

# Practical Cyber Risk Management for Tactical Commanders

---

Colonel Ron Iammartino

## ABSTRACT

*Risk management in today's complex threat environment necessitates decision rules that integrate cyber risk control into the overall mission risk profile. This article outlines cyber risk management decision rules that are based on lessons learned from the Expeditionary Signal Battalion-Enhanced (ESB-E) prototype, which adapted Special Operations Forces (SOF) and commercial-off-the-shelf (COTS) capabilities by applying a rapid fielding and feedback approaches within the scope of the Army Futures Command. Focus areas include the use of diverse COTS systems and satellite communications providers to mitigate risk, controlled system maintenance processes, capitalizing on behavioral bias in cybersecurity, integrating enterprise services, and keeping pace with technological innovation trends. Lessons learned are intended to give tactical commanders practical cyber risk management options within the overall scope of mission risk management.*

**R**isk management in today's complex threat environment necessitates decision rules that integrate cyber risk control into the overall mission risk profile. A decision rule is a statistical term that operationalizes principles through pre-determined decision criteria or algorithms for faster, authoritative risk management decision-making.<sup>[1]</sup> Network jamming, disruption, and penetration threats can change at a pace that outstrips enterprise-level resources available in a contested or congested electromagnetic (EM) environment.<sup>[2]</sup> Predetermined decision rules that provide practical risk management options appear to be particularly important for tactical units, since these units deploy on short notice to austere and rapidly changing environments where network management controls are limited. As demonstrated during two sensitive

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.



**Colonel Ron Iammartino** is a U.S. Army Signal Officer. He is currently the Army War College Fellow at Princeton University and most recently served as the Commander of the 50<sup>th</sup> Signal Battalion at Fort Bragg, NC. He previously served as an action officer on the Joint Chiefs of Staff and the Department of Army Staff in Washington, DC. He holds a Ph.D. in Systems Engineering from the George Washington University, an MA in Quantitative Methods from Columbia University, and an MBA in Finance from Monmouth University. He is a 2003 graduate of the U.S. Military Academy. His prior published work focuses on agent-based and statistical modeling.

Immediate Response Force (IRF) missions in 2019-20, division and brigade commanders now have access to decision rules and technologies that can more quickly shape communications systems capabilities within an operational environment without strict dependence on the enterprise to mitigate network risk.

Accordingly, the Army has undertaken a series of coordinated network modernization efforts intended to experiment with the adaptation of emerging commercial technology to improve tactical network resilience.<sup>[3]</sup> One of these efforts is called the Expeditionary Signal Battalion-Enhanced (ESB-E) prototype. The prototype calls for tactical communications assets that are faster, lighter, and easier to employ. These assets are largely modeled after Special Operations Forces (SOF) capabilities that had previously been limited to lower-scale development.<sup>[4]</sup> Whereas past conventional capabilities were deployed with a one-size-fits-all solution exposed to shared risks across the enterprise, the ESB-E provides supported commanders with far greater options for managing cyber risk across a more diverse set of command and control (C2) asset alternatives. This paper outlines decision rules that are based on lessons learned from the ESB-E prototype intended to give tactical commanders practical cyber risk management options within the overall scope of mission risk management.<sup>[5]</sup> These decision rules are related to employing multiple information technology (IT) vendor solutions, a range of satellite and cellular service providers, centralized maintenance processes and validation, the use of enterprise services for redundancy, a bias toward sharing with coalition mission partners, and leveraging commercial technological innovation trends.

The first decision-rule is to employ several different vendor solutions to mitigate hardware security risk as a means to ensure capability reliability. The ESB-E is comprised of IT solutions from a range of different vendors and service providers. This approach helps

manage risk exposure in that the risk to one system or communications kit is not evenly distributed across the full capability set as in past technology upgrades. One ESB-E component, for instance, may be particularly vulnerable to a software bug, supply chain risk, or embedded hardware faults attributable to a threat originating in the Pacific area of responsibility, while another is more vulnerable to a threat originating from a non-state actor in Europe.<sup>[6]</sup> The differences within the ESB-E capability set significantly reduces the risk that a single hardware or manufacturing vulnerability can result in a catastrophic outage.

