Artificial Intelligence Approaches for Modeling Social Terrain

Elizabeth K. Bowman, US Army Research Laboratory 4508 Wayberry Dr., Aberdeen Proving Ground, MD 21005

ABSTRACT

Advanced technologies are transforming the information environment and allowing individuals and groups unprecedented opportunities to share ideas, actions, emotions, conflicts, and activities. While this enables social groups to expand their membership in the global online community, it also allows scientists to use the social media environment as a real-world laboratory to study emerging behaviors in this space. For military analysts, this environmental laboratory provides an opportunity to study communities in advance of deployments to foreign soil. In the same way that military logisticians would study physical terrain to plan for equipment, analysts can observe activities in the information environment to plan for negotiations in the social terrain. This presentation will discuss key concepts for modeling the social terrain and will identify promising AI techniques for each. Key concepts will include Human, Information, Interpretation, and Influence considerations. AI technologies will be discussed for each of the following social terrain considerations: Human, Information, Interpretation, and Influence. Together, these elements form the underpinning science of sensemaking within the new information environment. The Human Systems Community of Interest (HS COI) within the US Department of Defense (US DOD) is exploring how to jointly establish effective capabilities in this sphere for rapid exploitation at the tactical operational levels. This paper will address the priorities and future needs of this Joint research effort and will explore technical challenges that face the transition of research results to system-level applications.

Keywords: Artificial intelligence, machine learning, social terrain modeling, human information interpretation, information environment

1. INTRODUCTION

"The future is already here—it is just not evenly distributed." This observation, made by William Gibson in 2003 [1], is truer today 15 years later with many implications for defense research. The elements of Gibson's perspective that we will address here are twofold; the rapidity with which advanced technologies are changing the defense landscape and the uneven distribution of technology use based on opponents' lack of regard for ethical information use. Our focus is on the military aspects of operating in the new Information Environment (IE) that is dominated by new communication technologies and social applications that are greatly transforming the speed, spread, and content of messaging. Central to our concerns are the many divergent ways in which these aspects of the IE serve as threats to defense operations. The US Army's concept of Multi Domain operations [2] presents insight into how such operations will be focused on emergent threats that embody the contested, complex, and expanded battlefield (e.g., the addition of cyber to the traditional air, land, sea, and space dimensions). Operations in the Information Environment (OIE) fall within the cyber domain and will be the focus of discussion in this paper. Relevant doctrinal sources for OIE can be found in [3] and [4]. Each of these documents establishes the requirements for military decision makers to understand perceptions and attitudes that drive human behaviors that can impact operations and the associated trends that will follow from social action. The ability to characterize, assess, synthesize, and understand these social trends and the likely engagement with defense forces in the IE is currently driving advanced technology development within the US and Allied defense establishments. However, the deployment of capabilities that exploit socially-created data and information are subjected to ethical and moral considerations within Western defense entities; a consideration that is not accepted by our adversaries. Hence, democracies around the globe are seeking ways to securely and safely identify information operation elements to correctly characterize and rapidly address harmful messaging.

Micro- and Nanotechnology Sensors, Systems, and Applications XI, edited by Thomas George, M. Saif Islam, Proc. of SPIE Vol. 10982, 109820J · © 2019 SPIE
CCC code: 0277-786X/19/$18 · doi: 10.1117/12.2516382

Multi-scale conflicts of varying intensity, many with novel strategies and tactics, continue to spread globally and threaten US and Allied security in an increasingly connected world. These conflicts require a wide range of military responses that are complex and involve uncertain battle rhythms that defy standard methods of planning, metrics of assessment, tactics, strategies and capabilities. From the new types of information conflicts, to the implications of burgeoning humanitarian crises (e.g., surges of refugees fleeing active warfighting, conflicts over water, ethnic strife, religious and civil strife), new problem spaces continue to arise that demand new capabilities to rapidly and accurately deduce the human aspects of operational environments in dense, complex, and culturally diverse regions. Failure to understand these human aspects, and the connections existing within the operating environment, compound the challenges for effective military response. Defining courses of action in highly disparate threat and humanitarian situations requires the rapid acquisition of deep understanding of the relevant human environment. Sensemaking within this context requires an emphasis on characterizing the various, but related, ways in which humans formulate and share information for the purpose of exerting influence through others' interpretation of the original message.

