Why Site Exploitation

Forcing the return on investment

by Maj David S. Pummell, USMC(Ret)

Circa 1980s, the posting of the warning order in the squad area drove training and patrolling. This was a single-page outline, completed with grease pencil or alcohol pen, providing the situation, mission, and then general instructions. Millions of patrols conducted during the Vietnam War proved this format. The general instructions contained a column for "special org. or teams." (See Figure 1.) One of the standard teams was the "search team," whose task was to search the enemy dead or captured as well as the objective area during the post assault or post ambush phase. Another team was the "POW Handling" team, responsible for executing the standard procedure "5 S": search, silence, segregate, speed, and safeguard. The items found could range from pocket litter of little intelligence value to notebooks and maps containing time-sensitive intelligence of value.

This was the analog age, the age of grease pencils, acetate overlays, lensatic compasses, and PRC 77 VHF FM communications. All forces operating today fully appreciate that we are now well into the digital age. The patrol warning order was replaced by the PowerPoint concept of operations, the CONOP, individual GPS devices, tactical software applications on smartphones, and satellite communications supporting today's patrols.

Our enemies and adversaries have also progressed into the digital age. Today's pocket litter is contained on thumb drives, cellular phones, and other electronic devices. The force must be trained and equipped to effectively triage collected exploitable material to determine value in order to drive immediate follow on targets and support the higher headquarters deliberate targeting process.

>Maj Pummell is a retired Explosive Ordnance Disposal Officer who spent the majority of his career supporting Force Reconnaissance and Special Operations units. As a civilian, he was the Sensitive Site Exploitation Program Manager for MARSOC and currently serves as a MARSOC Strategist.

1) ENEMY

A. SITUATION: 2) FRIENDLY

B. MISSION:

C. GENERAL INSTRUCTIONS:

1. NAME	2. CHAIN OF COMMAND	3. GEN ORG (ELEMENTS)	4. SPEC ORG (TEAMS)	5. DUTIES	6. ARMS, AMMO, EQUIP	7. GEAR COMMON TO ALL	8. TIME SCHEDULE A. WHEN	B. WHAT	C. WHERE	D. WHO
						UTILITIES		DRAW RATIONS		
						SOFT COVERS		DRAW WEAPONS		
						BOOTS		DRAW/TEST COMM		
						GOLVES, BLACK		DRAW AMMO/ORD		
						CAMO PAINT		ISSUE AMMO		
						ID TAGS		TEST FIRE		
						MILITARY ID				
						LBV				
						AMMO POUCHES				
						CANTEEN CUPS		CHOW		
						CANTEENS				
						FIRST AID				
						PONCHO				
						NOTEBOOK				
						PENCIL				
						LAMINATED MAP				
						GREASE PENCIL				
						EXTRA SOCKS		INITIAL INSP		
						EXTRA BOOTLACES				
						COMPASS				
						MOLLY GEAR		FINAL INSP		
						RIFLE				
						CLEANING GEAR				
								T.O.D.		

D. SPECIFIC INSTRUCTIONS:

1. A. _____, YOU ARE SECOND IN COMMAND AND THEREFORE IN CHARGE AT ANY TIME DURING MY ABSENCE. I WANT YOU TO ASSIST ME AT ALL TIMES THROUGHOUT THE DAY IN ENSURING THAT THE TIME SCHEDULE IS ADHERED TO. YOU WILL SUPERVISE PREPARATION AND DRAWING OF EQUIPMENT. ENSURE COMPLIANCE WITH WARNING ORDER BY ALL MEMBERS.

   B. ELEMENT LEADERS SUPERVISE PREPARATION OF RESPECTIVE ELEMENTS AND REPORT COMPLIANCE TO SECOND IN COMMAND.

2. SPECIAL PURPOSE TEAMS/KEY INDIVIDUALS:_____

Figure 1. Patrol Warning Order format, note column 4 Special Organization Teams. This is where the Patrol Leader would identify "Search Teams."

These tasks are commonly referred to as sensitive site exploitation (SSE) or usually site exploitation (SE). These tasks support identity intelligence (I2), the type of intelligence that helps connect the operations and intelligence fusion concept behind the intelligence-driven operations.