A second decision rule is to test and enable multiple military satellite, commercial satellite, and cellular transmission paths as condition for deployment. One might think of each respective satellite and cellular transmission path as representing a distinguishable and mutually exclusive route for accessing military networks, which is comparable to having multiple cellular providers and cable Internet packages. The idea is to get into the network securely any way you can.<sup>[7]</sup> The ESB-E has far greater flexibility for employing communications assets across SATCOM bands and commercial infrastructure, such that units can more easily adapt support in a degraded or contested electromagnetic spectrum communications environment.<sup>[8]</sup> Probabilistically, it is harder for an adversary to jam or deny network access to a user that can access defense networks through more than one means simultaneously.<sup>[9]</sup> This approach is analogous to the Army targeting guidelines in that the ESB-E model makes it more difficult to isolate or fix on a target that has an ambiguous or wide area attack surface.<sup>[10]</sup>

This emphasis on a probabilistic approach to mission management and risk is key to these first two decision rules. Even commanders without access to ESB-E resources can benefit from this construct in terms of understanding where their unit may have concentrated risks. The Primary, Alternate, Contingency, and Emergency (PACE) approach to communications risk management must be broken down into dimensions that allow commanders to understand where there is more than a single point of failure in each network layer. Predetermined decision rules that have already incorporated the probabilities of these risks and appropriate mitigation strategies are critical to the continuity of communications support to operation in a congested environment. In one recent example, a brigade-level IRF commander, who did not have access to ESB-E resources was able to immediately transition to a commercial satellite while waiting for repair components to fix failed organic government satellite assets. The commander had preplanned this decision through pre-mission training that included a pilot program commercial satellite system.

The third decision rule mandates that all systems go through a higher headquarters-controlled pre-mission and post-mission maintenance reset process as a condition for unit deployment. In line with the 2015 Defense Cybersecurity Culture and Compliance Initiative (DC3I), the ESB-E centralized maintenance and reset process helps to reduce common human errors through external validation and standardization prior to active employment. It also gives commanders better visibility on asset readiness. The centralized maintenance and reset

process applies the DC3I principles of dual verification, specific reset role assignments, and external validation for ensuring predictable readiness standards for all assets.<sup>[11]</sup> The process calls for all ESB-E assets to be inspected and validated in deliberate phases by communications-electronics (C&E) hardware and network operations (NETOPS) software sections in order to verify that all systems have functional hardware, the latest software version, and cybersecurity patches. It further includes an external certification through the Brigade NETOPS tactical hub to help identify and reduce errors during reset. In addition, the approach centralizes asset visibility on high-failure rate components, factory recalls, and other deficiency trends to facilitate knowledge transfer on risk.<sup>[12]</sup>

More generally, the centralized maintenance process reinforces better alignment with higher headquarters, together with closer cross-functional team integration between operations and maintenance so fewer risks can go unnoticed. This is akin to the cultural norms for dual verifications and external system maintenance checks long ago established by the nuclear Navy, which, until recently, have been hard to replicate on sometimes-dormant tactical network systems sitting in a large motor pool.<sup>[13]</sup>

A fourth decision rule is to select enterprise services as a back-up to any organic voice or video services for use during deployment. In the past, tactical units were limited to organic systems and devices for capabilities such as phone, email, or video teleconference during a deployment or exercise. In contrast, the ESB-E can much more easily use enterprise home-station capabilities due to its more advanced and lighter Internet protocol (IP) based routing systems. This has the potential to help with eliminating common human errors in cybersecurity, while also ensuring network and risk convergence across the enterprise. Risk is better balanced by the common standards, less proprietary complexity, authoritative identity management features, and increased service delivery mixes characteristic of enterprise services, such as enterprise email or Defense Information System Agency (DISA) global video services (GVS). At ROVING SANDS 2019, for instance, ESB-E teams were able to employ enterprise services seamlessly for secure voice communications when a network access denial prevented call-routing using organic call manager assets.<sup>[14]</sup> Even more, tactical units can more easily keep pace with changing threat vulnerabilities through reliance on enterprise-level software updates, rather than local replacement of vendor-specific systems or software.<sup>[15]</sup>

