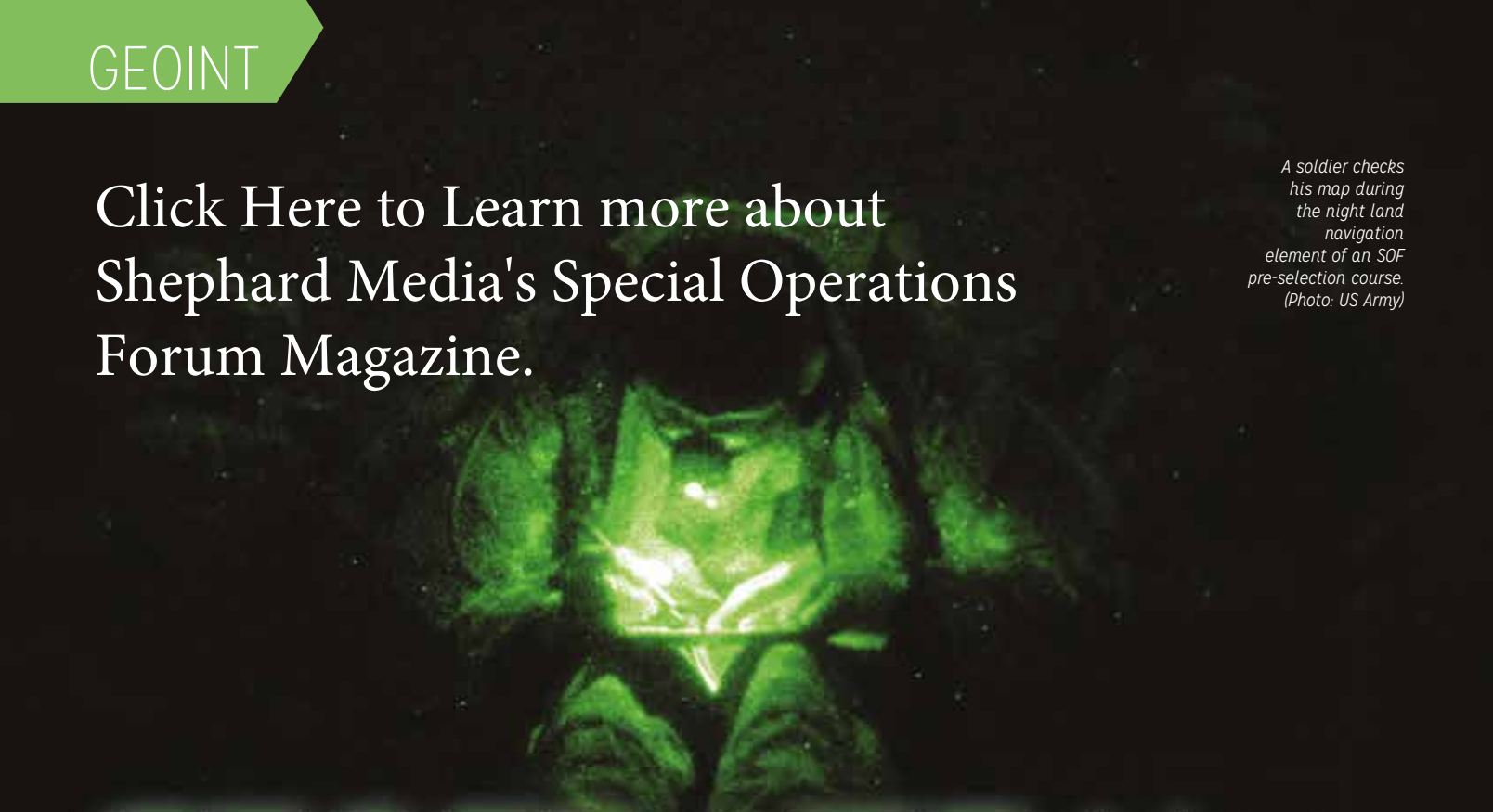


A soldier checks his map during the night land navigation element of an SOF pre-selection course. (Photo: US Army)

GEOSPATIAL APPRAISAL

Geospatial intelligence (GEOINT) has come of age in the 21st century, as network-enabled technology and high-fidelity, more ubiquitous sensors become ever more deeply integrated with the time-honored traditions and science of map-making.

