DOMEX: The Birth of a New Intelligence Discipline

by Colonel Joseph M. Cox

The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Army, Department of Defense, or the U.S. Government.

Introduction

Prior to 9/11, Document and Media Exploitation (DOMEX) capabilities were neither well defined nor sufficiently developed or understood to adequately support combat operations. Despite lessons learned from previous conflicts, U.S. forces entered the War of Terror without mechanisms to properly collect, process, and disseminate intelligence derived from DOMEX. In the past 18 months, the volume of captured digital information from law enforcement, intelligence, and civil court cases has exploded. Recent investigations of Umar Farouk Abdulmutallab, the alleged terrorist who attempted to detonate plastic explosives on board a commercial airliner, and U.S. Army Major Nidal Malik Hasan, the man accused of killing Soldiers at Fort Hood, rely extensively on close examination of personal computer data by federal law enforcement agencies. These are just two cases amid an avalanche of harvested digital media that create a national security issue which merits a system that can reliably sift intelligence and quickly share it in order to protect lives and preserve security.

In response to a recent congressional inquiry, two respected leaders of the Intelligence Community (IC) commented that "there is no doubt that "*DOMEX provides critical intelligence unavailable through any other discipline.*"[1] Without question, our DOMEX capabilities have evolved into an increasingly specialized full-time mission that requires a professional force, advanced automation and communications support, analytical rigor, expert translators, and proper discipline to process valuable information into intelligence.

This article will examine the historical roots of DOMEX operations to present day activities, explain why DOMEX should be an intelligence discipline, review how the Army improved DOMEX capabilities, and what steps can be taken to enhance operations, and then offer recommendations on how the IC and the Department of Defense (DOD) can better organize, train, man, and equip itself to meet DOMEX challenges in the future.

Historical Context

The U.S. military and other branches of our government relied on what was originally titled Document Exploitation (DOCEX) for as long as we have practiced the art of intelligence. Discovering the enemy's intentions through examination and exploitation of captured documents was nothing new. In warfare, exploitation of adversary documents normally begins at the point of capture and progressively becomes more detailed and sophisticated as the document moves through a process of triage, translation, and promulgation.[2]

The Civil War provides many examples of troops capturing and attempting to exploit enemy documents. The assassination of President Lincoln caused a detailed review of captured Confederate documents once thought trivial or of little value for military operations, seeking proof that Southern leaders were linked to the assassination plot.[3] By 1920, the U.S. Army War Department intelligence regulation emphasized the value of DOCEX: "Experience has shown that the information derived from documents is second in value only to that secured by the actual examination of prisoners. Too much stress cannot be laid upon the importance of the rapid and systematic examination of every document captured."[4]

Unfortunately, DOCEX was never a high priority in terms of training and resources as the Army entered World War II. In Europe, the 1st Army had a total of five personnel assigned to their DOCEX team for combat operations from January 1944 to May

1945.[5] This team would disseminate intelligence reports after documents were reviewed and translated, usually 48 hours after capture. But with the capture of between 250 to 1,000 pounds of documents each day, the organization was of marginal assistance to tactical operations.

1st Army reached several conclusions about DOCEX intelligence: "documents arrived too late for operational exploitation" and "sufficient personnel were not trained to help Corps and Division levels".[6] Through the Korean War and into Vietnam, DOCEX remained relevant and necessary to gain intelligence on the enemy, but it was viewed as something temporary in nature. When we needed it, we built organizations to meet the demand, then forgot about lessons learned after conflicts ended.

Why was U.S. Army DOMEX Not Prepared for 9/11?

The first problem was that after Vietnam, U.S. Army DOCEX missions and functions were doctrinally pinned to interrogators: "the first intelligence specialists who could examine or exploit captured documents, in addition to interrogating prisoners of war, and will scan documents and extract information."[7] Accordingly, DOCEX procedures became firmly rooted within the interrogator Field Manual (FM) under the human intelligence (HUMINT) discipline.

The second problem was the direct result of placing DOCEX responsibilities on interrogators within HUMINT. There simply weren't enough collectors (CI and interrogators) to accomplish the DOCEX mission. As the Army reduced its force size in the early 70s under a transformation initiative called "Army of Excellence (AOE)," it became apparent that an interrogation force would not be a large one. Close study of the AOE with respect to interrogator strength revealed early concerns that there weren't enough interrogators in Army inventories to conduct HUMINT missions and equally support DOCEX missions.[8]

What Were the Consequences of Not Being Prepared?

One intelligence leader stated: "DOCEX didn't work; we did our own DOCEX when we could. Otherwise, it was sent to some CJTF-76 DOCEX section for processing that was virtually a black hole because I never received any feedback from anything we sent forward. We just didn't have the manpower at our level to conduct any type of extensive DOCEX."[9] From the outset of Operations Enduring Freedom/Iraqi Freedom (OEF/OIF), there was a shortage of trained HUMINT collectors and they were a precious resource. Major General Barbara Fast, the Multi-National Corps-Iraq C2, stated that "it became imperative once we were in Iraq to establish a strong HUMINT capability to understand the situation on the ground, but we lacked the number and some of the skills required to be as successful as we needed to be."[10] Predictably, the scant numbers of HUMINT collectors were in high demand just for their core mission sets: tactical questioning, debriefings, source operations, and interrogation of detainees. *DOCEX wasn't a priority*.

