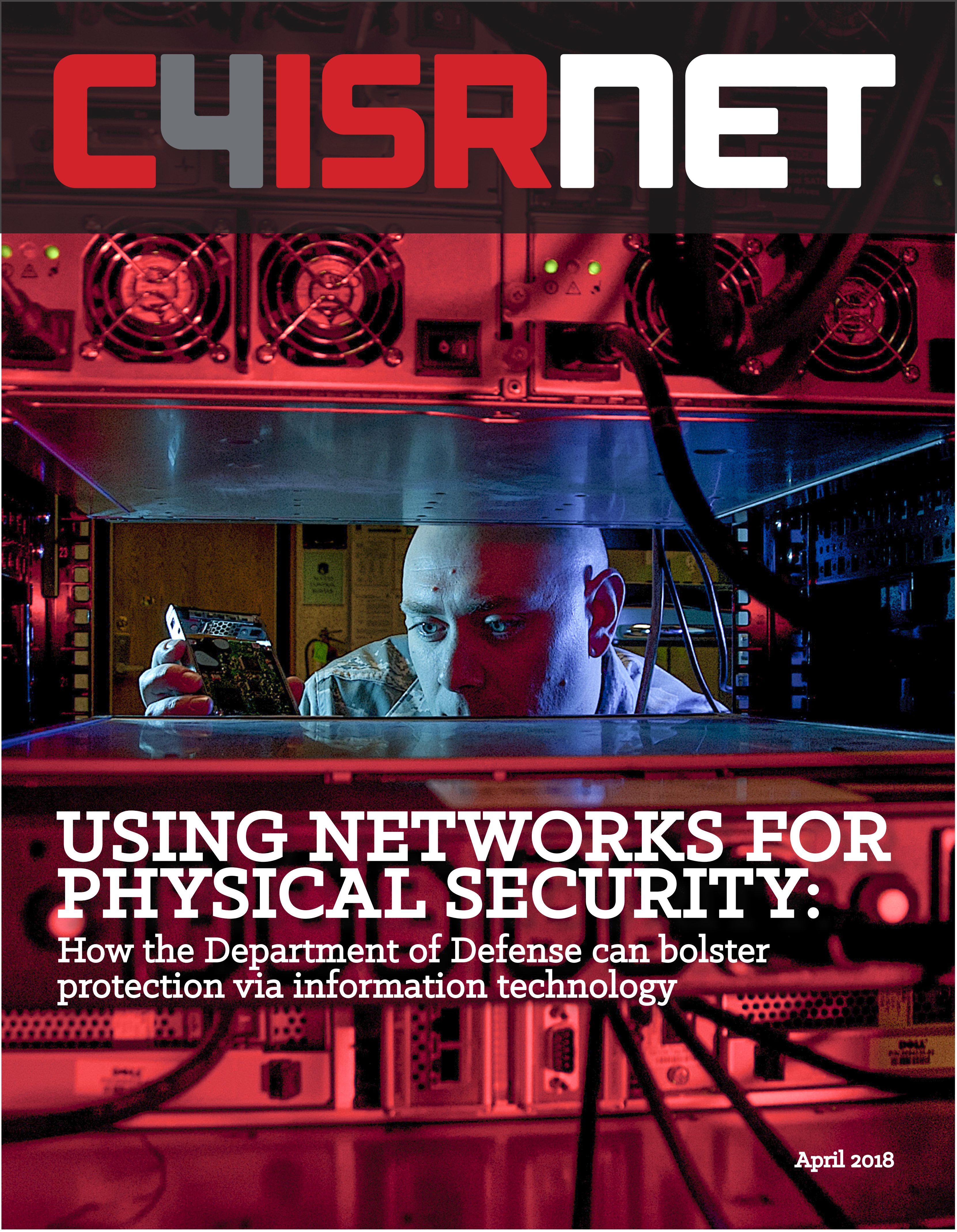
C4ISRNET



USING NETWORKS FOR PHYSICAL SECURITY:

How the Department of Defense can bolster protection via information technology

April 2018

SPECIAL REPORT:

Anyone who's been a visitor to the Pentagon in recent years knows the long lines that can twist through the visitor center as part of the security checkpoint.

But because it's not obviously visible, it's easy to forget the role that networks play in protecting the Pentagon as well as a host of military bases and assets around the world.

In the past, security has been characterized as a task of brawn and obstruction, but today's Department of Defense leaders are looking for savvier, modern solutions in determining who's allowed in and out. The network is the new bouncer. As a result, DoD leaders want to take advantage of those networks and streams of data that already exist.

DoD leaders increasingly want new technologies to bolster the physical security of military assets and bases. This means controlling who comes in and out, better tracking nearby vehicles, and helping create a stronger understanding of the region where troops are deployed.

To improve their current system, DoD officials are concentrating on a series of new capabilities, including:

- Breaking down silos to improve situational awareness.
- Creating more intuitive systems.
- Relying on new technologies.

This ebook explores the steps the DoD is taking, the new capabilities on the horizon and the possibilities for the future.

