ARL-SR-0327 ● JUNE 2015

US Army Research Laboratory

Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report

by Alexander Kott, David Alberts, Amy Zalman,
Paulo Shakarian, Fernando Maymi, Cliff Wang, and Gang Qu

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

ARL-SR-0327 ● JUNE 2015

US Army Research Laboratory

Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report

by Alexander Kott, ***Computational and Information Sciences Directorate, ARL***

David Alberts, ***Institute for Defense Analyses***

Amy Zalman, ***World Future Society***

Paulo Shakarian, ***Arizona State University***

Fernando Maymi, ***Army Cyber Institute***

Cliff Wang, ***Army Research Office***

Gang Qu, ***University of Maryland***

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
June 2015	Final	

4. TITLE AND SUBTITLE
Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Alexander Kott, David Alberts, Amy Zalman, Paulo Shakarian, Fernando Maymi, Cliff Wang, and Gang Qu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army Research Laboratory
ATTN: RDRL-CIN
2800 Powder Mill Road
Adelphi, MD 20783-1138

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-SR-0327

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report describes the proceedings and outcomes of an Army-sponsored workshop that brought together a diverse group of intellectual leaders to envision the future of the tactical ground battlefield. The group identified and discussed the following 7 interrelated future capabilities that they felt would differentiate the battlefield of the future from current capabilities and engagements: augmented humans; automated decision making and autonomous processes; misinformation as a weapon; micro-targeting; large-scale self-organization and collective decision making; cognitive modeling of the opponent; and the ability to understand and cope in a contested, imperfect information environment. The workshop concluded that a critical challenge of the mid-21st century will involve successfully managing and integrating the collections, teams, and swarms of robots that would act independently or collaboratively as they undertook a variety of missions including the management and protection of communications and information networks and the provision of decision quality information to humans. Success in this aspect of command and control (C2) would depend upon developing new C2 concepts and approaches.

15. SUBJECT TERMS
Long-term technology forecast; information technologies; Cyber affects; Military History

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Alexander Kott
Unclassified	Unclassified	Unclassified	UU	60	19b. TELEPHONE NUMBER (Include area code) 301-394-1507

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Tables

INTENTIONALLY LEFT BLANK.

1. Introduction

This report describes the proceedings and outcomes of a workshop that brought together a diverse group of intellectual leaders to envision the future of the tactical ground battlefield. This workshop, organized by the University of Maryland (UMD) on behalf of the US Army Research Laboratory (ARL)/Army Research Office (ARO), took place on March 10–11, 2015, at the College Park Marriott Hotel & Conference Center located near the UMD campus in East Hyattsville, Maryland. This workshop focused its attention on the impact that information technologies (broadly understood) would have on tactical ground warfighting circa 2050. In describing the nature of the workshop to participants, this workshop was alternatively described as "Future Cyber Warfighting," and "Information Technologies and Ground Warfighting."

The dominant technologically driven changes, including those of warfighting, of the last few decades have had much to do with the technologies and concepts that are associated with the Information Age. Therefore, it could be assumed that the continuing evolution of information technologies (and possibly revolutionary changes) will continue to be one of the significant forcing functions that will shape related warfighting technologies and capabilities between now and 2050. For the purposes of this workshop, information technologies include robotics, smart munitions, ubiquitous sensing, and extreme networking, along with the potentially massive impact of cyber warfare. The workshop critically examined this "Information Age" assumption and its implications.

We recognize that information-related technologies will continue to advance between now and 2050, and that these advances and their commercialization will change the economics of communications and information and, thus, change warfare. As a result of these changes, the roles of information technologies will co-evolve (i.e., will influence and be influenced by) with future concepts and technologies for key warfighting functions, including seeing (sensing), understanding, communicating, moving, and applying kinetic and non-kinetic effects. Further, that these developments will spawn a cascade of countermeasures and counter-countermeasures; the net result will be what the future Soldier will see and experience on the tactical battlefield. Therefore, it is apparent that one cannot correctly visualize the future battlefield by focusing on the evolution of information technologies alone. Thus, to avoid a vision that incorporates a mismatch between 2050 information technology and warfighting tools and techniques of 2015, workshop participants were asked to simultaneously explore future visions of both the informational and physical aspects of the battlefield.

For the purposes of this workshop, the term "information technologies" was interpreted in its broadest sense. Included in this term is the wide range of information-related and -enabled capabilities that are involved in obtaining, collecting, organizing, fusing, storing, and distributing relevant information as well as the capabilities associated with command and control (C2) functions and processes including reasoning, inference, planning, decision making, and collaborating (between humans and between humans and "smart" and/or autonomous systems). Finally, this term includes the capabilities that could be used to deny, deceive, disrupt, degrade, and compromise adversary information and information-related processes (e.g., cyber and electronic warfare).

A few disclaimers are in order here. First, not every author of the report or participant of the workshop agrees with every (or any) opinion presented in the workshop's report. Second, all statements of fact or opinion presented in this report are those of the workshop participants and do not reflect positions or views of their employers or any organizations with which they are affiliated.

1.1 Workshop Scope and Assumptions

The scope of this workshop was limited to tactical ground warfighting circa 2050. The battlefield was assumed to be on the order of 100 km by 100 km and include a population center with significant numbers of civilians present. The unnamed combatants were assumed to be technologically sophisticated. To avoid implicit and potentially constraining assumptions about how technology would be employed (constraining rules of engagement), participants were asked not to assume that one of the adversaries was the United States. Besides engaging in "conventional" warfare, the opponents could be assumed to be capable of employing irregular warfare.

In order to avoid potential diversions, keep workshop discussions unclassified, and make the conclusions accessible to the widest audience, the following topics were not included in the scope of this workshop: current programs, requirements, policy, budget, socio-cultural and geopolitical issues, weapons of mass destruction (WMDs), inherently naval or airspace issues, and anything that was not publically releasable.

1.2 Workshop Orientation

To assist workshop participants in their "visioneering" efforts, they were presented with the following "time travel" scenario to consider.

> "Imagine that you were asleep from 2015 until 2050. Upon awaking you found yourself in the middle of an on-going battle. What do you see? How different is it from what you might have seen in 2015?"

To help participants relate to a forward leap of 35 years, they were asked to think about fellow time traveler, one who fell asleep in 1881 to awaken into the middle of World War I in 1916 and another who fell asleep in 1907 to awaken in 1942 during World War II.

The first traveler would have awakened to a number of technological advances that reshaped the nature of ground warfare. These included the machine gun and long-range indirect fire artillery, the latter being the biggest killer of WW1. They would have also seen for the first time airplanes used for reconnaissance; field phones used for artillery spotting and control; trench formations for protection; and the dawning of the era of tanks, which would eventually transform ground warfare. However, at least half of what the time traveler observed would have been familiar. Not all that was new, though, involved new equipment. Advances in concepts and methods dramatically improve warfighting capability as well by using assets in different ways. For example, indirect fire used the same piece of equipment that was previously only used for direct fire.

Participants were encouraged not only to think about specific technological developments, but also of capabilities that might be developed without regard to its enabling technology. For example, in 1880, it would have been difficult to envision exactly what technological advances would enable a flying apparatus, but not so difficult to imagine such objects in action.

1.3 Participant Presentations

After the orientation session, a set of presentations were provided by participants. The following presentations were given to stimulate discussion (see the Appendix for the slides for a number of these presentations):

- Unleashing the Power of Networking: Critical Research (David Alberts)
- Defining the Environment for Ground War in 2050 (JC Ledé)
- Information Fusion in 2050 (Ajay Divakaran, Behjat Siddiquie)
- Some "Random" Thoughts: Information Technologies and Ground Warfighting (Jason Li)
- Future War (Paulo Shakarian)
- A Few Thoughts (Greg Shannon)

- Context for Battlefield of 2050 (Lin Wells)
- Warfare at the Speed of Light (Michael Zatman)

1.4 Workshop Sessions

After these presentations and some discussion, workshop participants broke into 2 groups. The first breakout group was devoted to "seeing, communicating, understanding, and deciding" and the second to "moving, shooting, effecting, and sustaining." With the exception of the session leaders, participants switched sessions half way through the afternoon so that everyone could contribute to both topics. The first day concluded with a plenary session consisting of debriefs from the breakout sessions reporting on their discussions regarding the nature of the 2050 battlefield and related topics.

