Secure Data Sandbox
US Army 18th Airborne Corp

CHALLENGE

Information Operations (CYOPS) Soldiers who are assessing the battlefield and make timely decisions in combat, cannot maintain decision advantage and lethality due to the lack of a secure, real-time environment to access, verify, and utilize publicly available untrusted information (e.g., social media) without dependency on traditional data systems or lengthy intelligence processes.

RELEVANT CONTEXT

- In modern combat and peacekeeping operations, ground force commanders and soldiers require rapid access to publicly available information, such as social media, to assess the battlefield and make timely, informed decisions. However, the current process is hindered by the need to securely verify information, process it through National Technical Means, and correlate it with other intelligence assets. This creates delays and dependencies on connected infrastructure, which may not always be available in denied or contested environments.
- Currently, there is no secure environment within the Army that allows soldiers to pull untrusted information from public sources, clean it, and use it in real-time. This limitation forces soldiers to rely on pre-approved, sanitized data, which often arrives too late to be actionable. The existing tools and processes are insufficient to sift through vast amounts of publicly available data, and there are cultural and legal barriers that complicate the handling of such information, as it transitions from raw data to classified intelligence.
- To address this, there is a need for a "data DMZ" (De-Militarized Zone)—a protected space where untrusted information can be accessed, verified, and utilized without exposing defense networks to risk. This would allow commanders to leverage local infrastructure and devices, like how soldiers in Grenada used tourist maps when military maps were unavailable. Such a system would empower lower-echelon commanders to make informed trade-offs between risk, opportunity, and speed, without waiting for higher-echelon support.
- The challenge lies in creating a secure, segregated environment that can establish trust in real-time for publicly available data, while complying with existing policies or adapting those policies to accommodate this new capability. This would enable soldiers to maintain lethality and decision advantage even when traditional data systems are denied.

IMPACT

If this problem were solved, ground force commanders and soldiers would gain the ability to access, verify, and utilize publicly available untrusted information in real-time, enabling them to make faster, more informed decisions in combat and peacekeeping operations.

POTENTIAL BENEFICIARIES

Intelligence Analysts, Special Operations Forces, Joint Task Forces, Cyber Operations Units, Homeland Security

TEAM RECOMMENDED SKILLSETS

Computer Science, Cybersecurity, Data Science, Information Systems, Software Engineering, International Relations, Computer Engineering