During Operations ENDURING FREEDOM and IRAQI FREEDOM, exploitation became a common "post assault" task. The terms SSE and SE were often used to describe the tasks not appreciating the difference in meaning.

Sensitive site. A geographically limited area that contains, but is not limited to, adversary information systems, war crimes sites, critical government facilities, and areas suspected of containing high value targets.[1]

Sensitive site exploitation. A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operation.[2]

Site exploitation. Systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution. Site exploitation contributes to exploitation, defined as taking full advantage of any informa-

tion that has come to hand for tactical, operational, or strategic purposes.[3]

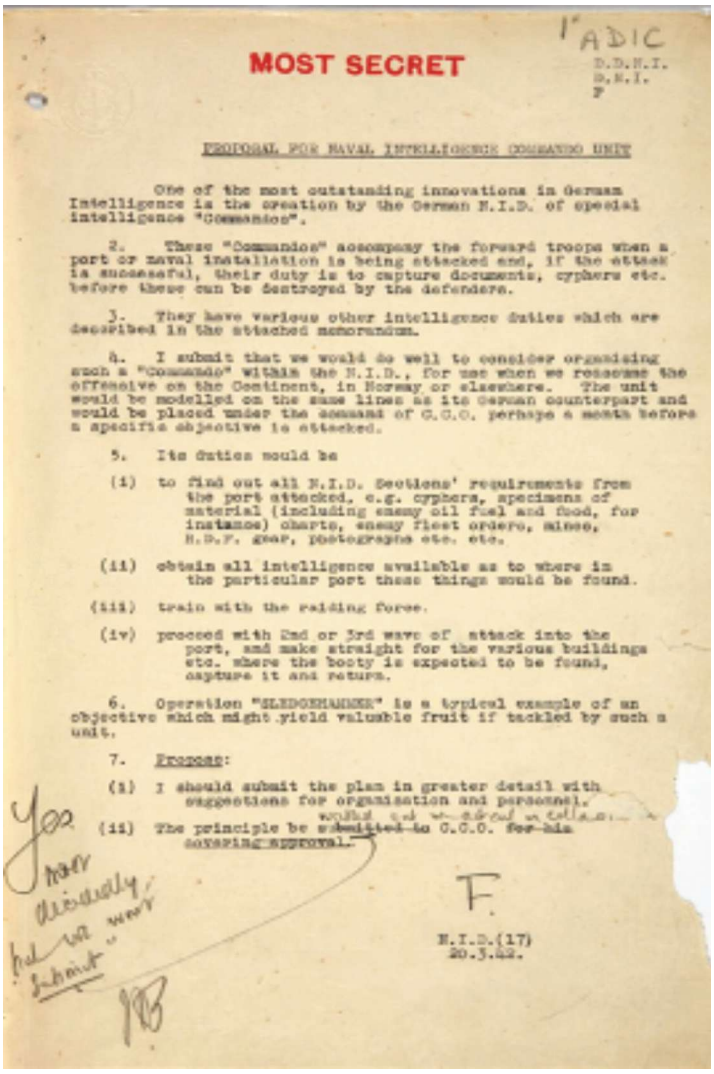
Identity intelligence. The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest—also called I2.[4]

History

Going back 75 years to the forced innovation of World War II, military forces recognized the value of taking the time on the objective to conduct post-assault tasks and collect items of intelligence value.

Most everyone is familiar with the Ian Fleming novels that supplied the movie industry the adventures of the secret agent 007, James Bond. In 1942, Ian Fleming was a British naval officer holding the rank of commander and responsible for the organization of "30 Commando Unit," initially known as the Special Intelligence Unit. Under the motto "Attain by Surprise," the elements were tasked to move ahead of advancing conventional formations to conduct infiltrations into enemy territory to capture items of intelligence value such as codes, new equipment, or high value personnel. During the Normandy Campaign, some of 30 Commando's accomplishments included the capture of a radar station, exploitation of German V-1 missile sites, and the capture of 20 German intelligence officers and 500 troops.