On day 2 of the workshop, each breakout group selected 5–10 key elements of their respective visions. For each of these key elements, they were charged with addressing the following 2 questions:

- What makes this development somewhat likely to emerge on the battlefield of 2050?
- What counteractions could opponents develop and employ in response?

The notes taken during these brainstorming breakout sessions and the plenary session presentations and discussions provided the basis for this report.

1.5 Workshop Participants

This was an invitation-only workshop, with invitations sent to individuals who had demonstrated an ability to think about the implications of emerging technology, particularly information technology, for military operations. Participants included not only individuals with a long association with the Department of Defense (DOD), but also individuals engaged in basic research and commerce applications. Table 1 provides the names and affiliations of the workshop participants.

Table 1 Workshop participants

Alberts, David S - Institute for Defense Analyses
Bullo, Francesco - University of California Santa Barbara
Chellapa, Rama - UMD
Divakaran, Ajay - SRI International Princeton
Dykstra, Josiah - National Security Agency
Hagerott, Mark – United States Naval Academy
Herr, Andrew – Helicase, LLC
Iyer, Purush - ARO
Jain, Manish – Armorway, Inc
Jajodia, Sushil - George Mason University
Kearns, Mike - University of Pennsylvania
Kott, Alex – ARL
Lede, JC - Defense Advanced Research Projects Agency (DARPA)
Li, Jason – IAI, Inc
Libicki, Martin – United States Naval Academy
Maymi, Fernando - Army Cyber Institute
Qu, Gang - UMD
Ray-Dulany, Walter - DOD
Scharre, Paul - Center for a New America Security
Shakarian, Paulo - Arizona State University
Shannon, Greg – Carnegie Mellon University (CMU)
Shin, Kang - University of Michigan
Subrahmanian, V.S. - UMD
Tambe, Milind - University of Southern California (USC)
Tucker, Patrick - Defense One
Wang, Cliff - ARO
Wells, Linton – National Defense University
Zalman, Amy - World Future Society
Zatman, Michael - SAZE Technologies LLC

2. Warfare in 2050: Seeing, Communicating, Understanding, and Deciding

This section summarizes workshop discussions and presents related findings with respect to what we called “seeing, communicating, understanding, and deciding.” Included in these battlefield capabilities are the methods, approaches, tools, and processes necessary to perform the functions associated with information preparation of the battlefield (IPB), C2, intelligence, surveillance and reconnaissance (ISR), and battle damage assessment (BDA).

2.1 Point of Departure for Discussion

The participants initiated the discussion of "seeing, communicating, understanding, and deciding" by considering the following questions:

- Should we anticipate the continuation of the current trend of rapid growth in the number of sensors on the battlefield to include sensors that are perhaps more mobile ground, air, more autonomous, micro-autonomous, along with human and social sensing?
- Would their density on the battlefield be orders of magnitude greater than today?
- Would they be extensively networked?
- Would the volume of resulting information be entirely beyond human management?
- How would these sensors be directed, controlled, organized, linked, and processed?
- How would one defeat such swarms of information collectors?
- Will we see widespread use of autonomous robots that seek and neutralize adversary sensors?
- Can we expect pervasive attacks on communication links and/or attacks on information processing nodes (cyber-attacks)?
- Will deception and dis-simulation greatly increase in importance?
- Will "deceptor" swarms be deployed?
- Will opponent's sensors be exploited as channels to present deceptive information, e.g., active multispectral camouflage and mimicry?
- Would this change the role and function of humans?
- Would the analysis of the enormous volume of information be handled largely by machines, with humans learning to collaborate with machines and thinking at higher levels of abstraction?
- Would far greater attention be devoted to counter-deception analysis with recognition that data and computations may be corrupted by cyber-attacks?
- Would augmented cognition become necessary?

- Would there be extensive attacks (via deception, confusion, etc.) on cognitive processes, individual and collective, of opponents C2?
- Will the Soldiers of 2050 simply abandon this morass of information and counter-information and find a way around all this unwieldy complexity? How?

2.2 Major Aspects of the Tactical Battlefield of 2050

The discussion of what major changes we could expect with respect to our ability to see, communicate, think, and decide on the tactical battlefield of 2050 was predicated upon a shared view that this battlefield would be characterized by the vastly increased presence and reliance on: automated processes and decision making; humans with augmented sensing; and information-related and cognitive capabilities. This breakout group posited that transport (getting capability to the battlefield) would not be a limiting consideration.

The group identified and discussed the following 7 interrelated future capabilities that they felt would differentiate the battlefield of the future from current capabilities and engagements:

- Augmented humans
- Automated decision making and autonomous processes
- Misinformation as a weapon
- Micro-targeting
- Large-scale self-organization and collective decision making
- Cognitive modeling of the opponent
- Ability to understand and cope in a contested, imperfect, information environment

For each of these developments, the group offered their reasons why they felt that these potential transformative capabilities would be found on the tactical battlefield of 2050. They discussed the ways that adversaries could counter or mitigate the effectiveness of these capabilities as well as how to counter to these counters.

2.2.1 Augmented Humans

The battlefield of the future will be populated by fewer humans, but these humans would be physically and mentally augmented with enhanced capabilities that improve their ability to sense their environment, make sense of their environment,

and interact with one another, as well as with "unenhanced humans," automated processes, and machines of various kinds. As a result, they would not only do things differently, but do different things compared to the human combatants of today with their limited forms of augmentation and enhancement.

This development can be reasonably expected by 2050 for a number of reasons. It is the logical extension of a number of current trends. There are a growing number of human capability enhancers that have been developed to help those who have suffered various injuries or have other disabilities. Great progress has been made in recent years to enhance vision, hearing, and cognitive skills. There are a growing number of devices that are being implanted in humans, and with each new and life-enhancing implant, there has been a growing acceptance of implants. Great strides have been made in enhancing the human-machine interface and this trend is expected to continue, enabling humans and machines to work together more "naturally." The computing power necessary for improving the performance and capability of these augmentations and enhancements is expected to increase at a rate sufficient to support new and more powerful enhancements that rely upon computational power. Miniaturization is expected to continue at an accelerating rate, which makes these capabilities more practical. Computer-assisted decision making is proliferating in virtually all aspects of our lives. The totality of these and other trends will make these capabilities available.

How can one counter the increased presence of "super-sensing and sense-making humans" on the battlefield? For one, these enhanced humans become high value targets and thus adversaries will focus more attention on neutralizing them compared to a "normal" human. The number of enhanced humans on the battlefield of 2050 will depend upon a number of factors, which include their organic capabilities and the expense necessary to equip, train, and support them. The general sense of workshop participants was that there will be relatively few of them. Thus, another counter would be to overwhelm them with large numbers of ordinary humans and/or machines. While these humans may be enhanced and may require less food and water to be sustained, they will likely be adversely affected by environmental conditions that are "hostile" for humans – radiation, chemical weapons, biological agents, and other area-denial techniques. An indirect means of countering "super human" capabilities would be to attack the supply chain needed to "develop and field" them, and thus, increase the cost of equipping and/or training. Finally, the computer capabilities inherent in augmented humans could be subject to spoofing, cyber-attacks, or other forms of electronic warfare. In addition, there are other attacks that would directly target the computer processors and communications capabilities needed to make super humans function as intended.

Countering these counters would involve developing better situation awareness of what could be encountered on the battlefield; reducing and protecting communications links (mobile networking); assuring our supply chain; and developing contingency plans that do not depend solely on augmented humans.

2.2.2 Automated Decision Making and Autonomous Processes

The tactical battlefield of 2050 will be qualitatively more automated with autonomous processes making many decisions that humans make today. Decision agents would be integral to all of the processes associated with C2, IPB, ISR, and BDA. The tasks that these agents would perform include filtering information, fact checking, fusion, dynamic access control (determining who has access to what information), and adaptive information dissemination (who should receive specific pieces of information and/or notifications). In addition, automated processes will task sensors (what to look at/for) and alter communications paths and priorities based upon their (machine) understanding of mission intent and context.

