Air Land Sea Application Center
Joint Base Langley-Eustis, Virginia
https://www.alsa.mil

WINNING THE COUNTERLAND BATTLE BY ENABLING SENSOR-TO-SHOOTER AUTOMATION

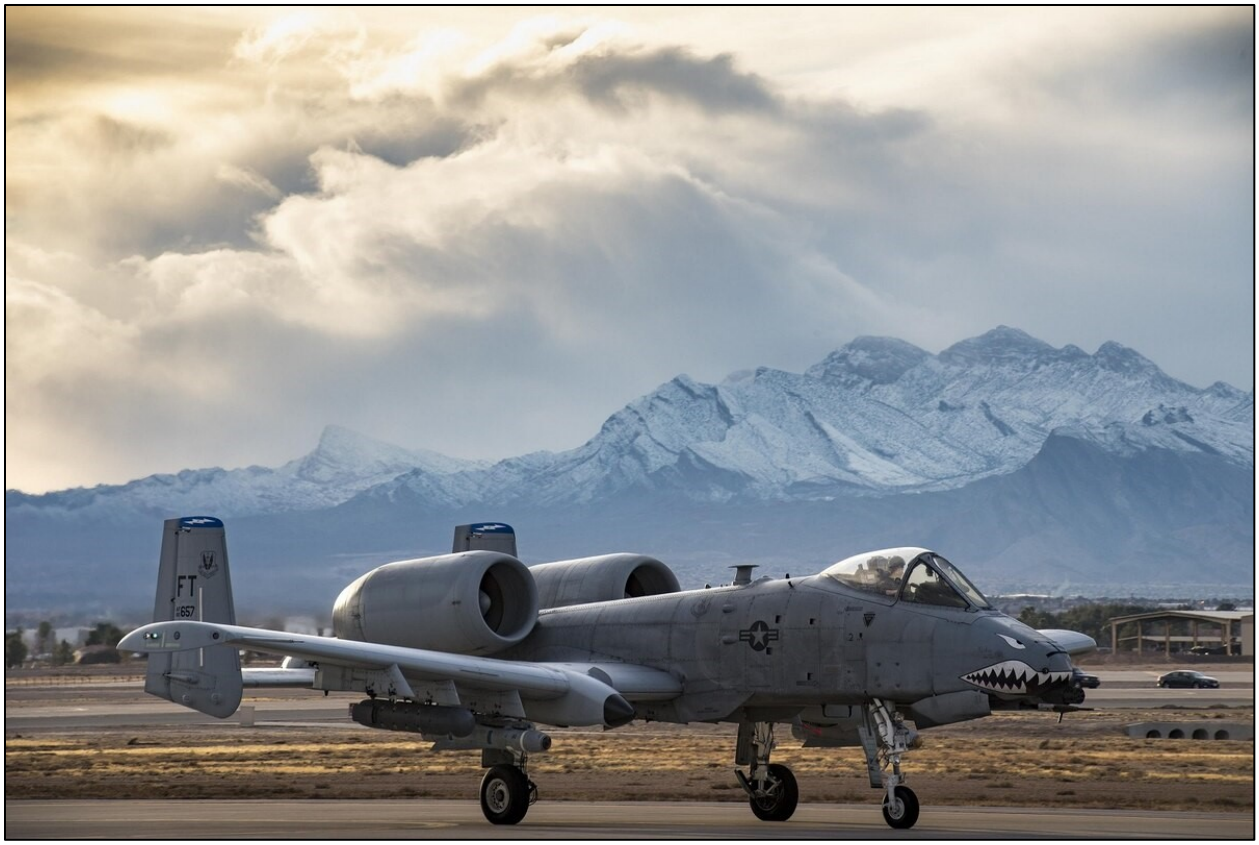
By Maj Ridge R. Flick, USAF

Twenty years of counterinsurgency (COIN) operations in Iraq, Syria, and Afghanistan created a construct where precision fires and low-collateral effects were prioritized. The enemy's detectable signatures (DSIGs) continued to shrink as they learned to evade our intelligence, surveillance, and reconnaissance (ISR) capabilities. In response, the Joint Force bolstered ISR capabilities with new sensors, platforms, and databases. The tactics, techniques, procedures, and habits from COIN operations create a significant hurdle in preparing for great power competition. However, the ISR capabilities developed in the last twenty years may be the single great advantage the US enjoys.

