Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Achieving Actionable Intelligence: Legacy Information Technology Systems and the Improvised Explosive Device Global Threat

CAPSTONE REPORT

Paul R. Plemmons Jr.
Deputy Program Manager
Pacific Architects and Engineers (PAE)

University of Oregon
Applied Information
Management
Program

May 2016

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Achieving Actionable Intelligence: Legacy Information Technology Systems and the Improvised Explosive Device Global Threat

Paul R. Plemmons Jr.

Pacific Architects and Engineers (PAE)

Abstract

The expanding use of the improvised explosive device (IED) around the globe requires Department of Defense (DoD) government and military organizational leaders and associated support staff to focus on achieving actionable intelligence aimed at successfully countering this enduring and evolving threat. This annotated bibliography focuses on literature published between 2012 and 2016 and discusses the use of decentralized legacy information technologies by the DoD and the impact on gathering, analyzing and sharing of critical IED exploitation data.

Keywords: actionable intelligence, improvised explosive device (IED), counter-improvised explosive device (C-IED) operations, legacy information systems, Department of Defense (DoD), exploitation, intelligence data

Table of Contents

Introduction to the Annotated Bibliography

Problem

In today's global counter-terrorism fight, the need to quickly and securely access, share and analyze intelligence data from anywhere in the world is a critical requirement, and achieved through "bilateral and multilateral exchanges of information and other forms of collaboration" (Deni, 2015, p.47). The use of decentralized legacy information technology systems to complete information exchanges effects critical global Counter-Improvised Explosive Device (C-IED) exploitation operations for many Department of Defense (DoD) organizations, requiring the identification of mission enhancing alternative solutions.

Effectively exploiting information and materials from terrorist attacks and related events requires enhanced reporting and dissemination of large amounts of associated incident data (Obama, 2013). With the increase in data volume and the ever-expanding need to share critical intelligence data around the globe, the DoD enterprise infrastructure is evolving to provide more technologically enhanced communications and data services to the warfighter. This evolution for the DoD presents many counter-terrorism organizations with challenges associated with implementing these enhanced services to forward deployed, tactical DoD and government defense contractor teams who may be utilizing decentralized legacy equipment and who do not always have connectivity back to a United States based network (Witherspoon, Quock, Lundberg, Elkins & Christou, 2014). Many existing DoD legacy information technology systems are slow, duplicative, and lack interoperability greatly effecting operations (Barno, Bensahel, Stokes, Smith & Kidder, 2013). For those counter-terrorism organizations and operational teams specifically focused on the fight against the Improvised Explosive Device (IED), secure access to data is limited by the lack of efficient and interoperable systems, effectively creating a "critical

mission gap" (Carter, 2015, p.1) and an operational environment lacking collaboration amongst the many agencies and organizations working to combat these deadly devices. Critical information sharing connections remain elusive based on many DoD organizations relying on separate databases, and differing methods for securing and facilitating data movement (Rubin, Lynch, Escaravage & Lerner, 2014). The differences that exist between organizations also create the need for manual intervention in order to successfully execute exploitation data transmission for many C-IED organizations. Legacy systems drive the scale of these manual efforts by the use of unsupported software operating systems and the lack of consistency in network technology implementation (Gosler & Von Thaer, 2013).

Access to actionable intelligence. The escalation of IED incidents and related casualties during Operations Iraqi Freedom and Enduring Freedom required the DoD to develop and implement enhanced technical and forensic IED exploitation techniques to link persons, places, things and events (Smith & Tranchemontagne, 2014). The large amounts of collected data associated with IED events helps with fusing technical, forensic, and biometric disciplines to produce "actionable intelligence" for countering the many terrorist organizations that rely on IED's as a primary weapon in their arsenals (Smith & Tranchemontagne, 2014).

Given the enduring nature of the global IED problem, careful consideration is required to ensure that all intelligence-gathering organizations have the necessary C-IED capabilities and capacity to meet future threats (Smith & Tranchemontagne, 2014). One goal for those organizations focused on the C-IED effort is to securely gather, analyze, exploit, and share large amounts of IED incident and device data in a short timeframe. Sharing data and conducting analyses across the government's "legacy stove-pipes of available information" is a challenge for many DoD organizations increasing overall analysis timelines for C-IED focused organizations

(Rubin et al., 2014, p.3). When presented with the opportunity to complete a rapid and thorough analysis of all gathered datasets, operational commanders gain the ability to interrupt an enemy's decision cycle and interdict IED tactical employment in real time across the globe (Smith & Tranchemontagne, 2014). Further disruption of the enemy's IED operations are made possible by achieving actionable intelligence, mitigating the costs of technical surprise in terms of personnel, equipment, and dollars by placing better and more relevant information in the hands of warfighters (Smith & Tranchemontagne, 2014).

Actionable intelligence is "intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process" (Department of Defense [DoD], 2016 p. JP 1-02, 1). The need to securely transfer large amounts of intelligence datasets is a critical component of the C-IED fight, and many of the current legacy DoD IT systems lack the computing capabilities needed to provide real-time information (Barno et al., 2013). The historical DoD legacy system construct includes large amounts of highly fragmented and perishable data, and maintained in formats making information difficult to discover, correlate and analyze (Voelz, 2015). The use of historical legacy systems by the DoD in addition to conducting operations in de-centralized austere environments, forces many C-IED organizations to identify new and innovative methods for integrating C-IED information and synchronizing C-IED activities (Bennett, 2013). These critical C-IED synchronization efforts include a strong focus on establishing a formal process for passing critical IED information and individual device advancements to and from interagency partners (Stevens, 2012). Even with operational and technological mission-impacting constraints present, many government organizations continue to rely upon legacy systems based on the need to preserve their core missions and operational functions (Alexandrova, Rapanotti, & Horrocks, 2015).

Purpose

The purpose of this study is to explore the effects decentralized legacy information technology systems have on today's critical global DoD C-IED exploitation operations in order to identify possible mission enhancing alternative solutions. Legacy systems introduce many "cross-domain friction points" as noted within the 2013 Annual Report on Army Business Transformation (Department of the Army, 2013, p. 6), and make it difficult for leaders, operators, and support personnel to achieve increased levels of actionable intelligence in support of the current C-IED mission. The current levels of available actionable intelligence require development and implementation of new and innovative tactics, techniques and procedures in order to successfully combat the global IED threat.

