Spc. Jordon Purgat (*right*), assigned to the 1st Battalion, 187th Infantry Regiment, fingerprints an Afghan villager 7 May 2013 during Operation Shamshir VI in Khoti Kheyl, Zormat District, Afghanistan. (Photo by Spc. Chenee' Brooks, U.S. Army)

Identity

Enabling Soldiers, Supporting the Mission

Matt McLaughlin

An enemy must be classified strategically (Is it conventional, terrorist, insurgent, or hybrid?) and identified tactically (Is the subject a combatant or noncombatant?). This may seem simple at first glance; however, unconventional warfare with asymmetric enemies makes such determinations difficult for today's joint force. Without such considerations, no staff can devise a coherent military operation, and troops in the field might not be able to differentiate between threats and harmless civilians.

An Afghan Local Police (ALP) officer looks into a biometric eye scanner 18 December 2011 while being processed into the force by members of the Afghan Ministry of Interior in Gizab District, Uruzgan Province, Afghanistan. The ALP is a defensive, community-oriented force that works to bring security and stability to rural areas of Afghanistan. (Photo by Petty Officer 2nd Class David Brandenburg, U.S. Navy)

Unconventional forces conceal themselves and their affiliations to improve freedom of maneuver, organize command and control, and create lethal effects. These capabilities are amplified by increasingly inexpensive and commonplace technologies such as encrypted wireless communications and small unmanned aircraft. The net effect is to obscure the identities of those acting against U.S. interests and confuse our response.

Identity activities, as articulated in Joint Doctrine Note (JDN) 2-16, *Identity Activities*, are aimed at mitigating this gray area for U.S. forces.[1] By uniting tools such as site exploitation, forensics, and biometrics with information systems, intelligence analysis, and training—and, in the future, artificial intelligence—identity activities enable the joint force to deny the enemy anonymity, distinguish combatants from noncombatants, and take the fight to our opponents.

The Problem of Anonymity

U.S. interests today are confronted by a myriad of state and nonstate threats, but most share a common thread—the difficulty of identification and attribution. Terrorists hide their true intentions and affiliations, and then attack city centers without warning. Insurgents pick up weapons, conduct violent operations against their governments, and discard the weapons to melt back into their native population. And, in hybrid wars, the soldiers of a hostile state leave their uniforms behind to foment unrest against the governments of rival states. In each case, the perpetrators rely on anonymity—in contravention of the Geneva Conventions—for their success.

As described above, being identified would render the terrorist, the insurgent, and the hybrid soldier operationally ineffective, but the reasons why vary, as shown in table 1 (on page 37). It is worth considering the differences in the nature of these threats before discussing how identity activities can best combat them.

As defined in Training Circular 7-100, *Hybrid Threat*, a terrorist is "an individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives."[2] Insurgents engage in "organized use of subversion and violence … to overthrow or force change of a governing authority."[3] In either case, they can most likely be classified as unlawful enemy combatants, "persons not entitled to combat immunity, who engage in acts against the United States or its coalition partners in violation of the laws and customs of war during an armed conflict."[4] A hybrid threat may make use of these unconventional constructs in conjunction with regular military or paramilitary forces.

"Terrorist" is a broad term; he or she may be a lone individual with idiosyncratic motives or a member of a more organized cell-based group such as al-Qaida. In either case, the terrorist's immediate objective is not to control territory or establish any specific authority but simply to stage an effective attack with primarily psychological effects on the targeted population (apart from the immediate carnage). This means *a terrorist requires anonymity to strike without warning*. He or she must be able to cross borders without being flagged and needs time to plan and gather supplies free of interference from authorities. But once the attack (usually lethal to the assailant) is complete, anonymity is no longer necessary; the very opposite may be the case, as attackers often want their biographies, grievances, and affiliations broadcast to the world in a final act of self-justification.

Matt McLaughlin is the strategic communications contractor lead for the Defense Forensics and Biometrics Agency. A certified biometric professional, he holds a BS from Northwestern University, an MBA from Loyola University Chicago, and an MA from the U.S. Naval War College. His active and reserve assignments included three ships and a forward-deployed naval staff.

A quick word on domestic terrorists: terrorist attacks by those who plan and launch them within their country of origin (e.g., the Oklahoma City bomber) are most likely to be a law enforcement matter with no military involvement. As a result, domestic terrorism is beyond this article's scope; hence, the "international" modifier in table 1. However, foreign travel for terrorist training squarely puts even a domestic terrorist in the "international" camp for this analysis. Since they must cross international borders, they assume the character of international terrorists by visiting terrorist sites abroad and may encounter military forces and engage in activity clearly linking them to hostile groups.

