



Will Cybersecurity Dictate the Outcome of Future Wars?

Alexander Kott, US Army Research Laboratory

David S. Alberts, Institute for Defense Analysis

Cliff Wang, US Army Research Office

A recent workshop envisions the impacts that information and communications technology advances will have on warfare by 2050 and the challenges these pose for command and control.

By the year 2050, advances in information and communications (ICT) technologies will transform the battlefield as we know it today. Systems that obtain, collect, organize, fuse, store, and distribute relevant data will support a wide range of command-and-control processes including reasoning, inference making, planning, decision making, and human-human and human-machine collaboration. In addition, electronic and cyber warfare systems will improve our capacity to deceive adversaries and disrupt, degrade, or deny their ICT capabilities.

In March 2015, more than 30 technologists, scientists, military professionals, and futurists attended a workshop organized by the University of Maryland and sponsored by the US Army Research Office to envision the novel

features of a hypothetical conflict in 2050—not necessarily involving the US—based on current technology trends and their projected application to warfare. Here we explore some of the insights that emerged from those discussions.

Workshop participants concluded that the 2050 battlefield will be defined by three novel elements: the prevalence of intelligent warfare and support system; a human force with enhanced physical and cognitive abilities; and a complex, highly contested information domain. Combatants who can more effectively command and control these elements are more

likely to prevail, making cybersecurity—or the lack thereof—a key factor in determining the outcome of future conflicts.

UBIQUITOUS INTELLIGENT SYSTEMS

Fueled by steady advances in machine perception and reasoning, robots and other intelligent systems operating with varying degrees of autonomy will be ubiquitous on the 2050 battlefield.¹ These systems will selectively collect and process information, support sense making, and—with appropriate human oversight—undertake coordinated offensive and defensive actions.

Many will resemble more compact, mobile, and capable versions of current systems such as unattended ground sensors, unmanned aerial vehicles (drones), and fire-and-forget missiles. Such systems could carry out individual

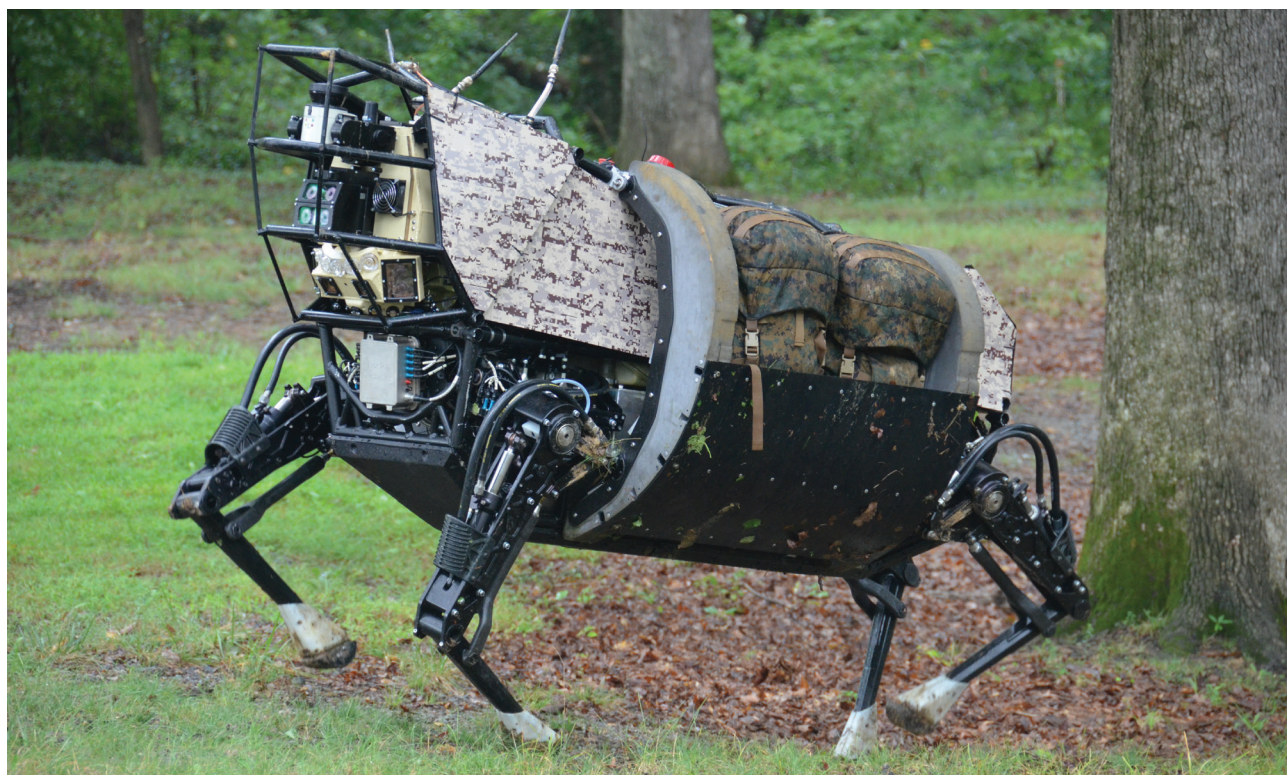


Figure 1. Robots will be a common presence on future battlefields, and many companies are already developing prototypes with support from US government agencies such as the Department of Defense's DARPA. One such prototype is the Legged Squad Support System, a robotic packhorse designed to operate in rough terrain and weather conditions. (Source: DARPA)

