TECH INSIGHTS

# THE CONNECTIVITY CHALLENGE

—

**DRONES AND PHONES:** CONNECTING COMMERCIAL TECHNOLOGIES FOR TACTICAL SUCCESS

## FASTER, CHEAPER… MORE CONNECTED

Commercial uncrewed aerial vehicles ("UAVs") and cellphones – drones and phones – create new possibilities for multiplying the tactical capabilities of ground forces. Both technologies have found applications in recent conflicts. Cellphones have been a key tool for insurgents and terrorist organizations since they emerged. More recently, commercial drones have appeared in conflicts in Crimea, Afghanistan and across Africa. However, the combination of these low-cost, widely available technologies has developed during the current conflict in Ukraine, and it is changing the way large-scale ground forces operate. Connecting drones and phones creates a new kind of distributed, low-cost combat power. When information can move easily from a low-flying commercial drone to an operator connected by phone or radio to tactical networks, the speed and lethality of ground combat increases. Commanders who can make these connections are changing the way large forces operate.

The impact of connecting drones and phones is obvious to observers of the Ukraine conflict. One senior Russian commander stated in blunt terms:

*"Commercial UAVs have revolutionized reconnaissance and artillery weapons fire, including target acquisition and adjustment, and become a true symbol of modern warfare."* [1]

–

*Russian General Yury Baluyevsky*

But the full military advantages of commercial UAVs and cellphones only appear when these technologies are integrated into a system for reconnaissance and artillery fire support. Without the right integration, soldiers are unable to move data between phones, drones, and commanders. They make mistakes and lose time when data is manually transcribed, coordinates are incorrectly recorded, or reports are garbled.

What can developers do to ensure that commanders gain the full advantages of emerging commercial technologies? The answer lies in solving the physical, digital and security challenges of connecting these commercial technologies. To win with drones and phones, developers must focus on the connectivity challenge.

# THE CONNECTIVITY CHALLENGE: MOVING POWER AND DATA BETWEEN DRONES AND PHONES

Commercial technology is inexpensive and easy to use. Connecting these technologies to allow easy, reliable movement of data, signals and power is not easy, because these technologies are usually designed as standalone products. Efficient connections require a systems approach to address physical, digital and security-related requirements.

## Making the Physical Connection: Keep It Open and Commercial

Commercial drone technology and cellphones are available from many vendors across a broad global supply chain. Tactical modernization approaches that focus on developing a closed ecosystem of sensor and communications technologies will miss the opportunity to incorporate hardware from a full range of potential providers. This approach makes forces more vulnerable by restricting the availability of commercial technology.

An open-systems approach such as those provided by USB and HDMI standards used for commercial technology can exploit common physical connections between devices. Soldiers should be able to make physical connections between the hardware components of their equipment to allow easy movement of power, data, and signals. Physical connections are likely to be more widely acceptable than wireless or Bluetooth-powered connections because of requirements to minimize radiated energy.

In practice, this is likely to mean that small, inexpensive hubs with the ability to connect phones, batteries, cameras, drone controllers, tactical radios and other digital equipment will convey significant advantages. Soldiers should be able to quickly configure a "mission set" with whatever digital technology is at hand, and to switch devices instantly with simple commercial connectors and cables.

This "open and commercial" approach also allows soldiers to power their digital equipment with commercial power banks and share power among devices, providing flexibility and extending mission times.

## Making the Digital Connection: It's All About the Software

Soldier-worn commercial devices can be physically connected, either directly or through hubs, but they must communicate with each other to create tactical advantages. A drone controller with GPS may be able to locate a target, but unless the target data can be passed to a battle management system and sent via phone or radio, the target coordinates must be manually transcribed and transmitted. This can lead to transcription or transmission errors and lost time.

Battle management software such as the US ATAK or Ukrainian GIS ARTA fire direction platform can provide a common base for integrating commercial devices through USB or other physical connections. Different devices require individual software utilities to make the data connection to ATAK/ARTA or other systems.

Software integration of commercial devices may prove to be the most challenging barrier to effective use of drone-generated data. Manual workarounds are used in today's operations, but a real "plug and play" approach for processing and transmitting data from hardware created by multiple vendors would provide an advantage for operators and commanders. Such an approach would also simplify logistics in forward areas, by allowing soldiers to integrate whatever device or power supply is at hand.

## Maintaining Security: No Edge Storage and No Easy Fix

Connecting commercial devices to military networks in a tactical environment is a real headache for security professionals because of the risks of infiltration, data spills or other security breaches. One challenge that has not emerged in Ukraine is large-scale cyberattacks on tactical networks equipped with commercial technology. A recent study of cyber operations in Ukraine concluded that Russia has "struggled" to integrate cyber and conventional effects on the battlefield due to the resilience of Ukrainian cyber defense and Russian focus on strategic cyber operations.[2]

However, widespread use of commercial drone technology, phones, power banks and other peripherals is unlikely without reliable security. An emerging approach is simply to avoid edge storage of tactical information – no map or mission data stored locally on phones or other soldier-worn devices. Encryption and other basic communications security procedures, combined with frequent movement by tactical units, may be an adequate solution in the short run.