These developments are likely to occur because they are critically needed, because humans will simply be unable to keep up with information flows and the pace of the battle as they do not have sufficient information-processing capabilities and cognitive bandwidth. Furthermore, the barriers to acceptable forms of automated decision processes will be reduced as we continue to grow more accustomed to automated decision processes in our everyday lives and come to appreciate that automated processes can produce better decisions than humans can under certain conditions (time requirements, stress). As in the previous discussion, computer processing power will not be a limiting factor.

Among the potential counters for dramatically increased automation of key battlefield processes, including spoofing and denial of service attacks for information-dependent processes. Other counters include direct and indirect attacks on computer networks and communications capabilities. Counter-countermeasures include developing an increased ability to filter out extraneous and unauthenticated messages and a better understanding of how these automated processes work under various stresses and attacks so that they can be made more agile.

2.2.3 Misinformation as a Weapon

When the only information a Soldier received was from a few authoritative and trusted sources, determining the source of information was not a problem. Of course, this also meant that Soldiers often did not have sufficient understanding of intent and context, and thus, were less able to exercise initiative and proactively deal with dynamically changing situations. As information became separated from

the chain of command, Soldiers began to have access to more information sources, but inherited the problem of assessing the quality of information sources.

This trend will, by 2050, result in an "information-rich" environment (some would call this a condition of information overload) where it will be difficult for an individual to assess the quality (correctness, authenticity, security) of each piece of information. This makes directed misinformation attacks relatively hard to detect. Thus, a little well-placed misinformation could go a long way to undermine appropriate trust, sow confusion, delay decisions, and make decisions more likely to be in error. By 2050, we anticipate that sensory misinformation will be in use (spoofed inputs that fool various senses), thus providing more ways to confuse, delay, and redirect adversaries.

This development is likely, because it is increasingly easy to synthesize believable material that is, in fact, misleading. Misinformation (deception) has always been an attractive weapon because of its relatively low-cost and covert nature (it cannot be easily traced to its real source).

There are a number of ways to counter misinformation, the most direct and obvious of which is to be able to authenticate sources or have trusted sources available. Lest this not result in denying ourselves the full range of good information that is available, we need to be able to employ various forms of analyses (data mining and context analysis) to arrive at appropriate conclusions regarding the veracity of information. Other counters include training individuals to be vigilant and depend less upon the availability of "perfect" information. Another is to be better at misinformation than an adversary, which might deter them. The counter to the counter of adopting a trusted source strategy is to compromise trusted sources.

2.2.4 Micro-targeting

Micro-targeting represents a considerable revolution in the concepts and capabilities associated with current instantiations of precision strike. For example, instead of being able to identify and engage a particular building or moving vehicle while minimizing collateral damage, the concept of micro-targeting involves the identification and surgical engagement of specific individuals employing either kinetic or non-kinetic means.

Workshop participants felt that micro-targeting was likely because advances in our ability to penetrate individuals' cyber environments coupled with the ability to effectively mine the enormous amount of available information relating to individuals makes it possible to understand what actions would have the desired effect for a given individual, as well as making it possible to locate a given individual with precision. These make micro-targeting possible. Workshop

participants felt that weapons miniaturization would continue, thus making engagement and hence micro-targeting possible. Micro-targeting would be an extremely valuable capability as it provides more control, results in less collateral damage, and is less detectable.

By virtue of its properties, micro-targeting would be difficult to counter. However, the following counters are possible. Covert movements accompanied by deception and misinformation could thwart timely location. Decoys could be effective, as well. Targeted organizations could dynamically restructure their organization and their delegation of decision rights thus changing the target value of specific individuals. An adversary could decide to escalate raising the costs incurred.

Counters to these counters involve better situation awareness to detect attempts to evade detect, spoof, or misdirect a micro-attack.

2.2.5 Large-scale Self-organization

An expected feature of the battlefield of 2050 would be the existence of new, more edge-like approaches to command and control where individuals, teams, and software agents would, when appropriate, self-organize, dynamically creating and modifying collaborative processes. As a result, these self-organized entities would manifest emergent behaviors in response to the environment and the tasks to be accomplished. This development is necessary to enable the adoption of new distributed, "network enabled" C2 approaches that have been shown to be more agile (a capability that is a necessary response to the complexity and unpredictability of the battlefield of 2050). An associated major aspect of this battlefield development will be the seamless integration of human and machine decision making. As a result, battle rhythm will increase to the point that, in many instances, humans will no longer be able to be "in the loop," but will instead need to operate "on the loop." The difference being that in the former, human decisions are a required step in a process and thus humans are exercising positive control; while in the later, humans can only observe the behaviors that are taking place (and in some cases the decisions that have been made and the reasons why), but they can only act after the fact or in anticipation of expected behaviors.

Participants expected large-scale self-organization involving humans and software-controlled machines and systems to occur because examples of this behavior, in very limited forms, and at a modest scale, already exist. To a large extent, "proofs of concept" can be seen everywhere. Application-to-application sharing is no longer a new development and we are beginning to see the emergence of collections of collaborating self-synchronizing apps. Learning apps, apps that dynamically adjust to different humans and situations are in use today and people have accepted

them as a matter of course. Workshop participants expressed the view that this development was not "optional" given the large number of "decision makers" that will be present on the tactical battlefield of 2050, since, at a minimum, they will need to de-conflict with one another and, overtime, will learn to choose behaviors that create synergies.

Included among the "existence proof" are the following: application-to-application autonomous sharing is a current feature of groups of applications; learning applications and machine-assisted learning also exist; and the "intelligence" that enables "plug and play" is a forerunner of self-organization. These capabilities are widely accepted and even sought out by many consumers. In addition, self-organization is necessary in order to de-conflict the many entities that will share the battlespace of 2050.

To counter the effectiveness of distributed, self-organizing, and self-synchronizing collectives, adversaries could inject "moles" that behave in mischievous ways and attack cohesion and trust. Attacks on communications and processing capabilities are also an attractive option. The possible counters to a distributed adversary include preventing the development of shared awareness by sowing distrust to reduce or prevent information-sharing. Counters to attempts to prevent accurate shared awareness from being developed or maintained include the establishment of tamper-proof identification and embedded information provenance.

2.2.6 Cognitive Modeling of the Opponent

A vastly improved capability to understand an opponent and predict their actions will enable a new and potentially disruptive capability in this time frame. Directed at both populations and key adversary decision makers on an individual basis, this targeting capability is based upon an understanding of population and individual motivations, biases, cognitive processes, and decision-making styles. In addition, physical and physiological states will be capable of being known. In terms of both individuals and populations, it will be possible to sense their moods and whether or not they are vulnerable to deception or primed to act in a certain manner (resist or be passive).

In addition to the enablers of micro-targeting previously discussed that make this capability likely, by 2050, sensors of various kinds will be ubiquitous and include sensors on and inside humans that can provide the information to support individual, dynamic cognitive modeling (physical state has an impact on cognitive abilities and processing). In addition to having the information available to vastly improve individual cognitive modeling, such models offer the opportunity to disrupt adversary organizations and operations in a cost-effective manner when

compared to existing capabilities. Development of these models is already underway as business are trying to better understand us as consumers and micro-target us with advertisements. This “neuro-marketing” is getting more sophisticated every day.

Counters are difficult as we are constantly creating data with every movement we make and every product we research and purchase. However, if key individuals can build a public profile that is misleading, adversaries will not have accurate information to use and their models will be incorrect. Even by 2050, cognitive modelling will be relatively resource intensive, and thus, be limited to a small number of key individuals and somewhat homogeneous populations. Organizations that delegate decision rights more widely could spread micro-targeting resources too thin and make an adversary turn to the more complex problem of understanding and predicting collective behaviors.

Counters to actions that make it more difficult to identify and model key individuals and population centers include being able to react in near real time, reducing the need to predict.