actions, either autonomously or under human control, collectively provide persistent and complete battlefield coverage as a defensive shield or sensing field, or function as a swarm or "wolf pack" to unleash a powerful coordinated attack.

Other intelligent systems will be robots with bio-inspired locomotion ranging in size from insects to humans to horses (see Figure 1), while others will be midsize vehicles—for example, troop transports—that move over the ground or in the air.² Still others will be virtual entities embedded in various systems, including wearables, to protect communications and information, prevent or warn about incoming threats, and advise decision makers. Virtual robots or cyberbots could

disguise their host's presence in the physical and information domains, as well as penetrate adversary systems to carry out proactive actions such as deceiving adversaries into making false observations and wrong decisions.

Systems that perform these roles on the battlefield will be robustly networked, interacting in real time with one another and their human controllers and clients. When required, they will self-organize. Using dynamically established priorities and rules of engagement, cyberbots will help determine each system's degree of autonomy. They will fact-check, filter, and fuse data; determine who has access to what information and disseminate it adaptively; route communications; assign tasks to

sensors; and coordinate actions with other cyberbots or robots.

Executing so many critical functions, intelligent systems will be valuable targets and present a large attack surface for adversaries. They will be particularly vulnerable to attacks targeting their information, information processing, and communications, in addition to being subjected to physical attack or capture. Security will therefore be a paramount consideration in the design and operation of intelligent warfare systems and their supporting networks.

HUMAN WARRIORS WITH SUPERHUMAN ABILITIES

The 2050 battlefield will be populated by fewer humans, who will carry out



Figure 2. Exoskeletons will serve future warriors as “personal combat vehicles” that provide greater ballistic protection, strength, endurance, and load capacity. Embedded computing and networking technology will likewise augment soldiers’ cognitive abilities. (Source: Daren Reehl; www.army.mil/-images/2007/01/07/1718.)

many of the same tasks they do today but very differently as well as do very different things. Human-robot teams will be the primary military unit, and cognitive and physical augmentation will increase soldiers’ lethality while reducing the risks of combat-related death or injury.

Cognitive augmentation in the form of advanced visualization and communication tools will improve future warriors’ ability to quickly sense and understand their environment, achieve accurate situational awareness, and interact with other personnel as well as various intelligent systems.³ The smartphone has already dramatically

extended our ability to obtain, process, and communicate information, and it’s safe to say that future ICT will revolutionize the collection, processing, and distribution of data on the battlefield as well as in the civilian world: soldiers will know more about the enemy, their surroundings, and the deployment of friendly forces, and thus will be able to adapt more quickly and effectively to circumstances.

Soldiers will regularly partner with both autonomous and human-operated robots—for example, to detect explosives or enemy combatants in a building, obtain tactical intelligence, patrol an area, deliver supplies, or recover wounded comrades. Wearable devices will provide seamless access to information and computing power. Augmented cognition technologies⁴ will improve reaction times, heighten concentration and alertness, reduce

fatigue, and even enable weapon control through thought.

In addition to cognitive augmentation, physical augmentation in the form of exoskeletons will provide soldiers more ballistic protection and enable them to move faster, stay in the field longer, and carry more gear (see Figure 2).

Workshop participants noted that with so much reliance on computing devices, the warriors of 2050 will be vulnerable—like robots and cyberbots—to various information attacks including denial-of-service attacks, eavesdropping, exploits, and spoofing. In addition, electromagnetic and

directed-energy attacks can compromise embedded computers and networks to prevent communication, collaboration, and access to processing power and information sources. Creating resilient, sustainable cyber-systems is thus critical to supporting augmented warriors.

COMPLEX AND CONTESTED INFORMATION DOMAIN

With so many smart, sharp-eyed entities blanketing the battlefield and reporting their detailed observations, hiding from the enemy will be much more difficult in 2050. At the same time, detecting the enemy’s presence and assessing his true intentions will be complicated by increasingly sophisticated misinformation and deception technologies: the ability to synthesize believable falsehoods and deliver these to adversaries through various network and malware channels will make it harder to assess the quality, correctness, authenticity, and security of data. In these circumstances, workshop participants concluded that the ability to extract valuable and reliable information while preventing adversaries from doing the same will become decisive in future wars.

