INSTITUTE FOR DEFENSE ANALYSES

19th ICCRTS Cyber Operations Model for Multi-Domain Conflict

Robert M. Rolfe, *Project Leader*

Francisco L. Loaiza-Lemos
Laura A. Odell
Jonathan R. Agre
Karen D. Gordon
Joshua Alspector
Thomas H. Barth

24 April 2014
IDA Non-Standard Document
NS D-5127
Log: H 14-000094
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract DASW01-04-C-0003, Task BK-5-3756, "Recommended Pricing Model for Modernized DISN," for the U.S. Army Program Executive Office, Enterprise Information Systems. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

19th ICCRTS
Cyber Operations Model for Multi-Domain Conflict

Topics 3 & 4

Authors: Robert M. Rolfe, Francisco L. Loaiza, Laura A. Odell, Jonathon R. Agre, Karen D. Gordon, Joshua Alspector, Thomas H. Barth

POC: Robert M. Rolfe, Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, VA 22311; TelNr.: (703-845-6665); email: rolfe@ida.org

ABSTRACT

Cyberspace is now recognized as the fifth operational domain, and future military operations will both rely on, and—at least in part—be fought within, it. In addition, the dependency on cyberspace of the entire national critical infrastructure will continue to increase.

This paper proposes an *analytic model for multi-domain cyber operations*, which, coupled with a comprehensive *cyber operation capability frame of reference*, can serve as the basis for a solution architecture to provide the required automated decision support (ADS) capability. The benefits of such an ADS capability are highlighted in the context of selected scenarios for multi-domain operations, and an implementation plan is proposed and discussed.

New Dangers for a New Era

The coming era will be characterized by increasing competition for scarce global resources such as water, food, minerals, oil, and labor. Some academics predict global instability and conflict in the next ten years.[1] Today, the richest people and the largest companies in the world are no longer American. In 2013, the Chinese bank ICBC unseated Exxon Mobil as the world's biggest company and takes the number one spot for the first time. Another Chinese bank, China Construction Bank, moved up 11 spots to No. 2 on the list. Mexican Carlos Slim is once again the world's richest person, followed by Bill Gates. Amancio Ortega of Spanish retailer Zara moved up to No. 3 for the first time.[2] The United States can no longer assume an undisputed leadership role in the global economy and politics, and thus can no longer set the economic trend or expect other leading economies to cooperate.

The 2010 Quadrennial Defense Review (QDR) noted that climate change is an "accelerant of instability or conflict," which will play a "significant role in shaping the future security environment"; will cause a "…need to adjust to the impacts of climate change on our facilities and military capabilities"; and will result in "…placing a burden to respond on civilian institutions and militaries around the world." The 2012 DoD national security report to Congress noted that "Chinese actors are the world's most active and persistent perpetrators of economic espionage…. Chinese attempts to collect U.S. technological and

economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security."[3] It is imperative for the United States to articulate strategies and identify the resources, tools, and techniques needed to confront the challenges of this new era.

Regardless of the strategy adopted by the Cyber community, there will be decisions that require access to information that is generally in non-federated repositories. The resources necessary to support cyber operations are extremely heterogeneous and require prepositioning of access mechanisms to non-federated repositories before events and operations, and every interaction required for cyber operation also requires pre-validated tools and techniques. For cyber-operational solutions to have the necessary level of robustness they must address these issues.

Cyberspace – A New Operational Domain

The U.S. Department of Defense (DoD) recognizes cyberspace as the fifth operational domain. In 2011, the Department published *DoD Strategy for Operating in Cyberspace*[4] noting that DoD must (1) Protect DoD networks and systems and (2) Partner with others to confront cyber threats nationally and internationally. Likewise, the 2012 *Capstone Concept for Joint Operations (CCJO)*[5] advocates globally integrated operations—which have networking and information technology (IT) at their core—as the principle upon which future Joint Forces operations should be based. Furthermore, the *Joint Operational Access Concept (JOAC)*[6] advocates the development of cross-domain synergy, i.e., "the complementary employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others." The cyber domain will be a key venue for applying these strategic concepts.