Go ahead and jump on in. No iris scans necessary.

Mike Gruss
Editor

Force Protect: Defending the Warfighter with One Common Operating Picture

Rebecca Perdue
Manager Technical Architecture NA Fixed Data Expansion
Motorola Solutions, Inc.

Joao Oliveira
Senior Technical Architect
Motorola Solutions Inc.

To make split second decisions, warfighters need the most accurate information possible, delivered in a way that's easy to process. In the field and in command, the military is continuously updating and operationalizing information using communications and networks such as Land Mobile Radios (LMR), video, geospatial data, and sensor networks. Today, many of those networks are siloed, hindering the ability to get the right information, in the right hands at the right time.

Force Protect, from Motorola Solutions, is a converged security and information management system that uses communications systems and networks already deployed to deliver a common operating picture of a force's assets in tactical operations and on base.

The platform can operate in a virtual, perimetered environment or installation-wide, integrating multiple systems to enable real-time voice, video, and data collaboration. With Force Protect, warfighters, operation centers, and first responders can rely on the communications infrastructure they already own, but with more powerful, streamlined information that greatly enhances situational awareness whether in the field or on base.

Force Protect is a prime example of a new wave of technologies that harness the power of networks to break down silos, improve decision making, and ultimately keep warfighters and assets safer.

AN INTELLIGENT LAYER OVER SUBSYSTEMS

It's no surprise that many critical systems and networks don't adequately speak to each other since they are often made by different vendors and installed at different times. Force Protect is vendor, network, and protocol agnostic. It acts as an intelligent layer on top of these disparate systems, using APIs to integrate all of an installation's systems and networks. Force Protect currently maintains a large library of over 300 APIs for some of the most popular integrations. The API library is continuously updated in step with the underlying systems and software. This COTS solution reduces complexity and cost. Everything just works. In addition, Force Protect can support custom APIs and can handle classified networks. The system runs on HTML 5 and can be hosted in the cloud, a hybrid cloud, on premise, or all of the above. Data is presented in an intuitive, streamlined user interface.

When systems and networks are tightly integrated in this way, it unlocks powerful functionality and value. For instance, in a tactical environment, warfighters gain access to LMR communications, cameras, sensors, communications networks, and other assets in the field and on base. While there may be dozens of systems operating on the backend, the operator just sees and interacts with one platform, making actions intuitive and fast.

IMPROVED SITUATIONAL AWARENESS, DECISION MAKING, AND COMMUNICATIONS

Force Protect is a game-changing situational awareness enhancer. It doesn't displace or remove any underlying systems or networks, instead it directly overlays those systems as assets on a map in one common operating picture. Once that picture is created, action plans can be incorporated along with corresponding smart procedural rules. So, an operator simply has to follow choices from a drop-down menu, depending on the specific scenario.

In addition, Force Protect helps guide actions pre-, mid-, and post-operation with full logging capabilities. This is significant from a training perspective, allowing command to analyze what actions were taken, what commands were followed, and how long actions took. All data is captured, and operators can add IDs and timestamps, so advanced analytics can be applied, after-action reports are more precise, and operational processes can be refined for better and faster outcomes in subsequent missions.

A FUTURE PROOF PLATFORM

Force Protect helps derive more value from existing systems and networks. But technology does not stand still. Force Protect's open protocols and APIs allow the platform to continuously integrate new technology and intelligence layers from any vendor. Whether that means new advances in AI, analytics, new types of sensors, or even technology we haven't imagined today, Force Protect provides the platform to integrate them.

With Force Protect, warfighters can operationalize information with more intelligence layered over the communications and networks they've already invested in. When voice, video, and data siloes come together in one seamless, powerful platform, situational awareness and decision making are greatly enhanced, keeping warfighters and assets safer in the field and on base.

To learn more about Force Protect, visit: www.MotorolaSolutions.com/ForceProtect

MOTOROLA SOLUTIONS

PHOTO: NAVAL DISTRICT WASHINGTON VIA FLICKR

THE NETWORK'S EDGE

New technologies are revolutionizing physical security *By Adam Stone*

From their perch in the operations center at Navy Yard in Washington, D.C., security analysts peer down like hawks over the Naval Research Laboratory, Walter Reed National Military Medical Center, Joint Base Anacostia-Bolling and a half-dozen other major military installations scattered around the national capital region.

It takes just 10 people to maintain constant surveillance over all those disparate sites, "but you need machines to help you," said Robert Baker, command information officer for Naval Facilities Engineering Command. Those machines include a complex network of cameras and sensors, supported by analytics software. When the software spots a suspect event — traffic headed in the wrong direction, for example — that video feed gets pushed to the foreground for human analysis.

This is just one example of how the military looks to technology to improve physical security.

The real-world influence of technology is evident across the military: Everything from targeting systems, to logistics, to intelligence, surveillance and reconnaissance has been enhanced in some way by IT. Physical security represents an emerging frontier, where artificial intelligence, machine learning, autonomous technologies and other advances could give the military an edge.