DOMEX Goes National

As the military struggled with DOMEX activities between 2001 and 2003, the first tangible effort to institutionalize DOMEX at the National and strategic level came with the creation of Defense Intelligence Agency's (DIA) National Media Exploitation Center (NMEC) in 2003.[11] The NMEC was created to serve as the lead government agency for the rapid processing, exploitation, dissemination and sharing of all acquired documents and media between strategic/national through tactical/local levels across the Intelligence, Counterintelligence (CI), military, and Law Enforcement (LE) communities to enhance the safety and security of the Nation.[12]

The swift expansion of DOMEX enterprise created many different efforts across the IC and DOD which required significant funding from congress. In 2005, the U.S. Senate Select Committee on Intelligence (SSCI) conducted an audit to review the practices of collecting, processing, translating, and reporting intelligence obtained from overtly captured and/or clandestinely acquired paper documents and electronic media.[13] The SSCI wanted to analyze and evaluate the intelligence value of DOMEX efforts and assess the budget implications for sustaining DOMEX over the long term. The SSCI audit findings concluded that:

- DOMEX had become an integral source of valuable intelligence information supporting both tactical operations in OEF/OIF and Iraq and strategic analysis in national intelligence agencies,[14] but there was a perception of slight duplication of effort and redundancy in terms of reporting intelligence.

- The IC allowed the DOMEX expertise to atrophy after each major conflict which caused a routine "reinvention of the wheel" phenomenon. This proved insufficient, and allowed for an information vacuum to exist during periods when policy makers and military planners most need DOMEX data.
- IC leadership needs to make tough decisions in the near term in order to improve the efficiency and effectiveness of DOMEX activities.[15]

The Office of the Director of National Intelligence (ODNI), as the head of the IC, oversees and directs the implementation of the National Intelligence Program and, by extension, provides oversight to DOMEX intelligence activities. The ODNI published Intelligence Community Directive (ICD) 302 in July 2007 assigning national DOMEX oversight to the Assistant Deputy Director of National Intelligence for Open Source Intelligence (ADDNI/OS), the NMEC, and the IC agencies.

One item within ICD 302 represents the center of gravity for the publication–NMEC became the DNI center for the national DOMEX enterprise and became chartered to:

- Support the development of the ODNI's DOMEX strategy, policy, and programmatic recommendations.
- Ensure prompt and responsive DOMEX support to meet the needs of intelligence, defense, homeland security, law enforcement, and other U.S. Government consumer, to include provision of timely and accurate collection, processing, exploitation, and dissemination of DOMEX.
- Implement policies and guidance on DOMEX including handling and dissemination polices.
- Develop training and tradecraft programs that expose all IC personnel to the benefits of DOMEX.

What the U.S. Army Fixed in DOMEX, What Can Be Improved, and What Can Other Services Learn?

For over 50 years, and until recently, U.S. Army intelligence doctrine preserved the DOMEX function within the HUMINT discipline and failed to maintain sufficient capability to conduct the mission. A post-mortem appraisal of the U.S. Army's OEF/OIF DOMEX experiences along the DOTMLPF framework offers lessons learned for other services:

Doctrine–DOCEX incorrectly resided under HUMINT with interrogators as lead.

Organizations–No Army units, to include intelligence units, were structured to conduct the function.

Training–Training was never formalized. Theaters established their own procedures and training. No effective blueprint existed for standardized DOCEX instruction.

Materiel–There was no family of systems to cover a DOCEX end-to-end approach.

Leadership–HUMINT staff directorates were overwhelmed.

Personnel–No professionalized force to accomplish the mission.

Facilities–Not applicable. DOMEX shortfalls were not caused by inadequate infrastructure.

The 2008 U.S. Army Training and Doctrine Command (TRADOC) and 2007-2009 Office of the Secretary of Defense overlapping studies assessed conventional and special operations forces and determined that a relatively small number of core and enabling capabilities was essential to sustaining an intelligence campaign against a networked adversary. The studies revealed one of the driving capabilities of the "find, fix, finish, exploit, access, and disseminate" cycle was DOMEX.[16]

Here are some thoughts and recommendations within the DOTMLPF framework which require immediate attention from the U.S. Army, and which other military services can digest, to capitalize on critical momentum generated by DOMEX over a relatively short period of time:

Doctrine. Figure 1 highlights that DOMEX spans all five steps of the Joint intelligence cycle and should be viewed as an intelligence discipline. JP 1-02 states that an intelligence discipline is "a well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources."[17] Without a doubt, DOMEX meets the doctrinal specifications outlined in the joint publication.

