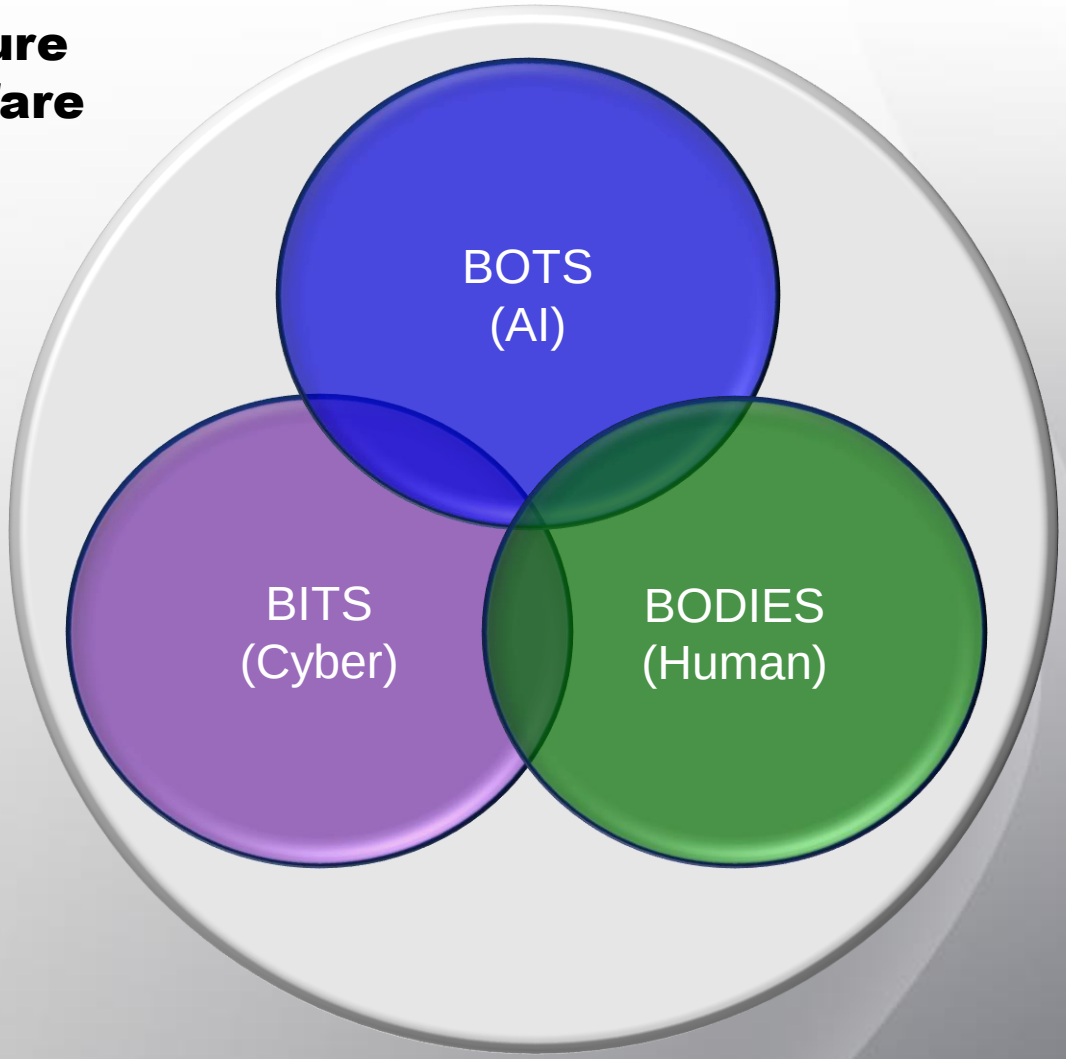
AI, Robotics and Cyber: How Much will They Change Warfare?