1.1 Human Information, Interpretation, and Influence

The US Department of Defense (DOD) Communities of Interest (COI) were established to encourage multi-agency coordination and collaboration in cross-cutting technology focus areas [5]. Among the 17 technical areas represented in the COI structure is the Human Systems (HS) COI. One Thrust area is the Human Information, Interpretation, and Influence (HI3) activity, which brings together scientists from Air Force, Army, and Navy Research Labs. The vision of the group is to use effective engagement with the dynamic human terrain to make better courses of action and predict human responses to military actions. Three objectives define the approach to that vision: 1) Process and exploit social data to understand adversary intent, 2) Inform Tactics, Techniques, and Procedures (TTPs) to assess information maneuvers and forecast adversarial social response, and 3) Rapidly deploy counter-measures against information threats. These capabilities will be delivered through the deployment of technologies that utilize Natural Language Processing (NLP) tools for extracting meaning in multimedia, and that encompass models and Machine Learning (ML) algorithms to forecast conflict/human intent/crises, that can be integrated with system-level tools and visualizations to allow understanding of computational outputs.

The HI3 Joint researchers are engaged in a number of shared activities exploring new technologies to deliver capabilities to tactical Warfighters in the near future. Research-level tools in development include software applications that rapidly and accurately extract socially-based patterns that signal intentional behaviors that threaten military courses of action. These tools perform a range of capabilities in the spectrum of understanding an unfamiliar society and accurately anticipating future actions, both from adversary groups and from the general populace. Information extraction tools provide features that identify influential actors, relationships in social networks, trending topics of discussion, sentiment expressed toward major entities, and discourse analysis in printed text. Additionally, cultural identification and representation tools provide distinct views of major cultural dispersions in an area of operations. Such tools not only allow rapid information sharing about cultural norms in an unfamiliar area, but provide a geographic indication of how cultural beliefs are arrayed in the population. Further, uncertainty assessments can be provided in two ways by this family of tools. One aspect is to identify deception in social media information flows (e.g., detecting bots and false claims). Another is to test the potential network effects that can be achieved by removing one influential node from a known network. Finally, conflict predictions based on discourse analysis and quantitative social modeling can be used to track the actual and forecasted spread of violence, or threats thereof, in an area.

The evolution of the HI3 Joint Thrust activity builds from the complex nature of OIE that are based on the foundations of *Humans* sharing *Information* that is subject to *Interpretation* by others and is designed to spread *Influence* to achieve desired outcomes. Within the Human element, we are concerned with individuals, social groups, organizations, analysts, and decision makers. Our foci there is to characterize the persons operating in a particular manner within the IE and any groups/organizations with which they are affiliated and to provide defense actors with the tools to accurately identify threatening messages and campaigns. Within the Information element, we concentrate on computer-mediated messaging that include an array of text, images, videos, geo-locations, and network associations. This is designed to help characterize the potential importance of the human engagement and to ascertain links to known threat networks. The Interpretation element contains NLP and ML approaches to include topic modeling, sentiment/social network/discourse analysis, narrative formulation, pattern of life estimation, relationship linking, and the detection of several messaging strategies to include deception detection, fake news, disinformation, misinformation, individual and coordinated bot campaigns, and distortion. The Influence element is focused on the development of ethical, truthful messaging with

relevant platforms and emic perspectives (e.g., views obtained from within the perspective of the subject) and informing TTPs for countering adversary messaging. Three focus areas have been defined within the HI3 activity that are designed to address the above challenges. These are Deep Understanding of Adversarial Information Campaigns, Common Social Analytics Workflow, and Maturing Capabilities through Exercise & Experimentation. We turn next to the research priorities and future needs of these HI3 research thrusts. For each priority area we will describe the relevance of the challenge to multi-domain operations and identify technical issues associated with transitioning research results to system-level applications.

2. RESEARCH PRIORITIES

2.1 Deep Understanding of Adversarial Information Campaigns

The ability to extract, characterize, and visualize elements of an adversary's information campaign is central to the US and Coalition forces' situational understanding. This includes the ability to accurately identify individuals and groups associated with a specific threat, recognition of strategies employed to reach and influence others, and estimation of strategies that might be employed to counter or disrupt adversary activities within applicable rules of engagement. Within the emerging threat environments that Western democracies can be expected to face in the future this can be an extremely complex undertaking, given the complex nature of the social terrain.