FORCE MULTIPLIER

At Edwards Air Force Base in California last summer, a security team installed a ground-based radar system to monitor a wide landscape using electro-optical and infrared sensors. The team turned to technology to give them insight across a massive 308,000-acre facility.

"The driving need for this system is to proactively defend Edwards AFB.

A SURVEILLANCE SYSTEM SITS ON TOP OF A REMOTE BUILDING AT EDWARDS AIR FORCE BASE. THE SYSTEM WAS DEMONSTRATED TO BASE LEADERSHIP AND 412TH SECURITY FORCES SQUADRON PERSONNEL ON JULY 10, 2017. THE GROUND-BASED RADAR SYSTEM HAS THE CAPABILITY TO MONITOR THE LAKE BED AT GREAT DISTANCES WITH ELECTRO-OPTICAL AND INFRARED SENSORS.

PHOTO: KENJI THULOWEIT/U.S. AIR FORCE

Given the mission of Edwards, and how much terrain we have, we need a system that can overcome the difficulties of patrolling the vast amount of land Edwards presents to our patrols," Staff Sgt. Alexander Deguzman, an installation security technician with the 412th Security Forces Squadron, said in a news release.

As at Navy Yard, the effort at Edwards is all about using some combination of remote sensing, networked surveillance and machine intelligence to create a force multiplier in physical security. Analysts say such initiatives could make bases and installations markedly safer at a lower cost and with less labor required.

The rise of artificial intelligence is a critical technology moving forward. Security often involves the constant observation of multiple video and data feeds for prolonged periods of time. Human analysts get tired. They look away for a moment. In short, they miss stuff.

"A human can look at things once or twice; but after 100 times, they start to lose their edge," said retired Air Force Lt. Gen. Bob Elder, chair of the cyber and emerging technologies division at the National Defense Industrial Association. "AI goes beyond what a human can do because it doesn't get tired."

Elder envisions a future in the near term in which routine surveillance can be carried out by software-supported machines, with computers scanning for anomalies and alerting human analysts to potential threats. That saves on labor. In addition, such an approach would also allow the military to use less highly skilled operators, relying instead on the machine's expertise and accuracy.

EYES IN THE SKY

Industry's interest in this subject has helped bring AI and autonomy to the fore as potential security assets. With the rise of drones and the imminent arrival of driverless cars, some experts are looking to autonomy as the next logical step in military security.

Drones alone don't offer a security fix: Their batteries run down too fast. The military might, however, consider the use of tethered drones, autonomous ISR assets that can hover in place and remain attached to a power source for ongoing operations. Put one at each corner of a base camp and leaders can put together a big-picture view of any approaching hazard.

"This kind of solution is really smart because you can constantly feed it power, you don't have to worry about it flying away, and if someone tries to damage it or take control of it, you know about it right away," said Steve Surfaro, chairman of the Security Industry Association's public safety working group.

Another key industry trend — biometrics — may also point the way forward on physical security. "Investing in facial recognition software … can improve perimeter security by automating aspects of it to speed up entry

STAFF SGT. ALEXANDER DEGUZMAN, LEFT, 412TH SECURITY FORCES SQUADRON INSTALLATION SECURITY TECHNICIAN, SHOWS BOBBY TRUONG, 412TH COMMUNICATIONS SQUADRON, THE MONITORS AND CONTROLS OF THE RAPTOR SURVEILLANCE SYSTEM THAT WAS DEMONSTRATED TO BASE LEADERSHIP ON JULY 10, 2017.

U.S. AIR FORCE PHOTO BY KENJI THULOWEIT

> "AI goes beyond what a human can do because it doesn't get tired."
>
> *Air Force Lt. Gen. Bob Elder (ret.), chair of the cyber and emerging technologies division at the National Defense Industrial Association*

to bases for those authorized and focus screening attention on those that represent a risk," according to a Deloitte report on smart military bases titled "Byting the Bullet."

THE NETWORKING NEEDS

To make the most of the technological imperative around security, experts say, the military will have to give serious thought to issues of infrastructure.

Security is becoming a data function: Sensor streams, video feeds, drone surveillance and other methodologies all will require robust network support and substantial compute resources. The data will need to flow freely, even in great quantities, with ample processing available to put it to use.

Much of the processing will be done in the cloud, "but you still need to have a reliable connection to that cloud, which means you want diversity and redundancy. At a minimum you want two connections and ideally you want three ways of doing it — wires, line of sight wireless and satellite," Elder said. "You need a reliable way to get to your cloud services."

Such an implementation will require, at the least, a significant amount of bandwidth. At Navy Yard, Baker said he is able to overcome that hurdle through thoughtful network design. In other words, rather than pushing all the information back to the operations center for processing, new video and sensor analytics takes place on the edge, shrinking the overall networking demand.

"The more processing you can do at the edge of the network, the less robust your network needs to be," he said. Efficient network design weeds out routine activity, "and then the really interesting information is being sent for human analysis."