## HOW "DRONES AND PHONES" CREATE TACTICAL ADVANTAGES

Integrating small, inexpensive commercial drones and cellphone technology has already delivered important tactical advantages for Ukrainian forces. Summarizing the effects of these commercial technologies, one analyst concluded:

*"Ukraine's ability to blend commercial drones into its broader aerial arsenal and team it (sic) with traditional weapons and ground troops is a bedrock of its success at resisting the more powerful Russian military."* [3]

–

*Kerry Chávez, Modern War Institute*

Looking beyond the Ukraine conflict, at least three future use cases seem likely to emerge from continued integration of drones and phones.

**USE CASE 1**

**Every Soldier is a Scout**

In earlier conflicts, tactical reconnaissance was often left to specialized troops or small units. In the future, soldiers equipped with inexpensive, well-integrated drones and cellphones or tactical radios will be fully equipped to transmit detailed intelligence on enemy force locations and movements. Small drones with GPS location capabilities will transmit precise coordinates to soldier-operators at the forward edge, allowing a full picture of real-time enemy deployments without using piloted aircraft or satellites. Assembling data from operators across a wide front will provide senior leaders with the clearest possible picture of an evolving battle. Forward area soldier-operators will be able to generate this intelligence with minimal risk because they can deploy expendable drones. Commanders wanting more detail will simply trigger drone cameras, without placing soldiers at risk.

Low-cost, well-integrated commercial technology makes this possible. Without this advantage, soldiers must rely on traditional reconnaissance techniques or request expensive, slow aerial surveillance.

**USE CASE 2**

**Every Soldier is an Artillery Observer and Firing Battery**

With small commercial drones, GPS, mapping software like ATAK or ARTA and cellphones, individual soldiers can send fire missions to artillery batteries, or deliver small warheads directly from a hovering drone.

This new use case, demonstrated regularly by Ukrainian forces, allows small units to maintain continuous contact and deliver harassing fires, or call for heavier weapons with speed and accuracy. One Ukrainian volunteer summarized the situation:

*"We almost always know where their major units are, what they are doing, and the routes comprising their supply lines…[A]rmed drones are…taking out personnel and…damaging vehicles and armor. Often the same drone that finds something also destroys it."* [4]

This new development in small unit tactics changes how armies plan and deliver fire support, and how attacking units think about massing and maneuver. Improved integration of drones and phones will accelerate these changes.

**USE CASE 3**

**Every Soldier is a First Responder**

Western armies made significant advances in care of battlefield casualties during the extended lower-intensity conflicts in Afghanistan and Iraq, where air superiority allowed use of air evacuation during the "Golden Hour" – the brief period following a soldier suffering an injury.

However, higher-intensity conventional conflicts between forces with less sophisticated battlefield medical capabilities – as in Ukraine – have increased front-line losses. If medical personnel cannot reach a casualty, then a soldier may not receive life-saving care.

The same integrated capability that sends drone-generated data over cellphones and radios may provide a new use case for battlefield medicine. A soldier equipped with a small video camera and a few simple biometric sensors can now be linked directly to a remote field hospital. This link can allow a trained medical professional to guide a first response, triage casualties and maximize the impact of scarce medical resources. "Drones and phones" may prove to be lifesavers, as well as tactical enablers, as the integration of video, GPS data and cellphones becomes more systematic and widespread.

Part of Conextivity Group

## YOUR ARMY'S PARTNER FOR SOLVING BIOMETRIC CONNECTIVITY CHALLENGES

Making the power and data connections that enable digital transformation is the core skill of the Conextivity Group, of which Fischer Connectors is part. From simple, reliable connectors and cables designed to meet strict military requirements and tactical hubs that connect sensors and minimize the soldier's physical burden, to advanced microelectronic solutions that optimize the performance of sensors and soldier-worn devices on military networks, the Group provides real solutions for the "Connectivity Challenge" facing today's commanders. Conextivity has the **innovation skills** to capture the military advantages of biometric technology, the **agility** to work on accelerated Army timelines, and the rigorous **attention to detail** in design and manufacturing to meet the most stringent Army requirements.

## FISCHER CONNECTORS EXPERTS

**Olivier THORMANN** – Defense Product Leader

**Xavier BIZE** – Lead Software Engineer, Defense Products

**Tomislav HAJAK** – Lead Hardware Engineer, Defense Products

## SOURCES

1. Cited in Chávez "Learning on the Fly" available at https://www.armscontrol.org/act/2023-01/features/learning-fly-drones-russian-ukrainian-war
2. See Mueller et al. "Cyber Operations During the Russo-Ukrainian War" available at https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war
3. See Chávez, op. cit.
4. "Ukraine Volunteer Transcripts" available at https://ukrainevolunteer297689472.wordpress.com/2022/11/05/and-by-god-it-worked; cited by Chávez, op. cit.