



2.3 CYBER RESILIENCE FOR MISSION ASSURANCE

Anthony Bargar

INTRODUCTION

I work for the Office of the Assistant Secretary of Defense for networks and information integration [OASD(NII)] under the Deputy Assistant Secretary of Defense for Cyber Information and Identity Assurance. I am leading the effort in Cyberspace Resilience for Mission Assurance, which was borne out of our analysis of how we can—and will—operate through and recover from sophisticated cyber attacks. To frame the discussion for this roundtable, I will outline our key approaches to ensuring DoD’s mission-essential functions and discuss how cyberspace resiliency depends on more than simply ensuring network security.

KEY INITIATIVES

To conduct a pragmatic analysis of what we need to ensure cyberspace resiliency, we must assume that our best efforts in defense have failed and that sophisticated cyber adversaries—at the governmental level or well-resourced groups, either ad hoc or

Mr. Anthony Bargar is a Senior Strategy and Policy Advisor leading DoD’s Cyber Mission Assurance for the Deputy Assistant Secretary of Defense for Cyber Information and Identity Assurance. Previously, he served as Senior Technology Advisor for the Counterintelligence Field Activity, and Senior Information Assurance Analyst for the Defense Intelligence Agency. Mr. Bargar led a research project on shared critical information infrastructure protection and defense with the U.S. National Defense University and the Swedish National Defense College. He holds a master’s degree in Information and Telecommunication Systems for Business from Johns Hopkins University. Additionally, he is a distinguished graduate from the NDU Information Resources Management College.

nation-state-based—succeed in degrading, denying, and manipulating our networks, our enterprise services, and the information that travels on them. It is not just about the circuit layer, which is unfortunately often the focus.

We have to make sure the technology underpinnings of our information environment—including our shared power, communications, and information infrastructures—work under fire, deflect attacks, restore trust in information, operate through the event, and recover quickly. The DoD, under the National Continuity Program, has defined certain primary mission-essential functions (Figure 1). Cyberspace resiliency focuses on protecting capabilities that enable those primary mission-essential functions.

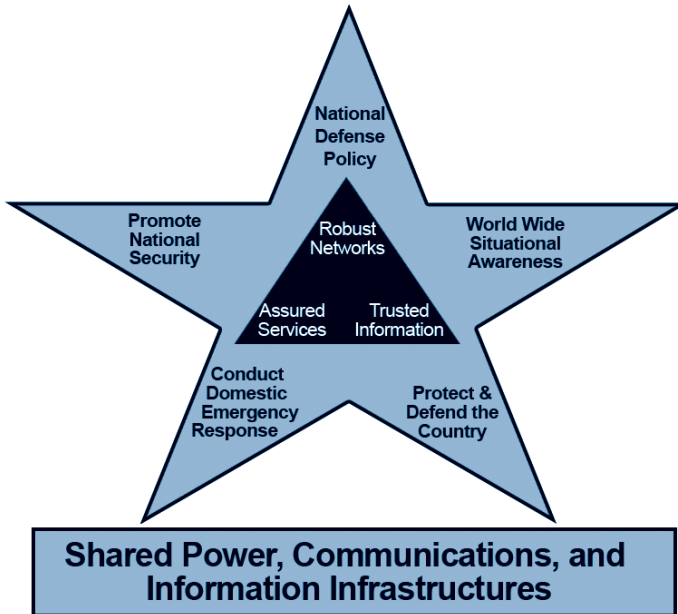


Figure 1 DoD's Primary Mission-Essential Functions

In this effort, we have recommended three key initiatives within the DoD. One is recognition that this is not just a technologist issue; this issue concerns the operator as well as the user.

In DoD, it concerns both the warfighter (J3) and the technologist (J6). That is why it is very important to improve our ability to plan, simulate, and execute exercises under serious cyber degradation. We have to take the gloves off when it comes to planning and training if cyberspace is truly a warfighting domain.

“Cyberspace resilience is much more than networks. . . it is the flexibility, adaptability, and trustworthiness among the human, the physical, and the information domain.”

We have to then enable cyber situational awareness, improve diversity planning, integrate policies and plans for resiliency, and take a holistic risk management approach, examining how we measure and manage risk, balancing the technology and operations. The opportunities to achieve this are through improving our models and simulations, understanding complex cascade effects as well as single points of vulnerability, and enhancing defenses against the top-tier adversaries. We must also improve risk management compliance and enforcement while recognizing the shared responsibility with the information, communications, and technology (IC&T) industry. We all share a common critical information infrastructure amongst government, private sector, and international entities. The common defense and approach to resiliency is incredibly important.

MORE THAN NETWORKS

Cyberspace resilience is much more than the creation of diverse networks—resiliency is more than just redundancy. It is the survivability, flexibility, adaptability, and trustworthiness among the human, the physical, and the information domain. It spans our people, processes, and technologies (Figure 2). Cyberspace resilience is the ability to operate through cyber conflict and recover quickly to a trusted environment.

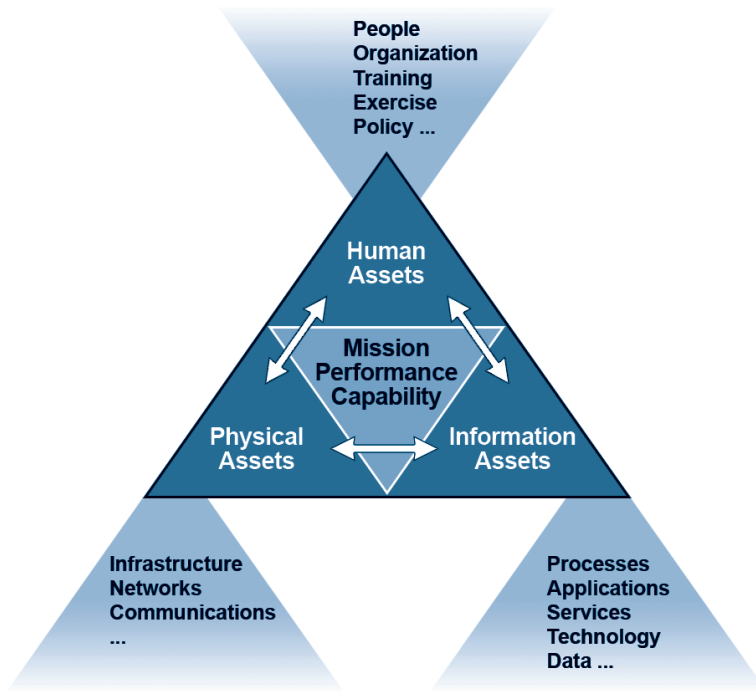


Figure 2 Nexus of Human, Physical, and Information Assets