Audience

The intended audience/stakeholders for this study include government and civilian military specialists and leadership responsible for the planning and execution of global DoD C-IED operations. The primary stakeholders for the study include Intelligence Analysts, Information Technology (IT) Technicians and Engineers, Forensic Scientists, Project Managers, Program Managers, Explosive Ordnance Disposal (EOD) technicians, Combatant Commanders, Division Heads, and Company Executives who work to support the global fight against IED's and tasked with focusing current "intelligence and information collection systems" (Flynn & Flynn, 2012, p.4). This large group of individuals and organizations would benefit from understanding the mission impacting interoperability conditions that exist between new and legacy information technology systems, and the need to identify more effective and efficient mission enhancing alternatives to obtaining actionable intelligence (Agarwal et al., 2015).

Research Questions

The purpose of this annotated bibliography is to identify literature that examines the use of decentralized legacy information technology systems utilized by DoD organizations supporting the global fight against IED's in order to identify possible mission enhancing alternative solutions. Focus is on the C-IED exploitation data gathering, analysis and sharing operations, and the need to increase actionable intelligence between C-IED organizations. The following research questions frame the annotated bibliography:

Main question. As the escalation of improvised explosive device (IED) incidents and related casualties occur as noted by Smith and Tranchemontagne (2014), do the decentralized legacy systems used to gather, analyze and share IED exploitation data limit the availability of actionable intelligence?

Sub-questions.

- Can the currently utilized legacy exploitation data gathering and sharing systems be considered resilient DoD systems with the ability to meet changing requirements, conform to new environments, and successfully meet the challenges of an adaptive foe (Goerger, Madni, & Eslinger, 2014)?
- Do standalone decentralized legacy exploitation data gathering and sharing systems limit the ability to conduct relevant and timely collection, analysis, and technical and forensic exploitation of current and emerging IED technologies (Joint IED Defeat Organization [JIEDDO], 2012, p.7)?

Search Report

Search strategy. The search strategy identifies relevant and recent published resources regarding the DoD's intelligence gathering, analysis, and sharing operations in support of the C-IED fight and the use of legacy information technology and associated combat systems. The search focuses on links to organizations operating within the DoD who support the fight against IED's, and the methods and processes for gathering and sharing IED exploitation information and creating actionable intelligence. Subsequent searches focus on the tragic events of 9/11, counter-terrorism organizational collaboration, data-analysis, and technologically advanced combat systems providing increased data availability and relevancy related to the fight against the IED.

Key terms. Gathered search terms originate from scholarly articles, books, published white papers, and civilian and government websites focused on the subjects of C-IED data gathering and exploitation, legacy information technology systems, and technologically advanced combat systems utilized to conduct C-IED operations. Relevant key search terms include:

- DoD actionable intelligence;
- 9/11 terrorist attacks;
- intelligence data;
- DoD system interoperability;
- DoD legacy IT systems;
- C-IED exploitation data;
- C-IED combat systems;

- intelligence data availability and relevancy;
- DoD data storage;
- DoD data analysis; and
- IED exploitation.

Search engines and databases. Searches included extensive use of the online UO Libraries via a virtual private network (VPN) connection. Use of the VPN connection provides full access to many relevant and scholarly research documents aligned with the study. All searches conducted in the UO Libraries databases focused on "articles, books, and more" within the "UO + Summit + Articles, etc." selected search criteria. This provides a unique set of database information and identifies potential relevant literature references based on expanded search criteria and the effects legacy information technology systems place on DoD C-IED organizations. Search engines used included Google and Google Scholar in addition to the UO Libraries online search tools. All databases and search engines used for the study include the following:

- IEEE Computer Society Digital Library (IEEE);
- Institute of Electrical and Electronics Engineers (IEEE) Xplore Digital Library;
- ProQuest;
- Science Direct;
- Google; and
- Google Scholar.

In addition to those listed above, one additional database and government defense-focused online search engine utilized is the Defense Technical Information Center (DTIC). This

is a government site that allows a user to search more than one million final reports on defense funded research, development, test and evaluation activities.

- Defense Technical Information Center (DTIC)

Documentation approach. Document and capture of all references takes place using two distinct methods. The first (and primary) method includes the use of Microsoft Word. Capture of all relevant searches occur within a Microsoft Word document and include citation information, abstract, associated online location data, and assigned color category. For resources found to have some relevance to the problem, but not included within the Annotated Bibliography section, each of these resources receives a yellow category assignment. The green category assigned to all formally cited references found within the study provides a clear delineation between the two utilized categories. This information allows quick key word and assigned color category searches of all gathered references, and hyperlinked direct access to many relevant documents. This method also provides a back-up of all identified resources in the event of file corruption or deletion. Saving of these files on an encrypted USB drive and within two separate folders on a local hard drive provide additional data redundancy.

The second (and alternate) method for reference documentation and capture is the use of the Zotero online citation organization tool. This method focuses on key terms and allows for an online accessible secondary source for gathered reference data. This method is an additional backup in the event of the main reference Word Document data corruption or file loss.

Reference evaluation criteria. The selection of all references in the Annotated Bibliography section of this paper are evaluated in accordance with the University of Florida Center for Public Issues in Education Evaluation Information Sources fact sheet (Center for

Public Issues, 2014). The criteria used to evaluate all included references focuses on identifying characteristics to check for authority, timeliness, quality, relevancy, and bias (Center for Public Issues, 2014).

Authority. A strong focus is placed on looking at the author's credentials, professional experience and overall credibility within the realm of the DoD information technology and C-IED operations. In addition to verifying the author's credentials, peer-reviewed sources are given preference.

Timeliness. For a reference deemed to be relevant and appropriate to the problem, the date of publication is considered. This study is limited to works published between 2012 and 2016 based on C-IED operations and associated technologies rapidly advancing to counter new and emerging global threats**.**

Quality. For all relevant references identified a check for accurate grammar, spelling and punctuation is required (Center for Public Issues, 2014). A strong focus on government and military references assisted with confirming the overall quality of all references.

Relevancy. References considered relevant to the study address the research questions and align with the most current information and data regarding C-IED operations and the associated legacy information technology systems utilized in the field today.

Bias. All identified resources are reviewed to determine if the author has a particular bias or if their goal is to sell a service or persuade a reader to their viewpoint (Center for Public Issues, 2014). Also, a check is completed to ensure the author's arguments and conclusions are supported by credible and cited sources (Center for Public Issues, 2014).

