existing technology.

All of the examples General Milley cited before the Senate Armed Services committee are real, and are functions of the nature of forward, expeditionary deployments. Expeditionary deployments often take place in an expeditious fashion. Whatever systems are currently the standard are part of the deployment; there is not much time available to fine-tune them to particular theatres of operation. The current standards have shown their shortcomings related to the operational needs of forces in the field, from military commanders to line warfighters.

The historical practice of hard-coding IP addresses for all deployed devices is one of the issues degrading the resilience of military networks. The sheer administrative overhead of managing all these devices in a fluid, real-time deployment scenario is a challenge given the physically distributed nature of these engagements. Software-defined networking can mitigate this challenge to some degree, but cannot change the basic nature of the deployment.

The physical landscape also contributes to instability. The physical topography of the battlefield, terrain issues, reception concerns in urban environments, connectivity while in motion, and interference with utilized bands of the electromagnetic spectrum both by happenstance and by cyberattack all play a part. A notable example of this is warfighters' radios not functioning when they're sitting inside their transport.

Physical network design needs to better accommodate the fact that individual nodes on the network – all sorts of devices ranging from routers to servers to wireless access points to devices carried by individual warfighters – may encounter these physical stumbling blocks and lose connectivity.

Resilience and Organizational Challenges

Technological improvements are in process, but cannot by themselves be considered overall solutions.

Overall solutions to resilience gaps require military leaders to think about more than just technology. The inherent physical complexity and distributed nature of military networks are accompanied by similar, overly

complex governance, management, operational, and control mechanisms.

The root cause of all this is a tension fundamental to military organization. For that matter, it is a tension fundamental to any large entity, military, civilian, or commercial.

The military is, by its nature and design, a hierarchy. From the head of the service, such as General Milley, to the frontline private in an expeditionary force, it is driven from the top down. Policies, directives, action orders, and commands are passed through the chain of command for implementation and execution.

THE SHARED MISSION CHALLENGE

This hierarchical perspective is more of an ideal than an operational reality. No service, or network, exists in isolation. Mission success is dependent upon coordination and cooperation between multiple entities and agencies. Mission responsibility is, in fact, shared, and while federal leaders recognize that a shared mission perspective is the best strategy for addressing problems such as network resilience, the reality is that in many cases, agencies and their staff find it difficult to collaborate and integrate with each other. With responsibilities effectively shared among multiple entities, decision-making in practice is also shared and divided. Command-and-control is, in practical terms, far lighter on control than is optimal in order to improve and grow network resilience. Like it or not, military networks are functionally and operationally matrixed, and closing resilience gaps is going to require accepting a more holistic perspective than the shared mission can provide.

Military leaders clearly acknowledge that network resilience needs significant improvement. We believe that addressing the organizational issues discussed above is the single most important action to be taken in order to optimize and improve current network infrastructure. Better leveraging of what is currently in place is an essential first step, and necessary to ensure that, going forward, technological advancements will in practicality provide the full mitigation of resiliency issues for which they are intended.

How to move forward? We believe that government agencies must, along with tailoring technological solutions to network resilience issues, modify their governance structures, update bureaucratic policies and procedures, and develop new leadership models supporting collaboration, cooperation, information sharing, and coordinated, synchronized action. This will enable them to transcend the control deficiencies of the shared mission perspective and advance to what we refer to as true Mission Integration.

NOTES

1. Defense Science Board Task Force Report *Resilient Military Systems and the Advanced Cyber Threa*t, January 2013, *https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf*

2. Statement of General Mark A. Milley, Chief of Staff United States Army, Senate Armed Services Committee, May 25, 2017, *https://www.armed-services.senate.gov/download/speer-milley_05-25-17*

OUR AUTHORS

Felix Yao, *Distinguished Engineer*
yao_felix@bah.com

Patrick Ward, *Chief Technologist*
ward_patrick@bah.com

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that – together – we will find the answers and change the world. To learn more, visit BoozAllen.com.