BY ANGUS BATEY

For the special operations community, GEOINT is becoming increasingly vital as the availability of real-time data at the front line increases, particularly in counter-terror or counter-insurgency missions where adversaries use commercial technologies to communicate and propagandize.

"If you'd asked me 20 years ago, I'd have told you that the geospatial world's dead – stick a fork in it, turn it over," said Stu Bradin, president and CEO of the Global SOF Foundation. "Now it's 180 degrees in the other direction." The networking and educational non-profit organization for the SOF community was established in 2014 and has over 1,500 members in 58 countries.

Bradin, a 32-year veteran of US Army Special Forces, retired at the rank of colonel after a career that included establishing and leading NATO Special Operations Headquarters and a stint as director of the Special Operations Fusion Cell in Afghanistan. He considers that among the most important of the various factors that have contributed to GEOINT's revival among special operators is the migration of what was once a strategic, headquarters-based capability to handheld devices that operators can use on missions.

"When I came into the military in the early '80s, all the computing power rested in these huge Cray and IBM computers that only governments could afford," he said. "Now you get that same computing power on a gaming laptop."

SUBTLETY AND DETAIL

Although regular military units will often use militarized, ruggedized computer equipment, SOF personnel usually prefer commercial devices.

"We need to hide in plain sight often," Bradin continued. "We need to be able to positively ID someone, and you need to be able to hold up what you do in a court of law. Most people live in urban areas, so that's where war is going to happen.

"You have to blend in: if you're doing close reconnaissance, you don't want something that's green and large and militarized – you want things that are small, and that don't make you stand out. You also want something you can destroy and throw away."

Bradin also pointed to the increasing levels of detail GEOINT systems are capable of providing as a key reason why SOF teams are becoming more enamored of them. Pointing to the growing availability of 3D mapping, he argued that the pace of innovation in GEOINT is helping to ensure enhanced relevance to special operators.

"I don't just need to know what building to go to – I'd like to know what floor, what side of the street it's on," he said. "I'd like a little bit more information than what's on basically just a digitized map. All that stuff is changing drastically, and it's happening in the commercial sector."

The SOF community's embrace of GEOINT, and the GEOINT community's ability to supply more SOF-ready solutions, appear to be mutually reinforcing trends.

Just as developments in commercial communications technology are helping bring digital mapping tools to smaller devices and educating the general public about how map-based intelligence can be used, so the innovations within SOF operations are changing the way GEOINT analysis is conceived and delivered.

The key enabler in the expansion of small-form-factor, powerful GEOINT tools has been the smartphone – a commercial technology that soldiers at all levels are familiar with and keen to use in their working lives.

But the major development driving GEOINT analysis has come from experiences in counter-insurgency warfare in Iraq and Afghanistan, led in many cases by special operations troops, which helped catalyze a new kind of GEOINT thinking.

INTELLIGENCE FUSION

GEOINT provides a useful baseplate onto which intelligence feeds can be overlaid. Most data collected by other intelligence sensors and methods, be it HUMINT (human intelligence, such as reports from agents and witnesses), OSINT (open-source intelligence, which includes information gleaned from news reports or social media posts), IMINT (imagery intelligence – data derived from photographs), SIGINT (signals intelligence, which includes transmissions from and to communications devices, both military and civilian) or anything else, will usually relate to a geographic location and a specific time.

If the data is time-stamped and geo-referenced, it can be imported into a geospatial information system (GIS) and represented on a map. The British military used a GIS as one of its primary means of organizing, managing and representing multiple intelligence feeds during combat operations in Afghanistan.

The system, referred to by both the names Dataman and Helmand GeoViewer, was the result of collaboration between the MoD's JAGO (Joint Aeronautical and Geospatial Organisation) and the UK division of GEOINT suppliers Esri.

The project involved the creation of a central repository of geo-tagged information stored on servers located at main operating bases; front-line troops were issued with laptops that could connect back to the servers and be used to interrogate the database.

Crucially, the front-line user could select information relevant to a specific area and of a type likely to be of use. The data was arranged in layers – more than 300 of them – and the user could specify which layers they wished to download. One layer might contain HUMINT about recent insurgent activity; another could include previous locations of IEDs; a third perhaps gave locations of known Taliban arms caches.