As with many specialized units during World War II, they were deemed unnecessary and disbanded in 1946. An interesting note, the Royal Marines formed the 30 Commando Information Exploitation Group in 2000 with the task to achieve information superiority through the process of find, exploit, and understand, influence, and enable. Operations in Iraq and Afghanistan drove the evolution of the modern-day capability.



MOST SECRET

1 ADIC
D.D.N.I.
D.N.I.
F

PROPOSAL FOR NAVAL INTELLIGENCE COMMANDO UNIT

One of the most outstanding innovations in German Intelligence is the creation by the German N.I.D. of special intelligence "Commandos".

2. These "Commandos" accompany the forward troops when a port or naval installation is being attacked and, if the attack is successful, their duty is to capture documents, cyphers etc. before these can be destroyed by the defenders.

3. They have various other intelligence duties which are described in the attached memorandum.

4. I submit that we would do well to consider organising such a "Commando" within the N.I.D., for use when we reassume the offensive on the Continent, in Norway or elsewhere. The unit would be modelled on the same lines as its German counterpart and would be placed under the command of C.O.O. perhaps a month before a specific objective is attacked.

5. Its duties would be

(i) to find out all N.I.D. Sections' requirements from the port attacked, e.g. cyphers, specimens of material (including enemy oil fuel and food, for instance) charts, enemy fleet orders, mines, N.D.F. gear, photographs etc. etc.

(ii) obtain all intelligence available as to where in the particular port these things would be found.

(iii) train with the raiding force.

(iv) proceed with 2nd or 3rd wave of attack into the port, and make straight for the various buildings etc. where the booty is expected to be found, capture it and return.

6. Operation "SLEDGEHAMMER" is a typical example of an objective which might yield valuable fruit if tackled by such a unit.

7. Progress:

(i) I should submit the plan in greater detail with suggestions for organisation and personnel.

(ii) The principle be submitted to C.O.O. for his covering approval.

F.

N.I.D.(17)
20.3.42.

World War II Memorandum from Commander Ian Fleming to the Royal Navy Admiralty outlining the concept for a special operations exploitation capability.

During the Korean War, North Korean troops used Soviet designed and Chinese built armor. As the attacks continued, the United States needed to learn about the threat systems being employed against our forces. The Foreign Material Intelligence Battalion at Aberdeen Proving Ground, MD, was established into order to conduct weapons technical intelligence to determine the effectiveness of the current friendly ordnance systems as well as the requirements for new weapons systems to defeat the threat. The command supported the exploitation by transporting captured T-34/85 tanks to technical intelligence elements for detailed exploitation both in theater and back in the United States. The technical unit supported the development of new tactics and weapons systems. The exploitation also provided political effects proving the Soviet involvement as captured enemy material was presented to the United Nations as evidence of Soviet involvement.[5]

Military Assistance Command-Studies and Observation Group (SOG) Exploitation (Hatchet Force) conducted small clandestine operations in the Republic of Vietnam and neighboring areas of influence, specifically along the Ho Chi Minh trail from 1966 until deactivation in 1973. The trail was a critical enemy supply route for trucks, tanks, weapons, and troops; SOG provided "eyes on" intelligence and capitalized on the opportunity to capture enemy personnel and material for intelligence purposes.[6] The SOG teams mastered the art of conducting special operations missions with the task of conducting exploitation to support the commander's information requirements. The operating procedures established by the SOG teams established the foundation for special operations forces conducting similar tasks today.

Desert Shield/Storm proved to be the largest joint exploitation effort since World War II, providing an enormous amount of captured enemy material in a short period. The Joint Captured Material Exploitation Center was formed and included personnel from across the DOD. The technical intelligence personnel were able to report the modification of tanks showing improved external armor presenting a greater threat to friendly forces.[7]

The U.S. military involvement in Bosnia further refined the exploitation capability by combining the results of

technical intelligence and human intelligence to determine the capability and intentions of warring parties. The capability of providing this level of intelligence into joint operational planning allowed force commanders to make informed decisions by the determining with high confidence the capability and intentions of the various threat organizations.[8]

September 11, 2001 placed our Nation in a war posture for at least the next two decades with the early years focused on Afghanistan and Iraq. The common threat in both areas of operation was the insurgent use of the improvised explosive device (IED). The enemy learned early that the tactical use of IEDs produced deadly results against our forces. Counter measures were quickly developed and utilized, but the IED cat and mouse game moved at an unpredictable pace; in 2002, commander's would accept a 30 percent solution to defeat the device.[9] Born from the "defeat the device" effort were the combined exploitation modalities aimed at defeating the network, the effort to stop the IED threat before it could even be emplaced. The early logic was purely defensive; the exploitation of IEDs and associated components then feeding the results into the intelligence channels was the offensive solution to take the fight to the enemy.