The socio-cultural landscape of noncombatants is increasingly complex, as hybrid conflicts are occurring in urban environments. Indeed, it is anticipated that much of the world's population will reside in large urban areas, or megacities, in the near future [6]. These areas are studied by defense planners and researchers because of they may serve as fertile ground for the spread of radicalism. A term used to address this type of conflict is the 'contested urban environment' (CUE) and is the subject of international study among defense science groups [7]. Wargaming and subsequent analysis from the North Atlantic Treaty Organization (NATO) study group concerned with exploring this emerging threat domain concluded that the essential military capabilities include "collect, communicate, process, fuse, assimilate, and distribute information from many different sources, especially HUMINT, in a responsive manner" (italics added) [7]. A description of the CUE is summarized below:

> "The urban environment is complex and diverse and ranges from sophisticated, metropolis-style superstructures within a well-developed infrastructure, to high and low density urban shantytowns with very poor infrastructure. It includes towns and cities that may themselves contain commercial, industrial and manufacturing areas, as well as a variety of communication and energy production facilities. The complexity of the current urban environment is perhaps best defined as the cumulative effect of a series of interconnected layers of society and infrastructure. These comprise different sized groupings of cultural, ethnic and social groupings living in differing conditions and with many diverse views about their role in the community." (NATO RTO SAS-30, 2003).

In these densely populated areas conflict can arise from many different environmental factors and often are enacted within the IE. Recent world events highlight the range of violent conflicts and the interactive/provocative role that mobile communication devices and networked social systems play in those events. The Arab Spring demonstrations that toppled leaders throughout the Arab world [8] were the initial signal that widespread use of social media could be targeted toward serious social purposes [9]. These events were followed by serious study of how the wide spectrum of social media information sources might be used for military Command and Control (C2) and decision making [10]. This awareness has led to military command and control (C2) efforts to take an integrative approach where the strengths of social media content can be combined with other, more traditional, sources [11].

2.1.1 Technical Challenges

To deliver an effective set of capabilities to assist Warfighters in gaining a deep understanding of adversarial information campaigns, several technology applications must be pursued. These typically involve leveraging a variety of Natural Language Processing (NLP) tools for extracting meaning in multimedia. These might focus on extracting topics, sentiment, entities and relationships, and patterns of interest according to some established models of adversarial behavior and belonging. Machine Learning (ML) approaches are often used to sort and categorize data to classify various actions or activities within the context of a problem of interest. Software tool development is most effective when specifically focused on small problems that may reflect shifting or temporary challenges. Take, for example, a software tool designed to identify messages in a social media stream that are machine produced, known as bots. Bots are used as force multipliers in the IE that are used to spread narrative and attack the counter narrative [12]. In the short period of time that these elements have been active, their use and behaviors are rapidly shifting with more coordination among the machines becoming apparent. Accordingly, the software used to identify and track bot behavior must be flexible to accommodate new threat behaviors and strategies. Another example could be a software tool designed to classify the top users in a social media dataset according to adversary models. Given the nature of threats posed by rogue nation states, non-state actors, and new adversary group actors, monolithic threat models would be unhelpful and need to be updated as new threats are discovered. In this case, ML algorithms must be monitored and shaped as true positive and true negative cases (that are used to train the classification algorithms) are identified.

A basic NLP application to understand adversary messaging is the wide range of speech and language translation tools. Common technologies for translation include Automatic Speech Recognition (ASR), Machine Translation (MT), and Optical Character Recognition (OCR). OCR is potentially useful in extracting information from imagery when an analyst is trying to determine the location represented in the image. For example, an image might contain a symbol that could be used for identification purposes, such as a flag, road sign, or building sign. Translation technologies have seen significant progress in resources with languages with high resources

Another challenge is managing the data exploitation problem. The information stream that must be monitored is a large mix of structured and unstructured data that includes text, imagery, and video coming from a mix of social media and open source platforms, each with their own data types and structures and metadata components. To compound this situation, the popular social media platforms can be transitory and may make tools that concentrate on one data type to be outdated rapidly. Due to the quickness with which information is posted, shared, and used to influence groups, software applications also need to be modular and flexible in terms of design time and ability to integrate into a larger workflow. From a Defense acquisition standpoint, traditional timelines of technology development taking years can no longer be feasible. Harkening back to Gibson's quote that the 'future is not evenly distributed', this is very true within the perspective of exploiting the information space (especially in the social media domain) when considering the contrasts between the US and Coalition forces and adversary State and non-state actors. While the former are constrained by legal and ethical considerations for information use, processing, and exploitation, the latter choose to be unfettered from the same restrictions. This ultimately causes delays in countering adversary messaging and may impact influence campaigns.

