Chapter 1

New age of warfare: How digital forensics is reshaping today's military

Not since the use of improvised explosive devices (IEDs) by the Irish Republican Army in the United Kingdom have we seen extensive use of IEDs as we have during combat operations against American and coalition forces in Iraq and Afghanistan as a primary force multiplier and sometimes tactical advantage. These IEDs have been taken to a level of use in modern warfare that has shown to be effective for an enemy with inferior technology or organized modern army. From homemade explosives to modified military ordnance, IEDs have become the preferred weapon of choice for insurgents operating in Iraq and Afghanistan. Weapons technical intelligence (WTI) is being developed daily on today's IED components so that tactics, techniques, and procedures (TTPs) can be developed to thwart activities directed at U.S. ground forces as they move about the battlefield. Weapons intelligence teams (WITs) are being fielded to further WTI collection as well as the exploitation of IED materials and electronic digital media. With so much emphasis on all realms of forensics, Baghdad has become the hub for battlefield evidence collection and relevant in prosecuting the war. Military intelligence and evidence have merged as a vehicle to capture and prosecute enemy combatants taking full advantage of modern technology to root out actionable intelligence through digital forensics, thus creating battlefield cops out of everyday modern soldiers.

YESTERDAY'S "BOOBY TRAP" IS TODAY'S IED

Today's battlefield in Iraq and Afghanistan has generated many changes in how U.S. military services conduct warfare in the twenty-first century. One evident change is how U.S. enemies are using anything they can to blow up U.S. ground forces and cause massive casualties instead of face-to-face combat as in past wars. Enemy forces that do not have superior numbers and firepower are creating IEDs as a force multiplier causing chaos and fear wherever they are detonated. Unfortunately, these devices are being used against civilian populations as well when enemy forces

Digital Triage Forensics. Doi: 10.1016/B978-1-59749-596-7.00001-2

target local government officials, such as host nation police and security forces. This tactic has proven to stall cooperation between our military forces and the host nation government. Judges and community leaders have been the target of IED attacks in an attempt to sap the will of the local population and further the enemy's political agenda.

In past armed conflicts, small explosive devices have been used or altered to create "booby traps," thus wounding, maiming, and killing a very small number of soldiers. These traps were not used as a major tactic to employ against our military forces, but as a way to slow us down and create casualties to tie up two to four personnel to take care of any dead or wounded created from the trap. Don't get me wrong, IEDs are not a new phenomenon; they just have not been as prevalent on the battle field as they are in this century.

There have been enormous amounts of military ordnance that have been created that are explosive in nature and are designed for specific missions, such as land and water mines. These devices are usually hidden from unsuspecting enemy forces and are detonated when struck, run over, or stepped on. The claymore mine is an antipersonnel explosive device that can be preset and detonated manually by the emplacer or set as a "booby trap" and set off by the unsuspecting victim. You may be wondering how this differs from IEDs. The difference is that military ordnance is manufactured to specific guidelines and in many cases for specific weapon systems that they can be fired from, such as mortars and artillery shells. IEDs are generally military ordnance that has been "improvised" in some way to be detonated by means other than the originally intended one (see Figure 1.1).

Other IEDs that have been developed by local insurgents have been created by manufacturing containers, filling them with military grade explosives or homemade explosives (HME) and rigging them with some sort of initiation device (see Figure 1.2). More will be discussed about different types of IEDs in Chapter 3.

The insurgents in Iraq have been quite successful in using IEDs against U.S. troops and other military forces since U.S. forces landed on their soil in 2003. In 2009, IED activity began ramping up in Afghanistan as focus turned to the U.S. military forces with the United States' attempts to defeat the Taliban. With all of the United States' high-tech ways of conducting warfare, IEDs have proven that low-tech still has its place in modern warfare. The amount of sophistication that goes into an IED depends on training and background of the actual IED maker and the amount of money available in the region to purchase bomb making materials, to

■ **FIGURE 1.1** Artillery Shell IED emplaced in a road. *Photograph taken by the author, Rich Watson.*

■ **FIGURE 1.2** Homemade IED container with victim-operated pressure switch. *Photograph taken by the author, Rich Watson.*

name just a few. During my time in Iraq, I was located in AR Ramadi, a large city in the Al Anbar province of western Iraq. Most of the IEDs I saw were not as sophisticated as devices seen in Baghdad. I referred to some of the common IEDs I saw as "Red Neck IEDs" as they were made from any materials they could find. Some worked and some did not.