This state of affairs is a direct result of the transition from Industrial Age to Information Age warfare.^{5,6} Until quite recently, a soldier only received information from a few authoritative and trusted sources. Today’s soldiers have access to more data than ever before, but this comes at a price: as information flows separate from the chain of command, assessing that information’s quality and trustworthiness become more challenging.

Disinformation attacks—particularly in cyberspace—are difficult to detect and, when undetected, sow mistrust and confusion as well as delay and undermine decision making.⁷ On the 2050 battlefield, exploiting accurate and useful information, and denying that ability to the enemy, will be more critical than ever before in the history of warfare.⁸

COMMAND AND CONTROL: A CRITICAL CHALLENGE

Deploying and managing assets on a crowded battlefield is already complicated; with the proliferation of autonomous and semiautonomous intelligent systems, soldiers augmented with ICT, and a complex and dynamic information domain subject to interference and manipulation by the enemy, this task could become almost overwhelming. This has profound implications for future command and control and the systems that support it.⁹


Existing command-and-control approaches consist of a set of hierarchical variants that have proven to work well in different situations. However, research and recent experience show that these approaches are not well-adapted to the enormous complexities of the 2050 battlefield. To prepare for future conflicts, military planners must devise strategies to

- ▶ manage the disparate new force-structure elements—including drone swarms, human-robot teams, and super-soldiers—to act independently, collectively, and in collaboration with traditional units as the situation requires; and
- ▶ monitor and protect the vast communications and information networks required to enable effective command and control.

Workshop participants envisioned a future in which a heterogeneous collection of entities can self-organize on a large scale and where collective decision making is the norm. This more collaborative, networked approach to command and control is critical to winning the unseen information war and, ultimately, prevailing on the battlefield.

It's important to add that workshop participants assumed that their hypothetical combatants complied with a ban on "offensive autonomous weapons beyond meaningful control" as called for in a recent open letter by

numerous scientists concerned about a potential AI arms race and the development of *Terminator*-style killer robots (<http://futureoflife.org/open-letter-autonomous-weapons>)—a concern we fully share. Although the US Department of Defense imposes strong restrictions on such systems,¹⁰ it's impossible to predict what other countries will do.

Warfare will continue to be transformed by ICT advances. Humans and human-operated devices and machines will still dominate the 2050 battlefield, but a large part of the decisive battle will be over information itself. As computing technology increasingly permeates weapons and command-and-control systems, the ability to leverage and protect that technology, and to prevent adversaries from doing likewise, will be as critical as physical force. Cybersecurity—or insecurity—could very well dictate the outcome of future wars. 

REFERENCES

1. P. Scharre, *Robotics on the Battlefield Part II: The Coming Swarm*, Center for a New American Security, Oct. 2014; www.cnas.org/sites/default/files/publications-pdf/CNAS_TheComingSwarm_Scharre.pdf.
2. H. Liu et al., eds., *Robot Intelligence: An Advanced Knowledge Processing Approach*, Springer, 2010.
3. D.D. Schmorow and C.M. Fidopiastis, eds., *Foundations of Augmented Cognition: Advancing Human Performance and Decision-Making through Adaptive Systems*, LNAI 8534, Springer, 2014.
4. C.A. Miller and M.C. Dorneich, "From Associate Systems to Augmented Cognition: 25 Years of User Adaptation in High Criticality Systems," *Foundations of Augmented Cognition*, 2nd ed., D.D. Schmorow, K.M. Stanley, and L.M. Reeves, eds., Strategic

Analysis, Inc. and ACI Society, 2006, pp. 344–353.

5. M. Libicki, *What Is Information War?*, Institute for Nat'l Security Studies, Nat'l Defense Univ., 1995.
6. D.S. Alberts, *Defensive Information Warfare*, Institute for Nat'l Security Studies, Nat'l Defense Univ., 1996.
7. A. Kott, ed., *Information Warfare and Organizational Decision-Making*, Artech House, 2006.
8. S. Jajodia et al., eds., *Cyber Warfare: Building the Scientific Foundation*, Springer, 2015.
9. A. Herr, "Will Humans Matter in the Wars of 2030?," *Joint Force Q.*, vol. 77, 1 Apr. 2015, pp. 76–83.
10. US Dept. of Defense Directive 3000.09, 21 Nov. 2012; www.dtic.mil/whs/directives/corres/pdf/300009p.pdf.

DISCLAIMER

This article does not reflect the positions or views of the authors' employers.

ALEXANDER KOTT is chief of the Network Science Division at the US Army Research Laboratory, where he leads research in network behavior and security. Contact him at alexander.kott1.civ@mail.mil.

DAVID ALBERTS is a Senior Fellow at the Institute for Defense Analysis, where he explores issues related to agility and command and control in a networked environment. Contact him at dalberts@ida.org.

CLIFF WANG is chief of the Computing Science Division at the US Army Research Office, where he manages a portfolio of research in cybersecurity. Contact him at cliff.x.wang.civ@mail.mil.



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.