MACV SOG holding a Soviet made helmet and gas mask found while conducting a battle damage assessment in Southeast Asia. ***(Photo courtesy of Mr. Jason M Hardy author* MAC V SOG: Team History of a Clandestine Army*.)***

The collection modalities associated with SE are broken down into subcategories. Each has the potential to provide information of intelligence value. This will only come full circle and be of value to the commander if they are processed properly and in a timely manner in order to provide accurate results. That information must then be incorporated into the battle rhythm that supports the commander's information requirements.

The early logic was purely defensive; the exploitation of IEDs and associated components then feeding the results into the intelligence channels was the offensive solution to take the fight to the enemy.

Exploitation Capability Defined

Many lessons were learned, unfortunately in blood. The experience demonstrated that the Nation must be able to transition from peacetime presence operations to major combat operations with an understanding of the "gray zones" in between. The lines of operation must be in place to defeat the enemy; a solid exploitation capability enhances the warfighting functions.

There may be times when items are provided to a partner nation for evidentiary reasons. This process was maturing during the final surge years of Operation ENDURING FREEDOM. The processed exploitation results were provided as an annex to the legal prosecution package for the partner nation. Based on the standard protocols used to support the targeting process, the information provided was of an acceptable standard.

The collection modalities producing information valuable to the targeting process are further explained below:

Biometrics. Process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics.[10]

Trace. Trace material is an amount so small that it cannot be reasonably weighed. It is described as residue or minute quantities. Trace evidence can consist of hairs, fibers, and a variety of residue solids.[11]

Latent print. When an item is touched the oils or contaminants from the finger, palm, and soles of feet leave an impression called a latent print. Latent prints can be left behind on most materials.[12]

*Field chemical analysis***.** Identifies unknown substances to a presumptive or confirmatory standard: typically, gunshot residue, drug, explosive, precursor materials commonly associated with a tactical significant activity. The level of tests conducted range from field presumptive tests using colorimetric methods to confirmatory tests using a combination of Raman spectroscopy and Fourier transform infrared spectrometers. The standards for the result vary based upon the regulation used (e.g., U.S. law, international agreements, DOD).[13]

The value of field chemical analysis is the potential to not only identify the hazard or differentiate between a drug lab and explosive making facility but to identify the materials used. The source of supply and potential facilitators can then be investigated and become lines of effort in the continued targeting processes.

Facial recognition. Images of the visible physical structure of a face for both identification and verification purposes. Many nations now use facial recognition as a standard method to identify someone. Facial recognition capabilities are being used at international ports of entry and closed-circuit television surveillance systems. Combine facial recognition with some of the current

artificial intelligence learning algorithms allows a positive identification to be made from searching thousands of hours of recorded video footage within minutes.

Voice printing is based upon the voice spectrogram using the vocal tract unique to the person; it can also be based upon speech patterns. Voice printing is another emerging technology and currently not a primary forensic tool.

DNA profiling is the technique used to assist in the identification of individuals by their prospective deoxyribonucleic acid (DNA) profiles. DNA profiles are a series of numbers that reflect an individual's DNA makeup and are a unique identifier. The DNA molecule is composed of two chains that coil around each other to form the double helix. The double helix carries the unique genetic instructions.

Generally, DNA can be divided into two categories: nuclear DNA, which is inherited from ancestors, and mitochondrial DNA, which is inherited from a single lineage. The single lineage is from the maternal link, whereas nuclear DNA is inherited from all ancestors. Nuclear DNA is usually referred to as the more informative DNA.[14]

DNA collected from tactical events can be from samples containing bodily fluid residue, skin, hair, or a buccal swab sample collected directly from an individual. DNA is another emerging technology and can be cost prohibitive for routine collections. DNA databases are becoming broader and individual information shared on the commercial market when people purchase DNA tests and associated reporting options (e.g., "23andMe").