It's also noteworthy to point out that ICD 302 states that "DOMEX activities support a wide range of intelligence activities, including all source analysis, Open Source Intelligence (OSINT), HUMINT, Signals Intelligence (SIGINT), Geospatial Intelligence

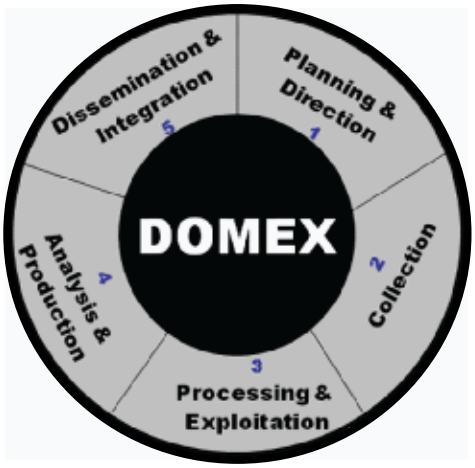
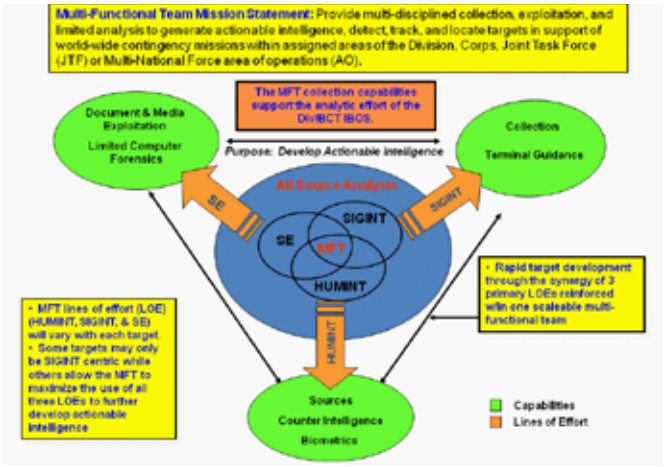


Figure 1.

(GEOINT), and Measurements and Signatures Intelligence (MASINT)–DOMEX reporting and analysis are considered intelligence products".[18] Aside from correct recognition of DOMEX as an intelligence discipline, the U.S. Army must also correct several doctrinal disconnects to set a better course for the future. Below are four key doctrinal items that Army intelligence leaders must address:

1. The most recent final draft of FM 2-0 Intelligence incorrectly states that DOMEX is "an emerging capability" but goes into profound detail spelling out the fundamentals of all other intelligence disciplines.[19] The FM misses a tremendous opportunity to devote a short chapter to DOMEX and bring together the central thoughts and themes thinly spread throughout the document into a single, concise framework that reinforces what DOMEX actually is–an intelligence discipline. *Recommendation*: Use FM 2-0 to state that DOMEX is an intelligence discipline.
2. TRADOC's Concept Capability Plan (CCP) for Intelligence, Surveillance, and Reconnaissance (ISR) for 2015-2024 fails to clearly articulate Army DOMEX capabilities required to succeed as we face future threats. The CCP barely mentions the term DOMEX and incorrectly states that DOMEX capabilities are required with HUMINT.[20] This doctrinal miscue makes it look as though TRADOC is out of step with current Army intelligence and ISR doctrine. *Recommendation*: TRADOC must develop a comprehensive DOMEX capabilities list in the CCP.
3. FM 2-22.3 HUMINT Collector Operations incorrectly maintains that "DOCEX" vice DOMEX is a HUMINT collection function and mixes DOMEX in the core HUMINT missions of tactical questioning, debriefing, source operations, and interrogation.[21] This must be changed immediately. We already know that Army DOMEX operations were not successful in the early stages of OEF/OIF because we expected interrogators to conduct the mission based on our doctrine. *Recommendation:* Publish an interim change to the FM and clarify DOMEX functions and responsibilities.
4. The U.S. Army Intelligence Center of Excellence (USAICoE) diligently worked the timely release of Training Circular (TC) 2-91.8 DOMEX Enabled Intelligence.[22] The publication codifies DOMEX doctrine and general tactics, techniques, and procedures from tactical to strategic environments. Unfortunately, based on restrictions on the number of FMs, the TRADOC Commander limits MI Doctrine to only four FMs. A DOMEX FM could better serve as a blueprint for other military services to follow as they develop their organization and training models. *Recommendation:* The U.S. Army should convert the TC into an FM and title the FM "DOMEX Operations" not DOMEX–Enabled Intelligence. Saying that there is DOMEX–enabled intelligence is akin to stating there is bullet-enabled infantry.