2.2 Common Social Analytics Workflow

Once a set of multiple information exploitation tools is available, assembling them into a cohesive, coordinated, and modular workflow is necessary. This is aimed at reducing analyst cognitive workload with AI/ML tools to support sensemaking. These tools should help to avoid group-think and perception bias, possibly with the use of computational course of action recommenders. The goal here is to reduce the manual search and memory requirements for human analysts. One promising approach is the integration of a specific knowledge base embedded with the relevant threat model in a network graph to aid discovery and reduce the complexity of human queries. Developing workflows will require leveraging tools and algorithms described in the previous section into an ensemble and modular software architecture with common data elements, ontological identifications, and data access/storage capabilities.

A high-level workflow envisioned in the Social Terrain Modeling component of Social Analytics is the interaction between social sensing, social dynamics, and data analytics. The goal is to provide algorithms and methodologies for tactical decision makers to navigate, exploit, and anticipate conflict in a social terrain. As depicted in Figure 1, an Army challenge is the dynamic social sensing of adversary and neutral groups' opinions and behavioral intent. The desired capabilities that support that challenge involve a range of AI/ML approaches involving social media platforms, context detection algorithms, and techniques for tailoring information and meaning to tactical Warfighters in real-time.

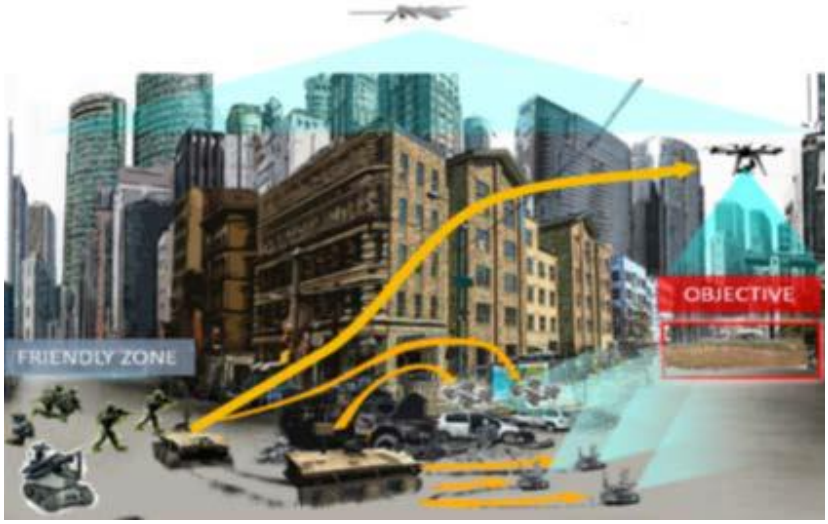

Figure 1. A depiction of a future Army challenge in a contested urban environment requiring dynamic sensing of adversary and neutral groups' opinions and behavioral intent.

A notional workflow is represented in Figure 2 for Social Terrain Modeling. This framework takes into account existing technical challenges with social exploitation and representation capabilities. One is the emphasis on analytics that are geared toward narrow aspects of social activity typically exploited through a single information channel (social media platform *du jour* or open sources, etc.). These pinpoint views give an incomplete picture of the wider group or social terrain and don't combine to equal the larger societal understanding of a region. Also, exploiting only 'available' signals can contribute to biased interpretations of ground truth. To bring defense capabilities to bear on existing information threats, we need to leverage multiple platforms and perspectives and consider operational effects in many situations (e.g., in competition and conflict), which allow a focus on multiple influence effects such as deterrence.