Ahead of a patrol, a commander could select the layers required, specify the area the patrol was due to cover, and download only the information from the server that was specific to that combination of location and information.

This ensured that troops in forward locations with limited digital communications infrastructure were able to use the system to access the most relevant and up-to-date information, rather than requiring a broadband internet connection to download large amounts of intelligence that had no value to their mission.

Efforts such as the Dataman project helped place GEOINT at the heart of military intelligence fusion, with the emphasis throughout being on ensuring everyone, regardless of their position in the command chain, had access to all the most relevant and useful intelligence available.

THE GREAT UNKNOWN

The drive to eliminate information stovepipes became all the more urgent with the evolution and deployment of ever-more-pervasive sensor systems. With some airborne sensors capable of imaging entire cities over prolonged periods, and the long loiter times of unmanned aircraft adding to the already vast reservoirs of data, it became clear that it would be impossible to analyze everything before turning it into an intelligence product that was then disseminated to the unit that needed the information it contained.

With increased computing power and the lower cost of digital storage, the idea that data could be retained and re-examined many times began to gain ground. Intelligence analysts working in Iraq and Afghanistan – including many from within SOF units – began to develop a methodology whereby this vast cache of already acquired data could be mined to help develop new insights, identify the "unknown unknowns," and – perhaps – use this more thorough understanding of the past to help predict what might happen in the future.

The emergent discipline became known as ABI – activity-based intelligence. It developed in classified circles but has begun to be discussed publicly over the past two years.

"The US Undersecretary of Defense for Intelligence defines ABI as a method of intelligence or analysis where subsequent collection is focused on the activity and transactions associated with an entity, a population or an area of interest," said Ben Conklin, a former US Marine and now the director of global national security marketing for Esri, during a presentation to the Defence Geospatial Intelligence (DGI) conference in London earlier this year.

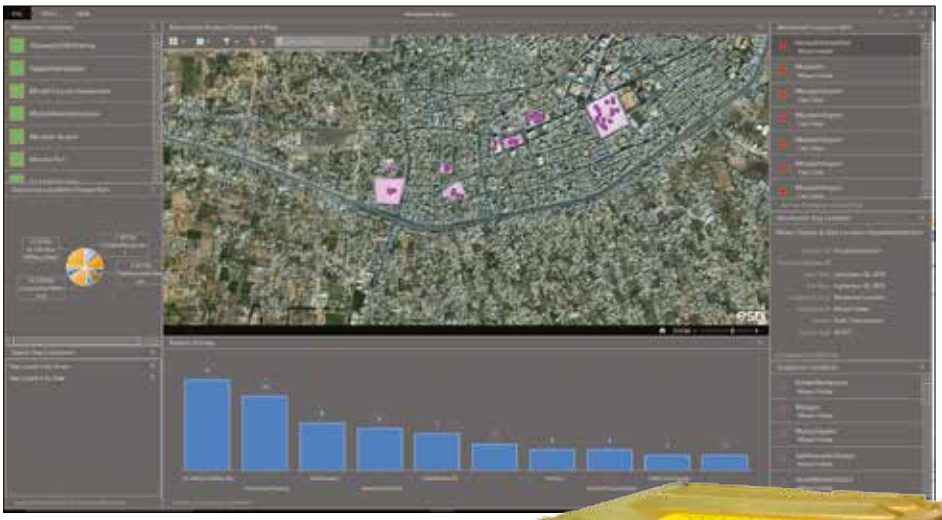
"The definition is actually the tip of the iceberg for what ABI can offer and what it can do for the intelligence communities," he added.