The majority of ISR assets in the Air Force will not be available for close air support (CAS) or strike coordination and reconnaissance (SCAR) in the next great power competition. However, theater and national-level reconnaissance assets cover large swaths of the battlespace, including the area between the forward line of own troops (FLOT) and the fire support coordination line (FSCL). However, there is one big problem with utilizing these assets in CAS; the slow and tedious information flow from sensor to shooter. Three factors hinder the ability to utilize intelligence gathered from strategic ISR assets in near real-time: 1) SATCOM downlink time; 2) intelligence processing, exploitation, and dissemination (PED); and 3) information flow from command and control (C2) to the joint terminal attack controller (JTAC) and CAS assets.

Addressing challenges with SATCOM downlink time are beyond the scope of this article; however, intelligence PED and information flow from C2 to the CAS team are worthy topics. In fact, the technologies exist to drastically hasten both processes today. Clever intelligence and operations personnel are exploiting automated intelligence reporting and machine-to-machine communication to solve specific problems within their communities. The combination of the two techniques provides a framework to develop a common operational picture (COP) across the services and improve the efficiency in sensor-to-shooter information flow. Advancing the two techniques to provide capabilities beyond an incremental improvement requires a significant alteration in how the USAF utilizes its intelligence, surveillance, and reconnaissance operations and datalink experts. This article serves as a call to action for all subject matter experts

to pitch in and help build the baseline rules and processes for military automation to succeed in the future.



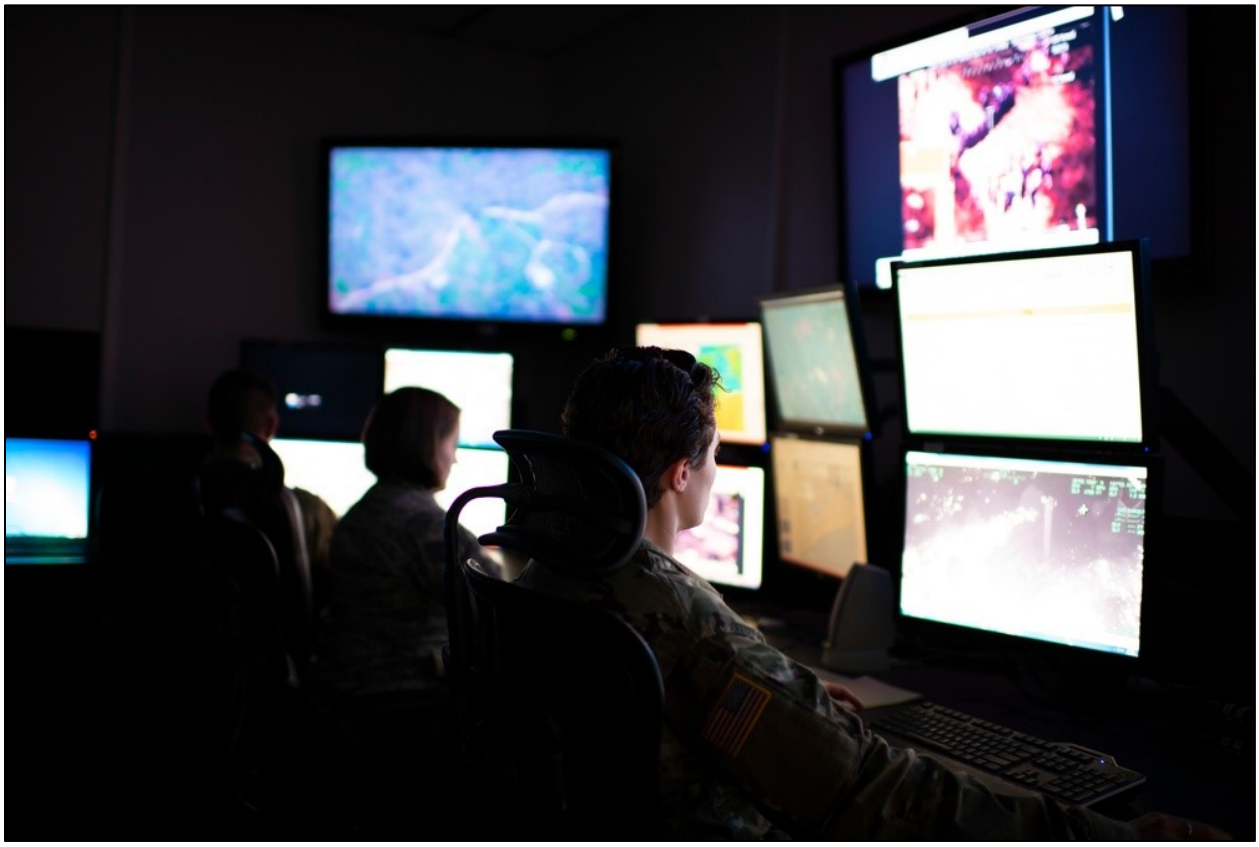
An A-10C Thunderbolt II from the 74th Fighter Squadron taxis down the runway during Green Flag-West 17-03 Jan. 23, 2017, at Nellis Air Force Base, Nev. (Photo by SSgt Ryan Callaghan, USAF; https://www.dvidshub.net/image/3129957/mountain)