2.2.7 Ability to Understand and Cope in a Contested, Imperfect, Information Environment

After a discussion of all of the improvements that could be expected in the quality of information, the workshop participants came to the conclusion that 2050 would not see the realization of the long-heralded era of perfect information. The attributes associated with the quality of information in this discussion included correctness, completeness, relevance, timeliness, precision, authenticity, secureness, uncompromisability, availability, trustedness, and ease of use. Participants concluded that on the battlefield of 2050 there would still be a significant amount of noise mixed in with information. Therefore, it would remain difficult to extract key information and identify misinformation, as well as identify unverified, unattributed, unsourced, and incorrect and/or out-of-date information.

What would be “new” would be individuals’ (and organizations’) ability to cope with an imperfect information environment and the ability to extract value in the form of actionable information. A major aspect of this new capability would be the ability to more accurately understand the imperfections and risks associated with the available information. Put another way, individuals would be far better consumers of information that is currently the case.

The participants felt this development was likely for a number of reasons. First, between now and 2050, individuals will have been born into this challenging information environment and, of necessity, will have developed information

survival skills. Second, there will be increased metadata tagging. Third, the multiplicity of sources assisted by information processing agents will help in verifying and cross-checking sources. Fourth, visualization tools will be vastly improved and help individuals deal with increased information. Fifth, organizations and processes will be more distributed and collaborative and thus be better able to bring a diverse set of eyes to the information.

The counters to this include more effective misinformation campaigns and attacks on information sources, processing, and communications capabilities.

The counters to these counters involve more training and better tools, as well as better defenses against information-related attacks.

2.2.8 Other Observations

While most of the discussion involved 1 of the 7 developments discussed above, the participants made a number of additional observations:

- Humans will take on a number of different roles vis a vis automated systems to include not only the traditional role of "human-in-the-loop," but also a new role "human-on-the-loop.'
- Micro-management will be rare, as mission command will be fully understood and practiced.
- It will be possible, at times, to take control of local or even adversary communications infrastructure and sensors.
- Situational awareness will include an understanding of the state of both friendly, local, and adversary networks and present a dynamic picture that can be used for a variety of purposes

3. Warfare in 2050: Moving, Surviving, Effecting, and Sustaining

This section summarizes the workshop discussions and presents related findings with respect to what we called "moving, shooting, effecting, and sustaining." Included in these are the battlefield capabilities of tactical maneuver, delivery of a diverse set of effects (lethal and non-lethal, kinetic and non-kinetic, and information and cyber-related), force protection, and logistics.

3.1 Point of Departure for Discussion

Workshop participants initiated their discussion of "moving, shooting, effecting, and sustaining" by considering the following questions:

- Will the trend toward highly intelligent weapon systems and munitions continue? Perhaps creating swarms of robo-munitions?
- Perhaps this trend would result in a convergence of robots and munitions: a smart killer that executes an assigned attack autonomously or in collaboration with distant human controller; these can be ground-mobile, air-mobile, or mixed-mode?
- Would the force consist largely of robotic shooters (vs. humans)?
- Would there be few humans manning platforms (e.g., tank with just 1 human pilot or 1 human to handle multiple tanks)?
- Will many (most?) of these robo-munitions be dedicated to hunting and killing the opponent's robo-munitions?
- What would this say about the required level of computational intelligence? Collaborative intelligence? Is it feasible by 2050? What would be feasible?
- Will such proliferation of machine intelligence in weapons and munitions engender massive use of electronic and cyber countermeasures? What forms might it take?
- Will the role of human Soldier change? How would Soldiers survive in this environment? What would be nature of their C2 or interactions with these munitions, counter-munitions, and electro-cyber weapons?
- If such “see” and “shoot” capabilities emerge, how would anything/ anybody move and survive on the battlefield? Would this imply short jumps between prepared strong points? A new era of trench warfare? Or mass use of stealth and deception in mobility, e.g., with informational smoke-screen? Perhaps hundreds of simulated movers, decoys, for each real one?

3.2 Major Aspects of the Tactical Battlefield of 2050

The discussion of what major changes we could expect with respect to our ability to move, shoot, effect, and sustain our forces on the tactical battlefield of 2050 was predicated upon a shared view that this battlefield would be characterized by the following:

- Ubiquitous robots
- Swarms and teams
- Dynamic hacking and spoofing

- Super humans
- Directed-energy weapons (DEWs)
- Force fields
- Reliable power sources

For each of these developments, the group offered their reasons why they felt that these potential transformative capabilities would be found on the tactical battlefield of 2050 and discussed the ways that adversaries could counter or mitigate the effectiveness of these capabilities, as well as counters to these countermeasures.

3.2.1 Ubiquitous Robots

Workshop participants envisioned the battlefield of 2050 as being populated by large numbers of autonomous entities of all kinds. These entities were referred to by participants as simply "robots." Many of these robots would be fairly similar to the systems that exist today, such as unattended ground sensors, small unmanned aerial vehicles (UAVs), and fire-and-forget missiles. However, their 2050 versions would possess significantly greater capabilities of machine reasoning and intelligent autonomy than those existing today. Participants saw these robots operating and maneuvering on the battlefield (in the battlespace) in a large variety of ways. They would move over the ground and in the air at low altitudes. Some of these would have locomotion that was bio-inspired. These robots would range in size from insect-sized entities to robotic vehicles capable of transporting a team of humans. They would also be "virtual" and able to navigate and "act" in cyberspace. The collection of battlefield robots would be robustly networked and capable of communicating and collaborating with one another, with a variety of systems, and with humans.

Many of these robots would have ISR-related roles with many (perhaps most) of them possessing autonomous sensors that would provide nearly continuous coverage of every inch of the battlefield. Other robots would act as intelligent, single-use munitions. These could operate in "teams," like wolf packs of fire-and-forget missiles and ground-crawling or jumping intelligent mines. Some of these robots would be employed in cyber/network defense, including defending electronic components resident on/in a human; serving as intelligent defense assistants able to prevent or warn about incoming threats, or acting in the role of advisors in complex decision-making tasks, such as performing a detailed course of action analysis prepared for local conditions observed in real time. These deployed robots would be capable of operating in a variety of "control" modes from total autonomy to active management by humans.

Adversaries could counter the effectiveness and utility of robots in a number of ways. An adversary could create physical obstacles to mobility and other robot capabilities. These particular counters could be mitigated by deploying a heterogeneous collection of robots with diverse forms of locomotion or providing a given robot with multiple modes of adaptive locomotion.

Another counter to battlefield robots involves engaging robots with conventional kinetic weapons or DEWs. To counter this counter, robots could be hardened in a variety of ways from the mundane to the very sophisticated with more sophisticated defensive measures involving the protection of high-value robots with a "force field" (discussed later in this section of the report).

Another counter involves attacks against robot power sources. To counteract such attacks, these power sources could be spatially dispersed, designed to have back-up alternative sources, involve wireless delivery of power, or have organic power sources. In the case of attacks on power sources, another counter would involve the robot's ability to detect the attack and adjust its behaviors in a variety of ways that reduce its power requirements.

Other counters to robots may be cognitive in nature. For example, spoof attacks that misdirect, degrade, or take control of a robot. To prevent spoofing attacks, robots could be deployed with bio- or behavior-based authentication. Another type of cognitive attack on robots would involve eroding trust, either the trust the human controller has in the robot or a robot's trust in information and orders received. These sorts of attacks could be mitigated or avoided by employing forensic introspection of robot behavior.

3.2.2 Swarms and Teams

Robots will commonly operate in teams or swarms in the battlespace of 2050 in the same way Soldiers act in teams today. These self-organized and/or collaborative collections of robots would operate with varying degrees of freedoms (from being actively managed to being autonomous) under dynamically established rules of engagement/priorities. Robot swarms and teams (as well as individual robots) would be assigned a variety of tasks. For example, as independent attack forces or as part of an orchestrated attack using a variety of weapons, as a collective defensive shield, and as a sensing field. Among the less obvious roles for a robot team, the participants of the workshop envisioned a team of robots warning civilians (e.g., in a battle raging in a mega-city environment) to keep away from dangerous areas and even acting as a defensive shield for the civilians against any stray projectiles.