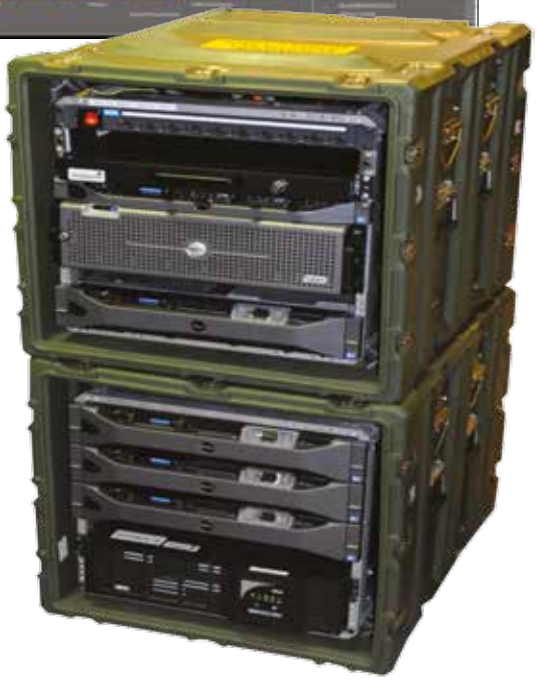
As Conklin explained, ABI evolved out of changing approaches adopted in counter-insurgency warfare, where traditional intelligence analysis – which focused on tasking collection assets to acquire data

that conformed to known signatures (such as movement of known military platforms in strategically important regions, or emissions from ground-based radar systems) – had proven inadequate.

The key challenges analysts needed to solve included an ability to identify adversaries who hid themselves among the general population, who communicated using commercial technologies and whose methodologies did not conform to known observable signatures.

"ABI is a set of spatial-temporal analytic methods to do a few different things," Conklin said. "To discover correlations; to resolve unknowns; to understand networks; to develop knowledge; and to drive collection, using diverse multi-INT data sets to help us understand the environment, not just to understand a specific location or facility. Many of the traditional intelligence methods were focused on analyzing and exploiting information based on known targets and known locations, or known behaviors or signatures of adversaries. ABI is really focused on tackling the 'unknown-unknown' problem."





Above: *A movement analysis tool screenshot showing various ABI-enabled data products from Zawiyah, Libya, in September 2016. (Image: Esri)*

Right: *Efforts such as the Dataman project helped place GEOINT at the heart of military intelligence fusion. (Photo: Esri)*

DATA COLLECTION

Early practitioners of ABI developed four core elements of the new discipline, which are now referred to generally as the "four pillars of ABI": geo-reference to discover; integration before exploitation; data neutrality; and sequence neutrality.

Geo-reference to discover is the part of the problem already solved, to some degree, by projects such as Dataman: including a geo-tag for every piece of intelligence data enables the information to be discovered by someone searching only for information from a location, not just those looking for a specific type of intelligence.

The second pillar notes that data should be integrated into the system before any attempt is made to exploit the raw intelligence.

Data and sequence neutrality refer to the concepts that analysts should not prioritize feeds from particular sensors or systems over others, nor give greater weighting to newer information. If no undue emphasis is given to information based on how or when it was collected, there is a greater chance of deriving a deep and broad understanding of an area and the entities operating within it. The implications for traditional intelligence collection and tasking are profound.

"Sometimes, the answer arrives before you ask the question," Conklin said. "This is really the most vexing problem in ABI. Often, by the time you know which question you're asking, it's too late to begin the collection tasking process. What you need to do is to have already been collecting the information in the first place to answer the question.

"You need to collect data without a question to find and store the data where it can be retrieved and analyzed easily. This changes how you think about tasking and collection. Rather than tying tasking and collection to fixed questions, you need to use incidental collection and other techniques to capture data and store it for future use."

"ABI is a great thing, but in special operations activities it's not a new concept; we've been doing it for a very long time, it just has a label now," said AJ Clark, president of Thermopylae Sciences and Technology, a provider of mobile and web-based geospatial solutions to clients including the US government and several branches of the military.

Clark previously worked in the US military where his roles included time heading up data fusion teams within various joint task forces. "Where special operations are different to conventional defense activity is that everything they do has a very short timeline," he continued, "so it needs to be operable where there's no reachback to a network or an enterprise. ABI really allows you to bring your intelligence into the same picture as your operations at the tactical level."

Thermopylae has worked as a reseller of the Enterprise version of Google Earth, probably the best-known geospatial tool in the world. The company's role has involved writing bespoke applications for customers that sit on top of the basic Google Earth Enterprise software, and which permit them to use the baseplate mapping technology to carry out their own specific tasks.

