THE IMPORTANCE OF COLLABORATION FOR BUILDING SUPERIOR MISSION CAPABILITIES

By Clyde Seepersad, Senior Vice President, General Manager, Education, Linux Foundation

Photo provided by Adobe Stock

Recently, I had a conversation with a Marine working on air-gapped, edge cloud solutions in the field. He pointed out that the military is focused on building IT workflows and tools that save time because, on the battlefield, time equals lives.

Since the *Art of War* was penned more than 2,500 years ago, militaries have sought the means to establish battlefield superiority to save lives and conquer the enemy. Today, the battlefield is less a plane and more of a sphere. We continue to have traditional boots-on-the-ground battlefields, but now every electronic device in every business, piece of infrastructure, and home around the world represents a potential virtual combat zone. Add space as a theatre of operations to this virtual combat zone and the volatilities, complexities, and ambiguities increase exponentially.

It's not uncommon to read comparisons of today's global geopolitical situation to those that led to World War II. The need for battlefield superiority in that war united a team of scientists to harness the power of fission in The Manhattan Project. Achieving superiority today will require uniting the whole of the United States civilian and military defense structure to build a sphere of technology that leverages the vast array of software, global networks, and massive data sets to deliver critical insights in real time to command leadership, as well as the boots on the ground. The biggest difference this time around is that much of the software powering these capabilities is collaboratively developed under open-source licenses, which has significant implications for the path of getting from an innovative idea to high-quality, mission-ready digital products that help the U.S. achieve its military objectives.

Unlike The Manhattan Project's clear end goal, realizing information advantage across this expanded "battlesphere" at echelon and across all domains require constant innovation just to keep pace with evolving technology. Constant innovation is not something the U.S. Army or the U.S. Department of Defense can achieve on their own. Success will require unified collaboration across the civilian and uniformed U.S. military, its foreign partners, and their technology industry partners. Among industry partners, the open-source community's systems operate at a global scale to collaboratively build and improve secure, efficient, and innovative software technologies that are easy to access and use.

CULTURE FIRST

While technology itself can do much of the heavy lifting, the effort must begin with an honest assessment of the culture. If organizational culture doesn't support an operational structure and strategic objectives, the effort to leverage rapid and persistent innovation is bound to fall significantly short of its goals if not outright fail. All civilian and military members of the armed forces must be seen as integral technology infrastructure of the organization. Their habits and behaviors will directly affect the security and capability of government information technology systems, but that extends beyond the official government networks and devices. Every person has their own personal devices — phones, watches, gaming consoles, and so on — that create both risk and opportunity. How users introduce and utilize personal or issued devices in military technology ecosystems can have a diverse, often unintuitive, cascade of operational or even strategic consequences.

Above, U.S. Army Capt. Jonathan J. Springer, fire support officer for 1st Battalion, 327th Infantry Regiment, 1st Brigade Combat Team, 101st Airborne Division, tests his new smart phone application in eastern Afghanistan's Pech River Valley Jan. 9, 2011. Capt. Springer, a Fort Wayne, Ind., native, invented the navigational application to find an inexpensive yet reliable tool for soldiers to use while at home or in a deployed environment.

Left, Capt. Springer tests his new smart phone application in eastern Afghanistan's Pech River Valley Jan. 17, 2011.

Photos by: U.S. Army Sgt. 1st Class Paul Shoemaker

There are two examples of this from the post-9/11 conflict in Afghanistan that articulate the risks and benefits of personal devices and individual user initiative. In early 2018, it was made evident that not seeing everyone's digital footprint — and not accounting for all of their devices — as part of the military's tech infrastructure exposed a significant vulnerability. The event revealed that watches with GPS tracking were revealing highly sensitive information about the locations and activities of service members at U.S. military installations overseas. Conversely, a U.S. Army field artillery officer built the app *TacticalNav* from the ground up to create a low-cost, highly accurate mobile navigation platform specifically for military service members. That self-financed effort shows the opportunity that untapped talent within the organization presents and reinforces the promising benefits of technological innovation driven from the bottom-up, as well as the top-down.

OPEN-SOURCE AND THE COMING TECH LEAP

Any leader who looks back at the ever-increasing rate of technological innovation and feels confident they are prepared for what is coming needs to shift their focus from the last 20 years toward an accelerating future. The coming confluence of quantum computing, generative artificial intelligence, ultra-high bandwidth, satellite proliferation, and edge computing will redefine our expectations of the rate of technological transformation. In the process, it will transform every aspect of warfare including how tools and armaments are deployed, where the so-called front of the battlefield is, and the roles humans will play.