A fifth decision-rule is to default to coalition partner information sharing when partners achieve predetermined COTS system cybersecurity standards. A large body of behavioral science research suggests that decision-makers are inherently biased toward risk aversion in that they tend to avoid losses more than taking prudent risks to improve information-sharing.<sup>[16]</sup> This tendency runs counter to the DOD and CJCS 2017 objective to establish a bias toward sharing with allies and mission partners.<sup>[17]</sup> ESB-E, however, seems to help to reinforce the objective to take reasonable risks – and improve network interoperability through COTS, its open architecture that provides allies and partners with standards-based alternatives for


interoperability instead of the acquisition of a single, closed proprietary hardware requirement. These considerations, combined with the previously outlined improvements to enterprise network visibility and ESB-E maintenance processes, encourages better cybersecurity readiness transparency among allies, thereby stimulating more operationally effective network management policy decisions that bias toward safer information sharing.<sup>[18]</sup>

Further, commanders can set a decision rule to use the ESB-E rapid prototype approach to deliberately capitalize on commercial market trends in technological innovation. It has become much tougher for a single vendor or product to maintain market dominance. Open-source innovation makes breakthroughs in capabilities or cybersecurity more accessible at lower cost.<sup>[19]</sup> The top technology firms today are competing for much smaller incremental improvements than the major advances that were achieved by technology firms like Facebook and Google in the early 2000s.<sup>[20]</sup> These trends make it far easier for ESB-E rapid prototyping of new technology to inform upgrade decisions, thereby adapting cybersecurity readiness more quickly.

This article emphasizes the importance of commander engagement to expand options and access to network resources, systems, and new technologies to manage risk. It prioritizes increasing access and availability for effective communications over cybersecurity defense limitations. Past work has shown that rigorously stress-testing new equipment, particularly when it is completed on live networks in partnership with tactical units, helps to ensure that security measures do not overly burden commanders with enterprise risk controls or change management inconsistencies.<sup>[21]</sup> Yet, commanders must be aware of the tradeoffs in potential exposure to unknown cyber risks associated with new or open-source technologies, such as zero-day vulnerabilities. The importance of strong controls, such as the aforementioned centralized maintenance process, end-point security, user training and discipline, multi-factor authentication, and network monitoring should not be understated.

In sum, there are six key conclusions from this article that can be practically applied to strengthen tactical cybersecurity risk management. The first two overlap. First, units should take advantage of the better technology and smaller form-factors of emerging capability sets like ESB-E and by having multiple solutions to solve a single IT or signal problem. Having options helps mitigate cyber risk associated with hardware vulnerabilities or enterprise inefficiencies that may not be resolved in a timely manner for a single system. Second, units should ensure the employment of multiple SATCOM bands and cellular service providers. It should not be assumed that these assets are readily available through unit training or enterprise-level resourcing without command emphasis. Third, commanders can leverage a controlled maintenance reset process to deliver an accurate picture of cybersecurity and system readiness. Fourth, commanders should apply COTS cybersecurity standards and behavioral science insights to reinforce a bias toward information sharing with coalition partners. Fifth, tactical commanders should emphasize the integration of enterprise services as part of the tactical communications plan to provide redundancy and network security reinforcement.

Finally, technological innovation trends suggest that rapid prototyping is an appropriate means to test and adopt new technologies, since smaller incremental technology improvements and open source software are characteristic of the emerging IT market environment. Rapid prototyping, as described through the ESB-E use prototype can help Army tactical units keep pace with changing cyber threats.