In addition to the importance of cyberspace to military operations, much of U.S. critical infrastructure is dependent on a safe and reliable cyberspace. *Presidential Policy Directive (PPD) 21* identifies 16 critical infrastructure sectors, including Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, IT, Nuclear Reactors/Materials/ Waste, Transportation Systems, and Water/Wastewater Systems. The nation's economic health is dependent on protecting cyberspace, which enables commercial activities and financial transactions. The complex interplay of international economic, kinetic, and cyber competition is illustrated in Figure 1 below.

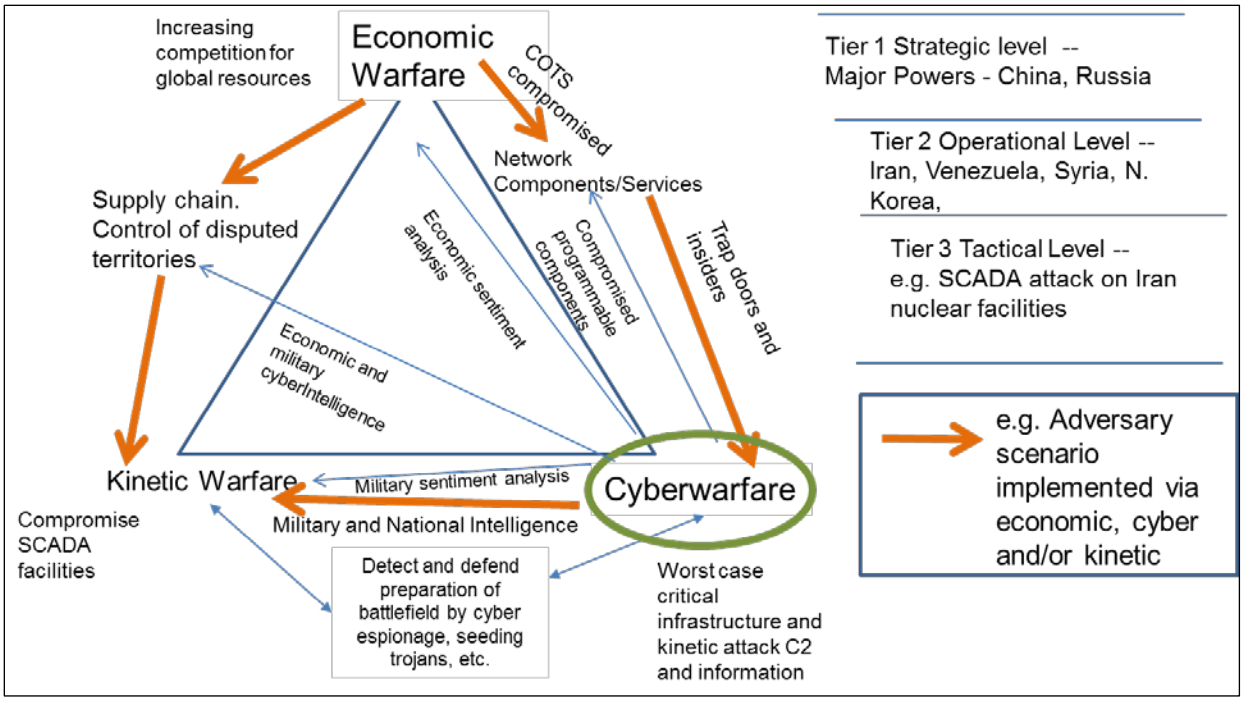

Figure 1. Interplay of Economic, Kinetic, and Cyber Competition Factors

This multi-domain competition can be at a strategic level, involving major players such as China and Russia. At an operational level it may involve second-tier players such as Iran, Venezuela, Syria, and North Korea. At a tactical level, it may involve focused operations such as the Supervisory Control and Data Acquisition (SCADA) attack on Iran's nuclear facilities. In the coming era of persistent conflict, the United States will increasingly find itself involved in multi-domain conflicts and should prepare accordingly.