While emerging technologies can enhance the military's security operations, some argue that IT capabilities are not, in themselves, a rationale for upgrading systems that may already be meeting mission. Budgetary constraints apply.

"You could make processing faster, but what is the threat that we are trying to counter? If we are seeing zero incidents, why would we gold-plate that area? We want to be good stewards of the taxpayer dollars," Baker said. "At the same time, if there was some high-risk area where we needed to do that better, we would absolutely want to put resources against that."

BIG DATA WILL MAKE A BIG DIFFERENCE WITH BASE SECURITY

By *Kara Frederick*

In 2011, the simple exploitation of an existing data set could have prevented a near disaster in northern Afghanistan.

Then, an entire operations center watched as the feed from an MQ-1 drone, newly reassigned from its original mission, displayed a growing group of protesters at the perimeter of a small U.S. forward operating base. Although conventional signals intelligence indicated a possible disturbance, full-motion video confirmed the severity of the threat only well after it had matured. Intelligence analysts didn't understand what the protestors were doing — and why they were doing it — until they had already massed at the entry point. If used properly, automated social media monitoring and geofencing, which calls for creating virtual geographic boundaries, could have filled this critical gap in situational awareness.

Kara Frederick is a research associate for the technology and national security program at the Center for a New American Security. She has worked as an intelligence analyst for Facebook and the Department of Defense.

GOODBYE GATES, GUARDS AND GUNS

New technologies are transforming physical security from "gates, guards and guns" to an imperative that's increasingly reliant on data systems. Efforts like last year's pilot program between the Air Force and AT&T to establish a perimeter network utilizing mulitprotocol label switching and SIM chip technology via an LTE network at Maxwell Air Force Base are the new normal. That system created a wireless smart perimeter with infrared sensors and facial recognition to detect and identify intruders as well as to alert base personnel of potential security breaches.

The military's use of biometric scanning through facial recognition software, license plate "grabbers," UAV and aerostat surveillance, and radar and seismic detection sensors are nearly requisite for access control. The application of technology of the internet of things — as evidenced by nearly $9 billion of federal money in 2015 — plus an embrace of artificial intelligence feed into the growing chorus for "smart bases."

HARNESSING NETWORKS FOR GEO-SITUATIONAL AWARENESS

Yet, one application of new technology could quickly exploit existing data sets and be rapidly employed, likely preventing surprises like the one in Afghanistan in 2011. Using geofencing to surface high-quality, publicly available information, layered atop conventional active and passive physical security measures, would enhance situational awareness around military bases.

While many bases already exploit social media data and integrate big data streams into a common operational picture, like Northrop Grumman's Critical Incident Response System and AT&T's Common Operational Portal, the U.S. military can more widely apply and emphasize this concept overseas. For starters, analysts at the tactical level could determine the latitude, longitude and radius of the area of interest around a forward operating base and adjust this geofence for monitoring. Designated social media aggregators would then comb available application program interfaces to surface information within the bounded area. These aggregators would deliver real-time data (e.g., geotagged photos posted to a variety of social media platforms) for analysts to triage and then paint a comprehensive intel picture, similar to targeters teasing out patterns of life through a watered-down version of activity-based intelligence. Such methodologies to identify patterns and predictive indicators — often through automation — are already staples of private sector and U.S. law enforcement physical security practices.

To go further, the use of natural language processing for sentiment analysis within this open-source intelligence would improve indications and warning. Sentiment indicators that identify potential threats in multiple languages are being used in the private sector and by U.S. law enforcement, with obvious applications overseas. Additional advantages of this big-data approach are a prodigious and archivable metadata trail, and the potential for interagency information-sharing that leverages the link analysis proficiency resident in many government organizations.

POTENTIAL OBSTACLES TO IMPLEMENTATION

Despite its quick deployment potential overseas, domestic applications for the U.S. military's use of geofencing and social media monitoring are limited. In a stark example of litigation risk, Facebook, Instagram and Twitter suspended social media monitoring startup Geofeedia's access after a challenge from the American Civil Liberties Union in 2016. Renewed reluctance by social media companies to share data with third parties, borne out of reported misuse of user data by the firm Cambridge Analytica, would likely hinder future development of similar technologies. And until costs are offset by more widely applied AI technology, monitoring and assessing the veracity of ingested information will eat into analytical capacity. Yet, the responsible integration of open-source methodologies that reduce risk and improve situational awareness surrounding U.S. military bases is worth the roadblocks. Otherwise, the risk of surprise is too great. ▣

UNLOCK MORE POWER TO DEFEND

Force Protect is a converged security and information management system that delivers a common operating picture for military resources and personnel. This convergence platform integrates multiple systems to enable real-time voice, video, and data collaboration in a common operating picture, allowing commanders, operation centers and first responders to unify workflows and act as one.

www.MotorolaSolutions.com/ForceProtect

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**

A U.S. ARMY IDENTITY INTELLIGENCE TEAM IS EXPLORING WAYS TO MAKE IDENTIFICATION DATA MORE READILY AVAILABLE TO TROOPS ON THE GROUND.