	Stage 1	Stage 2	Stage 3	Stage 4
	Social Terrain Sensing	***Social Terrain Dynamics***	***Social Terrain Networks***	***Social Terrain Computing***
Research Goals	Data collection	Behavior understanding and prediction	Network structure and function evaluation	Development of Intelligent C2 systems
Research Approaches	Reduction Filtering Extraction Fusion	Experimentation Modeling Simulation	Network analytics	Technological convergence of previous stages

Figure 2. The Social Terrain Modeling Workflow

2.2.1 Technical Challenges

Key technical challenges in developing a common social analytics workflow are the emphasis in Defense on stove-piped systems that limit integration opportunities for open source analytics. Developments such as Analytics-as-a-Service (A3SS) and enclave-based analytic providers offer promising solutions for component-based modular workflows. Research and development activity targeted toward Operations in the Information (OIE) domain workflows should concentrate on the integration/development of improved pattern of life models, normalcy benchmarks, and threat alerts. The value of rapid technology insertions would include tactical analysis and reachback capabilities that could derive from A3S support. This would enable human analysts to exploit dynamic information environments in real- & near-real time. Trend analysis and forecasts of adversary intentions would provide early indications and warnings for dynamic threat events. New technology applications like handheld devices and reachback to analytic services would provide expert guidance for regional areas. Data-driven activity models would provide interactive exploration of threat actions and the ability to perform what-if analyses on variable model selections. Scenario-based training would also increase analyst expertise. Finally, incorporating red team training would increase awareness of adversary goals and the viability of our own counter-measures.

2.3 Maturing Capabilities through Exercise & Experimentation

The nascent OIE field brings new challenges and capabilities to traditional Warfighting exercises and experimentation. Demonstrating automated sociocultural information exploitation capabilities at Joint and International exercises is a promising and essential element to hasten doctrinal understanding of and approval for these concepts and technologies. A secondary benefit of exercising these technologies at large wargames is the enhanced interactions between operators and developers to avoid usability and military applicability errors during the design/build/test process. In this way, Best-of-Breed real-time guides to understanding adversary tactics in the sociocultural information domain can be developed and evaluated in larger multi-domain operations simulations and analyses.

The specific capabilities HI3 tools bring to the field of military experimentation and exercise include information assessment toolkits to detect patterns/trends that signal threats and to identify relevant actors, sentiment, and trends impacting military operations. Further, TTPs can be developed, tested, and refined for rapid exploration of adversary signals in open source and social media platforms. Due to the constant change in the IE, TTPs will need to be flexible and adaptive to changing signals in the data. A Digital & Social Media Playbook would serve as an interactive training guide to information assessment and adversary tactics that would inform human analysts on the underlying human motivations and machine strategies (e.g., bots) used by adversaries in the IE.

2.3.1 Technical Challenges

Technical challenges for expanding the exercise and experimentation of technologies that exploit various elements of the IE are increasing with the appreciation across Defense establishments that social media and open source data exploitation can provide critical inputs to situational awareness and decision making. In addition to US Army, Air Force, Navy, and Joint venues, the international arena is an active area for demonstrating social media/open source exploitation capabilities. Of note is the NATO Trident Juncture series, hosted in Norway in November 2018, which contained a large social media exploitation demonstration of real Twitter data collected prior to, and during, the exercise. During the exercise analysts were able to identify a significant number of bot accounts that targeted NATO Twitter accounts. The analysis indicated these accounts were created daily and had different personas and lifespans. Analysis also was able to identify and visualize top actors and terms relevant to the NATO exercise, participating nations, and NATO as an institution. Daily information summaries were provided to the Trident Juncture senior leaders and received excellent reviews, confirming the value of this type of analysis in traditional decision support tools.

3. TRANSITION CHALLENGES

In the context of social terrain modeling and social media exploitation tool transitions, time and cohesive development funding are the primary factors of concern. From the Arab Spring revolution when social media platforms toppled political leaders, the rush has been on to develop a range of data collection, exploitation, analysis, and visualization tools aimed at popular media platforms. During that decade, Counter Insurgency (COIN) operations were the primary military emphasis and thus, tools tended to focus on understanding cultural nuances, social networks, and adversary perspectives that would inform decision making. With the move toward multi-domain operations, the factors that define COIN are not replaced, but incorporated into the larger concerns involving near-peer nations. The Information sphere is a critical

component of this strategy. Specifically, MDO calls for taking actions to expand options in the diplomatic, information, military, economic, etc. spaces for political leadership, which are anticipated to deter escalation to armed conflict. [2] Whether in the COIN or MDO domain, transitioning tools to users is never easy and depends on a research sponsor's access to operational units and exercise demonstration opportunities to showcase new capabilities. The end result of such activity is piece-meal transitions where one technology is used by one user, and another user selects a different tool. A compressive enclave that provided operational user groups with non-proprietary, open architecture systems and open source data integration services would be a major step forward toward providing an integrated information exploitation system for non-traditional information sources.