Dr. Alexander Kott

ARL Chief Scientist

Bits, Bots, Bodies

Future Warfare



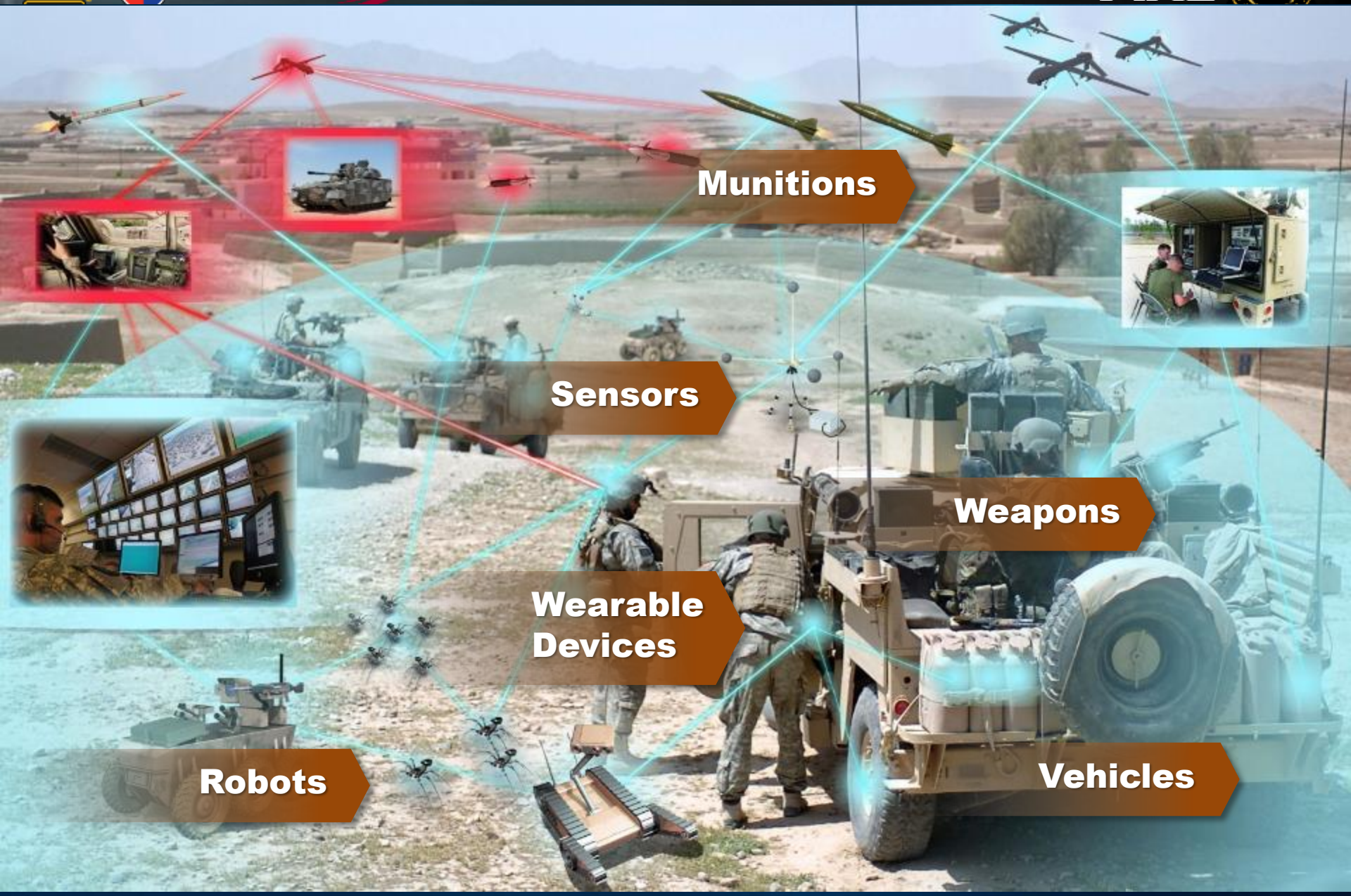
AI, Cyber, Humans in a Very Complex World

Everything is Connected

- AI is making the world more intelligent
- AI makes the world harder to manage
- AI makes the world more vulnerable to cyber
- Humans complicate things for AI
- Humans can add resilience
- Cyber thrives on attacking AI
- Cyber and humans don’t mix well
- Cyber defense will benefit from AI