Weapons technical intelligence

So where have all these developments taken us today in modern warfare? The use of IEDs is considered asymmetric warfare and is quite effective for the enemy to use. Because of the use of IEDs, WTI was added to traditional Technical Intelligence (TECHINT) of weapons as a response to the threat. TECHINT is basically the gathering of information about weapons systems of U.S. enemies. WTI is just a category of intelligence gathered from technical and forensic collection of IEDs. Intelligence and forensic evidence gathered help soldiers, sailors, marines, and airmen in their battle spaces to learn the TTPs of the enemies they face.

Every time IED materials are collected from pre- or postlast investigations, the components, wiring, and overall build of the device is examined to determine if new techniques are being implemented to develop IEDs that could defeat the United States' current TTPs. One device that we're focused on in this book is the use of cell phone technology and its use as an IED component.

As you will read in Chapter 5, cell phones are used extensively to detonate IEDs and to store and transmit photographs and data related to insurgent cells, IED sites, and future IED attacks. Cell phone technology has advanced rapidly in the last 15 years and they are now small computers that are capable of being used not only as phones but also powerful electronic processing devices. For a long time, desktop computers and laptops have been the most powerful sources of computing ability available for everyday use. Now cell phones are replacing even laptops as a primary means to conduct business and everyday life with the ability to access the Internet from almost anywhere. As you will see in Chapter 4, computers still have a major role in storing large amounts of data by insurgent cells that can effectively be exploited even when data is supposedly deleted from the system's hard drive. Because of cell phone and computer usage in relation to IED manufacturing, you'll no doubt see these items listed as part of WTI lexicon documentation in the future.

THE INVENTION OF WIT

During the early stages of the Iraq war, it was evident that IEDs were making a huge impact on U.S. ground forces. Something needed to be done to combat these devices and prevent them from producing casualties and causing fear among the U.S. ranks every time they left their forward operating bases (FOB); hence, the creation of WITs.

I interviewed United States Army Staff Sergeant (SSG) Lisa Dzienkowski about her initial experience as a WIT member, as she was selected to be one of the first to pioneer this new needed enduring capability. SSG Dzienkowski told me that in 2004 it was decided by the presidential staff that IEDs were becoming a problem for U.S. ground forces, which weren't really prepared or trained or equipped to cope with defeating the IED threat. The Counter-IED Targeting Program (CITP) was then established; however, CITP was not necessarily intended to conduct the "on the ground" exploitation and collection of IED devices, so WITs were established to take on this role. A task order was sent from the National Ground Intelligence Center (NGIC) to the United States Army Intelligence and Security Command (INSCOM), and INSCOM tasked the 732nd Military Intelligence (MI) Battalion from Schofield Barracks, Hawaii, and another unnamed unit from Fort Meade, MD. Between 15 and 18 volunteers were taken from each unit, and that group became the first Weapons Intelligence Detachment in Iraq. SSG Dzienkowski went through about a month of training, but actually only 2 weeks or so were focused on Weapons Intelligence. She really didn't know what would happen once they got to their mission. Their biggest challenge was interfacing with the explosive ordnance disposal (EOD) teams they were assigned to and selling the WIT mission to the unit they supported. Some EOD teams were resistant, along with some units who didn't even want to send the teams outside the wire. The teams fought through the hurdles and challenges, and did everything they could to prove that the WIT mission was important and needed. There were six teams; three were originally located in the Baghdad area, with one team bouncing around quite a bit and eventually ending up near the western border of Iraq. SSG Dzienkoski's team was in Baqubah, one team was in Samarra, and another team was in Mosul. Each team basically wrote its own standard operating procedures (SOPs) and reports with little guidance. All of the teams communicated with each other and would adjust if another team found something that worked better, but it really was a proof concept all around. Most teams were successful at convincing units and EOD teams that the WIT mission was important and much needed, even though it took practically her entire deployment to get that point driven home. SSG Dzienkowski is currently assigned to the WIT school house as the Non-Commissioned Officer in Charge (NCOIC) (Figures 1.3 and 1.4).