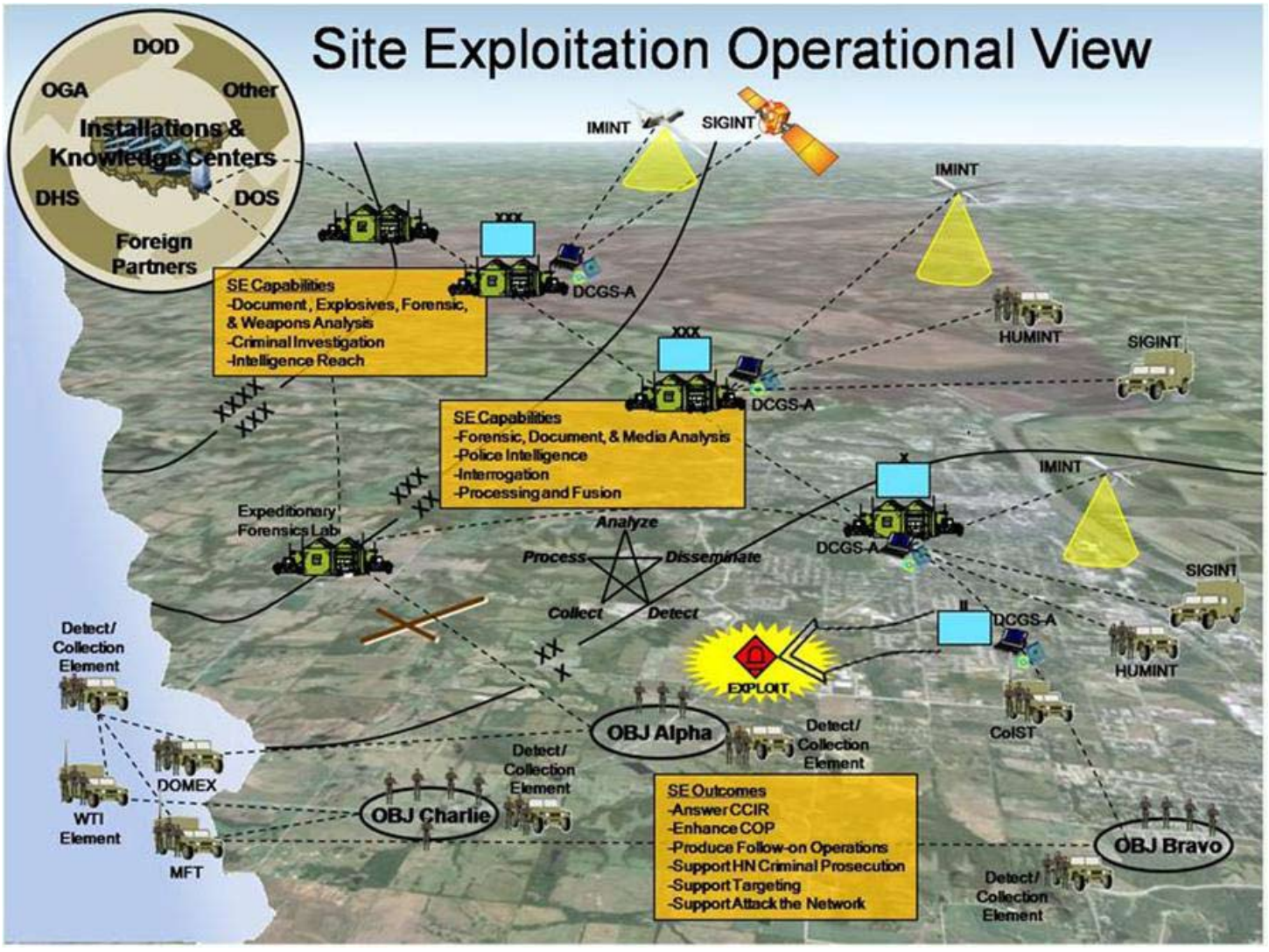
Organization. The need for tactical DOMEX capabilities *across the services* has never been greater; the services must address this organizational gap immediately. The Army learned that designating HUMINT Collection Teams (HCTs) for DOMEX missions was a poor strategy.[23] The Department of the Army (DA) G2 quickly recognized this and established Multi-Functional Teams (MFTs) within the Army's Battlefield Surveillance Brigade. The MFT task organization uses four intelligence military occupational specialty



(MOS) career fields: 35L CI Agent; 35M HUMINT Collector; 35N SIGINT Analyst; 35P Cryptologic Communications Interceptor/Locator, and 35S Signals Collector/Analyst.[24]

Each MFT fields sufficient personnel and equipment to exploit captured enemy materials (documents, media, and personal electronic devices), link biometrics data within the collection effort, and fuse tactical all source intelligence efforts for battalion and brigade S2s. *Recommendation*: Other military services should develop a similar approach as the MFT model within their intelligence organizations in order to provide a trained, tactically oriented, professionalized force to conduct DOMEX below National levels.

Training. The Army and other services must bring order and discipline to our DOMEX training approaches to professionalize a DOMEX force that is responsive to global demands, not just the urgent needs in Iraq and Afghanistan. DOMEX collection is not a task limited to intelligence Soldiers. Any Soldier can collect materials which require exploitation. Just as all Soldiers must be prepared to fight as infantry, they must also serve as information collectors. This is the premise for the "Every Soldier is a Sensor" model. Tactical collection skills are taught to Soldiers in all MOSs under the umbrella of Site Exploitation (SE) training. In SE, Soldiers enter and actively observe details at a site, use their cognitive skills to recognize information, materials, and personnel at the site that may help to answer the commanders' information requirements.[25] The graphic below portrays the relationship of the SE functional capabilities within levels of command and highlights the use of the Distributed Common Ground System-Army.



With respect to U.S. Army intelligence training, I recommend that a new MOS be designated that specifically covers DOMEX (exploitation of documents, media, and personal electronic devices) or at a minimum, an additional skill identifier (ASI). Currently, USAICoE provides baseline intelligence skills training for eight enlisted intelligence MOS career fields, the five MOSs mentioned in the MFT organization and MOSs 35F Intelligence Analyst and 35G/H Imagery/Common Ground Station Analyst.[26] Only MOSs 35M and 35T Military Intelligence Systems Maintainer/Integrator receive some DOMEX training. This is a start but it's not enough. *Recommendation*: At a minimum, I recommend that the MOSs 35F, 35M, 35L receive DOMEX training as well. Mobile training teams from the Defense Cyber Investigations Training Academy (DCITA) and National Ground Intelligence Center (NGIC) could also assist USAICoE to provide specialized computer forensic training to Soldiers.[27]

Materiel. Because DOMEX functions were historically linked to HUMINT as a function, a HUMINT reporting system was the only Program of Record (POR) to support DOMEX. The CI/HUMINT Automated Tool Set provided an HCT with a capability to collect, process and disseminate information obtained through document exploitation.[28] It wasn't nearly capable enough to satisfy a broad range of DOMEX equipment and software requirements to fully exploit information within computers, portable storage devices, video imagery, and a host of other items.