The workshop viewed such collaborative robot/human behaviors as highly likely to be common in 2050. As one participant pointed out, the well-known video of robot quadrotors performing James Bond theme (https://www.youtube.com/watch?v=_sUeGC-8dyk) already gives a vivid suggestion of what a collaborative attack by an intelligent team of munitions might look like. The feasibility of this capability is further supported by what is believed to be the scalability of swarm behaviors and by the relative ease of manufacture and deployment of swarm-suitable (smaller) robots. Because collective, collaborative behaviors are critical for survival in a contested environment saturated with sensors and robo-munitions, sufficient research and development (R&D) efforts will have been required to achieve these kinds of swarming or teaming capabilities.

There are a broad range of means that could be used to defeat a swarm or team of robots. Physical nets of other physical obstacles could be used to deny or shield some areas from robots. Robots could be equipped to wire cutters or other means to penetrate a net or a shield. Alternatively, some of the robot team members could be assigned suicide missions where they would explode themselves in order to breech a net or shield. Swarms or teams of robots could be kinetically attacked using area weapons or a high volume of fire. A counter to this would be to disperse the swarm and concentrate it only for a short period of time when a combined effect is needed.

Another means of countering a collaborative robot formation would involve attacking their ability to communicate with one another and/or sense their environment. This could involve jamming, EM pulse (EMP), a cyber-hack, or an attack on robot communications capability. Robot networks could be made more agile and less vulnerable to such attacks by being equipped with several alternative modes of communications, making it difficult to jam or otherwise attack of all these modes simultaneously.

A different approach to countering swarms or teams of robots involves reverse-engineering a robot team's behavior to create a predictive model that would be helpful in designing a plan to prevent the robot team from achieving its mission. The ability of an adversary to understand and predict robot behaviors could be countered by introducing a stochastic element into the algorithms that determine robot behaviors.

3.2.3 Dynamic Hacking and Spoofing

Hacking involves the ability to penetrate a system and change it in some way (change code, scramble data, insert malware). The results of a hack attack could vary from a one-time compromise to creating a vulnerability that can be exploited

at will. Spoofing can be considered to be "behavior hacking." The intent of behavior hacking is to influence behavior by altering the information upon which behaviors are based. Both hacking and spoofing can be used in "agile" attacks that dynamically, as a function of the circumstances and conditions, select the effects that are created.

Dynamic hacking and spoofing is likely to be a prominent feature of the tactical environment circa 2050 because 1) the "attack surface" of robot teams and swarms is large, which makes these forms of attack highly attractive; and 2) increased interest and attention is being paid to research that would enables such attacks. This includes efforts to automate reverse engineering and intelligent vulnerability analysis.

The designers of robots are well aware of the likelihood of hacking and spoofing attacks, and hence, will endeavor to design individual robots, robot networks, and robot-to-robot and robot-to-human communications capabilities with this in mind. Efforts will therefore be made to increase their internal security, harden their communications, and make robot sensing and processing less vulnerable to hacking and spoofing. The addition of hardware-based security (hard points, kernels of trust) will serve to make them less vulnerable to hacking (but may make them unable to adapt as attack vectors change). In addition to these countermeasures, decentralization (employing mission command) will reduce the reliance on communications and large numbers of heterogeneous robots will make them more difficult to attack or attrite. Other countermeasures would involve increasing the agility of individual robots by enabling dynamic repurposing and/or building in an override feature that could be exercised by human controllers. As a last resort, responses to the degrading or disabling of robot formations should be included in contingency plans.

3.2.4 Super Humans

The principal Army unit operating in 2050 will be mixed human-robot teams. To enable humans to partner effectively with robots, human team members will be enhanced in a variety of ways. These super humans will feature exoskeletons, possess a variety of implants, and have seamless access to sensing and cognitive enhancements. They may also be the result of genetic engineering. The net result is that they will have enhanced physical capabilities, senses, and cognitive powers. The presence of super humans on the battlefield in the 2050 timeframe is highly likely because the various components needed to enable this development already exist and are undergoing rapid evolution.

There are a variety of means available to countering the presence of super humans, ranging from simply overwhelming them with numbers of less expensive robots, area munitions, and directed EMP. Given that the powers super humans possess will in large part depend upon communications (as least internal to the super-human) and computer processing, hacking and spoofing attacks are also an option.

To counter these attacks on high value super humans, such humans could be protected/shielded by robot clouds or force fields. Given their capabilities, super humans would employ tactics that exploit their unique qualities and capabilities. They would be designed and outfitted to be able to continue to function even when damaged and, as a last resort, "battle plan" contingencies designed to operate without effective super humans would be standard operating procedure.

3.2.5 Directed Energy Weapons

The promise of DEWs was described in a 2007 Defense Science Board report of the same name. This report states that "directed energy continues to offer promise as a transformational 'game changer' as the DOD encounters new asymmetric and disruptive threats, while facing increasingly sophisticated traditional challenges." Several DEW technologies that have shown promise have also presented significant challenges. These include high power micro and millimeter wave, and lasers of various kinds (solid-state, chemical, fiber), both airborne and ground. However, in the past decade, these technologies have received increased attention and, as a result of the progress that has subsequently been made on both the technologies themselves and the sources needed to power these weapons, workshop participants consider it likely that a variety of these weapons will be employed in 2050.

There are a number of ways that the intended targets of DEWs can counter their attacks. Targets can be designed with a variety of characteristics and techniques to reflect, refract, and disperse the energy directed at them. These include surface features and contours and the use of active defenses like chaff or dust. The use of multi-spectral decoys can be effective, as well as can the ability to rapidly maneuver out of the effective envelope of the attack. Intended targets can also use cover and concealment to avoid attacks. Attacking the DEW power source can also be an effective counter strategy.

3.2.6 Force Fields

Force fields consist of particles, energy, or waves that destroy, cripple, or otherwise interfere with objects that attempt to penetrate them. Given the variety, precision, and lethality of the weapons and the ubiquitous nature of the sensors that will be found on the battlefield of 2050, considerable attention will be devoted to developing force fields that can both help protect easy to locate assets and track

high value targets. Workshop participants believe that sufficient progress will be made to make it likely that force fields will be employed in 2050 for some of the same reasons given for DEWs. In addition, workshop participants felt that force fields would be developed because they are seen as a counter to DEWs. Furthermore, the decreasing utility and cost-effectiveness of armor make force fields attractive alternatives.

A counter to the deployment of a force field is to use faster, bigger rounds and/or shoot from closer in, because the shorter the range, the easier it is to defeat the force field. Along these lines increasing the volume of fire, employing barrages or fire swarms could overwhelm a force field. Depending upon the nature of the force field, adjustments to DEWs or other weapons may help them better penetrate. Alternatively attacking the power source and/or hacking the systems that are involved could also be effective counters.

3.2.7 Reliable Power Sources

Power is needed to operate all of the robots, the technologies that make humans "super," DEWs, as well as force fields. Some of these 2050 battlefield capabilities require a great deal of energy to function effectively. The reliable supply of this energy is essential for mission effectiveness.

Workshop participants felt that as a result of the considerable attention that is being paid to the development of improved power sources and power storage (lighter, more efficient, more cost-effective, faster recharge) that power would not be the limiting factor in the ability to deploy the technologies discussed in this report. Confidence in this assertion was increased as workshop participants also envisioned more sources of power on the battlefield than are found today, including the following:

- mobile nuclear power
- wireless power
- organic renewable power
- an ability to tap into the power infrastructure indigenous to the battlefield
- an ability to hijack an adversary's sources of power

A variety of attacks on power sources is likely on the battlefield of 2050. These include direct kinetic attacks, EMP, cyber, DEW, and force fields to prevent wireless power transmission, and employment of power "leeches."

Counters to these attacks would include treating power sources as high value targets and defend them accordingly (harden, conceal). Deploying ample backup power sources is also an attractive option.