Document and media exploitation (DOMEX) is the processing and analysis of both hardcopy and electronic media. DOMEX sub-categories consist of document exploitation, media exploitation, and cellular phone exploitation. These terms are often used by those not familiar with the actual target material and processes involved in DOMEX.[15]

The scope of *weapons technical intelligence* (WTI) relative to site exploitation is the technical collection and exploitation of captured material associated to IEDs, improvised weapons, and other weapons systems. WTI, in the broader definition, also includes technical intelligence on threat weapons systems, and weapons seen for the first time in order to determine the capability, threat, and development of countermeasures. WTI is used strategically to conduct exploitation of ordnance residue used by our enemies and adversaries to confirm violations of international arms agreements and embargos.

Threat financing is the investigation of different forms of currency used to support enemy action against our Nation. Identifying the funding methods and key facilitators can severely limit the enemy's capability, often forcing them to operate in a stressed state that results in errors and opportunities for other exploitation. Recent practices showed the investigation of Hawalas showing funds to support weapons systems and components to cross-border facilitators. Today, the use of crypto currency is becoming more common as the cyber domain matures. The requirement for cyber dominance and the ability to follow crypto-currency transactions on the dark net will be a requirement for the success of military operations.

When conducting counterinsurgency operations or operating in the gray zone the insurgent or proxy enemies use of the IED has become the norm. The intelligence value of the IED and associated components are critical to attacking the network and having the ability to attack the enemy "left of boom." Processing this material has an obvious increased risk requiring additional subject matter experts to perform the collection tasks. Explosive ordnance disposal must render safe the IED and make the decision to gather items of intelligence value; items must then be transported to a safe area for detailed exploitation after confirming it is safe to do so. The many variations of IED are here to stay.

Exploitation Concept of Operations

A solid exploitation concept of operations is required to ensure the information gathered from the various exploitation modalities is incorporated into any unit's battle rhythm, feeding the appropriate events such as the targeting board. If exploitation does not support the commander's information requirements, the "So what?" value is questionable. In the early years of exploitation during Operations Enduring Freedom and Iraqi Freedom, it was a common perception that collected exploitable material, specifically IED components, disappeared into a black hole. This perception—often justified—drove the question of: Why should an individual or unit take the risk and time to exploit the area after a significant activity? Fortunately, over the years, the combined improvements of technology, training, and procedures specifically in the Special Operations Command program of record that has established a global architecture to man-

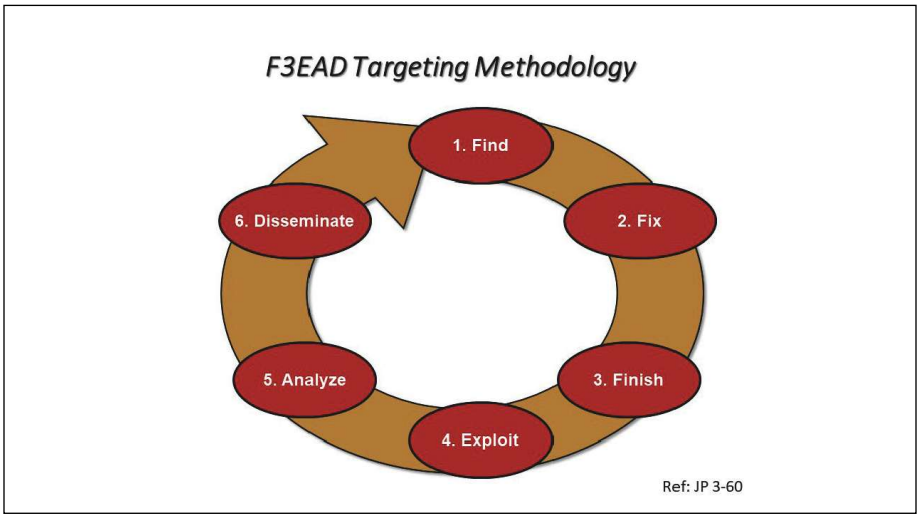


Figure 2. Legacy graphic depicting the process for HVI targeting. *(Figure provided by author.)*

age the amount of information being processed by the deployed forces.