Today's the Army's DOMEX equipment suite offers significant advances over what was available to theater forces three years ago. The U.S. Army Intelligence and Security Command, DA G2, and the Army DOMEX program manager worked hard to field a standardized set of DOMEX equipment that met operational needs in support of OIF/OEF across the Army and ensure that the equipment was compatible with inter-agency standards. The Army must align these QRC efforts into PORs which seamlessly integrate across existing core, collection, processing, and dissemination intelligence systems.[29]

Leadership. From a tactical and operational staff perspective, G2/J2/C2 (HUMINT) staffs are in position to supervise DOMEX. The 2X staff directorates are fully engaged in coordinating and managing numerous HUMINT and CI collection activities across the areas of operation; they cannot be responsible for the management and integration of DOMEX assets on the battlefield. I believe that we should closely examine the pilot strategy, underway in U.S. Forces Afghanistan, which created a J2E–the "E" standing for exploitation. By separating DOMEX from the HUMINT organization and assigning an intelligence officer to manage the DOMEX intelligence cycle, we are better postured to provide quality control of the entire DOMEX system. We can also look at methods to fuse science and technology (biometrics, crime scene forensics, etc.) along the DOMEX path to leverage opportunities to positively link individuals to networks. I expect lessons learned from the J2E concept will make a solid case for keeping DOMEX out of direct HUMINT management.

Personnel. Each service must determine which personnel in their force will be the primary operators of DOMEX equipment and assess what support personnel are required to maintain their programs. Support personnel are required to cover maintenance requirements and operate across the five functions of the Joint intelligence cycle. It's also important that the services track their DOMEX trained personnel with an ASI or separate MOS. Military officer and enlisted personnel management systems need to recognize and codify the new skill sets. Perhaps now is the time to develop and codify the multi-functional intelligence staff officer that has training in DOMEX tasks. These leaders will help intelligence manage three additional tasks (analyze, disseminate, and assess) that continually occur.

Thoughts on the Future of DOMEX

The true significance of DOMEX lies in the fact that terrorists, criminals, and other adversaries never expected their material to be captured. The intelligence produced from exploitation is not marked with deception, exaggeration, and misdirection that routinely appear during live questioning of suspects.[30] As our adversaries continue to move from paper to digital-based technologies, the exploitation of digital media, personal elec-

tronic devices, and video will require even more personnel and resources to maintain decision advantage. The ODNI has outlined *six DOMEX priorities* for the IC in order to create, mature, and sustain an efficient national DOMEX capability with a global reach.[31] Within the framework of these priorities, I offer some thoughts and recommendations:

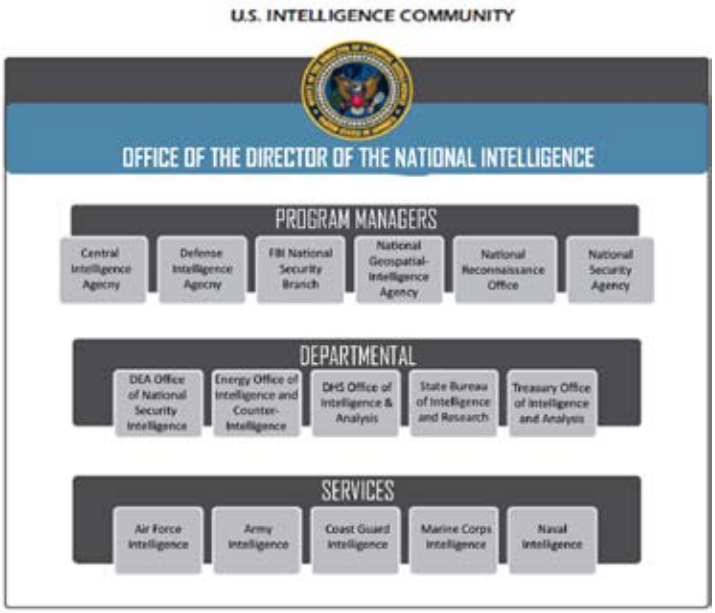
Effective Governance. *I recommend that the ODNI establish DOMEX as an intelligence discipline via an ICD.* ICD 302 states that DOMEX activities will support a wide range of intelligence activities.[32] Making DOMEX an intelligence discipline would be fully in line with the Under Secretary of Defense for Intelligence (USD-I) draft DOD DOMEX Directive.[33]

Collaborative and Integrated Planning/ Programming/Execution. If you search the Internet for the term "DOMEX," a web page from the U.S. Department of Justice's National Drug Intelligence Center (NDIC) will appear and readers can learn how the center supports National level policymakers and the IC by preparing strategic analytical studies on the trafficking of illegal drugs. NDIC provides real-time support to LE and ICs by conducting DOMEX associated with counterdrug and counterterrorism investigations. Like NDIC, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the DOD run their own DOMEX programs to support the missions and requirements of their unique organizations.