AUTOMATED INTEL PROCESSING, EXPLOITATION, AND DISSEMINATION

After two years of watching his beautiful intelligence collection plans lead to minimal effects in the battlespace, Captain Alex "Bomb" Milhous, from the 19th Weapons Squadron at the United States Air Force Weapons School (USAFWS), decided to find out why his plans failed. As an intelligence professional, "Bomb" looks at a kill-chain by analyzing the process from the first detection of an enemy system to a bomb, missile, rocket, or bullet achieving a desired level of destruction. For now,[1] the United States Air Force breaks a kill-chain down into six steps: find, fix, track, target, engage, and assess (F2T2EA). After combing through the data from dozens of large-force exercise missions, "Bomb" found individual assets responsible for a portion of F2T2EA rarely failed. However, the time required for information to move from one asset or platform to another could not keep pace with enemy actions.

The amount of information pouring into a distributed ground station (DGS) is immense. Multiple teams of specialized intelligence analysts perpetually sweep the information for reportable intelligence. Reportable intelligence is information that meets specific criteria established prior to an operation or mission. As an example, Russia having an SA-17 surface-to-air missile system is just information. A satellite imaging of the SA-17 site this

morning and having Category 2 coordinates for the location is reportable intelligence. In order to go from information to reportable intelligence, the DGS members process all the information, exploit the information meeting reportable criteria, then forward the intelligence to command and control for dissemination to the pertinent ground and air players. The system of processing, exploiting, and disseminating intelligence is called PED, and you'll regularly hear the term "PED team" in intelligence circles. The PED team essentially works hand-in-hand to turn information into reportable intelligence by cross-cueing multiple streams and/or databases of information. The PED team continually fights through using multiple disparate systems, waiting on other analysts to cross-cue their information, transposing information from one format into another, and rarely sees the final result of their efforts. After all, while typing the intelligence into another system, more information is inbound. Unlike Al Bundy or Uncle Rico, the PED team simply cannot dwell on the past if they wish to influence the future.



Indiana Guardsmen Intelligence Analysts train at Hulman Field Indiana National Guard Base, Ind., Oct. 22, 2019. (Photo by: TSgt Luke R Sturm, U.S. Air National Guard; https://www.dvidshub.net/image/5855644/intelligence-analysts-train-181st-intelligence-wing)

The PED of information into reportable intelligence regularly takes dozens of minutes depending on the system used to collect the information and the speed of the analyst. Like any human, analysts sometimes make mistakes while transposing the information from one system to another. Historical data from Weapons School integration exercises show about 30% of the reportable intelligence included some form of error when comparing the information in the database to the information received by the fighter or

bomber. If you can't hear programmers rolling over in their graves right now, you may not understand the value of databased information.

Databased information is extremely useful. Databases allow for custom filtering, sorting, and hiding or highlighting information. However, databased information becomes troublesome when multiple databases contain the pieces of information needed to create reportable intelligence. As an example, an electronic intercept in one database might prove a particular system is in a three-by-six-mile area; but, by most standards, that is just information. In another database, a picture from yesterday might show the system of interest in that area, but someone needs to FIND the system in the picture. Cross-cue is the process to take information and cue other sensors or exploit other information sources to reach reportable intelligence criteria. Right now, cross-cue requires an analyst of one variety to notify other analysts they have information requiring refinement. Then, other analysts must notice the request and begin looking through their information to refine the location of the system of interest. Cross-cue may also require a different analyst to change his/her current task in order to refine the information to reportable criteria. Cross-cueing is rarely fast and occasionally doesn't happen. Again, people make mistakes.