A common misspeak is that exploitation needs to support the find, fix, finish, exploit, analyze, disseminate (F3EAD) process. (See Figure 2 previous page.) F3EAD is a methodology, not a general staff process. F3EAD was originally designed to target personalities. The commander may find that a blend of several targeting methodologies (e.g., F3EAD, Decide, Detect, Deliver, and Assess [D3A], Find, Fix, Track, Target, Engage, Assess [F2T2EA]) will develop the best targeting process to fill the requirement.

The commander's staff will put the methodology into process by typically as a default following the dynamic targeting process:

- Objectives, guidance, intent.
- Development and prioritization.
- Capabilities analysis.
- Decision and force assignment.
- Mission planning and execution.
- Combat assessment.[16]

The phases of the process will be transferred to a functional task by way of the unit's battle rhythm and specifically the targeting board serving as the nexus. (See Figure 3.)

In summary, in order to master any skill, it must be continuously rehearsed and used in order to be of value to the force. This is the same with SSE collection tasks. All operational units must consider immediate follow-on tactical targeting opportunities based upon sound intelligence, and then continue to feed the intelligence community to refine targeting efforts on the operational level. The initial steps to facilitate those levels of targeting are SE techniques and procedures utilizing the associated individual and team techniques and equipment. A thorough understanding of the supporting architecture is needed to ensure all materials are submitted to the appropriate agency for further exploitation. Special Operations Command has a matured program of record connecting special operations forces, joint force, inter-agency, and other supporting elements. Communicating via the special operations exploitation web-based architecture collection submissions are enabled across the globe.

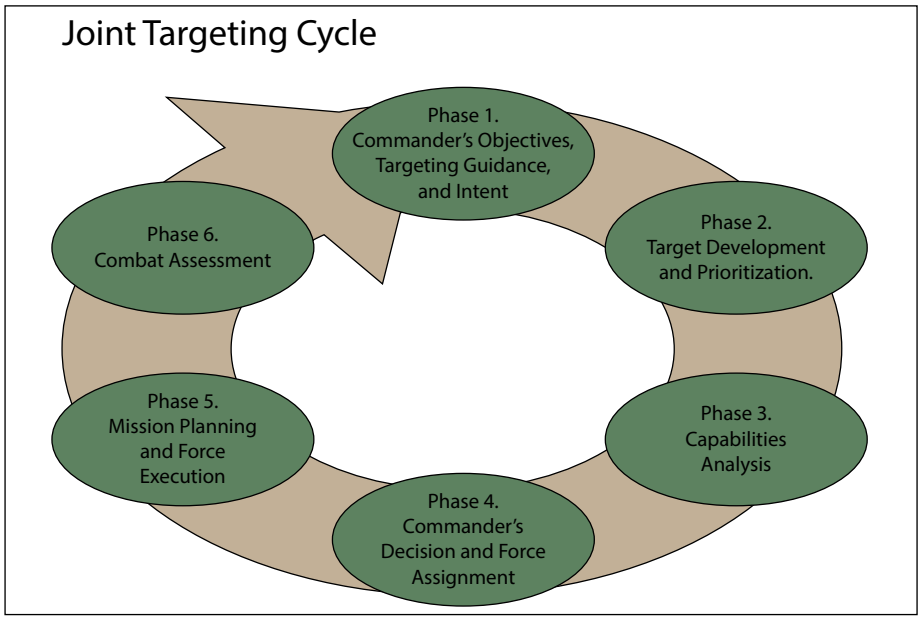


***Figure 3. Joint Targeting Process from* JP 3-60, Joint Targeting.**

Preparing for the next?

What is beyond the next ridgeline? The requirements to engage the next threat need to be resourced now. There is a lot of dialogue articulating the need to shift the focus from an asymmetric, counterterrorism focus to a near-peer adversary/enemy engagement. Will the force be operating in a declared theater of active armed conflict/Phase 0 environment or decisively engaged in a declared theater of active armed conflict/Phase 3? Are we postured to conduct both individually and consecutively?

The requirements to engage the next threat need to be resourced now.