Annotated Bibliography

The following Annotated Bibliography presents 15 selected references that examine the DoD's global C-IED fight and the use of legacy systems in support of IED exploitation operations required to achieve actionable intelligence. References selected help C-IED focused organizations, operators, and leaders address the current availability of actionable intelligence gained through successful IED exploitation. References presented in three categories describe three operational focal points aligned with legacy systems and the global fight against the IED: (a) evolving threats posed by the use of IED's, (b) challenges posed by legacy systems in countering IED threats, and (c) information sharing and countering IED threats.

Each annotation consists of three elements: (a) the full bibliographic citation, (b) author provided abstract, and (c) summary describing the relevance to this study. The abstracts included are either complete as published, or modified for length and/or content in order to align with the C-IED fight and legacy system problem area focus. The summaries for each reference highlight the global IED threat and the operational actions taken by the C-IED community to gather and share IED exploitation data.

Category 1: Evolving Threats Posed by the Use of IED's

Bennett, B. A. (2013). *Counter-improvised explosive device fusion cells and the brigade combat team: A modern day imperative* [Monograph]. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA606046

Abstract. The IED has been responsible for more deaths and injuries than any other weapons system in both Iraq and Afghanistan. Despite a $58 billion dollar investment in C-IED capability, the DoD has been unable to prevent this weapon from achieving

devastating effects on military and civilian targets and threatening national objectives. Within the Army, continued organizational refinements to fighting formations combined with formalization of specific capabilities will better prepare units for operations in high intensity IED environments. Specifically, the creation of an organic Brigade Combat Team C-IED fusion cell, sufficiently manned and singularly responsible for the integration and synchronization of all C-IED initiatives, will significantly improve targeting activities within the Brigade Combat Team and enable a more offensive posture when confronted with active IED threats.

Summary. This paper examines the evolving IED threat and the creation and implementation of the C-IED fusion cell as a possible solution to increasing actionable intelligence. It takes a high level look into C-IED operations and the need for combat leaders to have better information capabilities. The use of legacy information gathering, storage, and sharing systems impact this information flow. The author focuses on the IED as a weapons system and its use against United States forces in Iraq and Afghanistan to cause death and injuries. The paper clearly highlights the evolving IED environment is too complex and too lethal, requiring a sufficiently manned and dedicated staff element assigned the primary responsibility for integrating C-IED information and synchronizing C-IED activities. The author discusses how integrating C-IED information and synchronizing associated activities is key to mitigating the effects of the IED, and the implementation of a C-IED fusion cell providing an alternative solution to the use of legacy information systems and processes. The author describes how the C-IED fusion cell and use of new data gathering and sharing technologies provide a more thorough IED analysis and increased information dissemination among C-IED organizations. The paper

provides trends relating to continued global proliferation of IED technology and the affinity terrorists and insurgents have with the IED, and the reality combat leaders must be prepared to fight the IED in future conflicts for many years to come.

Joint IED Defeat Organization [JIEDDO] (2012). *Counter-improvised explosive device strategic plan: JIEDDO 2012-2016*. Retrieved from https://www.jieddo.mil/content/docs/20120106_JIEDDOC-IEDStrategicPlan_MEDprint.pdf

Abstract. This document discusses how JIEDDO uses a synchronized and integrated approach to coordinate the DoD's C-IED efforts and rapidly provide capabilities to counter the IED threat in support of operational commanders. Critical to these efforts are forces trained in the latest C-IED techniques and provided with tailored and fused intelligence support. As authorized, JIEDDO provides support to other federal agencies as they analyze, pursue, disrupt, protect, and respond to the terrorist use of explosives in the United States. JIEDDO will also aggressively seek to maintain the research and development advantages needed to neutralize the IED threat**.**

Summary. The document focuses on the IED and C-IED strategy the United States and its allies implement across the globe. The author focuses on the need to utilize a synchronized and integrated approach to coordinate the DoD's C-IED efforts providing relevance to the study and highlighting the need for increased actionable intelligence in the fight against IED's. A key component of achieving actionable intelligence is through the use of the DoD's information technology systems and associated databases currently deployed around the globe. This key information directly addresses the main study question regarding the impact decentralized legacy systems have on the gathering,

analysis and sharing of IED exploitation data, and the availability of actionable intelligence. The strategy also notes critical C-IED capabilities and solutions, and looks closely at the strategic environment and enduring threat posed by the evolving IED tactics, techniques, and procedures used by the enemy. The author notes the leveraging of current C-IED research and development (R&D) ensures innovation, addressing future challenges and providing a venue to discover and develop C-IED centric technology to aid with countering threats and creating actionable intelligence. The strategy provides a comprehensive response to the complex and dynamic threat of evolving IED's and involves the fusion of exploitation information, analysis, and partner support. All of which are critical components required to achieve actionable intelligence.

Obama, B. (2013). *Countering improvised explosive devices*. Washington, DC: Executive Office of the President. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA574504

Abstract. This policy statement discusses how the government has no greater responsibility than providing for the safety and security for the United States citizens, allies, and partners, while providing an economic environment that promotes opportunity and prosperity. The use of IED's threatens these interests by killing, injuring, and intimidating citizens and political leaders around the world, inflicting damage on United States forces on the battlefield, and disrupting transportation and the flow of commerce. The terrorists and criminals responsible for these attacks are resilient, technologically adept, and adaptable. They employ the most recent and successful tactics, techniques, and procedures gained from experience in Iraq, Afghanistan, and around the world. The use

of IEDs worldwide has increased in recent years, with the number of attacks exceeding 4,000 in 2011.

Summary. The 2013 policy statement issued by United States President Barrack Obama discusses how IEDs remain one of the most accessible weapons available to terrorists and criminals to damage critical infrastructure and inflict casualties and closely aligns with the main and sub-questions of the study. The policy focuses on leveraging, integrating, and aligning the United States Government C-IED efforts and enhancing information sharing resources across the United States Government. A major focal point is the need to effectively exploit information and materials from IED attacks conducted around the globe providing relevance to the study. Coordinating IED collection and exploitation efforts assists with gathering, sharing, and analyzing critical forensic, technical, and biometric information associated with incidents. The policy statement further identifies the critical need to maintain scalable and layered C-IED capabilities, including personnel and equipment. This includes enhancing legacy information technologies employed in support of the current C-IED fight and ensuring C-IED focused organizations have access to advanced analytic tools to better link IED related information across all collection sources. The desired end state for all C-IED operations is to gain actionable intelligence in order to counter the use of the IED across the globe.