Insurgents have more concrete objectives than most terrorists—they aim to undermine the legitimacy of existing authority in a given territory and replace it with their own. As such, insurgents must plan for the future and maintain their apparatus and organization. Consequently, *insurgents require anonymity to preserve their force* as well as to achieve tactical surprise. A particular terrorist threat may be over with the conclusion of a suicide attack; insurgencies, however, endure beyond any one incident. Its leaders, who may not be directly involved in tactical actions, must remain alive and free to provide both operational continuity and a propaganda stream; but, unless a third country is hosting them, they can only do this if hidden. Likewise, leaders without followers lack much power to influence events; so those foot soldiers of the insurgency must also remain anonymous if they are to avoid preemptive arrest by security forces.

Hybrid soldiers differ from terrorist groups and insurgencies in one key respect—they are answerable to a foreign government. This means *the principle purpose of anonymity is to provide a foreign government with deniability* of its people's actions. In this case, while hybrid soldiers' anonymity is used to enable their operations as terrorists and insurgents do, the bigger impact is to enable an aggressor state to avoid culpability for belligerent activities. The ability or inability to attribute actions to state actors has immense diplomatic and geostrategic implications.

Table 1. Variations of Anonymous Combatants

	Area of operation	Motivation	Density	Coordination	Principle value of anonymity
International terrorist	Foreign target, with cross-border travel	Various; individual or broad-based	As few as one individual	None; loose	Strike without warning
Insurgent	Home country	Inspire popular antigovernment movement	Cells, small to large	Cell-to-cell; leaders exist	Preserve own force
Hybrid soldier	Foreign country	Policy of home government	Depends on mission; likely a large group	Answerable to home government	Deniability for home government

(Table by author)

Providing Insight through Identity Activities

When operations require determining or verifying identity for any reason, identity activities will play a role in the solution. However, this one term encompasses a wide range of tools and doctrine.

According to JDN 2-16, identity activities are "a collection of functions and actions that appropriately recognize and differentiate one entity from another to support decision making."[5] They may accurately deconflict, link, or consolidate identities; detect shared characteristics of a group; characterize identities to assess levels of threat or trust; or develop or manage identity information. The Identity Activities Operational Cycle (figure on page 38) demonstrates how various aspects of identity activities support decision-making.[6]

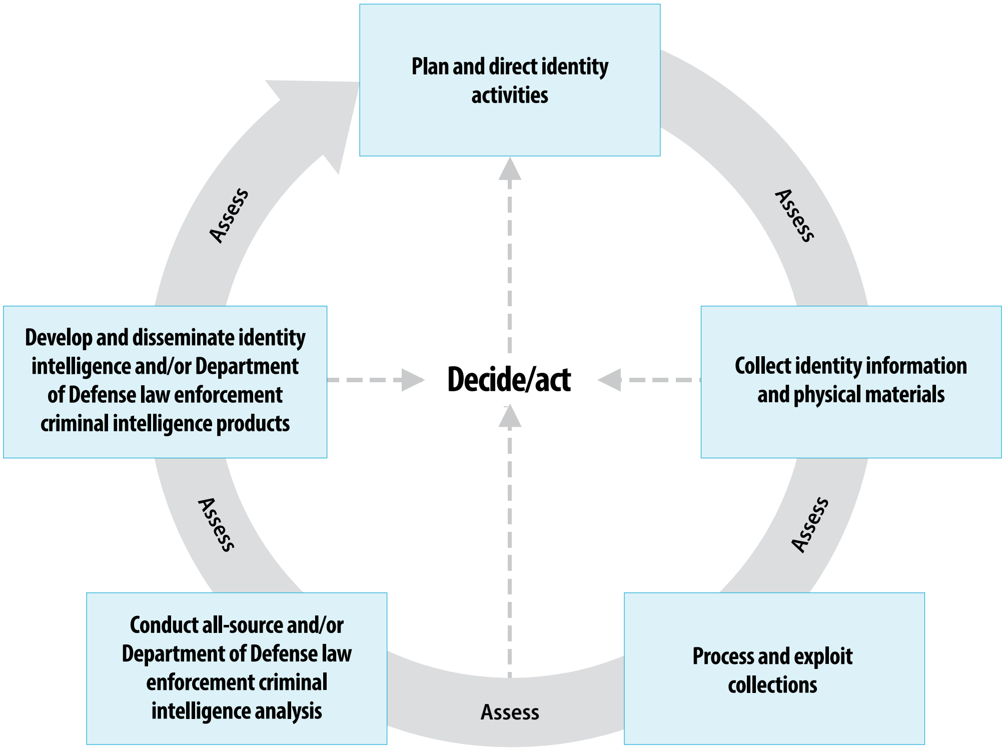
Joint Publication (JP) 3-0, *Joint Operations*, firmly places identity within the operational functions of intelligence and protection. In its discussion of intelligence, JP 3-0 states,