3.2.8 Other Observations

While most of the discussion involved 1 of the 7 developments discussed above, the participants made a number of additional observations:

- invisibility cloaks
- signature reduction cocoons
- scavenging and synthesis of stuff to reduce the challenges of sustainment
- delivery of supplies by cruise missiles or by small robots
- subterranean mobility and survivability
- demise of armor
- high-fidelity, predictive modeling of influence operations
- collecting and modeling the data about individual adversaries
- reversible effects
- sensors as decoys

4. Summary and Conclusion

The diverse set of workshop participants painted a vivid picture of the battlefield of 2050, one that brought reality more in line with the science fiction and fantasy the public is accustomed to viewing in the cinema and reading about. A time traveler from today would be immediately taken with the "over-crowding" of the battlefield of 2050 populated by all manner of robots, robots that greatly outnumber human fighters, and robot-looking humans. Not immediately apparent to the time traveler, but critical in determining which of the adversaries would possess the decisive edge, would be the capabilities and autonomy possessed by the armies of virtual robots, the "intelligent" programs and processes to 1) collect, process, and disseminate information to develop situational awareness; 2) direct and manage collections of robots that were engaged in executing C2, combat-support functions, as well as combat missions; and 3) undertake a full range of defensive and offensive cyber operations.

A critical challenge of the mid-21st century will involve successfully managing and integrating the collections, teams, and swarms of robots that would act independently or collaboratively as they undertook a variety of missions including the management and protection of communications and information networks and the provision of decision-quality information to humans. Success in this aspect of command and control would depend upon developing new C2 concepts and approaches, in particular, developing and fielding an effective hybrid cognitive architecture that leverages the strengths of artificial intelligence and human intelligence to go along with the development of new robotic, communications, information, and systems technologies. From the various observations of workshop participants, the traditional balance between offense and defense may shift as it becomes more difficult for the defense to keep up.

INTENTIONALLY LEFT BLANK.

Appendix A. Workshop Participant Presentations

Army Workshop on
Emerging Cyber War-Fighting Technologies

Unleashing the Power of Networking:
Critical Research

Dr. David S Alberts
March 2015

My Focus

- My focus is not on what is technologically possible, but on what will be adopted and how well it will be exploited (leveraged)

- Thus, a focus on what is likely to shape our capabilities and those of our adversaries.

- Assumption - By 2050, the 'internet of everything' will exist; but the networking of everything will be constrained by our ability to take advantage of the opportunities presented by ubiquitous inter-connectivity and the data available.

Critical Workshop Questions

that
Identify Key Impediments to Harnessing 2050 era ICT
and Represent a Core Research Challenge

- How would 'it' be directed, controlled, organized, *protected and assured* …?
- Would this change the role and function of humans *and systems*?
- What would be the nature of C2 or the interactions between humans and *smart* weapons?

How will we 'C2' the 'Network of Everything' ?

'Day After' Inspired C2 Research Priorities

- We can shape 2050 capabilities by the choices we make now with regard to our research priorities and our approaches to C2 and Cyber
- Will our concepts and capabilities constrain us or make us more effective, efficient, and agile?
- This will depend upon our ability to:
  - understand and shape the behaviors (dynamic integrated design) of multi-genre composite networks to make them secure, effective, efficient and agile.
  - understand and dynamically balance the tradeoffs between human and automated decision-making

- Day After' - Look at some future scenarios (dystopian) and see what could be done to make the outcomes more advantageous to us

SRI International

Information Fusion in 2050

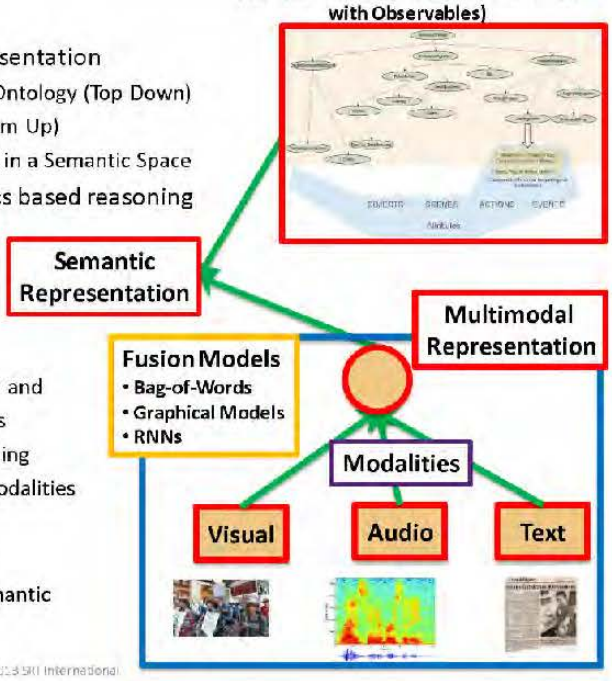
Ajay Divakaran Behjat Siddiquie

SRI International
Princeton, NJ

March 9th, 2015

Information Fusion

- **Semantic Representation**
  - Knowledge Base + Multimodal Representation
    - Concepts defined based on Functional Ontology (Top Down)
    - Concepts defined by observables (Bottom Up)
    - Concept Representation enables Fusion in a Semantic Space
  - Supports Spatial, Temporal, Semantics based reasoning and inference
- **Multimodal Representation**
  - Specifications
    - Handle co-occurrence, spatial, temporal and semantic relationships across modalities
    - Enable cross-modal prediction and priming
    - Handle incomplete information from modalities
  - Example Models
    - Bag-of-Words models – co-occurrence
    - Graphical models – spatio-temporal-semantic relationships
    - RNNs – compositional models



Information Fusion from Sensor Swarms

- **Swarms of Multi-Modal Sensors**
  - Swarm of hundreds or thousands of sensors gathering and streaming multimodal information
- **Information Fusion**
  - Detect *salient-important-relevant* sources of information and ignore extraneous content
  - Fusion should be able to scale-up to the number of sources, modalities and the high-fidelity data streams
  - Fusion should be able to deal with multiple asynchronos temporal streams of varying frequencies
- **Active Sensing**
  - Use current information to guide motion of the swarms
  - Focus on salient and relevant sources/modalities

Science, Aug 2014

Open Questions (Courtesy Alex Kott)

- **Fundamental or practical limitations of future information fusion?**
  - **Computational bounds. Perceptual limitations. Cannot think anthropomorphically**
- **Why did info fusion fail (or did not?) to deliver on the hype surrounding it in 2005-2010?**
  - **Expectations are anthropomorphic while systems are well short of human performance**
- **Would it deliver by 2050, and what would it be?**
  - **It will certainly deliver high volume naïve fusion and likely sophisticated fusion as well**
- **What can defeat info fusion of 2050?**
  - **Cyber-attacks, Counter-sensors, etc.**
- **What about cognitive constraints of human, or robots in dealing with fused info?**
  - **Humans can deal with human sensory fusion – Robots will need to transcend anthropomorphism**
- **What about deception or some form of injection/hiding of information?**
  - **With an exponentially larger number of sensors comes greater risk of that kind.**

Thank You!

Headquarters: Silicon Valley

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493
650.859.2000

Washington, D.C.

SRI International
1100 Wilson Blvd., Suite 2800
Arlington, VA 22209-3915
703.524.2053

Princeton, New Jersey

SRI International Sarnoff
201 Washington Road
Princeton, NJ 08540
609.734.2553

Additional U.S. and international locations

www.sri.com

Some "Random" Thoughts

Information Technologies and Ground Warfighting

"See/Understand"

- "All war is (based on) deception" – Sun Tzu
- The wisdom came from ground warfighting
- Broadly adopted for other contexts including cyber
- More sensors, information, fusion …
- Better situational awareness and coordination?
- At what level? Individual, squad, platoon?
- "Seeing is believing" and physical deception (smoke, decoy, etc.)
- In the future … "Sensing/perception is believing?"
- Reality vs. Virtual Reality → what is real?

Total Immersion? Human & Robots Integration?

- Virtual reality rules? Or is it real or augmented reality?
- Augmented reality – sounds great
- Immersive experience … we see what they can't see
- How much does this matter, on the ground, in cities, on mountains?
- Immersed and …. Drowned in our information ocean?
- Info-loaded vs. ammunition loaded
- How well can these IT cool tech integrated with ground troops "traditional" load-outs?
  - Example: current SOF operatives carry 4 radios with whip antennas; lots of problems with needed capabilities
  - Human factors and User Experience become drivers
- With Human + robots (e.g., Big Dog): consistent information; coordinated moves; kill chain in tactical environment; new ground warfighting paradigm

Deception & Denial (or Self-deception & denial?)