Smith, T. B., & Tranchemontagne, M. (2014). Understanding the enemy: The enduring value of technical and forensic exploitation. *Joint Force Quarterly 75, 4*, 122-128. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA622235

Abstract. This article discusses how the escalation of IED incidents and related casualties during Operations Iraqi Freedom and Enduring Freedom led to a new

intelligence field related to technical intelligence (TECHINT) called weapons technical intelligence (WTI), which combined technical and forensic IED exploitation techniques to link persons, places, things, and events. WTI operationalizes technical and forensic activities by fusing the technical, forensic, and biometric disciplines to produce actionable intelligence for countering threat networks. It is an especially powerful tool against terrorist organizations that rely on IEDs as a primary weapon in their arsenals.

Summary. This article closely aligns with the study and specifically with the value IED technical and forensic exploitation data provides C-IED organizations. With the IED threat evolving, a need to identify more advanced techniques and procedures to counter this weapon becomes a reality, and the need to enhance the information sharing platforms and technologies is a requirement for all C-IED focused organizations. To successfully conduct IED exploitation, the authors note that improved planning and interagency cooperation is required. The interagency sharing of information requires the use of both legacy and enhanced information systems, and fusing of critical technical, forensic, and biometric information into actionable intelligence permits more precise shaping of the operational environment for combatant commanders resulting in the identification and capture of high value individuals.

Category 2: Challenges Posed By Legacy Systems in Countering IED Threats

Agarwal, S., Pape, L. E., Dagli, C. H., Ergin, N. K., Enke, D., Gosavi, A., & Gottapu, R. D. (2015). Flexible and intelligent learning architectures for SoS (FILA-SoS): Architectural evolution in systems-of-systems. *Procedia Computer Science, 44*, 76-85. doi:10.1016/j.procs.2015.03.005

Abstract. This article discusses how the dynamic planning for a system-of-systems (SoS) is a challenging endeavor. DoD programs constantly face challenges to incorporate new systems and upgrade existing systems over a period of time under threats, constrained budget, and uncertainty. It is therefore necessary for the DoD to be able to look at the future scenarios and critically assess the impact of technology and stakeholder changes. The DoD currently is looking for options that signify affordable acquisition selections and lessen the cycle time for early acquisition and new technology addition.

Summary. This article discusses the interoperability conditions that exist between new and legacy DoD systems and possible solutions to overcome current performance issues related to the study. The author focuses on the DoD architecture evolution in context of SoS approach. The authors look to provide evidence the SoS approach and methodology takes into account the availability of legacy DoD systems and the many new systems required to adapt to rapidly changing mission specifics. The authors describe the SoS approach and methodology of consisting of many autonomous systems and their inter-connections, leading to a greater capability that fulfills the demand of a specific task. To accomplish this, the authors utilize current examples of legacy systems in use and supporting the intelligence, surveillance, and reconnaissance (ISR) combat mission. ISR is a critical component of the C-IED fight and requires a great deal of data exchange between organizations. The need for enhanced data transfer functionality and capabilities is a key component of the evolution into a SoS approach.

Alexandrova, A., Rapanotti, L., & Horrocks, I. (2015, May). The legacy problem in government agencies: An exploratory study. *Proceedings of the 16th Annual International*

Conference on Digital Government Research, UK, 150-159. Retrieved from http://oro.open.ac.uk/42604/1/dgo_2015_submission_11.pdf

Abstract. This study focuses on how government organizations continue to be heavily reliant on legacy systems to support their mission-critical functions. When practitioners embark on legacy systems replacement projects, they tend to use the legacy software's features as business requirements for its replacement application. This unnecessarily reproduces the business processes that have often emerged from the very technical limitations of the legacy system being phased out -- a phenomenon referred to as the "legacy problem." Overcoming the legacy problem is difficult because of the complex interrelationships of information technology, organizational culture, and government agencies' normative environments. As a result, legacy feature carryover occurs frequently within government organizations, because practitioners want to minimize business process changes during new system implementation. The study findings single out the procurement of commercial off the shelf (COTS) software as the most common approach to the replacement of legacy systems. The study findings assist government agencies with devising solutions for dealing with the legacy problem.

Summary. This study discusses how legacy systems are a known challenge for the operations of modern organizations, as they limit the capacity for change and overall growth. The authors highlight substantial investments the United States Government made in legacy systems since 2010, and the operational impacts these systems have on many operational levels and individual mission sets. A key link to the challenges legacy systems pose for countering IED threats is the discussion by the authors of how government agencies teeter between innovation and continuing to support the legacy

systems implemented and actively in use. The authors also discuss how government organizations define individualized operational requirements. This process may include the replacement of legacy systems in order to successfully complete evolving missions. Many government organizations (to include those focused on the C-IED fight) must conduct a balancing act between preserving the core mission functionalities supported by each legacy system and introducing newly enhanced features capable of increasing organizational efficiency and effectiveness. The article additionally highlights that the legacy problem involves dynamic interplay of technology, individuals and rigid organizational structures making a transition to new enhanced technological solutions very difficult.

Barno, D., Bensahel, N., Stokes, J., Smith, J., & Kidder, K. (2013). *The seven deadly sins of defense spending.* Retrieved from Center for a New American Security website: http://www.cnas.org/files/documents/publications/CNAS_SevenDeadlySIns.pdf

Abstract. The authors of this article discuss how the DoD faces a stark choice. With reductions in defense spending looming, decisions made during the next year will chart one of two paths: one that avoids tough choices about cutting excess and inefficiencies, or one that embraces painful but necessary reforms to the structural underpinnings of the department. The first path will inevitably follow the precedent of past defense budget drawdowns and lead to deep cuts in force structure, readiness and modernization, and produce a much-diminished United States military. The other, more difficult, path preserves these capabilities by fundamentally reforming the underlying causes of DoD cost growth. With the right choices for reform, the United States defense establishment

can consume fewer resources and still meet America's global strategy requirements for many decades to come – but bold and resolute action is required now.

Summary. This report looks closely at the DoD's defense spending and the ability to perform its core missions going forward into the future, with one of the most critical missions consisting of the C-IED fight. The authors focus on several key areas aligned with identification of redundant DoD organizations and the use of legacy systems related to C-IED operations and the impact this causes. The authors note that as the IED became the signature weapon for enemy forces around the world, the DoD rapidly increased funding to ensure greater safety for combat forces. Increased funding provides a new focus on intelligence gathering tools and processes aimed at identifying and prosecuting those responsible for the emplacement and use of IED's. With the rapid funding push, the authors highlight many military services and agencies began overlapping IED related intelligence analysis, C-IED hardware development and IED detection and technologies. In addition to the C-IED overlap the authors note the need for implementation of more efficient and interoperable DoD systems. The heavy use of legacy systems and technologies in support of current C-IED operations drives this urgent need.