> By first identifying the relevant actors and learning as much as possible about them and their interrelationships, the [joint force commander] can develop an approach that will facilitate decision making and behavior (active or passive) among relevant actors that is consistent with the desired end state of the operation. Sociocultural analysis and identity intelligence (I2) activities enable a better understanding of the relevant actors.[7]

Additionally, "identity collection activities" are specified as one of fifteen protection tasks.[8]

In both roles, understanding identity is ultimately a decision-support tool. Since decisions must be made in all phases of conflict and across the range of military operations, identity is applicable anywhere. In security cooperation missions, for example, identity tools may help the host nation maintain the rule of law by identifying criminals. Those same tools may help to identify insurgents or unmarked troops during hostilities. And, during stability operations, identity activities can help to establish proper governance by countering fraud and insider threats.

Identity activities began demonstrating their operational value with counter-improvised explosive device missions in Iraq and Afghanistan in the mid-2000s. Forensic exploitation of improvised explosive device (IED) debris and biometric identification of individuals enabled coalition forces to "attack the network" of IED builders and emplacers.[9] The infrastructure established for this mission gradually found other


Plan and direct identity activities
Assess
Assess
Develop and disseminate identity intelligence and/or Department of Defense law enforcement criminal intelligence products
Decide/act
Collect identity information and physical materials
Assess
Assess
Conduct all-source and/or Department of Defense law enforcement criminal intelligence analysis
Assess
Process and exploit collections

(Figure from JDN 2-16, *Identity Activities*, 3 August 2016; identity activities are not a single tool or procedure, but a collection of various tasks and decisions points all concerning individuals' identities)

Figure. Identity Activities Operational Cycle

roles such as screening the population for known and suspected terrorists and preventing them from joining police and military forces.

Thanks to sharing between biometric databases of the Department of Defense (DOD) and its interagency and international partners, identity information on nefarious persons encountered since 2004 remains available for border security and law enforcement needs long after hostilities have concluded. At the very least, those whose biometrics connect them to past belligerent activity may be subject to extra questioning; in the most serious cases, they may be denied entry to a country or even arrested. Whatever the outcome, their histories would have gone unnoticed without biometric enrollments and data sharing.

Varied Applications

The 2015 *National Military Strategy* lists twelve joint force missions, several of which can be seen playing out in the world today, and all of which can be supported in some way by identity activities.[10] For example, biometrics and other identity assurance tools can help to secure the nuclear deterrent just as well as they support a counterinsurgency campaign. However, the following discussion will focus on field operations and individuals whom soldiers, sailors, airmen, and marines may encounter. Real-world scenarios are included, along with missions defined in the *National Military Strategy*, as depicted in table 2 (on page 39).

Countering the Islamic State. The fight against the so-called Islamic State (IS) is a two-pronged effort: first, an international coalition rolling back its past territorial gains in Iraq and Syria; and, second, containing its terror threat to other distant states. IS is resisting the coalition as somewhat of a hybrid force; it has (or had) to defend territory, something terror groups do not typically do, but it uses terrorist tactics such as suicide bombs and nonuniformed combatants. Identity activities assist in identifying IS fighters hiding among the population, as if they were insurgents. But most pertinent to this discussion is the effort to contain its fleeing members. As IS is dismantled in Syria and Iraq, its surviving members disperse to their countries of origin or other countries. These individuals must be identified, tracked, and apprehended during their travels to prevent further atrocities at their hands. Some will be assessed as simple thrill seekers or foot soldiers and permitted to go; others will turn out to be senior leaders or directly connected by forensics to grisly acts warranting prosecution. Identity activities are *the* critical capability enabling post-IS cleanup.

Afghanistan. Although a long-standing example familiar to many readers, it is worth noting the relevance

Table 2. Identity in Practice

	U.S. missions (*National Military Strategy*, 2015)	Threat type	Immediate enemy objective	How identity thwarts enemy
Islamic State (actual terror; borderline hybrid)	· Combat terrorism · Respond to crisis and conduct limited contingency operations	Conventional ground attacks mixed with urban infiltration; decentralized global terror	Aim to govern a set territory from which to spread and inspire terror abroad	Prevent terrorist's international travel; attack terror network; identify known combatants among population
Afghanistan (actual insurgent)	· Conduct stability and counterinsurgency operations · Conduct military engagement and security cooperation	Insider threat; localized terror campaign	Govern limited territory; weaken the state	Attack terror network; detect insider threat; identify known combatants among population
Ukraine (actual hybrid, notional role for identity)	· Deny an adversary's objectives · Conduct military engagement and security cooperation	Foreign fighters foment unrest; conventional battle mixed with subversion	Destabilize rival government at minimal cost	Attribute belligerent activities to foreign government; identify foreign interlopers
South China Sea (notional hybrid)	· Provide a global, stabilizing presence · Deny an adversary's objectives	Unacknowledged maritime militia denying free access to sea	Secure maritime territorial claims	Identify legitimate maritime traffic; attribute belligerent activities to foreign government