Of particular relevance to the SOF community are those apps Thermopylae has developed that allow GEOINT products to be shared across devices that do not have an always-on internet connection, so they can be viewed in low-bandwidth environments and during phases of missions where communications tools need to "go dark."

"Often, people will want to do geospatial operations, but the tools that are available to them either aren't familiar to all their users – so they've got to send them to special training or something like that – or they have a license cost that is generally a lot higher than if you were just buying PowerPoint or Microsoft Word," he explained.

"Special operators can use those tools to get an image, but they need everybody on their squad to see it, not just the GIS analyst; but the license costs start to preclude use of that, because somebody may not have the budget to buy hundreds of thousands of versions of offline software because they've just got something running on their web-connected system."

SOF troops need to be more mobile than regular forces and using pocket-sized devices to receive GEOINT helps lighten the load. (Photo: USASOC)

OPEN TO INPUT

In 2015, Google announced that it was going to "deprecate" – cease funding, support and ongoing development of – the Google Earth Enterprise suite of programs. Thermopylae argued that the company should publish the source code and permit Google Earth Enterprise to continue to be developed and supported by the open-source community.

In March this year, Google Earth Enterprise went open-source, under the name Earth Enterprise, with Thermopylae playing a key role in the code's ongoing management while continuing to provide support to its extant customer base.

A key side-benefit of this new arrangement is that users with niche requirements will be able to write their own applications to carry them out in the familiar setting of the Google Earth interface.

"For years, we've tried to support special operations use, but so much of the investment goes into the national-level mission that the special operations folks are told, 'Yeah, just go to this website, you'll be good,'" Clark said. "The people spending the money on the big geospatial capabilities don't keep in mind that there's a really important customer that needs something special for their mission."

"You can also modify apps," said Bradin, pointing to another advantage of having the Earth Enterprise toolset available for open-source developers – which can now include members of special operations units.

"A lot of what we get, if you want to modify it, it's a two-year process. Now, you can get a system engineer, he cranks the new code, and, boom – the apps are modified, you're updated, and it happens in minutes and hours, not months and years."

The combination of open-source software that is familiar to users and very intuitive, coupled with the ability to run it on commercially available smartphones or small tablet computers, suggests that, for the SOF community, a new golden age of GEOINT may be about to dawn.

"Special operations is the largest consumer of imagery products, bandwidth, SIGINT and ISR platforms," Bradin said. "You have to have multiple sources to positively ID a person in a particular location; a picture on its own is not good enough."

SOF teams are not just among the highest users of modern ISR capabilities, they are also among the most frequently disappointed customers of its infrastructure. Bradin said that during 2010 in Afghanistan, "only about 14%" of SOF's ISR requests were being fulfilled.

Making the most of the available data becomes paramount, and using handheld, smartphone-like devices can help get as much of that intelligence as possible to the forward-deployed operator.

Bradin said that the risks of using commercial communications technologies on clandestine missions are often overstated. Certainly, he argued, having more data available is an advantage that outweighs any concerns over analysis of communications patterns revealing the presence of an SOF team to an adversary.

"It's the opposite of that," he said. "When you're walking around trying to find a building with terrorists in it, you want to be able to rely on the feeds that are coming in to you. There are ways to mask those feeds and ways to do it securely. And while it might look like an iPhone, it's not – it's just the same form factor, but with all the different waveforms. But to the average person you're just a bloke with a phone in your hand."

Acquisition processes by which SOF units can procure up-to-date commercial communications technologies are well established, and streamlined enough to ensure that special operators get the advantages in a timely manner without accepting security risks.

Similarly, the use of open-source software on secure military networks is not particularly unusual. Still, for SOF operators to be able to fully embrace the potential of handheld, open-source GEOINT, some careful steps need to be taken.

"The government are very open to open-source software, so long as it's secure and doesn't introduce risks of that nature," Clark said. "They recognize that they can't just take something out of the open-source community and plug it right in. But I think they also understand that there's a lot of ways to ensure security, and then they can benefit from the use.

"The open-source community really operates around the concept of transparency, and that what you see is what you get. If someone was to build a really great enhancement, and they wanted to contribute it, engineers would look at it very empirically in black and white and say, 'Is that good code? Does that enhance the code base? Is it secure?'" ■