Capts. Joe Spracklen (left) and Brad Pemberton of the 1st Cyber Protection Battalion, Army Cyber Protection Brigade, acting as battle captains for exercise Operation Tiger Stance, review and discuss a common operating picture in the blue team operations area at the Indiana National Guard's Muscatatuck Urban Training Center in Butlerville, IN., Aug. 23, 2018. ***(Photo by Bill Roche)***

ARCYBER JOC

Where Cyber Operations Come Alive

COL Thomas Nelson and MSG Amanda Kelley

Let's be honest: most articles about military operations centers are dry, technical, and quickly forgotten. This is not one of those articles. If you're expecting a standard, checklist-driven description of a Joint Operations Center (JOC), you'll be disappointed and maybe relieved. The US Army Cyber Command (ARCYBER) JOC is not a typical watch floor, and its story is anything but routine. When you walk into the ARCYBER JOC, the first thing you notice isn't the sterile glow of screens or the cold reflection of data. It's the movement of information flowing like electricity, connecting the land and cyber domains in real time. The JOC doesn't simply display information—it performs it. Every screen, workstation, and voice on the floor contributes to a living narrative of operations, intelligence, defense, and attack.

This article aims to interpret the ARCYBER JOC, giving leaders at every level—from junior officers to senior commanders—a clear, honest understanding of what it is, how it works, and why it matters. This is a story of convergence and adaptation, of people and process, and of how the JOC became ARCYBER's decisive edge in cyberspace.

A Room Built for Purpose

The JOC was designed to be more than a watch floor. It is a place where the Army's complex operational challenges are seen, understood, and acted upon quickly. The layout itself is intentional: screens and workstations are arranged around the three pillars of ARCYBER's mission—Operate, Defend, Attack (ODA). Soldiers, civilians, and contractors from different specialties work side by side, building a coherent operational picture for the command. This architecture reflects years of thought and experience, and a willingness to rethink how a command fights.

- **Operate** is the JOC's heartbeat. It is the persistent, real-time awareness of networks and signals across the Army. Screens show the status of key bases, communications architecture, and the health of the Army's global network. To Operate is to see everything. In cyberspace, the one who sees everything wins.

U.S. Army Cyber Command Command Sgt. Major Jebin Heyse speaks to soldiers Jan. 8, 2025 in Good Shepard Chapel at Fort Gordon, Georgia. Heyse led the brief as part of ARCYBER'S noncommissioned officer leadership development session. (U.S. Army photo by Staff Sgt. DeMarco Wills)

- **Defend** is the shield. The JOC's defensive posture is constant, aiming to ensure adversaries find no gap or moment of inattention to exploit. The doctrine of "defend forward" is about maintaining a presence that deters threats. To Defend is to deny the enemy their opening. In cyberspace, a door never opened is a battle already won.
- **Attack** is the JOC's sword. The JOC synchronizes cyber effects to disrupt adversary command and control, communications, and confidence. Not with bombs or bullets, but with precision, speed, and the invisible hand of a force that has spent years learning exactly where to strike. To Attack is to impose costs the adversary cannot absorb. And in cyberspace, the most powerful weapon is one the enemy never sees coming.

The convergence of these pillars is the JOC's purpose: to bring together offensive, defensive, intelligence, and information capabilities for decision-making.

The People Who Make It Work

Technology alone does not win battles. The JOC's strength is in its people—those who fill its seats, monitor displays, and carry the weight of a mission that touches every soldier and network. Intelligence analysts, cyber operators, signal warriors, plans officers, and Reserve Affairs professionals work together, bringing their own diverse backgrounds and perspectives.

The seating layout is deliberate and designed to break down silos. Operations sit next to intelligence. Plans are close to current operations. The JOC is the location for key meetings and decisions where the command comes together as one team. Months of preparation and countless hours of design led to a system that, when tested, could adapt and respond.

The Common Operational Picture (COP)

In the old stories, a wizard's power came from a crystal ball that showed the truth of the world. In the ARCYBER JOC, that crystal ball is the COP.