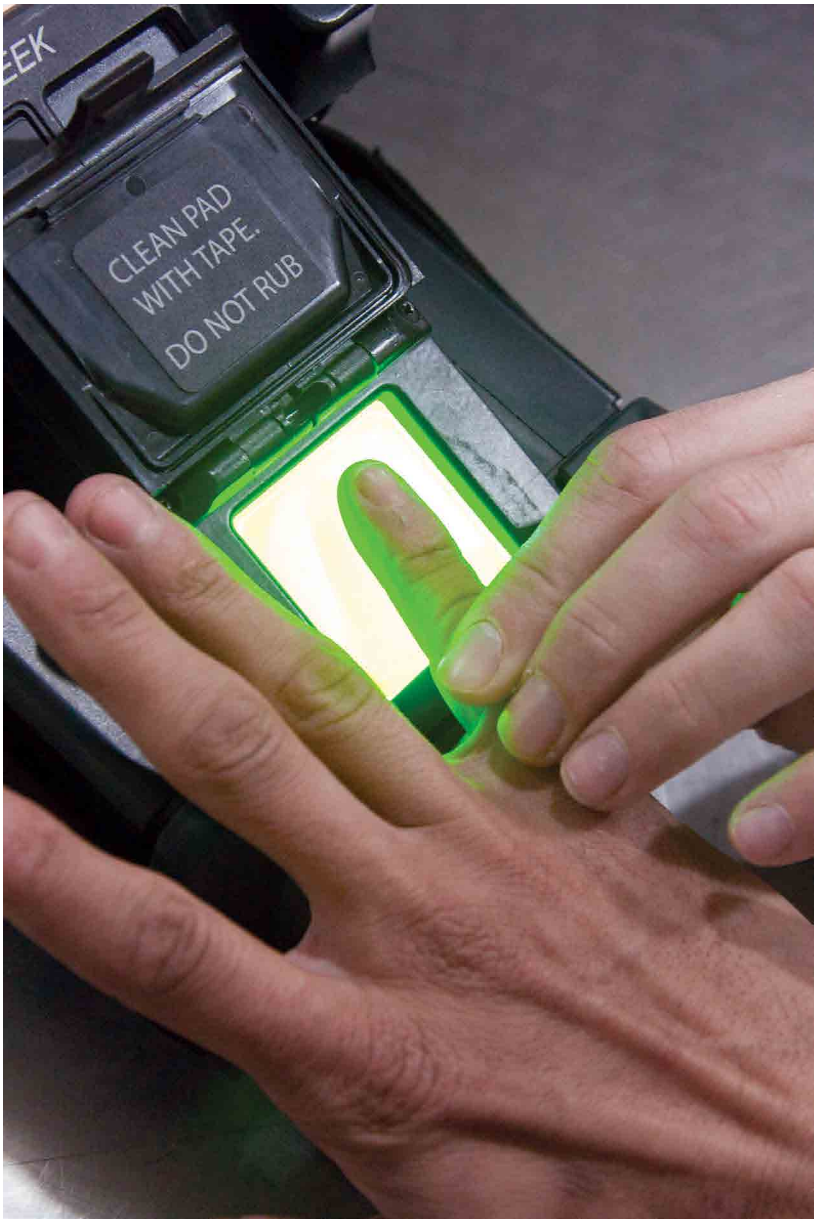
(Table by author)

of identity activities to ongoing counterinsurgency operations against the Taliban and other groups in Afghanistan. As an insurgency, the Taliban is focused on controlling territory and undermining government authority. Identifying anonymous combatants sprinkled throughout the population is key to breaking up its networks. It is also valuable in preventing insider threats. Sadly, insider attacks continue, but they likely would be far worse without the vetting and screening capabilities identity activities have brought to the table.

Ukraine. Russian hybrid operations in Ukraine are well known, if not well understood, in America. This is largely because Russia has been able to maintain a veil of deniability for its role in Ukraine's "internal" conflict. Individual anonymity certainly plays a tactical role, as exemplified in 2014 when unidentified troops took over various government buildings and a lack of attribution prevented Ukrainian forces from forcefully evicting the occupiers—though they were very likely Russian.[11] Ukraine implicitly acknowledged the potential impact of anonymous hybrid threats—and the difficulty of identifying them—by closing its border to all Russian males ages sixteen to sixty amid heightened tensions in November 2018.[12]

But more than that, anonymity allows the aggressor nation to avoid culpability. Overt invasions invite overt responses, such as in Operations Desert Shield and Desert Storm. Covert action, though, allows other risk-averse states to plausibly overlook it. Nevertheless, attribution *is* possible. For example, despite the supposedly internal nature of Ukraine's conflict, open-source reporting has continually identified funerals for Russian troops killed there.[13] If journalists can achieve this by simply monitoring social media, then a full-fledged, state-backed, identity-activities capability offers great potential to counter an aggressor state's narrative.[14]