- Again physical vs informational deception
- Goal: affect adversaries' MIND and DECISION → this hasn't changed
- Physical distances matter
- Informational: not as much
  - More reachable
  - Asymmetric information warfare may become more prevalent
  - Deception & denial may go to higher levels: manipulating minds
  - Cyber attacks may broaden and escalate
- "The supreme art of war is to subdue the enemy without fighting"
  - More IT gadgets and info: Will they help or hurt?

Some questions (non-pessimistic)

- More is better? In what context?
- How much is too much?
- Ground warfighting then
  - "Know the enemy and know yourself"
  - "Victorious warriors win first and then go to war"
- Ground warfighting in 2050 (imaginary)
  - Fool the enemy and fool ourselves (more)?
  - Victorious warriors fool everyone first and then go to war?
  - Manipulating minds … to conquer?
  - What rules? How much does it really matter and when? Deal breaker? (Analogy: Martial arts master vs. machine gun?)

CySIS Cyber-Socio Intelligent Systems Laboratory

Thoughts on Emerging Cyber War-Fighting Technologies

Paulo Shakarian
Arizona State University
Tempe, AZ
shak@asu.edu

ASU Arizona State University

CySIS Cyber-Socio Intelligent Systems Laboratory

Old Way of Thinking…

"You don't need to outrun the bear – just the slowest guy."

- Intuition: Maintain a certain level of security to ensure the adversary passes you by for "low-hanging fruit"
- Best suited for: most cyber-crime, hardening important sites against terrorist incidents, etc.

ASU Arizona State University

CySIS Cyber-Socio Intelligent Systems Laboratory

Current Way of Thinking…

"If you build higher walls, they will just build higher ladders."

- Intuition: A purely defensive posture will lead to an arms race that the defender cannot win.
- Best suited for: cyber-warfare and any form of warfare that is offensive-dominated

ASU Arizona State University

CySIS Cyber-Socio Intelligent Systems Laboratory

Maybe even that is flawed…

"If you build higher walls, then maybe the adversary will tunnel underneath."

- Intuition: Paradigm shifts can occur.

ASU Arizona State University

Some Case Studies…

I. The Islamic State:

Fight like an army, melt like an insurgency

CySIS Cyber-Socio Intelligent Systems Laboratory

Study: Mining for Causal Rules

- We collected a dataset of 2,200 combat incidents concerning the activities of the Islamic State (ISIS) from June 1 – Dec. 27, 2014. Incidents were categorized into 159 event types.
- We also identified weeks where spikes (either 1 or 2 standard deviations above the 1-month moving average) occurred for certain events of interest (i.e. suicide attacks, VBIED's, executions, etc.)
- We combined methods for rule learning and measuring causality to identify potential causal relationships.

ASU Arizona State University

Preconditions for Armed Attack Spikes

No.	Precondition	ϵ_{avg}	p	p^*
1.	indirectFire($Baiji$)	0.81	0.67	0.50
2.	indirectFire($Baiji$)∧ armedAtk($Balad$)∧ VBIED($Baghdad$)	0.81	0.67	0.50

Here, ISIS fights like an Army.

CySIS Cyber-Socio Intelligent Systems Laboratory

Preconditions for Spikes in IED Usage

No.	Precondition	ϵ_{avg}	p	p^*
10.	airStrike($Coalition, Mosul$)∧ armedAtk($Fallujah$)	0.97	0.67	0.33

Here, ISIS operates like an insurgency.

Preconditions for Arrest Spikes

No.	Precondition	ϵ_{avg}	p	p^*
8.	airStrike($SyrianGov, Damascus$)	0.91	0.67	0.00

Here we think ISIS is operating like an occupying force – weeding out potential intelligence sources.

Some Case Studies…

II. The Evolution of Russian Cyber

CySIS Cyber-Socio Intelligent Systems Laboratory

Russian Cyber-Warfare

Estonia (2007): Massive hacktivist DDoS

Georgia (2008): Botnet driven DDoS followed by hacktivist DDoS for the purpose of silencing news media and government sites

LiveJournal (2011): Massive DDoS attacks by the Optima botnet to silence anti-Putin journalism

ASU Arizona State University

CySIS Cyber-Socio Intelligent Systems Laboratory

2014 Russian Cyber-warfare in Ukraine and Crimeia

- Small-scale cyber attacks by independent hacking groups
- Some disruption of communication networks between Crimea and Ukraine by conventional forces
- Ukraine parilaiment member phones hacked, and Ukraine gov't website down for 72 hours
- Sandworm Cyber-Espionage platform (discovered Oct. 2014)
- No large denial of service on the scale of Estonia, Georgia, or LiveJournal
- **Where are the big DDoS attacks?**

ASU Arizona State University

"Information war is now the main type of war"

Dmitry Kieselev, the Kremlin's Chief Propagandist

CySIS Cyber-Socio Intelligent Systems Laboratory

Russian Policy

- Consider Russia's 2007 Foreign Policy Review
  - Describes "Human Rights Problems" experienced by native Russians in other countries ("Compatriots Abroad") and asserts that Russia must take an aggressive stance to protect their human rights
    - Ethnic Russian's, Russian speakers, Individuals who have been "Russianized" under the USSR
  - Russia's informational policy:
    - Create information campaigns in any place where Russian interests are challenged
    - Russia must develop its own means of information influence abroad
    - Russia must counteract anti-Russian information threats

ASU Arizona State University

CySIS Cyber-Socio Intelligent Systems Laboratory

What's the point…

- If you want insights into how tactics evolve, we should also consider the goals of the adversary
  - ISIS needs to retain land. The legitimacy of their caliphate hinges upon them holding and retaining ground – hence they need to protect the force while maintaining significant presence of their territories
  - Russia has informational goals – even when DDoS was used, they were trying to increase the amount of time they have to achieve tactical operations.

ASU Arizona State University

CySIS Cyber-Socio Intelligent Systems Laboratory

Thank You!

Contact shak@asu.edu for more information or visit http://shakarian.net/paulo

ASU Arizona State University

A few thoughts

G.Shannon
March 2015

Army Power

- Nye's "theory" of power
  - –Soft to medium to hard

Army Power

- Nye's "theory" of power
  - –Soft to medium to hard
  - –The army projects power
    - precision "metal on target" at scale

Army Power

- Nye's "theory" of power
  - –Soft to medium to hard
  - –The army projects power
    - precision "metal on target" at scale
  - –Kill ratio matters

IT technology trajectory

- 1980 v. 2015 v. 2050

IT technology trajectory

- 1980 v. 2015 v. 2050
- 6 orders of magnitude
  - 1Mbyte, 1Tbyte, 1Xbyte
  - 110 baud, 1Gbit, 1Xbit
  - KIP, GIP, XIP

Role of Computing

- Human's are failing today
  - Cybersecurity, assurance, IEDs

Role of Computing

- Human's are failing today
  - Cybersecurity, assurance, IEDs
- Compute everything
  - Prove everything
  - Model everything
  - Anticipate everything

Key Threat

- Moral constraints limit your thinking
  - Many innovations were considered immoral
  - The adversary will violate our limits

Context for Battlefield of 2050

- Trends and Shocks
  - Demographics; Economics; Energy and Environments; Identity, Culture & Governance; Nature of Conflict; S&T
  - Pace of tech change: if capability per unit costs doubles in 18 mo → 5 years up 900%, 10 years 10,000% Linear projects CANNOT work
    - 8 years ago smart phone didn't exist. In a few years half the planet will have a supercomputer and networked sensors in their pocket
    - What are OPSEC implications of every person a sensor, plus SkyBox, etc.
- Converging tech: BRINE (bio, robo, info, nano, energy)
  - Foresight, international governance, Public-Private Cooperation, Workforce Development
  - GeoInnovation
  - Democratization of Tech. IoT→ Cloud of Everything (but functionality trumps security)
  - What tech will children of today's graduate students use to befuddle their parents
- Tech is never enough. Must address People, Processes, Organizations and Technology
- Other studies:
  - Tom Friedman: The World is Fast: The Market, Mother Nature, Moore's Law
  - SMA work on Megacities
  - Bill Coleman—Evolution of the Information Age→constant empowering of the edge, information at the wall socket
  - Wicked problems—challenge assumptions, iterative approaches
  - USAF—Man-on –the-loop, vice Man-in-the-loop
- Implications
  - Cyber trumps OODA loop
  - Battle of the narrative—wars won and lost in living rooms of electorates
  - Can imagine combined arms warfare in Siberia
  - Megacities will swallow any army
  - What honors will be accorded to future robot-augmented warrior?