Department of the Army. (2013). *Annual report on business transformation: Providing readiness at best value* (1 March 2013 Report). Retrieved from http://www.defenseinnovationmarketplace.mil/resources/2013ArmyAnnualReportlBusinessTransformation.pdf

Abstract. This report discusses how the emerging environment presents a complex range of threats, challenges and opportunities, making it likely that United States forces will be called on to fulfill a broad range of military operations. The Army will prevent conflict

by remaining a credible force with sufficient capacity to dissuade adversaries from challenging American interests. The Army will shape the environment, building positive relationships and capabilities that enable nations to effectively protect and govern their citizenry. Finally, when called, the Army will fight for the Nation and win decisively and dominantly. At the same time, fiscal constraints require us to deliver strategic land power in the most cost-effective way possible.

Summary. This report addresses the challenges posed by numerous evolving global threats, and specifically how these affect the United States Army. As one of the largest DoD military components participating in the C-IED fight, the report discusses the approach for enhancing current and legacy combat systems and the associated network capabilities utilized globally. The authors focus on the expeditionary aspect of the Army and its need to create a single, secure and standards-based digital environment within which information technology programs operate. The study highlights several reforms identified to assist the Army with implementing a network modernization strategy, and possible solutions for addressing the overall study problem. The need to improve regulations for developing and enforcing architecture rules aimed at reducing waste and risk to the Army's information technology (IT) systems. The report also provides critical relevant information regarding the development of a common operating environment including enhanced user identification, management uniformity, situational awareness and increased system interoperability.

Goerger S. R., Madni, A. M., & Eslinger, O. J. (2014). Engineered resilient systems: A DoD perspective. *Procedia Computer Science.28*, 865-872.doi: 10.1016/j.procs.2014.03.103

Abstract. This article discusses how DoD systems are required to be trusted and effective in a wide range of operational contexts with the ability to respond to new or changing conditions through modified tactics, appropriate reconfiguration, or replacement. As importantly, these systems are required to exhibit predictable and graceful degradation outside their designed performance envelope. For these systems to be included in the force structure, they need to be manufacturable, readily deployable, sustainable, easily modifiable, and cost-effective. Collectively, these requirements inform the definition of resilient DoD systems. This paper explores the properties and tradeoffs for engineered resilient systems in the military context. It reviews various perspectives on resilience, overlays DoD requirements on these perspectives, and presents DoD challenges in realizing and rapidly fielding resilient systems. This paper also presents promising research themes pursued by the research community to help the DoD realize the vision of affordable, adaptable, and effective systems. This paper concludes with a discussion of specific DoD systems that can potentially benefit from resilience and stresses the need for sustaining a community of interest in this important area.

Summary. This article focuses heavily on the mission of the DoD to equip and deploy military forces as required to deter war and assure national security. This focus aligns closely with the study's main question regarding the use of legacy information systems, and the availability of actionable intelligence achieved through the use of the DoD's complex cyber infrastructure systems, logistical data and deployed information systems operating around the globe. The authors look closely at the DoD's legacy military systems and the topic of resiliency for these systems. In addition to resiliency the authors highlight the rapid changes in DoD missions and mission requirements, as well as the

emergence of new asymmetric threats in today's operational environment. A large and growing asymmetric threat is the use of the IED by terrorists and enemy combatants conducting operations throughout many areas of the world, requiring a unique operational systems footprint to combat the threat. Possible enhancements to current DoD systems noted by the authors include development of more affordably adaptable and effective systems identified through the close examination of current DoD mission volatility.

Patacsil, J. A. (2013). *Sustaining eleven years of counter-improvised explosive device relevancy for tomorrow's war* (Master's thesis, Marine Corps Command and Staff College). Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA601583

Abstract. Since the start of Operation Iraqi Freedom and continuing through Operation Enduring Freedom and Operation New Dawn, a weapon that is simplistic, inexpensive has plagued United States forces, and effective known as the lED. C-IED has thus been a major focus ever since. This focus has evolved so much that in 2006 the Joint lED Defeat Organization (JIEDDO) was established to address the lED issue, which has been the greatest cause of U.S. casualties since the start of the Global War on Terror. Those same critics believe that the time has come for the Marine Corps to focus on its foundation of expeditionary warfare. And their desires may come to fruition as United States forces have already withdrawn from Iraq, will soon be withdrawing from Afghanistan, and will shift its focus to the Pacific Theater. Despite this however, through creative alternatives and adjusting budget priorities the DoD can effectively sustain and improve its C-IED capabilities which will undoubtedly be necessary for future global conflicts.

Summary. This paper focuses heavily on the requirement for the DoD to improve IED threat-intelligence gathering operations, the acquisition of enhanced C-IED technologies and systems, and increased C-IED training for United States service members operating on today's battlefield. The author describes intelligence information fusion, collaboration, and analytical support to combatant commands are key pillars in the fight against the IED threat. A critical link to the study and main question is the discussion of the current strain placed upon intelligence resources supporting both C-IED and non C-IED missions on the battlefield, and the associated unique organizational systems and processes in use by each. The author highlights the lack of a DoD or individual military service standardization requirement for the many C-IED technologies and methodologies currently employed. These C-IED technologies and methodologies include the use of many legacy information systems and associated infrastructures with the DoD footprint.

Stevens, G. D. (2012). *Whole of government approach to countering domestic IED's: Leveraging military capabilities.* (Civilian Research Report 29-05-2012). Retrieved from the Defense Technical Information Center website: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA593378

Abstract. Law enforcement authorities, together with the intelligence community, have been successful in thwarting many recently attempted IED attacks targeting the United States. However, the potential for a sustained IED campaign against our nation remains. Considering that the means available to respond to domestic IEDs have grown considerably with Homeland Security grants, the issuance of Homeland Security Presidential Directive-19, and the recent expansion of military counter-IED capabilities,

we have a responsibility to optimize these resources to provide our nation with the best possible response. Moreover, current fiscal constraints demand a more efficient use of our ample resources in this critical area of vulnerability. Shortfalls in current law, military doctrine, organizational structure, training, and information sharing protocols are preventing an optimized and united, or whole of government approach to addressing this threat as called for in HSPD-19 and the National Security Strategy. This paper explores these shortfalls and recommends several solutions. Chief among them is establishment of a DoD C-IED Joint Task Force (JTF) headquarters to facilitate improved response, training, and sharing of information from military EOD forces in support of civil law enforcement authorities.