AI and Cyber Make Warfare Increasingly Complex

Intelligent Things will be Diverse



U.S. ARMY RDECOM

They will Perform a Variety of Tasks

ARL 25

Sense

Attack

Collect & Process Information

Fix

Sustain

Communicate

Defend

Collaborate
with each other
& human Soldiers

The Complexity Becomes Enormous

Number of nodes for a future Army brigade might be several orders of magnitude greater than in current practice

Million Things per square kilometer is not an unreasonable expectation

Can be advantageous: availability of very large, densely-positioned number of Things, such as sensors

U.S. ARMY RDECOM

Human Cognition will be Challenged

ARL 25

Will far exceed advances predicted by Moore's Law

Will far exceed any likely improvements in bandwidth

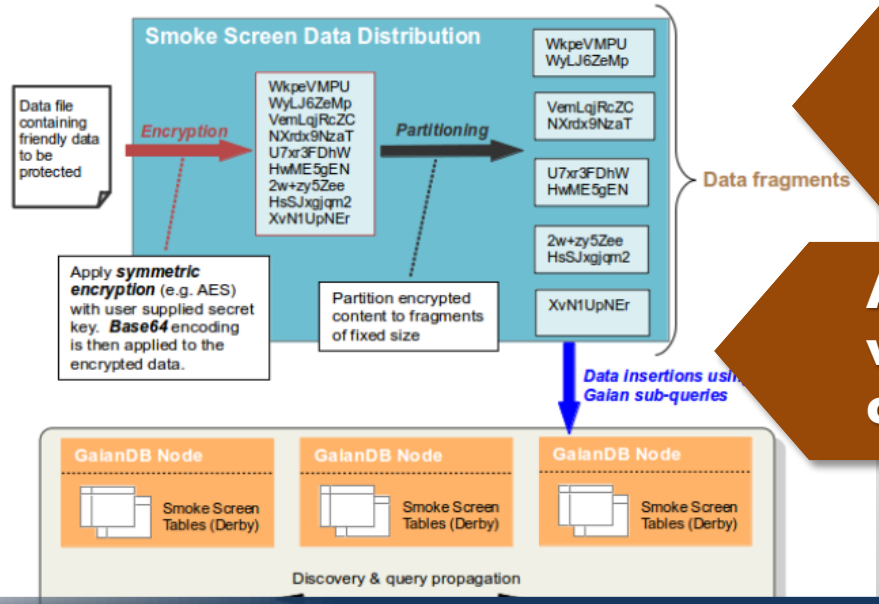
Volume and complexity of information will be truly unprecedented in their extent

Similarly, trustworthiness and value of information arriving from different things will be highly variable

Compression and fusion of data into information would have to be by a factor of 10^15

Beyond Big Data

Complexity of Intelligent Things: Use it as a Smoke Screen?



Friendly forces will be challenged to find, manage, aggregate information

Any one device and its information is vulnerable to cyber or physical capture

Use Intelligent Things to disperse friendly information, make any one device useless to the adversary

Increase resiliency, confuse and deceive the adversary

Kott, A., Swami, A., and West, B., "The Fog of War in Cyberspace," IEEE Computer, November 2016
Wampler, Jason A., et al. "Heterogeneous information sharing of sensor information in contested environments." *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII*. Vol. 10190. 2017