4. SUMMARY

In this paper we reviewed the major priorities and challenges associated with the HI3 and Social Terrain Modeling research thrusts. We considered the impact of hybrid warfare on operations in the information environment and the requisite actions needed to understand strategies and tactics employed by adversaries in that domain. These challenges are compounded by the realities of contested urban environments that will only grow in scale in the future. We described baseline technology development efforts that have been demonstrated in US and NATO military exercises with sound results. Within this context, we identified remaining challenges that must be addressed for full realization of technology dominance in the social media domain. We explored the dynamic challenges of that domain, which include the velocity with which processing platforms are changing and the ways in which adversaries are using those platforms to move against us. As the world's population continues to grow in size, economic inequality, and unequal access to basic resources, we can expect threats from terrorist groups to expand and spread. Kinetic military weapons will have a limited role to play in responding to these threats. Non-kinetic, diplomatic, and socio-political actions will play a major role in preventing, alleviating, and responding to threat behaviors. The continued development of text, video, and integrated text/video analysis is a key enabler for C2 in this complex, connected battlespace. The final critical challenge for US and Allied defense establishments to correct Gibson's 'distribution challenge' is to rapidly confront the ethical and moral constraints to social media exploitation of adversary intent and activities through continued study, exercises, doctrine, and TTPs.

REFERENCES

[1] Gibson, William. The Future is Already Here. The Economist, December 4, 2003.

[2] US Army Training and Doctrine Command. "The U.S. Army in Multi-Domain Operations 2028," Available on the Web: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf, December 6, 2018.

[3] Department of Defense, "Strategy for Operating in the Information Environment," Available on the Internet: https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf, June 2016.

[4] Joint Chiefs of Staff, " Joint Concept for Operating in the Information Environment," Available on the Internet: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830, July 25, 2018.

[5] Assistant Secretary of Defense (Research & Engineering), "Reliance 21 Operating Principles: Bringing Together the DoD Science and Technology Enterprise, " Available on the Internet: http://www.acq.osd.mil/chieftechnologist/publications/docs/Reliance21OpPrinciples-Jan2014.pdf, January 2014.

[6] Harris, M., Dixon, R., Melin, N., Hendrex, D., Russo, R., and Bailey, M. "Megacities and the United States Army, Preparing for a Complex and Uncertain Future," Available on the Internet: https://www.army.mil/e2/c/downloads/351235.pdf, June 2014.

[7] NATO RTO Studies, Analysis and Simulation Panel Study Group (SAS-030), "Urban Operations in the year 2020". Available on the Internet at http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-071///TR-071-$$TOC.pdf., 2003

[8] Haddad, B., Bsheer, R. and Abu-Rish, ., Eds. [The Dawn of the Arab Uprisings: End of an Old Order?], Pluto Press, London.
[9] Kase, S. E., Bowman, E. K., Al Amin, T., & Abdelzaher, T. "Exploiting social media in Army operations: Syrian crisis use case", Proc.of the 2014 SPIE Sensing Technology and Applications Conference. Baltimore, Maryland.
[10] Forrester, B.,"Providing Focus via a Social Media Exploitation Strategy", Proc.19th International Command and Control Research Technology Symposium, June 16-19, 2014, Alexandria, VA. Available on the Internet at: http://www.dodccrp.org/events/19th_iccrts_2014/post_conference/papers/039.pdf, June 16-19 2014.
[11] Cowan, N. P., "Rethinking Command and Control Of Intelligence, Surveillance, and Reconnaissance," Proc. of the 20th International Command and Control Research Technology Symposium. Available on the Internet at: http://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/55a64e86e4b0e88cf27dcc6d/1436962438969/094.pdf, June 2015.
[12] Michael J. Lanham, M. J., Morgan, G.P. and Carley, K.M., "Social Network Modeling and Agent-Based Simulation in Support of Crisis De-escalation." *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 44(1): 103-110, 2014.