In an effort to reduce the workload of the analysts at the DGS, "Bomb" began working with the civilian sector on a new process. CACI International developed software called the Multi-INT Spatial Intelligence Toolsuite, or MIST.[2] MIST exists under the Fusion Analysis Development Effort (FADE) program. The combination of the overarching program and the underlying software is commonly referred to as "FADE-MIST." FADE-MIST accesses as many intelligence databases as the user is cleared to access and incorporates a visual interface (think Google Earth). Users can sort, filter, and view a significant majority of all the information available to the intelligence community on a convenient 3D or 2D global projection. The plotting capability alone makes FADE-MIST excellent for creating intelligence products and assessing enemy trends through their playback feature, which allows a user to look at specific information collected on a particular day.

WATCHBOX is an additional tool in FADE-MIST allowing users to create a series of if-then logic filters. The if-then logic filters run against multiple intelligence databases to find and extract reportable intelligence. Through selecting unambiguous detectable signatures for specific systems and filtering results to a specific area, WATCHBOX combs the databases for the user. When all if-then logic filters are met, users may select three notification options. Internal to the user's profile, WATCHBOX can send a notification on the app (think Facebook notification on your phone). More importantly, WATCHBOX can send an automated, user-formatted Mardam-Bey Internet Relay Chat (mIRC) message into specific chat rooms.[3] Finally, the user may opt to receive an email.

Once a WATCHBOX logic chain is developed, any other user may subscribe to the results (email or notification). The owner of the chain is the only one able to control the pre-formatted mIRC messages and chat rooms. Current PED processes involve analysts knowing which mIRC chat room is appropriate for the information they have exploited. WATCHBOX allows the room to be predetermined based on the type and accuracy of the information. WATCHBOX also pulls the information directly from the

database, so there are no transposition errors from one system to the other. As a notional example, let's look at a mission where the SA-37 surface-to-air missile system needs to be located within the Republic of Merlin.

The first if-then logic filter weeds out all other systems. The SA-37 has multiple *ambiguous* detectable signatures, which means a particular intercept could be the SA-37 acquisition radar, or it could be something completely unrelated like an air traffic control radar. These signals are good for cross-cueing other sensors, but we're going to look at a completely automated example. The SA-37 has a few *unambiguous* detectable signatures, which means those signatures are unique to the SA-37. The unambiguous detectable signatures allow significant automation, as they do not require cross-cue of other intelligence sources to confirm the presence and/or location of the SA-37. Our first filter will focus on finding the unambiguous detectable signatures associated with the SA-37 across all databases. For visualizing the automation, we'll say this filter takes five billion pieces of information and pares the group down to 10,000 pieces of information.

The second if-then logic filter weeds out all pieces of information that don't meet reportable intelligence criteria. In this example, we'll say the mission commander did not want any SAM locations passed to the fighter and bomber pilots unless the fidelity of the location is better than two nautical miles. Applying this filter to our group of 10,000 leaves only 50 pieces of information. These 50 include *unambiguous* detectable signatures for the SA-37 and include better than two nautical mile accuracy.

Finally, the third if-then logic filter is designed to eliminate information that is not in the operating area of the mission. This filter creates a geographic boundary around the Republic of Merlin and removes all information outside of the boundary. After applying this filter, our 50 pieces of information are cut down to five pieces of information that meet all of the "reportable intelligence" criteria set by the mission commander. Now, WATCHBOX pulls the critical data fields out of these pieces of information, populates the pre-formatted mIRC messages, and posts them into the pre-determined chat rooms. At the same time, USAF, USA, USMC, and USN C2 entities gain situational awareness on the location of the SA-37's in the Republic of Merlin.

The example above shows the value of automated intelligence reporting. It is critical to understand the SA-37 is just one system with a fingerprint made up of ambiguous and unambiguous detectable signatures. Nearly every system on the modern battlefield transmits, leaves tracks, makes a wake, makes noise, or creates some type of signature. As the intelligence community defines a system's fingerprint, new if-then logic filters may be created to "find" the system within the DoD's ever-growing databases.