PHOTO: SPC. BRIAN J. SMITH DUTTON/ARMY

CERDEC WANTS A QUICK ANSWER TO 'IS THIS PERSON A BAD GUY?'

By *Adam Stone*

The Army has already started leaning on biometric data for base access control and to share fingerprint and facial recognition data with coalition partners.

Now, a team at the U.S. Army Communications-Electronics Research, Development and Engineering Center wants to take that data one step further: to the battlefield.

CERDEC is expanding its range of biometric measures and devising new ways to more effectively share that information with soldiers.

"We want to empower the soldier to make decisions," said Keith Riser, the biometrics-enabled intelligence team lead.

Identity management is a hot topic in industry, specifically with biometric solutions emerging for physical and cyber access. CERDEC hosted a Big Ideas Day in August with partners from academia and industry and has since been working to implement a range of strategies around the issue.

C4ISRNET recently assembled a roundtable of experts from within CERDEC's Intelligence and Information Warfare Directorate and asked about the state of Army biometrics.

C4ISRNET: **Biometrics has gone beyond the fingerprint. What does your work encompass?**
MICHAEL SEMENORO, ELECTRONICS ENGINEER: When we seek identity technology, it can be how someone looks, their hair color, their gait, their face. It could be their voice, how they speak, their tone. Or it can be how they behave, how they interact on a network or in social media.

C4ISRNET: **Big picture, how will that information help the soldier in the field?**
SEMENORO: What we want is to give the soldier the ability to make a determination very quickly. We want to automate the process and we want it to come with a high confidence level. So, we are looking to fuse biometric information, physical characteristics and behavioral characteristics in order to identify without making a mistake or misidentifying people.

C4ISRNET: **What's the major sticking point?**
COURTNEY COULTER, SITE EXPLOITATION TEAM LEAD: Most of our users are disconnected or have disadvantaged comms, while most of the tools that we currently use require some network accessibility. So we are looking at a lot of tools and ideas that could address those kinds of constraints. This is significant because often you can't afford to wait several hours to find out who this person is. You want to identify that person beforehand and you want to do it in a short time frame.

C4ISRNET: **What's the fix for that?**
COULTER: When you get to comms-disadvantaged scenarios, you want to be able to process that data at the edge. The approach is to understand how much the user actually needs to know that far forward. They don't need to know everything, but they need a tip or a cue to say whether this person is a bad guy. So we want to use the predictive nature of these technologies to get them just what they need to know.

C4ISRNET: **How will video analytics help with that?**
KEITH RISER, BIOMETRICS INTEL TEAM LEAD: Right now, there is lot of video being produced, not just from our own sensors but also publicly available sources, and we want to see how much information we can get out of that.

There are two parts to that. Detection: Is there a face in the scene? And then matching that against the data base. Both of those can be challenging. It is graphics-processing intensive. So we are looking at ways to put that in smaller computers, to do rapid detection on many sensors with live videos and then possibly convert that into localized watch lists to help soldiers in disadvantaged areas identify people.

C4ISRNET: **How do machine learning and artificial intelligence factor in?**
RISER: As you train on the data, computers can become more capable of pulling faces out of a crowd, for example, or being able to identify specific individuals because of their behaviors rather than just because they are on a watch list. Those are the things AI brings to the table. AI can also regionalize the situational awareness. Maybe [soldiers] don't need to know the entire world: They just need that area that they are in. AI can help to decipher that, which in turn enables sending that data at high speeds, even when communications are limited.

C4ISRNET: **Biometric intel has been stovepiped in the past. Can and should its use be broadened?**
COULTER: Absolutely. Identity management used to be used just for force protection. Now this data is being combined with more data types to provide better intelligence. Now we can use it for larger things. For example, if we combine it with documents for forensics, maybe you know who the bomb maker is, who is his network of people, what other information is associated with him. You remove the anonymity of your enemy. That's one goal of all this.

NEW TECHNOLOGIES FOR FORCE PROTECTION REQUIRE NEW POLICIES

By Todd Rosenblum

When the Department of Defense undertook a comprehensive review of its insider threat and force protection policies, it followed catastrophic, insider threat, active shooter events at Washington Navy Yard (2013) and at Fort Hood Texas (2009 and 2014). That review was led by the Office of the Under Secretary of Defense for Intelligence, in coordination with the Office of the Under Secretary of Defense for Policy, the Joint Staff and the military services.

By chance, this review took place during the devastating breach of federal personnel security clearance records from the Office of Personnel Management in 2015. But it was this second event that underscored for DoD leaders that staff on the ground had major problems accessing key data stores and protecting information vital to the integrity of our security clearance processes.

Our national inability to detect indicators of violence, along with the larger U.S. government's inability to protect vital data stores, compelled new thinking about how to make better use of emerging information technologies and network protection tools. It catalyzed a new push in the Department of Defense to acquire modern tools for data analysis, shore up penetrable data stores, and refresh department policies and decision-making in this area.