Economic and Societal Conflict

Perhaps the domain most difficult to understand is that of economic and societal conflict. The coming era will be characterized by increasing competition for scarce global resources such as water, food, minerals, oil, and labor. Intelligence will play a key role in understanding adversaries' behavior.

Understanding the sentiment underlying the decisions of a nation will be important in dealing with conflict situations that may arise. Such sentiment can depress markets and foment revolutions.[7] Failing to foresee the political disintegration of countries such as Libya and Egypt following the Arab Spring is a widely noted U.S. intelligence failure. Could analysis of publicly available data (twitter, news feeds, blogs, and government economic projections) have identified hot spots such as those in Egypt where organizers used Twitter and social media to rally protestors?

An example of how an adversary can affect important infrastructure is the AP News Twitter hack on the White House that caused a brief market crash.[8] In economic scenarios, another example is that although the oil markets predicted the Arab embargo in 1973, the intelligence community (IC) did not. A further example of economic intelligence is information provided by prediction markets that use crowd sourcing.

Machine learning (ML) technology can help mine social media, news sources, and other intelligence for the purpose of sentiment analysis and prediction of possible future scenarios. One can use machine

learning to design a prediction agent. Wall Street uses ML technology for trading based on predictions based on observed sentiment. In DoD, the office of Naval Research's (ONR) Social, Cultural, and Behavioral Sciences program aims to develop socio-culturally informed human behavior models to enhance training in, planning for, and analysis of irregular warfare and Stability, Security, Transition, and Reconstruction (SSTR) operations.

There is a rich global sensor network for Intelligence, Surveillance, and Reconnaissance (ISR) containing information on agriculture, materials, energy data, transportation routes, weather disruptions, credit ratings, currency exchange, interest rates, and stock markets. Systems are being researched to mine this information.[9][10][11] Because economic and social science intelligence can often be obtained from open source and other digital sources, it is important to consider using these sources for cyberspace operations to aid prediction of economic and social stress.

Cyber Operations

The DoD has extensive operations in cyberspace. A frame of reference for cyberoperations is illustrated in Figure 2 below:

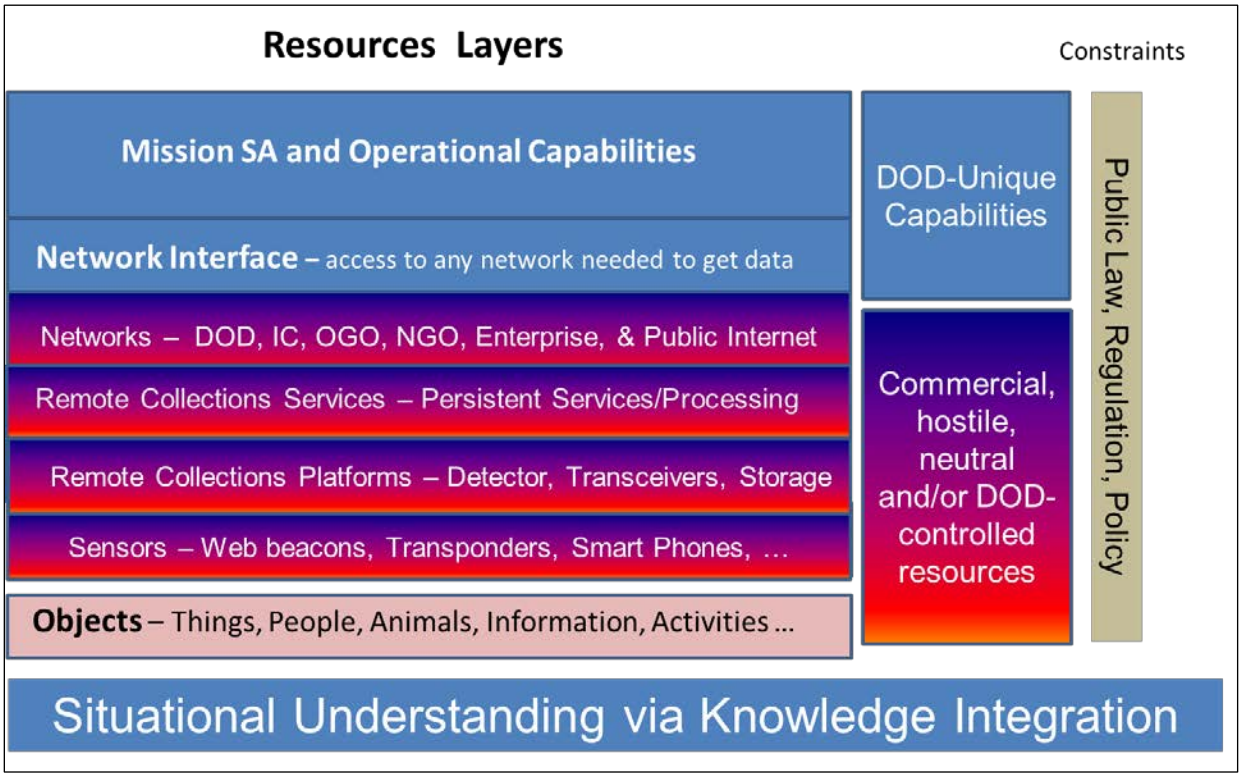

Figure 2. A Cyberoperations Frame of Reference

The goal of cyberoperations is situational understanding via knowledge integration. To do this requires knowledge of objects, which can be represented in cyberspace in a variety of ways. Objects can be people, perhaps those composing organizations, represented by attributes (faces, activities, roles) such as terrorist leader or group. Objects may also be weapons, vehicles, and information which may need tracking. Key needs are tagging, tracking, and locating (TTL) these objects. A *cyber tag* may be embedded in cyber transactions that may allow the identification of the owner, creator, or modifier of the transaction. A *cyber track* makes possible the pursuit of a transaction by following signatures left behind

as files move or are at rest throughout cyberspace. One goal is to *cyber locate* tagged objects so they are resolved to a region in space and time.

DoD does not generally own the networks capable of TTL and must attempt to operate under commercial, neutral, or hostile conditions. Cyberspace has many parts: the public internet, commercial and financial enterprise, foreign military, foreign government, allied and U.S. military, foreign and domestic SCADA networks, etc.[12] The Department of Homeland Security (DHS) has become increasingly concerned about the lack of security of such control networks because such control systems are owned by private companies and are increasingly being interconnected to improve efficiency.

Information within Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks and cyberoperations can be affected by intrusion, denial of service, or disabling of network or services. This may compromise other information, weapons and command centers, and other infrastructure. A goal of cyberoperations may also be perception management of the targeted countries population.

Situational Understanding for Decision Support

There are significant challenges in understanding a situation. First, there is a large amount of data relevant to a situation and it changes constantly. The topology of nodes, links, nodal equipment, architecture, protocols, and networks is always in flux. Also, network traffic is changing, together with software applications for the user and for the managers of the networks. Constantly evolving threats force the evolution of mitigation strategies to confront them. Network and component sensors are either integrated or temporarily deployed. Some types of information change rapidly (traffic loads, node and link faults, attacks – physical or cyber), whereas others change more slowly (configuration of elements, maintenance status, modeling of proposed changes).

Another challenge is that information needed is difficult to capture and of variable quality. Databases of the network elements, computers, and architectures are often incomplete, and the information is kept in disparate databases and comes from different sources assembled by a variety of collection strategies with incompatible data collection tools.

Furthermore, the knowledge to be gleaned is difficult to understand. There is a heterogeneous infrastructure of many networks, many operators, and many users. There are different dependencies and relationships among equipment, applications, and protocols. There are also many complex information assurance strategies for areas such as access control and for computer network defense.

An overriding issue is how to merge, and efficiently manipulate information from disparate sources, and then provide adequate analytical capabilities without getting bogged down in the “schema-to-schema mapping” swamp. A possible architecture for accomplishing this is depicted in Figure 3 below.

