

Working to create cyber defense experts

Signaleers,

I have been looking forward to this edition of the *Army Communicator* because there are some significant questions we need to engage openly and honestly.

Everyone realizes that our Mission Command and network communications systems have grown in magnitude and complexity. It is not as apparent that there has been a shift in advantage from the defensive to the offensive. The historic degree of difficulty due to the complexity and cost of reverse engineering communications systems that were mostly proprietary was a huge barrier for our potential adversaries. That's no longer true. Today we use a plethora of commercial off the shelf equipment in the same manner as the rest of the world. This allows common universally applicable exploitation tools to be used against the U.S. Army.

Because of this massive shift in favor of the offensive (i.e., toward our adversary in comparison to our cyber defenders), can our cyber defense experts be expected to stop every attack? Think of it like this: do you expect even the best goalie to stop every shot at the goal? What if the oppos-

ing team has an unlimited roster of players on the field and each has multiple pucks that can all be shot at the same time. What would you expect to happen?

We are working hard to ensure we create the best cyber defense experts possible. We must take more of a holistic approach through sound principles of Network Operations.

Even though we have a NetOps construct, are we really conducting, or even able to conduct true Network Operations? Could it be that we merely stage a transport and routing architecture and then reactively optimize based on bandwidth demands? Could it be that we establish data services based upon a static model of Mission Command service expectations? Could it be that we systematically employ Information Assurance measures based upon forensics of successful CNE and/or CNA actions? What happens when the adversary moves from a CNE posture of data exfiltration to a CNA posture to manipulate data and/or to disrupt, deny, and/or destroy our information systems due to political or kinetic triggers?

Are we prepared to hunt for potential adversarial activity in accordance with an established playbook that includes immediate preemptive transport routing modifications; data screening, filtering, and transition to alternate servers (e.g., COOP); and ensure uninterrupted Mission Command Essential Capabilities while a near-peer adversary aggressively attempts to disrupt and/or manipulate our essential information and key Cyberspace terrain? In other words, can we conduct NetOps?

This and many other aspects of cyberspace defense are addressed in this edition. Additionally, we solicit your thoughts, expertise, and support in taking back the advantage though holistic, integrated, and synchronized NetOps functions.

As always, thank you for your dedication and service in being ever Watchful for Our Country.

Pro Patria Vigilans!