We have had the luxury of operating in a posture of dominance across all domains. How will our systems perform in a space or cyber contested environment? In the digital age, one critical requirement is the capability to transfer large data. Multiple formations conducting a large campaign will require a reliable digital architecture to communicate while performing collection tasks involving the upload of large data files. This has become a common task to all maneuver elements of any size.

In a force reliant upon the full spectrum of communications equipment, what signature is presented every time a handset is keyed or the "send" button pressed? Tactics, techniques, and procedures must be refined to reduce the potential of being geo-located by the "digital exhaust" created when conducting operations.

During DESERT SHIELD/DESERT STORM, Iraqi Army detainees were in the thousands, each individual had pocket litter of the analog age, notebooks, and letters from home. Handling the same amount of detainees today, each individual can be expected to have a cellular phone with a minimum of a terabyte memory capacity. Commander's battle plans will no longer be visually identified as map folders but as digital media products contained on hard drives and peripherals.

To process, exploit, and disseminate collected materials, the force must be able to triage all items and determine the immediate value for continued or follow on operations. The remaining material will continue triage by higher headquarters to determine what items are of value and worth the effort to transmit across the already strained digital network. Physical items will be

Iraqi soldiers surrender during Desert Storm. *(Official U.S. Army photo.)*

shipped by established air, land, and sea lines to a regional collection node and potentially supporting agencies in the continental United States.

Robust supporting systems utilizing innovative technology will be the critical element for success. Artificial intelligence and deep learning algorithms utilized at the tactical level will reduce the digital load significantly. As an example, incorporating this technology will reduce the time to review thousands of hours of full motion video to complete collection tasks such as facial recognition matching from hundreds of hours to minutes.

Success across all domains can only be achieved by a tested joint solution including partnering with specific interagencies. Established DOD programs of record should be reassessed to ensure the scope meets the requirements then assigned by the Joint Chiefs of Staff as the coordinating authority to establish a globally reliant and survivable architecture.

Forcing the Return on Investment

This is the vital discussion that facilitates the answer to "So What?" How does a commander force the return on the investment when taking the risk and time to conduct exploitation related tasks? The process, exploit, and disseminate cycle must move at a pace to provide timely intelligence to answer information requirements and support the targeting cycle. Not through lack of effort, the early years of exploitation 2004–2009 had a hard time in returning information of relative intelligence value to the submitting unit. Today, the list of tactical to strategic wins attributed to exploitation efforts is significant. Through the Special Operations Command program of record, a global supporting architecture is in place that facilitates the sharing of information across the combatant commands and inter-agency networks. Collection triage and collaboration is at a performance level to provide results to the submitter in a timely manner. Depending on the forensic modality, results range from minutes to months. The effort continues with the goal to provide near-time exploitation results across the range of military operations. Success will only be accomplished by the tried and true process of research and development, education, exercising, operational testing capturing metrics, and facts via the lessons learned and after-action reports.

Success across all domains can only be achieved by a tested joint solution ...

Notes

1. Joint Staff, *Joint Publication 3-13, (JP 3-13) DOD Dictionary of Military and Associated Terms*, (Washington, DC: January 2020).

2. Ibid.

3. Department of the Army, *FM 3-90.15*, *Site Exploitation Operations*, (Washington, DC: July 2010).

4. Joint Staff, *JP 2-0, Joint Intelligence*, (Washington, DC: October 2013).

5. Department of the Army, *FM 34-54, Technical Intelligence*, (Washington, DC: November 2009).

6. Jason M. Hardy, *MACV SOG: Team History of a Clandestine Army*, (Las Vegas, NV: Hardy Publications, 2018).

7. *FM 34-54, Technical Intelligence.*

8. Ibid.

9. Ibid.

10. *JP 2-0, Joint Intelligence.*

11. U.S. Special Operations Command, *USSOCOM SOF Identity Intelligence Smartbook Version 2015-01*, (Tampa, FL).

12. Ibid.

13. Ibid.

14. Ibid.

15. Ibid.

16. *JP 3-60, Joint Targeting.*

>Author's Note: Some terms used in this article are specific to the USSOCOCOM SSE Program of Record and currently being staffed for Joint use approval.