South China Sea. Through various diplomatic and military means, the People's Republic of China is building a footprint in the South China Sea. Actions such as arming artificial islands and declaring an air defense identification zone have attracted great attention over the years.[15] Less noticed, if no less significant, is the use of "maritime militia" forces to enforce Chinese claims to fishing grounds and islands within other countries' exclusive economic zones (some of these countries dispute claims among themselves, but all agree the areas are not Chinese). Ostensibly fishing boats, these blue-hulled vessels perform little fishing but reliably appear in contested locations.[16] They are the lynchpin of a Chinese hybrid strategy of asserting dominance in Southeast Asian waters. Owners, captains, and crews can be tracked—often using public records—and this information can help determine the true nature of a vessel's duties.



An Iraqi security forces soldier has his fingerprints scanned 10 January 2017 during pretraining screening at Besmaya Range Complex, Iraq. Besmaya is one of four Combined Joint Task Force–Operation Inherent Resolve locations dedicated to building partner capacity where Spanish and Portuguese soldiers enhance Iraqi security force readiness through training. (Photo by Sgt. Joshua Wooten, U.S. Army)

Identity Activities' Current State

Today, most work on identity activities is done behind the scenes by organizations like the Defense Forensics and Biometrics Agency and the National Ground Intelligence Center. Ultimately, their work depends on data gathered by soldiers in the field and their interservice and interagency counterparts, which enables and enhances their decision-making.

At the level of the individual service member, most will recognize handheld biometric equipment (and, to an extent, forensic exploitation equipment) as the front line of identity activities. For more than a decade, it is through these portable biometric devices that soldiers have been enrolling faces, fingerprints, and irises of millions of individuals and recording contextual information to build the DOD's authoritative biometric repository. And through watch lists loaded onto the devices themselves, these records have permitted soldiers to identify wanted individuals within minutes or seconds of enrollment.

Today, most training on this equipment is provided either during predeployment training cycles or after having already arrived in theater. It is not repeated throughout a typical soldier's or unit's life cycle but is attached to mission needs. Training includes the currently fielded systems: the Biometrics Automated Toolset-Army (BAT-A), a laptop with peripherals; and the Secure Electronic Enrollment Kit (SEEK II), a self-contained handheld device.

Some soldiers, notably military police and combat engineers at the Maneuver Support Center of Excellence, receive more specialized training in the forensic exploitation of sensitive sites or for postblast analysis. The Army is currently developing a standardized forensics kit. Other services also bring forensics to the field—notably, Marine Corps law enforcement detachments have been providing an organic exploitation capability ashore and afloat since 2014.[17]

No field-level system for identity intelligence exists, unless one counts the watch lists loaded onto SEEK II devices as an identity intelligence tool. Instead, the analytical and decision support work associated with identity activities takes place on the back end, with responses provided to the "customer" who requires it. If an individual is not on a device's watch list of several tens of thousands of identities, a request can be sent to check against the entire DOD biometric database. Responses vary according to circumstances such as priority and communications infrastructure. Special operations forces reliably get responses in minutes; others may take longer due to more indirect data pathways or getting queued behind higher priority requests.

At the operational level, the combatant commands each have a small identity staff in either the J2 (intelligence) or J3 (operations) directorates. However it is configured, the J2 and J3 closely coordinate on planning for identity activities, which function as a fusion of intelligence and operations. Operations generate the data that feeds intelligence, and intelligence helps drive further operations, in a virtuous circle.

Current State: Common Scenarios

With the current configuration described above, identity activities have enabled successes by both the DOD and its interagency partners over the years. The following common scenarios demonstrate how identity activities can be used successfully.

Counter-IED. Material recovered from post-blast analysis or from a bomb-making site is provided to a forensic exploitation facility. Technicians recover fingerprints from the material and compare them with records in the DOD's authoritative biometric database. If the owner of the fingerprints is known, that individual can be watch listed and detained for questioning if encountered. If the fingerprints belong to an unknown individual, then that individual will be identified if biometrically enrolled in the future.

Counterinsurgency. A computer recovered from an illicit command post is forensically exploited. Its hardware contains the fingerprints of its owners and exploitation of the data reveals photos of cell members. This permits biometric identification of these individuals later on should they attempt to gain access to coalition facilities or be encountered by coalition troops.

Fraud prevention. A host-nation troop commander attempts to collect pay for several nonexistent "ghost" soldiers allegedly in his unit. However, biometric enrollment is required before allotting pay to any individual. The lack of unique biometrics from nonexistent soldiers permits disbursing officials to spot the attempted fraud, prevent wrongful payments, and implicate the dishonest commander.