In 2004, when SSG Dzienkowski was assigned to a WIT element, they took with them five pelican hard cases of equipment to their mission, not knowing what kind of equipment was really needed. As each iteration of WITs has completed tours of duty in Iraq, the U.S. military has gotten a

■ **FIGURE 1.3** SSG Dzienkowski receiving an incident briefing from Iraqi security forces. *Photograph courtesy of SSG Dzienkowski.*

■ **FIGURE 1.4** SSG Dzienkowski standing in a blast hole while investigating a postblast scene. *Photograph courtesy of SSG Dzienkowski.*

better understanding of the evolution of the WIT mission and the equipment required to exploit IED evidence. Now in 2010, the WIT kits consist of one large pelican case with some of the most technologically advanced exploitation tools available. The primary focus of a WIT element is to collect evidence found at pre-post blast scenarios and weapons caches using the tools provided in the WIT kits. This includes basic biometrics, explosive residue detection, and digital media exploitation. Chapter 3 will discuss in more detail the actual mission sets required of WITs and how they process the scenes that they respond to during their tours of duty.

WIT training found a home with the 203rd MI Battalion at the Aberdeen Prooving Ground, MD from 2004 to 2008 and then was moved to its current school house located at FT Huachuca, AZ. Currently, students are "volunteered" to be participants in this critical mission. Typical career fields selected are members of MI, Military Police, and EOD technicians taken out of their traditional roles. In past operations, personnel from the U.S. Air Force and U.S. Navy have been selected and put together to create a joint mission. Career fields from those services have included Special Agents of the Air Force Office of Special Investigations (AFOSI), Intelligence, and Master of Arms (Figure 1.5).

Today, WIT members go through 7 weeks of training to prepare for their mission, in addition to Combat Skills refresher training and Combat Life Saving skills training. Some of the subjects taught at the WIT school house include, but are not limited to, the following:

- Report Writing
- FOB Operations
- IED Threats
- Foreign Weapons
- Media Exploitation
- Tracking
- Biometrics

■ **FIGURE 1.5** WIT 5, AR Ramadi, Iraq. Pictured from left to right; author Rich Watson (AFOSI), MSgt Kyle Waller (EOD), SSgt Nick Bradley (Intel), TSgt Travis Goes (Intel), and SPC Landon Lang (25th ID Airborne). *Photograph courtesy of author Rich Watson.*

At the end of their WIT training, all students take an extensive written test and are placed in a field training environment for 3 days where they operate as WIT members and go to scenarios, day and night, designed to test all of the skills they learned throughout the course. WITs are now training Iraqi Army personnel to conduct WIT operations as part of assisting the Iraqi government's transformation to take charge of their country. WIT has a very important and dangerous role in today's modern warfare scenarios and can be utilized anywhere in the world and against any enemy that our nation may face.

"CSI" BAGHDAD: TODAY'S INTELLIGENCE IS TOMORROWS EVIDENCE

Intelligence gathering plays a major role in today's warfare as intelligence provides us with knowledge about what the enemy may be doing or is going to do in the future. Intelligence can be about enemy weapons, troop strengths, troop movement activity, and future operational plans, to name just a few. Intelligence gathering techniques are widely varied from human informants on the ground to satellites orbiting the earth and taking photographs of targeted locations. No matter how it is gathered, intelligence information is used in determining courses of action to be taken in offensive and defensive combat actions in the affected battle space, but when does that intelligence information start to fade into the gray area of evidence? www.dictionary.com defines intelligence as "information of strategic or military value." It also defines evidence as it is applied to law as "data presented to a court or jury in proof of the facts in issue and which may include the testimony of witnesses, records, documents, or objects."

IED materials today are considered to have intelligence value and evidentiary value as well, but how can we use these materials in both categories to make cases against IED makers and employers? The answer is sound, and ethical collection processes as well as documented collection actions requiring a chain of custody to be established on all materials collected. A lot of intelligence that is gathered cannot be used in a court of law as the many varied collection techniques would not meet the standards of our justice system as information (evidence) that was "lawfully" collected. Yet, if our intelligence collectors knew ahead of time that the information they gather could be used as evidence in the future, they could be trained to properly collect and document that information whether the intelligence gathered is in the form of documents, IED components, or digital media.

Now that you understand the difference between military intelligence and evidence, you will be able to better understand the role and mission of WIT. WIT members are not only gathering evidence at pre-post blast scenes they investigate, but are gathering intelligence on enemy TTPs and activity within their area of responsibility (AOR) as well. The information and evidence collected by WIT will be used to successfully prosecute enemy insurgents in courts of law.

ACTIONABLE INTELLIGENCE AND ITS EFFECT ON THE BATTLEFIELD

Actionable Intelligence can be defined in several ways such as "having the necessary information immediately available in order to deal with the situation at hand," but for the purposes of this book, we will define it as "intelligence that can be acted upon within a 12 to 72 hour period of time." No matter which definition is used, the meaning is the same, useful information that can be quickly acted upon.