The JOC's COP is central to its function. One screen carries the Current Assessment, which is a real-time narrative of ARCYBER's activities, framed by Priority Intelligence Requirements (PIR). The CENTCOM COP is linked by VTC to the CENTCOM battle bridge, ensuring timely communication. Other displays show operational options, ongoing missions, and the readiness status of cyber teams. A map of the Area of Responsibility (AOR) brings the geospatial dimension to life, showing friendly and adversary actions in real time. The ARCYBER Big 5 are the command's five most critical efforts and are displayed to keep focus.

This is not information overload. It is an effort to distill technical data into what leaders need to make decisions quickly.

A Test of the System

Every great organization faces its test—when the walls shake and the heroes must decide who they truly are. For ARCYBER, that test was Operation Epic Fury. When the crisis broke, the JOC shifted into 24/7 operations. The first 72 hours were challenging as the teams found their rhythm, and the volume of work was high. There were moments of friction and confusion, but the system held. The staff adapted quickly. A sustainable battle rhythm emerged, daily products were produced, and situational awareness improved. The JOC performed as designed, meeting the demands of the moment. The crisis had not broken the JOC—it had forged it.

Noncommissioned officers across U.S. Army Cyber Command attended professional development training led by the ARCYBER command sergeant major October 9, 2025. (Photo by Staff Sgt. DeMarco Wills)

The Wizards Behind the Curtain: G5 and the Power of Learning

While the G33 manages current operations, the G5 (Plans and Policy) became the command's strategic reserve and institutional memory. They instituted a process for capturing observations, insights, and lessons learned (OIL) using AI-assisted analysis to identify trends and friction points in real time. Standard operating procedures (SOP) were refined during the operation, ensuring lessons were not lost. The JOC SOP was crafted by those experiencing it firsthand, making learning immediate and relevant.

Decision-Making Tools

Every great commander needs a mirror that shows the truth—not what they want to see, but what is. The Power BI dashboard was built through the collaborative genius of the Data Management and Analytics (DMA) section, and the G33 became that mirror. It aggregated data from across the enterprise, allowing leaders to track requests, monitor workflows, and anticipate requirements. This was not just a reporting tool, but a support for decision-making.

The JOC Today and Looking Forward

The ARCYBER JOC today is a converged decision-making apparatus that integrates offensive, defensive, intelligence, and information capabilities. The screens still display Operate, Defend, and Attack. The team remains at their posts, carrying the lessons of experience.

As ARCYBER prepares for future exercises and challenges, the foundation is stronger. The lessons of Operation Epic Fury are part of the SOPs, the battle rhythm, and the culture. The future will require continued adaptation and collaboration. The JOC must keep evolving to meet new challenges.

This is not just a story about a Joint Operations Center. It is a story of how Army Cyber learned, adapted, and continues to prepare for what comes next.

Col. Paul Stanton, commander of the Army Cyber Protection Brigade, briefs visitors on his unit's activities in exercise Operation Tiger Stance, in the blue team operations area at the Indiana National Guard's Muscatatuck Urban Training Center in Butlerville, IN., Aug. 23, 2018. ***(Photo by Bill Roche)***

COL Thomas Nelson is the ARCYBER chief of current operations (G33). He and his wife, Allison, have five children: Alex (15), Charlotte (13), Grady (11), Grace (10), and Tristan (8). Nelson commissioned into the Infantry in 2004, graduating from the US Military Academy with a degree in mechanical engineering. In 2025, he earned a PhD in mathematics from UNC-Chapel Hill. He served as a platoon leader with the 82nd Airborne Division, deploying to Afghanistan in 2005 and Iraq from 2006 to 2008. He later commanded a company in the 4th Infantry Division, deploying to Iraq from 2010 to 2011. Transitioning to the Cyber branch, Nelson has served in operational roles with the 780th Military Intelligence (Cyber) Brigade and Army Cyber Command, to include battalion commander of the 782nd MI Battalion (Cyber).

MSG Amanda Kelley is the sergeant major for the ARCYBER G33. She has a 3-year-old son, Huxley. Enlisting in 2011, Kelley transitioned to electronic warfare and is a leading voice in cyber and electromagnetic activities. A veteran of Operation Inherent Resolve, she served with the 3rd Special Forces Group (Airborne) as an SOT-A noncommissioned officer in charge. Kelley holds the Ranger Tab, the Jumpmaster qualification, and a master's degree in business administration. She is a member of the Sergeant Audie Murphy Club.