Insider threat mitigation. An individual applies for a job as a laborer at a forward operating base. However, his biometric enrollment matches to database records demonstrating links to a radical group. He is evaluated as a counterintelligence threat and permitted no further access.

Border protection. Fingerprints discovered on an IED are uploaded to the DOD's biometric database but never matched to an identity. Years later, an unknown individual attempts to enter the United States at the southern border. When his biometrics are checked and he matches the old IED record, it causes him to be detained for further questioning and adjudication, rather than continuing into the country.

Support to law enforcement. An individual arrested for drug trafficking by an allied coast guard is biometrically enrolled. Through international biometric data sharing, he is matched to U.S. records showing a prior history of affiliation with terror and criminal groups, helping host-nation law enforcement build a case against him.

Vignette

The largest single biometric "hit," as measured by a number of connected incidents, remains a 2011 case from Iraq. Special operations forces encountered an individual 21 July 2011 whose fingerprints were familiar to examiners the instant their images arrived. His prints matched 121 separate latent prints that had been identified over the prior fourteen months, totaling a record thirty-five separate IED cases. U.S. forces detained the individual and removed him from the fight through quick-acting computer algorithms, professional biometric examiners, and global datalinks.[18]

Future State: Aspirations

Identity activities have proven their worth time and time again. With continuous improvement to technology and processes, future warfighters will derive even more value from them. But whatever form identity activities may take in the future, the DOD should ensure that the following conditions are met.

Training. Future soldiers will need to be trained and equipped to conduct identity activities in a wide variety of scenarios. Rather than thinking of it as a particular system warranting a specific career field, it is better to consider identity activities like a rifle—a tool the infantry may use the most but with which everyone must be familiar.

It is for this reason a military occupational specialty (MOS) for identity activities, forensics, and biometrics may be unintentionally restrictive. An MOS would have to fall within a career field such as the infantry, military intelligence, military police, signal corps, or something else altogether—but if its practitioners were stovepiped within a single community, the availability of the skill set to others is open to question. This may either create duplication, as other communities find they need to develop the same capabilities among their own soldiers, or lack of interest, as other communities ignore the potential of identity activities because it's too hard to access.

A preferred structure for training would be a single course open to any soldier to diffuse awareness of identity activities across the Army. A single schoolhouse would have to be responsible for it (e.g., the U.S. Army Military Police School), but this would not mean that community is the sole custodian of the requisite knowledge. Graduates could earn a qualification and service record entry but need not carry a new MOS. This baseline course could be followed by periodic refreshers, online or otherwise, taking advantage of the latest curriculum changes validated by the relevant Training and Doctrine Command (TRADOC) authorities, such as the TRADOC Capability Manager for Terrestrial and Identity (TCM-TI). This would be most important for units preparing to deploy.

Equipment and networks. Soldiers in the field should have the very best gear available for ease of enrollment, matching, and decision support. First, a simple handheld electronic tool is necessary for conducting biometric enrollment of fingerprints, faces, and irises in the field. With an additional forensic exploitation kit that fits in a cargo pocket, that same device should be able to capture latent fingerprints as well. Second, a device that passively captures face or iris information—perhaps a camera attached to a soldier's eye protection—should be able to identify individuals within its field of view and alert the soldier to potential persons of interest.

These mobile devices would interface with the DOD's authoritative biometric database via common data transmission tools and networks such as the Army's next tactical radio and WIN-T network. This would enable real-time searching and matching against full interagency databases, going beyond devices' preloaded watch lists. Stable communications using whatever nodes are available would also be key. Current bottlenecks in identification workflows are less due to database capabilities than communications pathway capacity.

When planning acquisition strategy, it is worth recalling two opposing phenomena: First, mobile devices' rapid obsolescence due to fast-changing industry capabilities and standards; and, second, the global defense community's need to purchase large quantities of rugged and interoperable equipment able to interface with global data networks over a very long term.[19] The U.S. government must enter with the assumption that it is *not* the leader in information technology, and whatever purchases it makes will be obsolete by industry standards before they are actually fielded. Thus, the government must be prepared to sustain a singular system with minimal industry support, perhaps in partnership with other allies. Alternatively, it can establish an open

Richard A. Swearengin, a latent fingerprint examiner assigned to the U.S. Army Criminal Investigation Division, Joint Expeditionary Forensic Facility 6, uses a monitor 4 May 2010 to compare a latent fingerprint (*left*) and a recorded finger print (*right*) at Kandahar Air Base, Afghanistan. (Photo by Tech. Sgt. Michele A. Desrochers, U.S. Air Force)

architecture in which a wide variety of devices, servers, and applications procured through decentralized processes are usable as long as they conform to platform-agnostic standards.

