BATTLEFIELD FORENSICS

THE CHANGING FACE OF BATTLEFIELD IDENTIFICATION

WORDS MATT BLACK
PICS MATT BLACK & ADF

The poster on the wall is what battlefield identification and target acquisition was primarily about. It hangs in a Scandinavian Special Reconnaissance and Surveillance unit amidst candid photos from past exercises undertaken with other European units. The historical context is clear – while the rest of the world was busy fighting East-West proxy-wars in Malaya, Vietnam, Rhodesia and the like, those based in Europe were busy preparing for The Main Event.

The poster, therefore, depicts every vehicle and aircraft the Soviets might have thrown NATO's way had World War III ever eventuated. Many schools still hold courses in the identification of foreign vehicles and aircraft, along with every uniform and rank badge under the sun. While such information may remain important, there are arguably more pressing security issues today in Afghanistan. Rather than being able to spot the difference between a BTR-70D and a BTR-80 personnel carrier charging across the Fulda Gap, the larger problem today lies in identifying an enemy from within a veritable sea of identically clothed Afghan civilians.

Much of the behaviour we're seeing in the complex environments of today's military operations have more in common with countering gangs and organised crime than anything the military has traditionally handled. Oftentimes the 'insurgents' are quite simply crooks, with a vested interest in the financial opportunities that instability provides, rather than any hard-line political motivations.

For guidance on appropriate techniques, Allied military forces have therefore logically turned to a group of people with a long history of identifying bad guys who don't wear uniforms – the police.

The investigations arms of the law-enforcement fraternity routinely use foot, mobile and electronic surveillance techniques, financial analysis and forensic science to identify and interdict criminals and, more importantly, criminal networks.

This mindset shift was graphically depicted in a recent Australian Intelligence Corps recruiting poster in ARMY Newspaper picturing an M4-equipped Australian operator discovering an AK, load-bearing kit and other items discarded by a fleeing Afghan militant. The tagline read, "Once the shooting stops, the battlefield becomes a giant crime scene".

The poster brought to mind the words of one of the founding fathers of forensic science, Edmond Locard, translated here by Paul Kirk. *Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these, and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study, and understand it, can diminish its value.*

CSI Tarin Kowt

Identifying your adversary and understanding the capabilities of his weapons has always been important regardless of whether you were a Frenchman facing English longbows at Agincourt, or Allied intelligence faced with Hitler's V2 rockets and heavy water program during WWII. Over recent years a new crop of military acronyms and terms has emerged – WTI (weapons technical intelligence); WITs (weapons intelligence teams); SSE (sensitive site exploitation); battlefield forensics and biometrics. Modern-day WITs were reintroduced by the US in 2004 in Iraq and, these days, WTI is recognised for its key role in the counter-improvised explosive device (C-IED) fight in Afghanistan. Each time an IED is discovered, whether pre or post-blast, a WIT is deployed to gather information.

Gathering intelligence regarding enemy tactics, techniques and procedures (TTPs) and on the people responsible for IEDs are the key goals of the WIT. As occurred in Iraq up to – and even more so, after – the introduction of the Status of Forces Agreement (SOFA), the value of usable evidence has increased dramatically in Afghanistan.

While 'evidence' can be used to describe anything used to prove an argument, the term has a strict legal connotation.

A functioning legal system is a vital requirement of any society and soldiers deployed in Afghanistan are therefore increasingly required to adhere to strict evidentiary procedures.

We've all watched CSI or a similar program where the bad guy walks from court a free man thanks to insufficient – or worse, incorrectly collected evidence.

Many ISAF personnel have therefore become somewhat of a 'battlefield cop' not only with respect to an investigative mindset, but with respect to the mountain of evidence paperwork required to ensure a conviction in an Afghan court.

While a recruit freshly arrived at Kapooka might conjure his own ideas as to what 'military exploitation' could possibly involve, it is in fact very straightforward in an operational context. Exploitation simply entails the ability of an operator to exploit a site itself for information, along with collecting items from that site to be analysed later for more detailed intelligence or evidentiary value.

A vital skill in the exploitation operator's arsenal is therefore that of visual tracking. Tracking is, after all, simply linking one piece of evidence to the next and formulating reasonable deductions regarding the events that have taken place.

Given our reliance on technology, the 'personal topology' that resides in our electronic devices can often be tracked more completely than our physical movements across the landscape. As Locard says, everything we do leaves a trace – including digitally.

The sorts of items that might be recovered from an Afghan incident scene are similar to those recovered by a domestic-police high-risk arrest team countering paedophiles, narcotics, people smugglers or any other type of organised crime or gang. They might include weapons (improvised or otherwise), documents, digital media and mobile/cell phones. Hence the corresponding acronyms DOMEX (document exploitation) MEDEX (media exploitation) and CELLEX (mobile/cell phone exploitation).


A foreign weapon is photographed, identified and exploited by a weapons intelligence team member at Al Asad Air Base, Iraq. (US Air Force photo/Staff Sergeant Joshua Strang)

A US soldier practices biometric enrolment using an iris imager. (US Army photo)

A latent fingerprint from an improvised explosive device incident is measured and photographed by a weapons intelligence team member during evidence exploitation. (US Air Force photo/Staff Sergeant Joshua Strang)
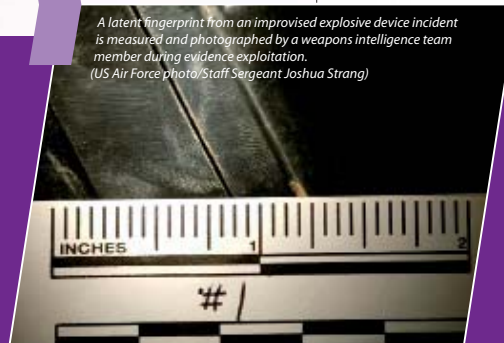
A US Navy weapons intelligence team member in training transforms a vehicle into a training vehicle-borne improvised explosive device during a WIT course at Fort Huachuca, Arizona. (US Air Force photo/Staff Sergeant Joshua Strang)