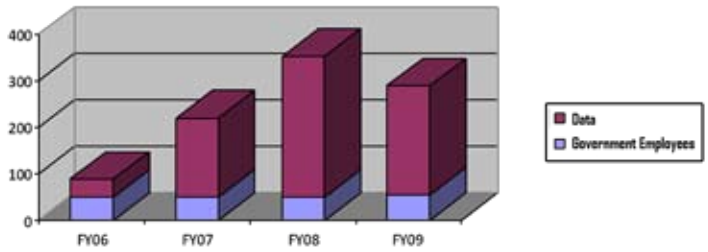
Unfortunately, these organizations have many cultural and security firewalls which limit their ability to provide access to their intelligence holdings to the IC stakeholders. We must continuously work to open these barriers through improved cooperative arrangements that provide the right information to a wider audience in order to reduce our intelligence gaps.

ICD 302 created the DOMEX Executive Committee (DOMEXCOM)[34] which includes senior members from the DIA, CIA, FBI, Defense Cyber Crime Center (DC3), U.S. Army, National Security Agency (NSA), Department of Homeland Security (DHS), and the Drug Enforcement Administration. The DOMEXCOM is great forum to hammer out agreements and roadmap strategies to enhance effectiveness of DOMEX across the IC. *I recommend that the ADDNI/OS request that each military service provide a representative to the DOMEXCOM if the U.S. Navy, U.S. Marine Corps, and U.S. Air Force desire successful DOMEX programs.*

Development of NMEC as our National DOMEX Enterprise CoE. I *recommend that the DOD/USD-I convert the NMEC into a National DOMEX Agency (NDA) to become the Program and Mission Manager for the IC*. By converting NMEC to the NDA to govern DOMEX, we would then follow the same approach used in the creation of the National Geospatial-Intelligence Agency (NGA) to produce GEOINT; NSA to produce SIGINT,[35] and CIA to be the center of gravity for HUMINT.[36] If there is no NDA, then NMEC will fail to meet its responsibilities as detailed in ICD 302 and not be in a position to "advise and assist the ODNI in identifying requirements, developing budgets, managing finances, and evaluating the IC's performance."[37]



If we don't commit ourselves to long overdue organizational changes, make DOMEX an intelligence discipline, and expand NMEC resources then the IC will not be able to achieve DOMEX goals and missions established by ODNI. One noteworthy



data point reveals that since Fiscal Year 2005, DOMEX data at NMEC has witnessed nearly a tenfold increase while government employees assigned to manage one of the most challenging intelligence missions in the IC has remained fairly flat (around 50 employees).

With the ever increasing demands for DOMEX, flowing from homeland security LE activities (FBI, DHS, etc.), we are now at a critical junction to either make a change to improve capacity to handle the volume of expected data or continue on course and risk not being in a position to thwart terrorist acts while in the early stages of planning.

The FBI's National Virtual Translation Center (NVTC) should be realigned within *the newly created NDA to gain more efficiency on the management of translation resources not only for timely and accurate translations of foreign intelligence, but for DOMEX as well.* The NVTC is currently the clearinghouse for facilitating interagency use of translators, partnering with elements of the U.S. Government, academia, and private industry to identify translator resources and engage their services. NVTC is a DNI Center, and the FBI is its Executive Agent. [38]

The USD-I should direct the establishment of a Military Support Branch in the NDA under the leadership of a one-star general. The military support branch should include liaison officers from each combatant command (COCOM) in order to improve global mission management of DOMEX activities. The support branch could help COCOMs link their DOMEX priorities into the NDA and better harness national DOMEX holdings to consumers supporting host nation counterterrorist efforts. Creation of a military support branch at NDA would follow similar constructs already in place at NSA and NGA. The lack of a military support branch assisting NDA prevents traction to fully synchronize and leverage DOMEX collection capabilities across the services and align large-scale DOMEX procurements and solutions for the services as research and development drives change.

The USD-I should direct that the U.S. Army designate the Army DOMEX Office (ADO) as DOD lead for service DOMEX program procurement. DA G2 designated NGIC as the dedicated DOMEX Program Manager responsible for the development and training of Army tactical DOMEX teams. In this capacity, the NGIC/DOMEX PM worked closely with NMEC over the past three years to field and sustain an Army tactical DOMEX presence in OIF/OEF. To better support strategic through tactical DOMEX research, development, test and evaluation appropriation initiatives, the ADO should serve as the DOD lead and action arm for the NDA. The ADO would be for DOMEX what the Army Cryptologic Office is for SIGINT, placing it in an ideal position to assist the other services reach their DOMEX equipment and standardization goals.