Summary. This paper discusses the shortfalls in current law, policy and practice related to C-IED support, coordination and information exchange within the DoD. The author calls for the establishment of a DoD C-IED Joint Task Force (JTF) focusing on facilitating improved IED response, training and sharing of associated information. This information aligns closely with the study and assists with gaining a better perspective of several legacy DoD IED information gathering and sharing systems that enable C-IED focused organizations to obtain critical device trends and observed enemy tactics utilized when employing these deadly devices. The author also includes relevant information regarding the possible use and the countering of IED's within the United States. This provides a great deal of information regarding the opportunities for increased data sharing amongst all C-IED organizations within the DoD and externally. The need to gain actionable intelligence requires the most current information systems, databases, and processes, in addition to use of lessons learned from the large volume of IED

exploitations conducted during the wars in Iraq and Afghanistan. The author notes the lack of any centralized effort to consolidate and share domestic IED incident reports amongst EOD units and other C-IED organizations external to the DoD.

Category 3: Information Sharing and Countering IED Threats

Carter, J. G. (2015). Inter-organizational relationships and law enforcement information sharing post 11 September 2001. *Journal of Crime and Justice, 38*(4), 522-542. Retrieved from https://scholarworks.iupui.edu/bitstream/handle/1805/4544/carter-2014-inter-organizational.pdf?sequence=1&isAllowed=n

Abstract. This article discusses the lack of information sharing among law enforcement agencies leading up to the September 11, 2001 terrorist attacks. Contemporary counter-terrorism efforts place an emphasis on interaction among law enforcement agencies with other government and private sector organizations. The present research utilizes two federally-funded national surveys to explore the collaborative relationships between law enforcement, other government organizations, and private sector organizations. Findings suggest collaboration across sectors exists, however it appears significant room for improvement remains.

Summary. This article focuses on intelligence information sharing between organizations as a tactical means to prevent and mitigate threats of terrorism and crime as key in the C-IED fight. The author focuses on the events following the September 11, 2001 attacks, and the findings of the 9/11 Commission Report. This report highlighted information sharing failures existed across all levels of law enforcement and counter-terrorism focused organizations, similar to those observed throughout all organizations conducting counter terrorism operations. The need for increased situational awareness

sparks the development of fusion centers and departure from legacy systems to facilitate the sharing of information and intelligence across organizational boundaries. As utilized within the C-IED fight the fusion center (or cell) actively assists with collecting, analyzing, and disseminating critical information and intelligence. The fusion center concept requires the use of many unique information technology systems to execute critical data gathering and dissemination. The collection and analysis of information results in actionable intelligence.

Deni, J. R. (2015). Beyond information sharing: NATO and the foreign fighter threat. *Parameters, 45*(2), 47-60. Retrieved from http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Summer_2015/8_Deni.pdf

Abstract. This article discusses that despite disagreement among experts and policymakers over its significance, the foreign fighter threat to Europe is very real. Intergovernmental organizations (IGOs), such as NATO, have an important role to play in countering this threat, including through information sharing. Even though the North Atlantic alliance has its hands full at the moment, member states can further leverage NATO's unique advantages.

Summary. This article focuses on the critical need to share intelligence information between counter terrorism organizations operating around the globe in order to reduce the possibility of future high profile attacks. The author focuses on the specific issue of foreign fighters and the threat each poses. Bilateral and multilateral exchanges of information and other forms of collaboration highlight the critical need to gather and share intelligence data as a means of countering the terrorist threat. The United States

plays a critical role in this information exchange, along with assisting nations with standardizing and institutionalizing common practices for sharing information and countering terrorist attacks and the use of IED's. Key elements of the article include the launching of a five-year security strategy for the European Union (EU), and strong focus on information technology enhancements to encourage increased organizational collaboration.

Flynn, M. T., & Flynn, C. A. (2012). Integrating intelligence and information: Ten points for the commander. *Military Review*, *92*(1), 4-8. Retrieved from http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20120229_art005.pdf

Abstract. This article discusses after ten years of war, there are a number of truisms developed from hard-fought battlefield experience. One that has gained prominence is the concept of intelligence and information integration. Integrating intelligence and information means different things to different people, but one thing is certain: without integration, the entire decision-making process is compromised, rife with gaps that can lead to miscalculations. The article is a compilation of thoughts and ideas the authors call "Ten Points for the Commander."

Summary. This article aligns closely with the study based on the strong focus regarding the integration of intelligence and information across today's battlefield. The authors discuss the need to create a data gathering and analysis solution aligned with the operational environment where the volume and velocity of information is at its highest levels. The authors utilize their own extensive personal combat experiences to discuss the fusion of battlefield intelligence data requires the focusing of the many diverse

information collection systems currently in use. The authors note the need to communicate and disseminate information data rapidly up, down, and laterally across organizations without restrictions is a critical need in order to achieve increased levels of actionable intelligence. A key component of the article is the discussion on how the intelligence community as a whole needs to view itself as the critical enabling capability of decision making, whether is at the tactical or strategic level.

Rubin, D., Lynch, K., Escaravage, J., & Lerner, H. (2014). Harnessing data for national security. *The SAIS Review of International Affairs, 34*(1), 121-128. Retrieved from http://libproxy.uoregon.edu/login?url=http://search.proquest.com.libproxy.uoregon.edu/docview/1552151745?accountid=14698

Abstract. This article discusses that since 9/11, the United States government has initiated efforts to enhance its information-sharing capabilities and doubled its investment in counterterrorism, spending nearly $80 billion. Sharing data and conducting analyses across the government's legacy stovepipes of information is challenging but mandatory to reduce redundancy, increase cost efficiency, and improve national security mission performance. The challenges involved in harnessing big data analytics for a more enlightened approach to national security center on striking the optimal balance between complex opposing forces-opportunity versus risk, collective security versus individual privacy, and innovation versus protection. While the government has made progress in identifying existing data sources and sharing high-level metadata, it is still in the early phases of the maturity curve in terms of enabling access across the federal ecosystem to leverage the valuable analytics that inform evidence-driven decision-making. This paper

explores the strategies and frameworks to expedite effectively analyzing and using data to drive national security activities.