As mentioned in the introduction, PED is one of two areas ripe for improvement. The other area is information flow from intelligence agencies through command and control to the tactical edge.

MACHINE-TO-MACHINE COMMUNICATION[4]

In Korea, the long-range artillery threat posed by the Democratic People's Republic of Korea (DPRK) against the Greater Seoul Metropolitan Area (GSMA) presents a unique challenge to joint targeting. The DPRK utilizes various types of bunkers and tunnel systems to protect its long-range artillery, and trains to shoot and take cover within

those protective bunkers. In many cases, the first detectable signature is the enemy artillery round flying through the air, which the US and Republic of Korea (ROK) Army detect via counter-fire radar systems, like the AN/TPQ-53 Radar System (Q-53).[5] Unfortunately, due to the limited signatures associated with a vehicle driving out of a bunker, the required timeline for a successful engagement against a DPRK artillery system is extremely short. However, the Q-53 feeds the Advanced Field Artillery Tactical Data System (AFATDS), which allows rapid dissemination of targets across the Army's fires platforms.[6] When Army artillery units are within range, it is only a few minutes from the Q-53 locating the enemy firing position to friendly rounds raining down. When Army artillery units are not in range, the *fires cell* passes the targeting information up to higher headquarters for relay to air force C2, who passes the information to the nearest untasked fighter. In practice, the manual passage of the information regularly exceeds 20 minutes and cannot keep pace with the most liberal associated timelines.

In order to shorten the kill-chain, A-10C pilots from the 25th Fighter Squadron and artillery officers from the 210th Field Artillery Brigade developed a system called ATTACKS; the Automated Tactical Targeting and Counter-fire Kill-chain System. Despite the corny homage paid to the Warthog in the acronym, the system is brilliant.

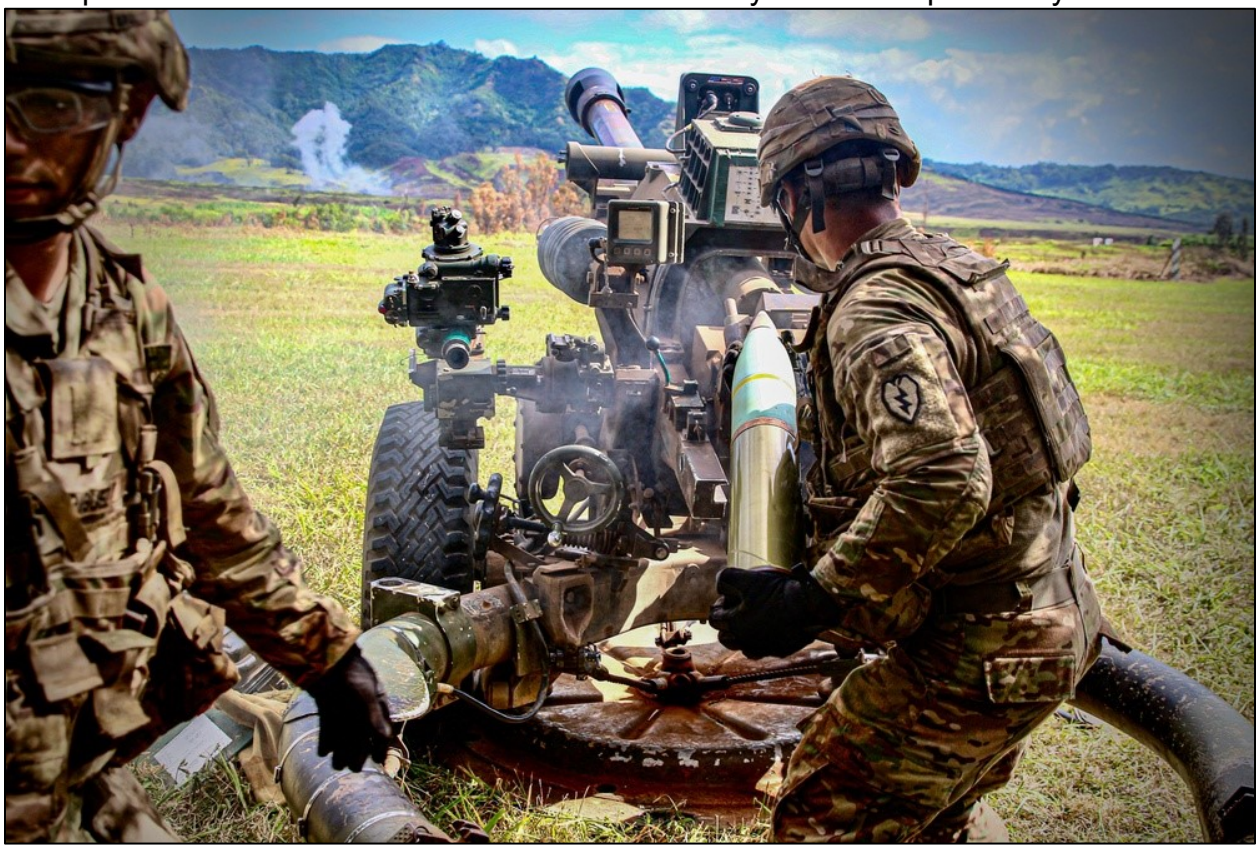
AFATDS uses variable message format (VMF) and the message types are all various "K-series" messages. As an example, a fire mission, which is typically a transmission made to target the enemy with artillery, can be sent over AFATDS as a K02.4. There are hundreds of other message types in VMF, but that's not important. The Air Force's primary datalink is Link-16. Link-16 speaks in "J-series" messages. As an example, a pilot in a Link-16 equipped aircraft can "show" what they are targeting by transmitting a J12.6, which other Link-16 equipped aircraft can see. Again, hundreds of message types are available in Link-16, but that's not important either. The important part is that Link-16 and AFATDS can't talk directly to each other due to differences in the message formats. All messages going from one datalink structure to the other require a person to transpose information or a machine-to-machine translator.