Deployment of a Federated DOMEX IT Infrastructure. *I recommend that the NMEC and ADO publish collection and processing standards to industry in order to select the best solutions for our DOMEX architecture.* Clearly an advanced IT infrastructure is required at the National level to help quickly organize, process, and disseminate captured information in virtually all formats in many languages. If the National DOMEX architecture is to truly be a "single, dynamic, integrated, and federated system, with cutting edge automation using the best-of-breed tools,"[39] then our collection and processing systems must tackle two distinct problems that Dr. Simon Garfinkel labels "deep" and "broad".[40]

The *deep* DOMEX problem covers the kind of document or data-storage device (a hard drive, DVD, or personal electronic device) that is captured and becomes available for analysis. The analytical goal is to find out everything possible about the data storage device. The DOMEX operators and analysts who receive a laptop, for example, want to know everything possible about it; not just the content, but the application programs, the configuration settings, the other computers with which these machines had come into contact, and so on.[41]

The *broad* DOMEX problem is the reverse. Instead of having unlimited resources to spend on a particular item, analysts are given a large number of digital objects and a limited amount of time to find something useful to their mission. In recent years the volume of captured digital information seized on the battlefield or within LE investigations has exploded. The landslide of digital media makes the broad problem quite compelling from both a national security and commercial perspective, a system that can reliably find the

"good stuff" can save money, time, and perhaps even lives.[42]

Future DOMEX collection systems (hardware and software) must provide solutions to cover the deep and broad DOMEX problems and minimize the number of stand-alone systems the operators must learn, use, and maintain. We should take advantage of equipment already fielded rather than providing more "boxes." This is not to say that there will not be some need for unique stand-alone systems to ensure needed capabilities. Each military service must ensure their DOMEX systems (hardware) fit within their Command, Control, Communications, Computers, and Intelligence construct and integrate into a cohesive and seamless entity within the national system.

Global Presence. Global presence starts by linking state and federal LE entities through Homeland Defense mechanisms and into our National ICs (CIA, DOD, and other government agencies). For example, we must be able to share and connect intelligence from a captured computer in Kuala Lumpur, Malaysia to our federal LE efforts to opportunities for our adversaries to conduct successful attacks.

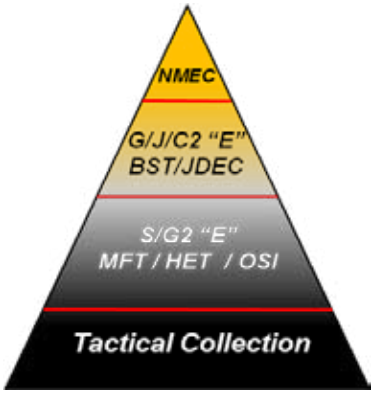
NOTE: All DOMEX operations conducted by Army intelligence personnel must comply with the legal restrictions in AR 381-10, and be conducted within the guidelines of U.S. law and applicable policies.

DOMEX practitioners who posses linguistic skills or provide access to linguists, must be strategically positioned (forward based) throughout our COCOMs to capitalize on opportunities as the present themselves. Ideally, the NDA could provide fly-away teams who are trained to operate in austere environments and have ready access worldwide to essential equipment, communications, and immediate reachback to the IC.[43]

Professional Skills and Training. Despite heavy investment in DOMEX training programs since 9/11, there has been uneven emphasis across organizational and training programs as ICs focus on their needs and culture. Inconsistency in content, quantity, and quality of training across the DOMEX community persists through varied processes for developing training requirements and standards. The result is costly duplication of effort, uneven performance during deployments, and significant unmet training requirements, particularly with regard to DOMEX analysis and technology integration.

The military services and IC must maintain a professionalized DOMEX force that follows a standardized and certifiable training program. We also lack a single set of standards or roadmap that outlines which DOMEX skills are required to meet basic, intermediate, and advanced DOMEX requirements at every level (tactical through strategic).

There are numerous training venues which are considered "accredited" to meet DOMEX mission requirements but there is no published community directive or message that aligns the total IC. Successful DOMEX operations hinge on proper collection; all military services must be organized to conduct *tactical collection* in land or maritime operations. Most importantly, the IC and DOD must be prepared to assist other nations in understanding the value of DOMEX and aid in training their forces as well. The proper inventory and collection of captured materials is no longer confined to intelligence personnel, anyone can collect. That cultural shift is based on lessons learned from combat operations. "It became clear that the existing intelligence gathering, analysis, and evidence collection methods were all inadequate for countering an insurgency, our ability to successfully prosecute intelligence operations was directly linked to the ability of our Soldiers to collect, preserve, and exploit evidence."[44] The organizational requirements above tactical collection are primarily intelligence-based and make up the processing, exploitation, and dissemination process. This is the layer that includes personnel from the Army's Multifunctional Teams, the Marine Corps HUMINT Exploitation Teams, U.S. Air Force Office



of Special Investigations, or sailors from the Office of Naval Intelligence.

One thing is certain–all military services must identify DOMEX training requirements for their forces and develop an appropriate communications infrastructure to relay DOMEX intelligence laterally and upward into the national intelligence system. *I recommend that the ADDNI/OS or USD-I designate the Navy and Marine Corps Intelligence Training Center, and USAICoE as the primary DOMEX institutional training bases for the military services*. The roles and functions of the Joint Military Intelligence Training Center and the DCITA as authorized training venues need to be clearly spelled out within an ICD or USD-I message to clarify their interaction with the IC and DOD DOMEX education system.

We must take several additional steps to strengthen each of the six ODNI priorities in order to achieve an enduring DOMEX capability across the national, military, intelligence, homeland security, and law enforcement communities, at all levels–strategic, operational, and tactical.