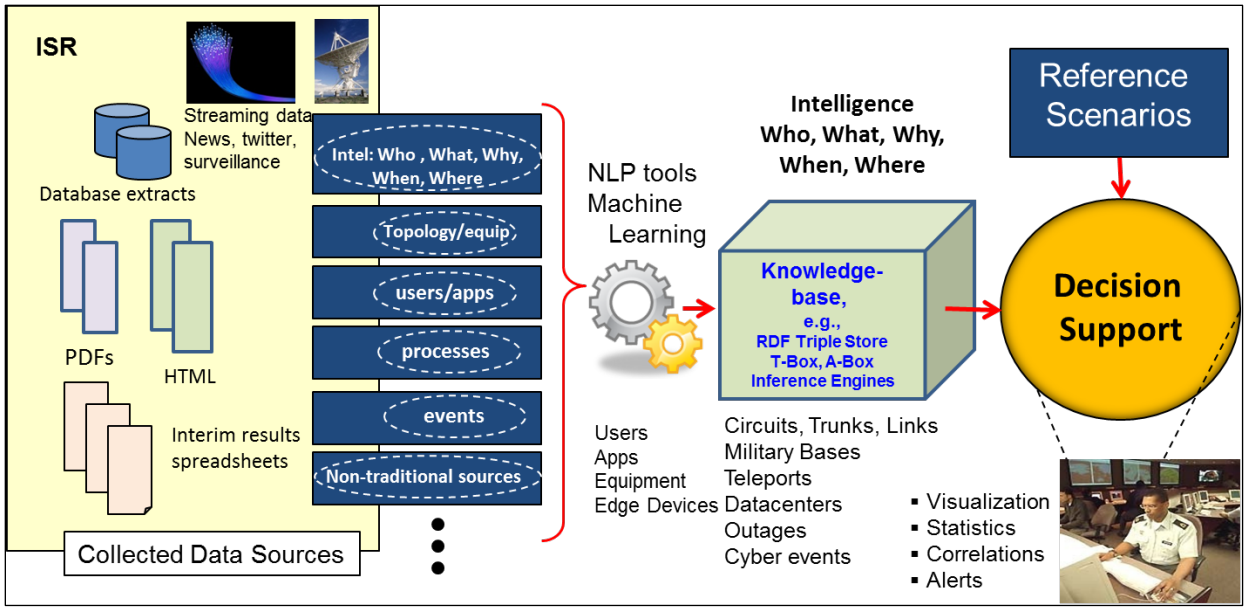

Figure 3. Proposed Solution Architecture to Address Information Heterogeneity and Disparity in Cyberspace

Note that the collected data sources include non-traditional items, such as news and social networks, as well as traditional DoD surveillance sources. To extract knowledge requires advanced artificial intelligence software, including natural language processing, machine learning, and rule-based inference software that makes use of an extensive knowledgebase.

Scenarios for Multi-Domain Operations

A variety of scenarios for using this system for cyber incident analysis and decision support can be envisioned. They include a SCADA attack with physical destruction, information-destroying cyber-attack on financial institutions, analysis of known preparations for attack in kinetic or cyber domains, a security compromise in the DoD supply-chain with cyber-bombs in critical systems, and cyber-espionage of Defense Industrial Base (DIB) strategic companies.

Another group of scenarios for economic and market signals include the IC issuing a National Intelligence Estimate (NIE) signaling a crisis ahead, the oil market signaling an oil embargo as in 1973, and financial intelligence (FININT) alerting the system to suspicious trades by persons or organizations of interest.

Additionally, the system may be used for execution of a planned response to cyber-attack by a major power such as China or by a small hacker group that executes a distributed denial of service (DDoS) attack on banks.

Conclusion

The DoD has long believed in the value of C4ISR, but it has not focused on collecting, processing, and understanding these new types of intelligence. To a degree, the IC has filled the void, but with a heavy reliance on labor-intensive analytical support. The time has come to automate and upgrade general intelligence gathering capabilities to reflect the new global realities and the capabilities made possible by new technologies and information sources.