Summary. This article aligns with the study by discussing data sharing and conducting analyses across the legacy DoD networks and associated government systems. The authors focus on reducing systems redundancy, increasing cost efficiency, and improving overall national security mission performance within the government defense space. The author notes a more productive and leaner government enterprise will assist with harnessing the large amounts of existing data it currently has at its disposal. This is a critical need in support of current C-IED operations and especially for organizations gathering, storing, and sharing large amounts of exploitation data. The author notes there are many challenges involved in harnessing data analytics through the use of the government's current information systems, and without this critical information evidence-driven decision making is not possible. The author also highlights that our connected society of today continuously produces valuable data, which is key in providing real-time and strategic intelligence related to terrorist activities.

Conclusion

Common ideas, operational processes, and organizational performance information identified during the analysis of the selected references focus on the critical C-IED mission. This information serves to provide DoD C-IED mission focused government, civilian, and contractor organizations a better understanding of the mission impacting interoperability conditions that exist between new and legacy information technology systems. This information also serves to highlight the critical need to identify more effective and efficient mission enhancing alternatives to achieving actionable intelligence. Relevant recommendations consist of both qualitative and quantitative scholarly articles, books, published white papers, and civilian and government websites.

Each of the organizing themes used to frame the presentation of the references annotated in this study highlights the critical need to achieve increased levels of actionable intelligence as the global IED threat expands and evolves, and the methods for accomplishing this. Themes include (a) evolving threats posed by the use of IED's; (b) challenges posed by legacy systems in countering IED threats; and (c) information sharing and countering IED threats.

Evolving Threats Posed by the Use of IED's

The IED environment is constantly evolving and the technological and information gathering solutions designed to counter these deadly devices have a limited time frame (Bennett, 2013). In this study, the focus on the evolving threat posed by the IED around the globe has confirmed the need for C-IED focused organizations to rapidly reduce the effectiveness and lethality of IED's to allow freedom of maneuver for joint forces, federal agencies, and partner nations (JIEDDO, 2012). This requires C-IED organizations to aggressively seek to maintain

high levels of research and development (R&D) aimed at achieving increased levels of actionable intelligence and neutralizing the global IED threat.

The literature indicates the IED threat consists of an overlapping consortium of networks spanning the entire threat continuum including criminal gangs, insurgencies, and terrorists who maintain a global reach and use the IED as a common weapon of choice (JIEDDO, 2012). As the IED threat continues to evolve across the globe this deadly weapon remains one of the most accessible tools utilized to inflict fear and casualties (Obama, 2013). As the individual IED devices become more technologically advanced and widespread, the requirements to effectively exploit information and materials from attacks are a key to successfully countering this global threat (Obama, 2013).

The literature also indicates the IED poses a fundamental, significant and enduring threat for the foreseeable future (Smith & Tranchemontagne, 2014). Smith and Tranchemontagne (2014) specifically note that the enduring threat has resulted in C-IED organizations operationalizing technical and forensic activities by fusing the technical, forensic, and biometric disciplines to produce actionable intelligence used to counter threat networks. This shift provides the ability to conduct relevant and timely collection, analysis, and technical and forensic exploitation of current and emerging IED technologies (JIEDDO, 2012). The study confirmed the capture and analysis of large amounts of associated information require the use of many information technologies and platforms across the DoD spectrum. Many of these decentralized forward deployed technologies and platforms do not always have connectivity back to a United States based network, and considered legacy systems that impact current operations (Witherspoon et al., 2014).

Challenges Posed By Legacy Systems in Countering IED Threats

Legacy systems found throughout many United States government organizations and agencies required an estimated $35.7 billion spent on their support and upkeep in 2010 alone as noted by Alexandrova et al. (2015). The large amount of funding dedicated to maintaining legacy systems places a financial and operational burden on many organizations, and has a profound impact on operations such as those conducted to counter the evolving global IED threat (Alexandrova et al., 2015). Many of the existing legacy systems utilized by government organizations are "slow, duplicative, and lacking interoperability" (Barno et al., 2013, p.19). The study highlighted the need for the DoD to introduce more efficient and interoperable systems aimed at achieving greater levels of actionable intelligence. This becomes a reality with today's rapid changes in missions and mission requirements, as well as the emergence of new asymmetric threats found within a complex operational environment (Goerger et al., 2014).

The study also highlighted challenges posed by legacy systems in the fight to counter the global IED threat and the limited ability to fully synchronize and integrate all available C-IED capabilities and associated IED exploitation information for operating forces forward deployed (Patacsil, 2013). The literature identifies the use of legacy systems to support the C-IED fight directly impacts information sharing connections between C-IED organizations, in addition to highlighting the widespread use of separate databases and differing methods for securing and facilitating data movements across government networks (Rubin et al., 2014). The decentralized network of information C-IED gathering, analysis, sharing and operations limits the forward deployed combatant commander's ability to achieve and utilize actionable intelligence to counter the IED threat (Smith & Tranchemontagne, 2014).

The literature also indicates that to achieve increased levels of actionable intelligence, the IED must be viewed as an intelligence opportunity that can yield information about the network of bomb designers, builders, emplacers, triggermen, financiers, component suppliers, and operational leaders who make up the complex web of actors who execute IED attacks (Smith & Tranchemontagne, 2014). All of this information must be gathered, analyzed, and disseminated through many currently utilized decentralized DoD legacy systems that lack the ability to complete this task in real-time (Barno et al., 2013).

Information Sharing and Countering IED Threats

Countering the global IED threat requires collection and analysis of large amounts information that includes biographic, biometric, and forensics data, along with the use of network analysis for linking identities to places, activities, to those directly responsible for the fabrication and use of IED's (Voelz, 2015). The literature highlights that today's fight against the IED threat is unlike the analytical challenges of industrial age warfare, requiring development and implementation of new tools, systems, and methods for collecting, processing, and communicating information across the entire United States Government security apparatus (Voelz, 2015). The study focuses on the information sharing relationships post September 11, 2001. This tragic event markes the transformation point for current intelligence gathering and sharing practices utilized by the United States (Carter, 2015).

Flynn and Flynn (2012) note that focusing and fusing of current intelligence and information collection systems, assists with successfully countering the IED threat, and provides C-IED organizations with the ability to communicate rapidly up, down, and laterally without restrictions. Flynn and Flynn (2012) explain that enhanced information flow is achieved through the creation of a dedicated C-IED fusion cell and the use of enhanced information systems and

infrastructure. The fusion cell acts as a single point for the synchronization of gathered C-IED information helping provide more reliable and credible actionable intelligence (Flynn & Flynn, 2012). The literature indicates information sharing is a key component of countering global IED threats. For example, enhanced intelligence information allows operational commanders to interrupt an enemy's decision cycle and interdict IED tactical employment in real-time (Smith & Tranchemontagne, 2014). The literature also highlights the requirement for enhancing information sharing and collaboration efforts to prevent, prohibit, and respond to the growing global terrorist and IED threats (Deni, 2015).