Conclusion

We have reached the point where a national decision is required to designate DOMEX as an intelligence discipline and to create a National DOMEX Agency. Similar conditions and decisions were made over 50 years ago as our government created agencies for HUMINT and SIGINT. If the strategic objectives are to extend intelligence to all who need it and to facilitate Homeland Defense through extensive collaboration, then if we fail to create a National DOMEX Agency, then I believe DOMEX will return to its previous condition of atrophy across the IC and DOD and our nation will not be in a position to effectively safeguard itself from multiple threats.

Endnotes

1 Response to Congressionally Directed Action, LTG Maples and Dr. Briscoe, 1 March 2009.

2 Kevin M. Woods, *Captured Records–Lessons from the Civil War through World War II*, Institute for Defense Analysis, 2009.

3. Ibid.

4. Intelligence Regulations, U.S. War Department, Washington, DC, 1920, 39-40.

5. Jared B. Schopper, "*The Collection and Processing of Combat Intelligence During Operations in Northern Europe*," Command and General Staff College Monograph, June 1964, 82.

6. Ibid., 84.

7. FM 30-15, Intelligence Interrogation, March 1969, 3-7.

8. Mark S. Partridge, "*Asking Questions: Will Army Tactical Interrogation Be Ready For War?*" School of Advanced Military Studies Monograph, 17 December, 1986, 37.

9. *Operational Leadership Experiences Project*, Combat Studies Institute, Fort Leavenworth, Kansas, Interview with CW3 Kenneth Kilbourne, February 2009, 8.

10. Donald P. Wright and Timothy R. Reese, *On Point II, Transition to the New Campaign: Operation Iraqi Freedom*, June 2008, 195. (Interview with MG Fast, CJTF-7 C2)

11. ODNI, 2009 DOMEX Annual Report.

12. NMEC Mission Statement, 2009.

13. U.S Senate, Select Committee on Intelligence. Report Number 111-16, Period Covered–4 January 2007 to 2 January 2009, 42.

14. SSCI Audit of IC Domex, April 2007.

15. Dan Butler, Paula Briscoe, Roy Apselloff, ODNI, National Document and Media Exploitation Enterprise Vision Pamphlet, Message from DOMEX Seniors, April 2009.

16. Richard P. Zahner, "*Rebalancing the Army Military Intelligence Force*," AUSA Green Book, October 2009, 186.

17. JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 31 August 2005.

18. ODNI Intelligence Community Directive 302, Document and Media Exploitation, 6 July 2007.

19. FM 2-0, Intelligence (Final Draft), March 2009, 1-30.

20. TRADOC Pam 525-7-9, Version 1.0, 12 August 2008, 40.

21. FM 2-22.3, Human Intelligence Collector Operations, September 2006, 1-6.

22. TC 2-91.8, Document and Media Exploitation Enabled Intelligence (Final Draft), 25 July 2008.

23. FM 2-22.3, 2-6.

24. U.S. Army MI BN (BFSB) MTOE, DOCNO 34105GFC18, Para 206, Lines 02-17.

25. U.S. Army Combined Arms Center, Site Exploitation Concept of Operations (CONOPS), 2010-2016.

26. Army Enlisted Job Descriptions, About.com: US Military at http://usmilitary.about.com/od/enlistedjo2/a/35.-xiW.htm.

27. DOD Cyber Crime Center at http://www.dc3.mil/dcita/dcitaAbout.php.

28.CHATS AN/PYQ-3(V)3 at http://chams.it.northropgrumman.com/brochures/CHATS%20V3%20Factsheet.pdf.

29. Intelligence Programs and Systems, at http://www.globalsecurity.org/intell/systems/index.html.

30. NMEC, 2009 Resource Management Plan, 5.

31. ODNI, National DOMEX Enterprise Vision Pamphlet.

32. ICD 302, DOMEX.

33. USD(I), DOD Directive 3300.aa, Document and Media Exploitation (DOMEX), Draft.

34. ICD 302, DOMEX.

35. Mission statement at http://www.nsa.gov/about/mission/index.shtml.

36. Establishment of the National Clandestine Service, CIA, 13 October 2005 at https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr10132005.html.

37. Deputy Director of National Intelligence for Policy, Plans, and Requirements, *2009 National Intelligence: A Consumer's Guide*.

38. Ibid

39. ODNI, National Document and Media Exploitation Enterprise Vision Pamphlet,

40. Simson L. Garfinkle, *"Document and Media Exploitation,"* Association for Computer Machinery, accessed at http://queue.acm.org/detail.cfm?id=1331294.

41. Ibid.

42. Ibid.

43. ODNI, National Document and Media Exploitation Enterprise Vision Pamphlet.

44. Ralph O. Baker, "Developing Actionable Intelligence in the Urban COIN Environment," *Military Review*, March-April 2007.

Colonel Joseph Cox served as Commander, 519th MI Battalion (BfSB) during OIF 07-09 between September 2007 and December 2008. He is a 1987 graduate of OCS and has also served in the 525th MI Brigade; 82d Airborne Division; 75th Ranger Regiment; 205th MI Brigade, and the 525th BfSB. He recently completed a U.S. Army Senior Service College Fellowship Program in Washington, D.C. and is now the Commander, 501st MI Brigade, Korea. Colonel Cox may be reached at joseph.cox@us.army.mil.