What is the key to integrating these technologies to generate advantage and build mission superiority? Software, specifically open-source software, is the answer. For example, listed below are several opensource technology projects that currently impact this new spherical theater of cyberspace, space, and the rest of the battlefield:

QIR ALLIANCE enables a community-driven effort to develop a forward-looking, fully interoperable specification for quantum computing programs.

PYTORCH and **LLAMA** for AI were both originally developed by Meta and are now open-source projects supporting the development of generative AI platforms and products.

ONAP is an open-source platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers and enterprises along with **FDO** (FIDO device onboard). Both open-source platforms are considered essential for effective cloud and edge management and security.

EDGEX FOUNDRY is an open-source platform that facilitates interoperability between devices and applications at the internet of things' (IoT) edge while **AKRAINO** is an open set of application and infrastructure blueprints for the Edge.

The advantages of select open-source or commercial off-the-shelf technologies are significant, especially when it comes to opportunities to build on innovation, as well as capitalize on battlefield superiority. Firstly, because open-source is built by a community of interested organizations and IT developers, it attracts the best and most experienced technology professionals. Secondly, because the most useful open-source software is constantly being used ("consumed" in open-source parlance), it is being continuously vetted for security, resulting in some of the most secure technology solutions available.

OPEN-SOURCE CAN BE PUBLIC? PRIVATE? PERMISSIONED? ALL OF THE ABOVE?

Perhaps the biggest and least understood advantage of open-source is that it easily enables confidential solutions that stay confidential. Open-source usually sits at the core of a technology or software solution enabling developers and engineers to start with a fully built framework. This saves time and resources, allowing IT professionals to focus on building the more intricate customized tools and solutions needed. Importantly, those solutions, once developed, can remain highly confidential, subject to all the typical security considerations. Any organization or individual that uses open-source software has the option to share ("contribute" in open-source parlance) anything they create, but they are under no obligation to do so.

There are many well-known examples in the commercial sector, such as public cloud service providers Amazon AWS, Microsoft Azure, and IBM Bluemix, which are all built on the open-source operating system Linux and use Kubernetes. Similarly, public and private network operators including AT&T, Verizon, Nokia, Ericsson, and T-Mobile all rely on open-source versions of ONAP and FIDO to keep their network operations consistent, efficient, and secure.

A particularly excellent example for the military comes from the U.S. Joint Office of Energy and Transportation, which has just adopted the EVerest open-source framework for developing the nation's electric vehicle (EV) charging infrastructure. The EVerest open-source technology project develops and maintains a software stack for energy communications across charging stations, vehicles, generation resources, batteries, adjacent chargers, power grids, backend payment systems, user interfaces, and mobile devices. The project will enable the nation to overcome the incompatibilities of proprietary systems as it builds out its EV infrastructure.

The true power of open-source lies in the massive opportunities it creates for decentralized innovation. It is built through a culture of community that has proven, strong structures and tools to facilitate that innovation. That culture attracts passion and creativity that encourages the kind of interdisciplinary collaboration needed to solve complex problems. For example, to successfully thwart enemy missile attacks, a team of co-operators will need to intercept and interpret intelligence, infiltrate launch software, distort GPS data to affect its course, or use quantum-powered AI to intercept it in flight if all else fails. All of these capabilities require leaders who are willing to invest in building the right culture, providing outcome-focused training and conducting structured experiments that deliver repeatable results.

How do you build and nurture a collaborative community mindset across all our military domains to ensure technologically superior mission capabilities? The old-fashioned way, by following the principles of mission command to build trust and esprit de corps that facilitates and encourages decentralized collaboration. The first step? Recognize that everyone—all Soldiers, all leaders, all people—are technologists. With the right training and skills, everyone has data and ideas to contribute to the community. Ideas that, when parsed by the community, will result in time and lives saved.

Author bio: Clyde Seepersad is responsible for the education arm of the Linux Foundation. Over the past decade, Clyde held senior leadership positions in the education space.

Prior to his involvement in education, Clyde was a Principal at the Boston Consulting Group, He started his career in the public sector, working within the Ministry of Finance in Trinidad and Tobago. He holds a master's in business administration and a master's in economics from Oxford University, where he was a Rhodes Scholar.