Pentagon leaders concluded force protection at DoD installations and bases is far more complex than standoff perimeters, posting sentries, and conducting badge checks and vehicle inspections. Force protection needed to meet data analytics.

***Todd Rosenblum** is a nonresident senior fellow at the Atlantic Council and a former senior defense and intelligence official at the departments of Defense and Homeland Security.*

One important lesson learned from the failure to identify insider threats in 2009, 2013 and 2014 was that the department failed to maximize information residing in available data stores. Traditionally, military personnel, and indeed all government officials with security clearances, were subject to periodic reviews of self-declared information by background investigators. Personnel were (and are) required by law to declare ongoing foreign contacts and international travel, relevant mental health information, financial distress, and significant personal events such as marriage, divorce or court proceedings. This approach relied on individuals self-reporting and redoing security reviews every few years.

Technology provided a force multiplier for the DoD's ability to monitor certain behaviors of its personnel. The DoD shifted from periodic reviews and self-reporting of potential conflicts and concerns to the ability to continuously monitor for scrutiny and intervention. Using new data aggregation and correlation tools gave the DoD the ability to proactively monitor court, bank and travel information, inappropriate browsing, and transactional patterns of its personnel. This kind of government intrusion is inappropriate for civilian and uncleared personnel, but it vastly improves security situational awareness of those in uniform and defense civilians entrusted with access to classified information.

The ability to continuously access relevant information of its personnel needs to be accompanied by new policies. One conundrum the department faces is whether the additional information is just more circumstantial information or if it constitutes a higher probability of threat.

Algorithmic predicators of violence (akin to the concept in the 2002 movie "Minority Report") can alert human monitors of red flag activities but have yet to prove their worth in deciphering intent.

Continuously accessing vastly more data stores can overwhelm front-line decision-makers, especially when it involves quick searches of uncleared personnel seeking access to protected areas. Base entry guards still need to make spot calls about allowing a pizza delivery person on base if suspect information surfaces during real time data searches. What if the new, expanded data searches reveal the individual watches an unusually large number of graphic violence videos on YouTube or is flagged for inappropriate behavior on Facebook? What if searches reveal the person travels frequently to a region in which the U.S. military is prosecuting war? Traditionally, base guards would search for arrests and warrants, but never before could they reach so deeply and so fast into a person's digital patterns of life.

Data analytics is revolutionizing so much of our world. It expands access to patterns of behavior and interactions of interest. This is vital for increasing force protection, improving counterintelligence and possibly intervening before someone becomes an active shooter. The challenge is not in acknowledging the power of being able to continuously monitor witting personnel with security clearances and/or in uniform, but rather what to do with ambiguous information and determining whom to empower with force protection decision-making at home and abroad.

THE NEW BIOMETRIC SYSTEM INTEGRATION LABORATORY.

PHOTO: ARMY

A NEW LAB TO ACCELERATE THE LINK BETWEEN SOLDIERS AND BIOMETRIC DATA

By Adam Stone

With the opening of a new biometrics lab, the Army is pushing to make fingerprints, iris scans and other physical identifiers a more central part of the war-fighting endeavor.

The Biometric System Integration Laboratory, which opened in February at Fort Belvoir in northern Virginia, will serve as a proving ground for emerging biometric devices and networking capabilities. The aim is to more easily collect data and to speed communications between soldiers and biometric databases.

“We see a huge expanding role for biometrics,” said Col. Donald Hurst, project manager for DoD biometrics for the Program Executive Office Intelligence, Electronic Warfare and Sensors. “We are going to use it in counterterrorism to map high-value targets. You’re also going to have a robust force protection for your rear area and your base scenarios.”

The Army is looking at multiple ways to enhance its emerging biometric capability.

Planners want to move away from a hardware-based system of transport and storage for vast volumes of biometric data. The present Automated Biometric Information System lives in servers in the FBI Biometric Technology Center in West Virginia. Virtual computing would be a smarter way to go, Hurst said.

Virtualization would offer more scalable systems, giving military planners the ability to ramp up their biometric processing capacity on short notice. “I can go from 10,000 to 40,000 transactions with just a phone call and have it up and running in a matter of hours,” Hurst said. “That saves a lot of money in physical hardware and it gives us greater operational capabilities.”

He’s looking to have a conversion to a virtualized system underway in 2020 with a potential delivery in 2024.

The emerging specs also put an emphasis on connectivity: A soldier should be able to query the database and get a timely response, even under challenged conditions. “The system needs to be able to leverage whatever network capabilities are available in the theater,” Hurst said. “We are trying to ensure that the device is the ‘perfect parasite’ where it can use any transport mechanism, whether it is [satellite communications] or fiber, commercial or military, whatever pathway is available.”

Assuming a new device can connect to the needed network, the task will still require a vast amount of data in motion here, and planners are looking for new methodologies to ensure that data can flow as needed.