ESB-E is one of many ongoing initiatives contributing to better cybersecurity risk management across the Army. Future efforts should incorporate more sophisticated artificial intelligence and quantum computing risks. Cyber risk will also soon be impacted by the advance of 5G, Mid-Earth Orbit and Low Earth Orbit satellites.<sup>[22]</sup> Decision rules must consequently evolve as practical tools for tactical commanders.<sup>[23]</sup> 

## NOTES

1. Carl Hauser, Yeow Meng Thum, Wei He, and Lingling Ma, "Using a Model of Analysts' Judgments to Augment an Item Calibration Process" *Educational and Psychological Measurement* 75, no. 5 (October 1, 2015), 826-49, <https://search-ebsco-host-com.proxy1.ncu.edu/login.aspx?direct=true&db=eric&AN=EJ1073524&site=eds-live>.
2. Ray Dalio, "Principles: life and work." First Simon & Schuster hardcover edition. New York: Simon and Schuster, 510-523.
3. Joseph Lacdan, "G6: Greater Integration across unified network will strengthen force," *Army News Service* (October 30, 2020), [https://www.army.mil/article/240404/g\\_6\\_greater\\_integration\\_across\\_unified\\_network\\_will\\_strengthen\\_force](https://www.army.mil/article/240404/g_6_greater_integration_across_unified_network_will_strengthen_force), accessed November 3, 2020.
4. Amy Walker, "Army Pilots New Signal Battalion for Scalable Expeditionary Comms Support," *PM Tactical Network/PEO C3T Public Affairs*, October 11, 2018, [https://www.army.mil/article/212220/army\\_pilots\\_new\\_signal\\_battalion\\_for\\_scalable\\_expeditionary\\_comms\\_support](https://www.army.mil/article/212220/army_pilots_new_signal_battalion_for_scalable_expeditionary_comms_support), accessed September 1, 2020.
5. Ron Iammartino, "ESB-E Cyber Risk," White Paper, January 2020, Unpublished Manuscript.
6. Ruby B. Lee, "Security Basics for Computer Architects," Morgan & Claypool, 2013, 1-10.
7. This concept is based on discussion and input from the 50th ESB-E Network Operations Section in January 2020.
8. Ibid.
9. Iammartino, "ESB-E Cyber Risk."
10. Army Techniques Publication 3-60: 2015.
11. U.S. Department of Defense, "Department of Defense Cybersecurity Culture and Compliance Initiative (DC3I)." October 2015, 1-12.
12. Ron Iammartino & Christopher O'Connor, "Army Networks at a Crossroads," *ARMY Magazine*, August 2019, 1-3.
13. Ibid.
14. Iammartino & O'Connor, "Army Networks at a Crossroads." *ARMY Magazine*, 3-5.
15. Ron Iammartino, Todd Doherty, & John Fossaceca, "Transforming DoD Information Technology Networks through Coalition Partner Trust," *Small Wars Journal*, 12 (1), December 30, 2018.
16. Amos Tversky & Daniel Kahneman, "Judgment under uncertainty: Heuristics and biases," *Science*, (1974), 185(4157), 1124-1131.
17. General Joseph F. Dunford, "Allies and Partners Are Our Strategic Center of Gravity," *Joint Force Quarterly* 4, no. 87 (2017): 5.
18. Ron Iammartino, Todd Doherty, & John Fossaceca, "Transforming DoD Information Technology Networks through Coalition Partner Trust." *Small Wars Journal*, 3-5.
19. "Tech firms are suddenly the corporate world's biggest investors." *The Economist*, July 28, 2018, <https://www.economist.com/business/2018/07/28/tech-firms-are-suddenly-the-corporate-worlds-biggest-investors>, accessed November 3, 2020.
20. "Silicon Valley's giants look more entrenched than ever before" *The Economist*. August 10, 2019. <https://www.economist.com/graphic-detail/2019/08/10/silicon-valleys-giants-look-more-entrenched-than-ever-before>, accessed November 3, 2020.
21. Ron Iammartino, "Army Networks at a Crossroads."
22. Ron Iammartino, "ESB-E Cyber Risk."
23. Author Note: Sections and ideas throughout this article have, in part, been derived from a series of experiences and white papers written during my time in command of 50th ESB-E, Fort Bragg, NC. Many of the ideas and concepts are based on the lessons learned, input, and mission employment of capabilities by 50th ESB-E soldiers, non-commissioned officers, and officers. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.