In summary, the references included in this study identify legacy systems as known challenges for many government organizations as noted by Alexandrova et al., (2015). These challenges directly impact achieving greater levels of actionable intelligence for those specific DoD organizations focused on the C-IED fight. To increase current levels of actionable intelligence in support of C-IED operations noted by Smith and Tranchemontagne (2014), government and military leaders must identify mission enhancing alternative solutions for the use of decentralized legacy information systems. As noted by Alexandrova et al. (2015), legacy systems present government organizations with a great deal of operational and financial risks. With these risks present along with the ever-evolving threat of the global IED, a "synchronized and integrated" JIEDDO (2012, p.1) approach of information gathering, analysis, and dissemination is required for achieving greater levels of actionable intelligence.

References

Agarwal, S., Pape, L. E., Dagli, C. H., Ergin, N. K., Enke, D., Gosavi, A., & Gottapu, R. D. (2015). Flexible and intelligent learning architectures for SoS (FILA-SoS): Architectural evolution in systems-of-systems. *Procedia Computer Science, 44*, 76-85. doi:10.1016/j.procs.2015.03.005

Alexandrova, A., Rapanotti, L., & Horrocks, I. (2015, May). The legacy problem in government agencies: An exploratory study. *Proceedings of the 16th Annual International Conference on Digital Government Research, UK, 150-159.* Retrieved from http://oro.open.ac.uk/42604/1/dgo_2015_submission_11.pdf

Barno, D., Bensahel, N., Stokes, J., Smith, J., & Kidder, K. (2013). *The seven deadly sins of defense spending.* Retrieved from Center for a New American Security website: http://www.cnas.org/files/documents/publications/CNAS_SevenDeadlySIns.pdf

Bennett, B. A. (2013). *Counter-improvised explosive device fusion cells and the brigade combat team: A modern day imperativ*e [Monograph]. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA606046

Carter, J. G. (2015). Inter-organizational relationships and law enforcement information sharing post 11 September 2001. *Journal of Crime and Justice, 38*(4), 522-542. Retrieved from https://scholarworks.iupui.edu/bitstream/handle/1805/4544/carter-2014-inter-organizational.pdf?sequence=1&isAllowed=n

Deni, J. R. (2015). Beyond information sharing: NATO and the foreign fighter threat. *Parameters, 45*(2), 47-60. Retrieved from

http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Summer_2015/8_Deni.pdf

Department of the Army. (2013). *Annual report on business transformation: Providing readiness at best value* (1 March 2013 Report). Retrieved from http://www.defenseinnovationmarketplace.mil/resources/2013ArmyAnnualReportlBusinessTransformation.pdf

DoD, U. S. (2010). Department of defense dictionary of military and associated terms. *Joint Publication, 1-02*. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Flynn, M. T., & Flynn, C. A. (2012). Integrating intelligence and information: Ten points for the commander. *Military Review, 92*(1), 4-8. Retrieved from http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20120229_art005.pdf

Goerger S. R., Madni, A. M., & Eslinger, O. J. (2014). Engineered resilient systems: A DoD perspective. *Procedia Computer Science, 28*, 865-872.doi: 10.1016/j.procs.2014.03.103

Gosler, J. R., & Von Thaer, L. (2013). *Task force report: Resilient military systems and the advanced cyber threat*. Washington, DC: Department of Defense, Defense Science Board, 41. Retrieved from http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

Joint IED Defeat Organization [JIEDDO] (2012). *Counter-improvised explosive device strategic plan: JIEDDO 2012-2016*. Retrieved fromhttps://www.jieddo.mil/content/docs/20120106_JIEDDOC-IEDStrategicPlan_MEDprint.pdf

Obama, B. (2013). *Countering improvised explosive devices*. Washington, DC: Executive Office of the President. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA574504

Patacsil, J. A. (2013). *Sustaining eleven years of counter-improvised explosive device relevancy for tomorrow's war* (Master's thesis, Marine Corps Command and Staff College. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA601583

Rubin, D., Lynch, K., Escaravage, J., & Lerner, H. (2014). Harnessing data for national security. *The SAIS Review of International Affairs, 34*(1), 121-128. Retrieved from http://libproxy.uoregon.edu/login?url=http://search.proquest.com.libproxy.uoregon.edu/docview/1552151745?accountid=14698

Smith, T. B., & Tranchemontagne, M. (2014). Understanding the enemy: The enduring value of technical and forensic exploitation. *Joint Force Quarterly 75, 4*, 122-128. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA622235

Stevens, G. D. (2012). *Whole of government approach to countering domestic IED's: Leveraging military capabilities.* (Civilian Research Report 29-05-2012). Retrieved from the Defense Technical Information Center website: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA593378

University of Florida Center for Public Issues. (2014). *Evaluating information sources.* Retrieved from http://ce.uoregon.edu/aim/Capstone1Perm/evaluateinfo.pdf

Voelz, G. J. (2015). The rise of iWar: Identity, information, and the individualization of modern warfare. Army War College Carlisle Barracks Pennsylvania, Strategic Studies Institute. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA624745

Witherspoon, G., Quock, K., Lundberg, M., Elkins, A., & Christou, C. (2014, October). Evolving the tactical edge: Delivering unified capabilities and mobile enterprise connectivity to the deployed user. Military Communications Conference (MILCOM), 2014 IEEE, 1269-1274. doi: 10.1109/MILCOM.2014.211Appendix

Definitions

The definitions below describe technical and operational terminology as used in the annotated bibliography. Definitions derived from associated research literature:

Actionable Intelligence- intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process (DoD, 2016 p. JP 1-02, 1).

Counter-Improvised Explosive Device Operations (C-IED) - The organization, integration, and synchronization of capabilities that enable offensive, defensive, stability, and support operations across all phases of operations or campaigns in order to defeat improvised explosive devices as operational and strategic weapons of influence (DoD, 2016 p. JP 1-02, 52).

Counter-Terrorism- Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals (DoD, 2016 p. JP 1-02, 54).

Exploitation-Taking full advantage of any information that has come to hand for tactical operational, or strategic purposes (DoD, 2016 p. JP 1-02, 83).

Improvised Explosive Device (IED)- A weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract (DoD, 2016 p. JP 1-02, 108).