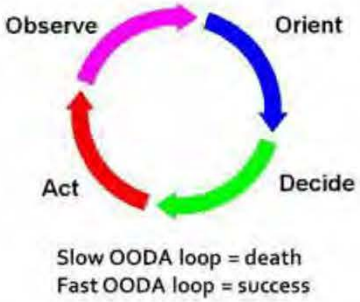
Other work:

- DTP-50: Assessment of STAR 21
- DTP-92: Enhancing Army S&T

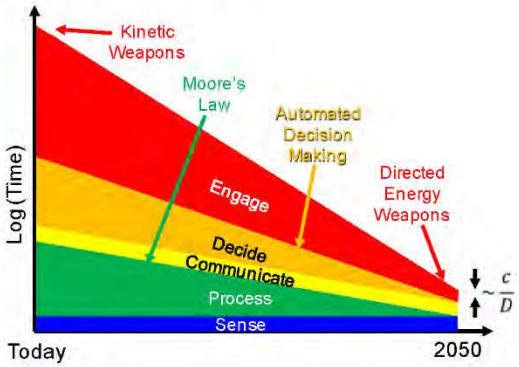
Warfare At The Speed of Light

SAZE TECHNOLOGIES, LLC

Engagement Timeline



Slow OODA loop = death
Fast OODA loop = success



- Military success depends upon two factors:
  - Lethality and speed of your weapons.
  - Strength and agility of your defenses.
  - Ability to get inside your adversary's decision loop.
- Today the propagation time for sensing and communication is a small fraction of the engagement timeline
- In 2050 the propagation time may be the majority of the engagement timeline
  - Directed energy weapons (e.g. lasers) propagate at the speed of light

SAZE TECHNOLOGIES, LLC

Commercial Example

Alpha, New Jersey, is a sleepy hamlet in the Lehigh Valley, near the Delaware River. Somewhere in town (the owners won't say exactly where) is one of ten 2,000-square-foot amplifier facilities that dot the landscape every 75-or-so miles between Chicago and New York City, ensuring that fiber-optic signals travel between the two points as clearly and quickly as possible. Spread Networks, the firm that operates the facility, may have seen some poetry in the community's name—"alpha" is the term investment managers use to describe the performance of an investment after adjusting for risk.

Spread is part of a growing industry dedicated to providing hyperspeed connections for financial firms. A faster trader can sell at a higher price and buy at a lower one because he gets there first. A connection that's just one millisecond faster than the competition's could boost a high-speed firm's earnings by as much as $100 million per year, according to one estimate.

Because of this, trading firms are increasingly pushing the limits to establish the fastest connections between trading hubs like New York, Chicago, and London. Every extra foot of fiber-optic cable adds about 1.5 nanoseconds of delay; each additional mile adds 8 microseconds. That's why companies like Spread have linked financial centers to each other by the shortest routes possible. Spread's Alpha facility is one of more than a dozen similar centers arrayed along the path of its 825-mile-long, $300 million fiber-optic cable between Wall Street and the Chicago Mercantile Exchange. Spread reportedly charges traders as much as $300,000 a month to use its network. Exchanges like the NYSE charge thousands of dollars per month to firms that want to place their servers as close to the exchanges as possible in order to boost transaction speeds. Industry experts estimate that high-speed traders spent well over $2 billion on infrastructure in 2010 alone.

SAZE TECHNOLOGIES, LLC

Cont.

Traders' need for speed has grown so voracious that two companies are currently building underwater cables (price tag: around $300 million each) across the Atlantic, in an attempt to join Wall Street and the London Stock Exchange by the shortest, fastest route possible. When completed in 2014, one of the cables is expected to shave five to six milliseconds off trans-Atlantic trades.

But why stop there? One trading engineer has proposed positioning a line of drones over the ocean, where they would flash microwave data from one to the next like the chain of mountaintop signal fires in *The Lord of the Rings*.

Propagation is air is faster than propagation in fiber!

Propagation time is already a significant factor in "Financial Warfare"

SAZE TECHNOLOGIES, LLC

What Does This Mean for the DoD and The Army?

- Minimizing propagation time for sensing, communications and the weapon will be important.
- Locating the sensor, decision maker and weapon closer to the enemy is better – Go Army!
- The end of radar?
  - It has to propagate two ways instead of one, which means it takes twice as long to sense!

SAZE TECHNOLOGIES, LLC

List of Symbols, Abbreviations, and Acronyms

ARL	US Army Research Laboratory
ARO	Army Research Office
BDA	battle damage assessment
C2	command and control
CMU	Carnegie Mellon University
DARPA	Defense Advanced Research Projects Agency
DEWs	directed-energy weapons
DOD	Department of Defense
EM	electromagnetic
EMP	EM pulse
IPB	information preparation of the battlefield
ISR	intelligence, surveillance and reconnaissance
R&D	research and development
UAVs	unmanned aerial vehicles
UMD	University of Maryland
USC	University of Southern California
WMDs	weapons of mass destruction

1 (PDF) DEFENSE TECHNICAL INFORMATION CTR
DTIC OCA

1 (PDF) GOVT PRINTG OFC
A MALHOTRA

2 (PDF) DIRECTOR
US ARMY RESEARCH LAB
RDRL CIO LL
IMAL HRA MAIL & RECORDS MGMT

2 (PDF) DIR USARL
RDRL CIN
A KOTT
RDRL CIN T
ANANTHRAM SWAMI

1 (PDF) INSTITUTE FOR DEFENSE ANALYSES
D ALBERTS

1 (PDF) WORLD FUTURE SOCIETY
AMY ZALMAN

1 (PDF) ARIZONA STATE UNIVERSITY
PAULO SHAKARIAN

1 (PDF) ARMY CYBER INSTITUTE
FERNANDO MAYMI,

1 (PDF) ARMY RESEARCH OFFICE
CLIFF WANG
PURUSH IYER

3 (PDF) UNIVERSITY OF MARYLAND
GANG QU
RAMA CHELLAPA
VS SUBRAHMANIAN

1 (PDF) UNIVERSITY OF CALIFORNIA SANTA BARBARA
FRANCESCO BULLO

1 (PDF) SRI INTERNATIONAL PRINCETON
AJAY DIVAKARAN

1 (PDF) NATIONAL SECURITY AGENCY
JOSIAH DYKSTRA

2 (PDF) UNITED STATES NAVAL ACADEMY
MARK HAGEROTT
MARTIN LIBICKI

1 (PDF) HELICASE, LLC
ANDREW HERR

1 (PDF) ARMORWAY, INC
MANISH JAIN

1 (PDF) GEORGE MASON UNIVERSITY
SUSHIL JAJODIA

1 (PDF) UNIVERSITY OF PENNSYLVANIA
MIKE KEARNS

1 (PDF) DARPA
JC LEDE

1 (PDF) IAI, INC
JASON LI

1 (PDF) DOD
WALTER RAY–DULANY

1 (PDF) CENTER FOR A NEW AMERICA SECURITY
PAUL SCHARRE

1 (PDF) CARNEGIE MELLON UNIVERSITY (CMU)
GREG SHANNON

1 (PDF) UNIVERSITY OF MICHIGAN
KANG SHIN

1 (PDF) UNIVERSITY OF SOUTHERN CALIFORNIA (USC)
MILIND TAMBE

1 (PDF) DEFENSE ONE
PATRICK TUCKER

1 (PDF) NATIONAL DEFENSE UNIVERSITY
LINTON WELLS

1 (PDF) SAZE TECHNOLOGIES LLC
MICHAEL ZATMAN