In both methods, either a human or a machine pulls the data fields out of a message in one format, plugs them into the data fields of a message in a different format, and sends them to the entire network, or a specific address. Humans are inherently worse at transposing information than machines. We make mistakes, get distracted, and certainly can't type as fast as a machine can "think." To avoid human transposition delays and errors, a particularly clever A-10 instructor pilot, Captain Benjamin "TOD" Baumann, leveraged a relationship with the Sierra Nevada Corporation, which makes the Tactical Radio Application eXtension (TRAX).[7] TRAX enables machine-to-machine communication by translating over two dozen different message formats (more in development). "TOD", in conjunction with an Army Fires Center of Excellence graduate, defined the specific Link-16 messages they wanted to automatically translate into AFATDS messages, and vice versa, then sent their information exchange requirements (IERs) to Sierra Nevada. Within a few weeks, "TOD" installed a new, prototype version of TRAX in Korea and began testing to refine the message translations and user interface of the software. In a few months, the 210th Field Artillery Brigade and 25th Fighter Squadron completely automated the process of passing specific Q-53 target

data from AFATDS into Link-16, including formatting the Link-16 messages to convey the accuracy of the radar's target data.

In addition to moving information from AFATDS into Link-16, the team in Korea worked with Sierra Nevada to enable moving information from Link-16 into AFATDS. Now, when aircraft identify a target within range of friendly artillery but lack the weapons to engage, the pilot is able to digitally send targeting information directly to the brigade fires cell.

The advances made in Korea represent a significant improvement in the counter-fire kill-chain across services. The process of defining information exchange requirements and utilizing message translation to enable machine-to-machine communication creates a template to shorten thousands of kill-chains in every area of responsibility.



Soldiers with 2nd Battalion, 11th Field Artillery, 25th Infantry Division work with M119 Howitzers to enhance their basic artillery skills on Schofield Barracks, Hawaii, June 14, 2020. (Photo by 1st Lt. Stephanie Snyder, USA; https://www.dvidshub.net/image/6682381/field-artillery)

COMBINING M2M COMMUNICATION AND AUTOMATED INTEL REPORTING

Machine-to-machine communication and automated intelligence reporting seem unrelated. However, just like AFATDS uses K-series message formats and Link-16 uses J-series message formats, automated intelligence reporting uses text message formats. The process of pulling data fields from one message type and plugging them into another is not format agnostic; however, the mIRC messages created by WATCHBOX are designed by pulling data fields from ISR sensor data. The messages are also designed in a standard format.