Staff planning integration. Identity activities can offer powerful benefits if integrated into operational planning, but staffs must first understand how and why. This can begin with training at the highest echelons on the importance of collections and the analysis it enables. Once identity activities are incorporated into the commander's intent, lower echelons should have the means to incorporate them into their operations, ideally becoming part of a standard operating procedure. There is no single natural champion for identity activities at the staff level, as evidenced today by their managers at the combatant commander level being in either the J2 or J3, depending on commander or staff preference. In a new construct, it would be reasonable to make the J3 responsible for collections, the J6 (command, control, communications, computers/cyber) for routing, and J2 for analysis and reporting, with a single staff assistant (an identity operations officer, or some similar title) coordinating their actions.

Such institutionalization would also require the gradual editing of numerous Army and joint publications such as those governing operations orders. Specifying a paragraph or annex in a standard operations order format for identity activities (via Field Manual 6-0, *Commander and Staff Organization and Operations*, and other references) would be of immense value in encouraging soldiers to consider the role of identity in their pending operations.[20]

Future State: Artificial Intelligence

As an essentially cognitive process, identity activities provide numerous points at which future iterations of artificial intelligence (AI) and machine learning will play a role. Collecting, processing, and analyzing identity information all require separating relevant data from noise

A Spanish trainer takes a photo of an Iraqi security forces (ISF) soldier 10 January 2017 prior to the start of his training course at Besmaya Range Complex, Iraq. The screening process is part of the initial phase for all ISF personnel enrolled in courses throughout Iraq. (Photo by Sgt. Joshua Wooten, U.S. Army)

and looking for patterns and trends in what remains. AI and machine learning will increase the speed and precision of these processes—and in some cases, are already doing so. AI offers great promise in support of obtaining biometric enrollments in challenging conditions, identifying matches with imperfect data, placing identity in context using data analytics, and countering adversaries' attempts to evade or confuse the system.

At the point of collection, AI can assist in creating usable files even with suboptimal data. Military operations often occur in "nonconstrained" environments; that is, the lighting is erratic, cameras are wobbly, background noise is deafening, and prevailing conditions are otherwise not conducive to capturing quality data, whether it be facial images, iris scans, voice recordings, or latent fingerprints. Humans can identify acquaintances in these circumstances but legacy biometric systems may not. AI can alleviate this, even to the point of identifying faces beneath masks, sunglasses, and other "occlusions."[21] Already, laboratory tests have demonstrated algorithms capable of correctly identifying faces obscured by scarves and hats up to 77 percent of the time.[22] The concept could extend to enhancement of images with poor lighting, angles, or other factors.

This potentially shifts the burden of creating a usable file from enrollment hardware to intelligent software. For example, one way to obtain facial images at long range would be to use advanced cameras systems with sensitive optics. An alternate method is to employ inexpensive consumer-grade cameras but enhance the images they produce by applying AI to create usable files. Either way, the user obtains the same result, but the latter solution may be simpler to deploy and use in an operational environment.

Once an enrollment is collected, AI can increase the speed and precision of matching that enrollment to past data to establish identity. Both new enrollments and old records may contain only partial data or other suboptimal traits (such as the faces behind scarves mentioned above). In such circumstances today, human examiners analyze the enrollment images to make match/no-match verifications when existing algorithms are unable to, which are only a small percentage of cases, but a significant commitment of time and manpower nonetheless. Properly "trained" AI, though, will enhance algorithms' accuracy, reliability, and efficiency, further reducing the need for humans in the loop. Algorithms trained through machine learning and a large, complex data set of diverse individuals' characteristics will be powerful tools.

Above the level of matching enrollments and building galleries, AI will be important to achieving holistic understandings of individual identities. Identity information is a series of data streams, such as biometric, biographic, and reputational, as defined in JDN 2-16.[23] Ideally, all these streams flow into a data "lake." AI will provide the means of finding useful information in the lake of disparate data, in the form of patterns, trends, and associations that human analysts and legacy technologies may have never identified on their own. More than a financial record here or biometric identifier there, this is where "identity" will truly be found.

At all stages of identity activities, AI will contend with an ever-present threat: other AI. Doctored imagery—even in video—is increasingly prevalent and convincing.[24] To use a well-known but harmless example, movie producers digitally removed Henry Cavill's moustache during reshoots of 2017's *Justice League*, with lackluster results. In response, an internet user with essentially zero budget used a "deepfake" algorithm on a desktop computer to improve on the studio's work.[25] With the diffusion of technology to create fakes in the biometric and other realms, the day may come soon that only AI can differentiate between genuine data and forgeries—between real identities and false ones. Identity activities will continue to be a vital capability, but it will also be a contested operational environment.