“The movement of the data to the database and back to the soldier is absolutely critical,” Hurst said. “Bandwidth is a commodity, and there are a lot of other higher-priority users, so we are looking at data compression to get that biometric file to be less of a consumer in that already-constrained data pathway.”

The future vision also calls for increased on-board storage: A device capable of internally supporting 50,000 to 100,000 identities would help to ease network congestion.

In addition to streamlining the processing, the Army is taking a deep diving into the collection tools it uses to harvest biometric information.

The present state of the art is the Biometrics Automated Toolset—Army, a clunky agglomeration of laptops, peripherals and servers. With roughly the dimensions of two reams of paper, the device is too big to fit in a soldier’s pocket, and much of the underlying technology has gone stale.

“We can no longer upgrade the software. It can’t take Windows 10. It is capable and durable, but it’s yesterday’s technology,” Hurst said. “We are looking for a device more like a large commercial cellphone — the size, weight and power along those lines. We want to add a voice collection modality, and we’re looking for a system that can process classified and unclassified in a single device.”

New specs call for more user-friendly peripherals. For example, a subject unwilling to offer a hand could be fingerprinted via a touchless sensor. Such tools exist at base level, but planners say they’d like to develop more mobile, field-ready versions.

Meanwhile at the new lab, Army researchers are looking to explore all these avenues hand in glove with industry partners. The commercial side has been investing heavily in biometrics, and the Army is looking to leverage those investments to lighten its own research and development load around the new technologies.

In the new lab, “a vendor will be able to bring in a [commercial off-the-shelf] item and we can test it against our standards,” Hurst said. “Biometrics is a standards-based enterprise: We all have to speak the same language, we all have to format in a like manner in order to effectively share this data. That is going to be one of the primary benefits of the lab.”

ARPA'S FACE RECOGNITION PRIZE CHALLENGE HOPES TO ID IMPROVED ALGORITHMS TO PROCESS UP TO 150 DIFFERENT LAYERS OF DATA.

PHOTO: MAXIPHOTO/GETTY IMAGES

IARPA WANTS TO MAKE THE EASIEST BIOMETRIC EVEN EASIER

By Adam Stone

Officials from the Intelligence Advanced Research Projects Activity, or IARPA, say they hope the organization's Face Recognition Prize Challenge will help them move the needle on biometric security.

"Face recognition is a critical technology for national security and the intelligence community," said Chris Boehnen, a senior program manager at IARPA, part of the Office of the Director of National Intelligence. "Many of the adversaries we face don't wear uniforms, and that means we have to have some other way to recognize who people are."

Last year, 16 teams submitted software solutions intended to make face recognition faster and more accurate. IARPA will test the various algorithms against a standard data set to see how they perform.

While industry and military leaders lately have put a heavy emphasis on facial recognition as an identification tool, challenges remain. A chief problem lies in the arena of variability: If the pose, the lighting or the facial expression changes, it can be hard for even the best software to match a live subject to a file photo.

"When you get your driver's license, you look straight at the camera in good lighting," Boehnen said. "But if you have one face in heavy shadow and another in direct light, if you have one face frowning and another smiling, all those changes make it harder for a computer to compare two faces."

The military has recently pursued several avenues in the search for better face-recognition solutions.

In 2016, U.S. Special Operations Command put out a call for small businesses with strong research and development capabilities to tackle advanced tactical facial recognition at a distance, as called for in Special Operations Command's science and technology mission statement.

The Defense Forensic Science Center in late 2016 went to industry for face-recognition solutions that could operate independent of gender and ethnicity. At about the same time the U.S. Army Research Laboratory's Sensors and Electron Devices Directorate published early findings on the possibility of using thermal infrared band scanning to provide face-matching capabilities.

While issues around accuracy have long plagued facial recognition efforts, military and intelligence planners are eager to see the capability enhanced. Unlike other biometric scans, a facial match can be done discreetly and from a distance — a potential tactical advantage.

"With fingerprint and iris, you tend to need a close-range, fully cooperative subject," Boehnen said. Facial recognition "is not the most accurate biometric, but it is the easiest one to capture."

Even with so many diverse efforts in play around the subject, prize challenges can fill a special niche. Because biometrics developers may be reluctant to take part in conventional solicitations that require them to transfer their intellectual property rights to the government, challenges can bring ideas to the table that planners otherwise might not see. Challenges also tend to attract smaller players, those outside the usual round of major contractors. "I can let everyone talk, from the garage tinkerer to the large company," Boehnen said.

Organizers said they expect the strongest proposals will likely focus on "deep learning," a computer science discipline that enables machines to process vast volumes of data at high speed.

Thanks to such techniques, "even something a grad student could whip up in two or three months today performs as well as something that a team of the best engineers in the world could have produced five years ago," Boehnen said.

In facial recognition, a computer can be tasked to consider anywhere from six to 150 different layers of data. More layers mean greater accuracy, but at some point the process can get sluggish, without really adding any new information of value. The winning algorithm likely will strike that balance between speed and volume.