Leveraging Capt Baumann's contacts at Sierra Nevada, I worked with the TRAX programmers to create a standard mIRC message format to enable translation into J-series and K-series messages. When WATCHBOX creates an automated intelligence report and sends a mIRC message to command and control, it also sends another mIRC message to a chat room TRAX is monitoring. Using the standard mIRC message format, TRAX pulls the data fields required for J-series and K-series messages, and depending on the type of system and fidelity of the information, TRAX publishes the information into Link-16 and AFATDS.

Combat Air Forces' Close Air Support Working Group at the 2021 Weapons and Tactics Conference focused on improving surface-to-air and air-to-surface target transfer. During one day of the conference, the group focused on shortening a particularly difficult kill-chain. Using the same machine-to-machine communication techniques developed in Korea, the group was able to shave about 5 minutes off the timeline, but the enemy system still survived. Incorporating automated intelligence reporting shaved another 20 minutes off the timeline and enabled advanced exploitation techniques not available through standard datalink classifications. Once we integrated machine-to-machine communication with automated intelligence reporting, the entire kill-chain shortened by 30 minutes. Again, shortening one kill-chain is a small step forward. The process of educating tactical experts on the use of automated reporting and M2M communication, then cutting the experts loose to shorten a kill-chain is a giant leap.

THE WAY FORWARD

Machine-to-machine communication and automated intelligence reporting provide incremental improvements when used alone. Combining the two techniques significantly shortens a kill-chain. In order to fully harness the existing architectures, databases, datalinks, and communication pathways in the DoD, tactical experts need education on how to leverage new software and computer processing technologies. Once educated, experts from each area of responsibility need to make a concerted effort to sit down together on a regular basis. At the table, educated experts need to work down the joint prioritized target list with a laser focus on shortening each kill-chain. The focus cannot stay on widgets and gadgets to find things faster or track them better. The focus must shift to the specific tactics, techniques, and procedures to move information *between* the widgets and gadgets comprising the kill-chain. Technology allows for faster information flow today, but smart intelligence professionals, operators, and controllers need to pitch into the fight with their expertise and minds open to new ways of doing business. If-then logic filters and digital translators are only as smart as their creators. To shorten thousands of kill-chains, we'll need a few hundred clever creators.

Major Ridge "KELSO" Flick is an active duty USAF A-10C Weapons Officer Instructor Pilot with assignments in the 25th Fighter Squadron, 354th Fighter Squadron, 355th Operations Support Squadron, 355th Operations Group, 66th Weapons Squadron and will serve at the USAF Warfare Center as a Combat Air Force's Fellow this summer. He has over 2,000 hours in the A-10C and flew combat missions in support of Operation INHERENT RESOLVE and Operation FREEDOM SENTINEL in Iraq, Syria, and Afghanistan.

End Notes

[1] Benitez, Mike. "It's About Time: The Pressing Need to Evolve the Kill Chain," War on the Rocks, last accessed October 22, 2021, https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/

[2] CACI. Multi-INT Spatial Temporal (MIST) Toolsuite [Fact sheet]. https://www.caci.com/sites/default/files/2020-02/F367_2002_MIST.pdf

[3] Wikipedia. (n.d.). *mIRC*. Retrieved October 22, 2021, from https://en.wikipedia.org/wiki/MIRC#History

[4] Shea, Sharon. (2019, August). *Machine-to-Machine (M2M)*. TechTarget. https://internetofthingsagenda.techtarget.com/definition/machine-to-machine-M2M

[5] Lockheed Martin. AN/TPQ-53 Radar System [Fact sheet]. https://www.lockheedmartin.com/en-us/products/tpq-53.html

[6] United States Army Acquisition Support Center. Advanced Field Artillery Tactical Data System (AFATDS) [Fact sheet]. https://asc.army.mil/web/portfolio-item/advanced-field-artillery-tactical-data-system-afatds/

[7] Gouré, Dan, (2020, March 20). *SOCOM Has Solved the Military's 'Tower of Babel' Problem*. RealClear Defense. https://www.realcleardefense.com/articles/2020/03/20/socom_has_solved_the_militarys_tower_of_babel_problem_115132.html

Disclaimer. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.