Conclusion

Born in combat and maturing as both an operational capability and in the DOD's business enterprise, identity activities present an enduring enabler to military operations and internal functions. It reduces fraud and increases accountability, both in civil affairs and everyday business. Most importantly to soldiers in the field, it permits them to better separate friend from foe in any circumstance. Technology and procedures will only improve in coming years, and the Army and the DOD must be prepared to capitalize to deny the enemy anonymity. ■

Notes

1. Joint Doctrine Note (JDN) 2-16, *Identity Activities* (Washington, DC: U.S. Government Publishing Office [GPO], 3 August 2016), vii.

2. Training Circular (TC) 7-100, *Hybrid Threat* (Washington, DC: U.S. Government Printing Office, November 2010), 2-4.

3. Ibid.

4. Ibid.

5. JDN 2-16, *Identity Activities*, vii.

6. Ibid., I-15

7. Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 17 January 2017), III-24.

8. Ibid., III-36

9. David F. Eisler, "Counter-IED Strategy in Modern War," *Military Review* 92, no. 1 (January–February 2012): 13, accessed 19 March 2018, http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20120229_art006.pdf.

10. U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (Washington, DC: U.S. Joint Chiefs of Staff, June 2015), 10-13, accessed 19 March 2018, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

11. John Chambers, "Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the U.S. Army" (report, West Point, NY: Modern War Institute, 18 October 2016), 15, accessed 19 March 2018, https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.

12. "Ukraine Closes Border to Russian Men," PBS News Hour, 30 November 2018, accessed 6 December 2018, https://www.pbs.org/newshour/show/news-wrap-ukraine-closes-border-to-russian-men.

13. James Miller, Pierre Vaux, Catherine A. Fitzpatrick, and Michael Weiss, "An Invasion by Any Other Name: The Kremlin's Dirty War in Ukraine," *The Interpreter* (report, New York: Institute of Modern Russia, 2015), 49, accessed July 7, 2017, http://www.interpretermag.com/wp-content/uploads/2015/11/IMR_Ukraine_final_links_updt_02_corr.pdf; Catherine A. Fitzpatrick, "Finding Putin's Dead Soldiers in Ukraine," The

Daily Beast, 16 September 2015, accessed 19 March 2018, http://www.thedailybeast.com/finding-putins-dead-soldiers-in-ukraine/.

14. Patrick Tucker, "The Science of Unmasking Russian Forces in Ukraine," Defense One, 16 April 2014, accessed 19 March 2018, http://www.defenseone.com/technology/2014/04/science-unmasking-russian-forces-ukraine/82693/.

15. Colin Dwyer, "The Multiplex and the Plane: China's Moves in Surrounding Seas Raise Eyebrows," National Public Radio, 25 July 2017, accessed 19 March 2018, http://www.npr.org/sections/thetwo-way/2017/07/25/539248350/the-multiplex-and-the-plane-chinas-moves-in-surrounding-seas-raise-eyebrows/.

16. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2017*, 15 May 2017, 56, accessed 19 March 2018, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770.

17. Matthew Finnerty, "SPMAGTF MPs Exploit Vital Material," Defense Visual Information Distribution Service, 21 December 2014, accessed 19 March 2018, https://www.dvidshub.net/news/151673/spmagtf-mps-exploit-vital-material/.

18. Biometrics Identity Management Agency [now Defense Forensic and Biometrics Agency], *Annual Report FY11*, "The Super Hit," 25.

19. Sean Lyngaas, "Can the Pentagon Keep Pace on Biometrics?," *FCW* (website), 11 March 2015, accessed 2 April 2018, https://fcw.com/articles/2015/03/11/can-the-pentagon-keep-pace-on-biometrics.aspx.

20. Field Manual 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. GPO, May 2014).

21. Amarjot Singh et al., "Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network" (paper presentation, IEEE International Conference on Computer Vision Workshop (ICCVW), Venice, Italy, 22–29 October 2017), accessed 10 April 2018, https://arxiv.org/pdf/1708.09317.pdf.

22. Matt Reynolds, "Even a Mask Won't Hide You from the Latest Face Recognition Tech," *New Scientist* (website), 7 September 2017, accessed 16 March 2018, https://www.newscientist.com/article/2146703-even-a-mask-wont-hide-you-from-the-latest-face-recognition-tech/.

23. JDN 2-16, *Identity Activities*, I-13.

24. David Pierson, "Fake Videos Are on the Rise. As They Become More Realistic, Seeing Shouldn't Always Be Believing," *Los Angeles Times* (website), 19 February 2018, accessed 16 March 2018, http://www.latimes.com/business/technology/la-fi-tn-fake-videos-20180219-story.html.

25. James Vincent, "Cheap AI Is Better at Removing Henry Cavill's Superman Mustache Than Hollywood Special Effects," The Verge, 7 February 2018, accessed 16 March 2018, https://www.theverge.com/tldr/2018/2/7/16985570/superman-mustache-ai-deepfakes-henry-cavill.