Inside the Pentagon

NATO Biometrics Working Group To Create Tech Standards, Policies

By Fawzia Sheikh

22 April 2010

A new NATO working group assessing how to create a long-term capability to use biometrics information in operations ranging from the Afghanistan war to humanitarian missions will develop technology standards and concepts of operation in an effort that could last years, a Pentagon official said.

The intelligence directorate (J2) of NATO's Supreme Headquarters Allied Powers Europe created a working group that will meet for the first time at the end of May to look at institutionalizing the collection of biometrics information like facial, fingerprint and iris scans, said Lt. Col. Tom Pratt, the military operations branch chief at the Biometrics Identity Management Agency, formerly known as the DOD Biometrics Task Force. BIMA is now a permanent organization rather than a temporary task force.

All allied nations will send representatives to the biometrics-related meetings, which "probably will last a matter of years as they begin developing these standards and getting all of the signatory countries signed up," Pratt told Inside the Pentagon this week.

Alliance working groups meet about every six months for update discussions, he said, adding they can meet "as required, I would assume" and maybe "more often upfront, as they begin working to establish this capability formally, and then drop it down to an annual event once it's established."

In contrast, a simultaneous effort to develop a database sharing biometrics information among coalition forces operating in Afghanistan will likely "progress much quicker," he noted. The ISAF-Automated Biometric Identification System initiative is meant to assist with carrying out tasks like peacekeeping missions, countering improvised explosive devices and protecting International Security Assistance Force member countries by ensuring individuals whose fingerprints are found on improvised bombs are not working on coalition troop bases, as Afghan security force members or listed on ISAF countries' criminal watch lists, a former defense official recently told ITP.

Biometrics is also being tapped in theater for detainee management, including "building a prosecution case to take to court or moving the individual around from cell block to cell block or prison to prison," Pratt said.

The J2-led meetings will initially be like a primer on biometrics offering details about how other allied nations have used the capabilities, he said, adding, "It's not just detainee management and targeting. It can be used for a host of other uses and mission threats anywhere."

At the same time, the working group will begin developing standard agreements (known as NATO STANAGs) that will include the technology that will eventually be adopted, he said. "I know there are ways for fast-tracking things like STANAGs," Pratt noted, adding that a counter-IED STANAG moved along more quickly than many others.

"I would assume even in our doctrine process, service doctrine can take 18 months to two years to even change, let alone develop," Pratt added.

Because many of these standards have already been developed from the perspective of the International Organization for Standardization, "it shouldn't be that difficult from a technology point of view to come to an agreement," he said.

On the policy side, the J2 will also craft concepts of operation, said Pratt. For a humanitarian mission such as a disaster-relief operation, NATO would come up with policy on how a force commander can implement biometrics, he said. "Whether it be ensuring nobody gets inoculated twice to knowing who has been given their weekly ration of rice," Pratt noted. The alliance would also outline using the capability in Afghanistan, he said, noting, "It's not directive so much as, 'here are the use cases.'"

While there are similarities between the use of biometrics in Afghanistan and Iraq, the counterinsurgency strategy of Gen. Stanley McChrystal, the commander of ISAF and U.S. forces in Afghanistan, is a "little bit different than, say, when biometrics was at its high point in Iraq," Pratt said. In the 2005 to 2006 time frame, biometrics was used "offensively" in Iraq to help "segregate who belonged where, who were the bad guys, who were not," he said. "It was done very much hand-in-hand with the Iraqi government and the Iraqi security forces."

The lesson U.S. forces have garnered from the war in Iraq is the need to set up a biometrics system in Afghanistan as quickly as possible, he said. This is important to McChrystal's strategy to put an "Afghan face" on the effort and "give that kind of security reassurance to the local populace that it's not just the ISAF people that are out there taking their fingerprints, it's their own people," Pratt explained.

The Afghan government has begun to use biometrics capabilities and has built a database with the help of the Combined Security Transition Command-Afghanistan, Pratt told ITP. As the Afghans become more comfortable with the technology, he explained, "you can begin to enable the host nation" to carry out tasks, including conducting a census or managing their borders. The database is in its infancy and now Kabul is beginning to develop what is called the enterprise, which is the communication architecture to help move the data and enrollment systems, he added.

While Iraq was "very flat [and] much easier to move communications through," Afghanistan suffers from "what they would call the tyranny of distance and terrain," he said, noting that Afghanistan's mountainous nature affects the communications architecture. In some cases, it may be hard to move biometrics-related data from a hand-held device or a laptop "that's out there on the edge of the fight, back to a more centralized database," he added. "They're creating new communication architectures out there that are not only more robust but are more inclusive of the entire coalition."