WIT members exploit cell phones, computer hard drives, thumb drives, SD cards, SIM cards, and other digital media, looking for actionable intelligence that could be used immediately to thwart planned attacks against U.S. and coalition forces. Actionable intelligence gathered could be, but is not limited to, pictures taken by the enemy showing convoys, pictures of key buildings on FOBs, pictures of insurgents placing IEDs, and written plans for future operations against U.S. and coalition forces. Such actionable intelligence could change the course of battles and save many lives. Actionable intelligence is the "golden nugget" that WIT members are in constant search of.

SOLDIERS TO "BATTLEFIELD COPS"

As discussed earlier, WIT members are culled from many career fields within our military services. For most of them, conducting battlefield investigations is a new and foreign concept. Throughout WIT training, they are given crash courses in basic investigative techniques that most police officers spend months learning and spend years perfecting. WIT members become "first responders" of the IED world with their EOD counterparts. Some teams become very successful and glean great results during their tours of duty, but because WIT is not a voluntary assignment, there can be problems associated that can have major effects on our military's success in defeating the IED threat and could ultimately cost soldiers their lives.

Unfortunately, there have been WIT members who do not want to be part of the WIT mission and while they are in school, fail to rise to the occasion, and prove they are capable of being flexible to the mission requirements placed upon them. Those WIT members then deploy and do the minimum amount of work required, do nothing to be successful, and help place negative stigmas upon WIT members and the WIT mission. Like any career field, people who want to be in that career will strive to be successful and bring credit upon themselves and the organization they work for. These negative attitudes some military members bring to the mission not only discredit the Counter-IED initiative, but also discredit their service. The U.S. Army has identified the WIT mission as a sustainable mission and is taking measures to create an additional skill identifier (ASI) for those U.S. Army soldiers who attend the WIT training. The end goal is to create a military occupational specialty (MOS). Once an MOS is created, we will see soldiers who want to be part of the WIT mission enter the career field and bring unprecedented successes to the IED defeat mission. It is not known at this time what the other services may do to identify those who will be trained in the WIT mission.

Rule of Law challenges

The U.S. Army Field Manual 3-07, Stability Operations, defines the Rule of Law as "a principle of governance in which all persons, institutions, and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, and independently adjudicated, and which are consistent with international human rights norms and standards."[1]

On January 1, 2009 a Security Agreement was established between the U.S. Government and the Government of Iraq. Since then, we have been performing operations with Iraqi Security Forces and have developed prosecutable cases based on Iraqi criminal practice and procedures. Now U.S. and coalition forces are not only mandated to follow developed Rules of Engagement (ROE), but also Rules for Escalation of Force. These rules help our military members make use of force decisions and require constant updating as enemy TTPs evolve and change.

So how does Rule of Law affect WIT members in Iraq? We are seeing a shift from U.S. forces conducting the WIT mission to training Iraqi police and security forces in forensics, biometrics, and digital forensics so that they can perform the mission. WIT may now arrive on a pre-post blast IED scene and conduct only a partial investigation of the scene as

the Iraqis conduct most of the scene investigation. This is all part of partnering with the Iraqi Government so that they can take control of their country.

Afghanistan police and security forces are not quite that evolved, but the Rule of Law will come more into play as that country is stabilized. Until then, WIT members must realize that the role they were trained to play will eventually turn from evidence collectors to WIT trainers for the host nation. This is an evolution that will be a constant in any conflict U.S. forces become involved in.

SUMMARY

In this chapter, we have discussed how IEDs have evolved from basic booby traps to primary attack methods of insurgents in Iraq and Afghanistan to the point where traditional TECHINT created a subcategory called WTI that includes technical and forensic collection as part of IED makeup. We have also discussed the need that arose to counter IEDs and the development of the WITs to actually do the hands-on collection of IED evidence and components and pioneer a new sustainable need within the U.S. military forces. We have also looked at the evolution of military intelligence and evidence merging to create a sustainable vehicle for successfully prosecuting enemy combatants under the Rule of Law in Iraq as our soldiers, sailors, airman, and marines become "battlefield cops" outside of their normal military duties and responsibilities.

REFERENCES

1. Headquarters Department of the Army. U.S. Army Field Manual 3-07, Stability Operations. Washington, DC: Stability Operations; October 6, 2008.