Notes

[1] http://rbth.ru/society/2013/04/18/academics_predict_new_world_war_for_next_decade_25163.html
Academics predict new world war for next decade, April 18, 2013 Inna Soboleva, RBTH
[2] http://www.forbes.com/sites/scottdecarlo/2013/04/17/the-worlds-biggest-companies-2/
http://www.forbes.com/sites/luisakroll/2013/03/04/inside-the-2013-billionaires-list-facts-and-figures/
[3] http://www.csoonline.com/article/707035/chinese-cyber-espionage-threatens-u.s.-economy-dod-says
[4] http://www.defense.gov/news/d20110714cyber.pdf
[5] http://www.defenseinnovationmarketplace.mil/resources/JV2020_Capstone.pdf
[6] http://www.defense.gov/pubs/pdfs/joac_jan%202012_signed.pdf
[7] http://www.intereconomics.eu/archive/jahr/2012/1/805/
Bas van Aarle, Marcus Kappler, Economic Sentiment Shocks and Fluctuations in Economic Activity in the Euro Area and the USA, Intereconomics Volume 47, January/February 2012, Number 1
[8] http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
[9] http://www.tkl.iis.u-tokyo.ac.jp/top/modules/newdb/extract/310/data/49760001.pdf
Kitsuregawa et. al. - Socio-Sense: A System for Analysing the Societal Behavior from Long Term Web Archive Y. Zhang et al. (Eds.): APWeb 2008, LNCS 4976, pp. 1–8, 2008,
[10] http://blogs.hbr.org/cs/2012/09/predicting_customers_unedited_behavior.html
Predicting Customers' (Unedited) Behavior by Alex "Sandy" Pentland | 11:00 AM September 19, 2012
[11] http://www.npr.org/2012/10/08/162397787/predicting-the-future-fantasy-or-a-good-algorithm
http://arxiv.org/pdf/1201.6655v1.pdf Alina Beygelzimer, John Langford, David Pennock Learning Performance of Prediction Markets with Kelly Bettors Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012),
http://cs229.stanford.edu/proj2012/ShenJiangZhang-StockMarketForecastingusingMachineLearningAlgorithms.pdf Shunrong Shen, Haomiao Jiang, Tongda Zhang - Stock Market Forecasting Using Machine Learning Algorithms
[12] http://www.securityfocus.com/news/11351/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
24-04-2014	Non-Standard	

4. TITLE AND SUBTITLE

19th ICCRTS Cyber Operations Model for Multi-Domain Conflict

5a. CONTRACT NUMBER

DASW01-04-C-0003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)

Francisco L. Loaiza-Lemos, Laura A. Odell, Jonathan R. Agre, Karen D. Gordon, Joshua Alspector, Thomas H. Barth

5d. PROJECT NUMBER

5e. TASK NUMBER

BK-5-3756

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

NS D-5127
H 14-000094/1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Glen James Stettler
ASD(R&E)/RD/Technology Security Office
4800 Mark Center Drive,
Mailbox #46,
Alexandria, VA 22350-3600

10. SPONSOR'S / MONITOR'S ACRONYM

ASD(R&E)/RD

11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Robert M. Rolfe

14. ABSTRACT

Cyberspace is now recognized as the fifth operational domain, and future military operations will both rely on, and—at least in part—be fought within, it. In addition, the dependency on cyberspace of the entire national critical infrastructure will continue to increase.

This paper proposes an analytic model for multi-domain cyber operations, which, coupled with a comprehensive cyber operation capability frame of reference, can serve as the basis for a solution architecture to provide the required automated decision support (ADS) capability. The benefits of such an ADS capability are highlighted in the context of selected scenarios for multi-domain operations, and an implementation plan is proposed and discussed.

15. SUBJECT TERMS

cyberspace, cyber-attack, automated decision support, semantic models, triple store, knowledgebase, network operations, machine learning, natural language processing, situational awareness

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Unlimited	12	Hari Bezwada, Chief Technology Officer
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER (Include Area Code) 703-806-3213