Deep learning could be a key to help identify that sweet spot. "That has been the turbocharger in face recognition," Boehnen said. "All available evidence says deep learning has increased performance of face recognition potentially by several orders of magnitude."

THE DEFENSE DEPARTMENT IS MAKING A NUMBER OF IMPROVEMENTS TO THE COMMON ACCESS CARD TO ENHANCE IDENTITY AUTHENTICATION AND PHYSICAL AND NETWORK SECURITY.

PHOTO: DEFENSE DEPARTMENT

THE PROS AND CONS OF COMMON ACCESS CARDS

By Eve Keiser and John Edwards

Traditional authentication mechanisms, such as username/password combinations, offer only a single factor of authentication: something the user knows. Common access cards (CAC), on the other hand, provide two: something the user knows (the PIN) and something the user has (the card).

"With username and password, the adversary only needs to obtain the password in order to gain network access," said Bob Fedorchak, a principal information security engineer supporting the Army's Communications-Electronics Research, Development and Engineering Center, or CERDEC.

"With a CAC, an adversary must physically obtain the CAC and also obtain the PIN to the card," said Fedorchak, who specifically works within the Space and Terrestrial Communications Directorate in the Cyber Security and Information Assurance Division

Also contributing to CAC adoption are recent memos and tasking orders from the Department of Defense chief information officer, U.S. Cyber Command and Army Cyber Command, which mandate the use of CAC and SIPR tokens — the CAC equivalent on SIPRNet — to improve security on other networks, such as tactical and research development test and evaluation networks.

But until authentication technologies and approaches improve, struggles associated with management of CACs will continue to counter the security benefit within a variety of DoD end-user environments.

STRENGTHS AND WEAKNESSES

The CAC's physical form factor, along with policies governing its use, supply the card's greatest strength as an authentication tool, Fedorchak said. Yet, CACs can be easily lost or damaged, requiring a replacement card to be issued. CACs are also difficult to use with many types of mobile devices, including smartphones and tablets.

"These challenges can be an inconvenience to civilians, contractors and soldiers operating in the rear, but have a major impact on mission performance for soldiers at the tactical level," Fedorchak said.

Kayvan Alikhani, senior director of technology at security solutions provider RSA, noted that the challenges associated with use of CACs with mobile devices is actually a key security attribute.

"Because a CAC needs an insert-based, contact-based reader, it's not contactless," he said. "The reason why the DoD went with contact versus contactless cards was that the contact system closed the challenge of someone eavesdropping on the traffic that goes between the card and the card reader."

The CAC is also highly vulnerable to "the bathroom effect," he said, where somebody inserts the card and has to go to a conference, a meeting or the restroom, and they leave their card in the reader. "They have to remember to remove the card, yet the card is kept inserted and so it's very easy to steal it," he said.

Another drawback to CAC technology emerges when troops in a brigade command post need to simultaneously access multiple systems, but have only a single CAC on hand. That doesn't meld well with systems that need to remain active and visible at all times and cannot be impacted by one soldier removing their CAC and another soldier inserting their CAC during shift change, Fedorchak said.

"CERDEC S&TCD is working to identify courses of action that can be used to improve the use of the CAC in the tactical environment and reduce the impacts to our soldiers," Fedorchak said.

Despite its drawbacks, CAC technology isn't likely to go away anytime soon, according to John Padgette, a senior manager at the cybersecurity practice of Accenture Federal Services. "Augmentation, however, is definitely needed in order to raise the level of authentication trust for the entire enterprise, as well as improve usability for mobile clients."

LOOKING FOR ANSWERS

Driven by the lack of CAC support on mobile platforms and other issues, several federal agencies/services are piloting the use of derived credentials — carried in a mobile device instead of the card — to generate authentication, Padgette said.

Authentication needs to be more comprehensive in order to provide better protection against increasingly sophisticated threats, said Peter Romness, cybersecurity programs lead for Cisco Systems' U.S. public sector group. "It needs to be more than just who a person is," he said. "We need to know who the user is, where they are connecting from, when the connection is being made and how the user is trying to connect — wired, wireless, internet or VPN."

Tracking such characteristics can help analysts identify potential anomalies in user behavior, Romness added, which could signal a potential threat. And the capability to report who, what, where, when and how is already available in most network devices using features of the 802.1x standard as well as other features, such as secure group tags. Many organizations, including groups in the DoD, are starting to use this technology.

Alikhani noted that technologies that promise to make the CAC even stronger in the years ahead are beginning to become available. "There is group level work in terms of ultimately making it so that you can have, for example, a fingerprint reader or a fingerprint sensor on the CAC card, along with the ability to do matching and verification on the CAC card as well," he said.

Fedorchak said other technologies may eventually emerge to challenge the CAC's dominance. "There are ongoing efforts to evaluate other form factors, such as virtual tokens, mobile devices, flexible tokens and wearable form factors, such as ID bracelets, as alternatives for user authentication," he said. "CERDEC S&TCD is performing the research and development to address these issues and to help shape how authentication will be performed in the future." ▣