Turn Complexity into Your Weapon

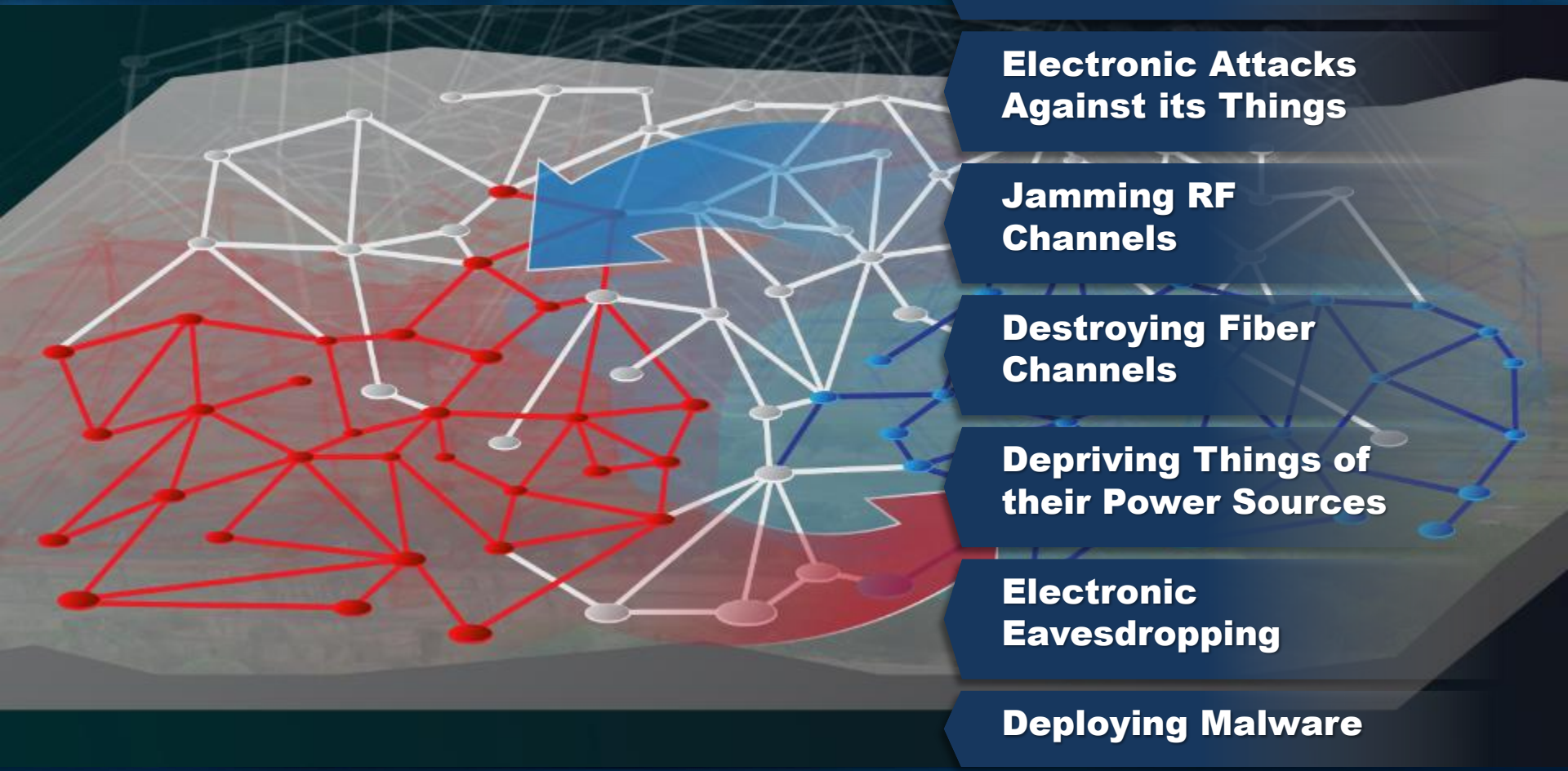
AI and Cyber Multiply Threats and Vulnerabilities

U.S. ARMY RDECOM

Intelligent Things are Threats and Targets

ARL 25

Pervasive connectivity and intelligence open opportunities for cross-domain attack and defense



- **Kinetic**
- **Directed Energy**
- **Electronic Attacks Against its Things**
- **Jamming RF Channels**
- **Destroying Fiber Channels**
- **Depriving Things of their Power Sources**
- **Electronic Eavesdropping**
- **Deploying Malware**

Intelligent Things fight Intelligent Things

Humans are a Class of Intelligent Things

Perhaps most importantly, the enemy attacks the cognition of human Soldiers

Humans will be "Intelligent Things" that are most susceptible to deceptions

Humans' will be handicapped when they are concerned (even if incorrectly) that the information is untrustworthy

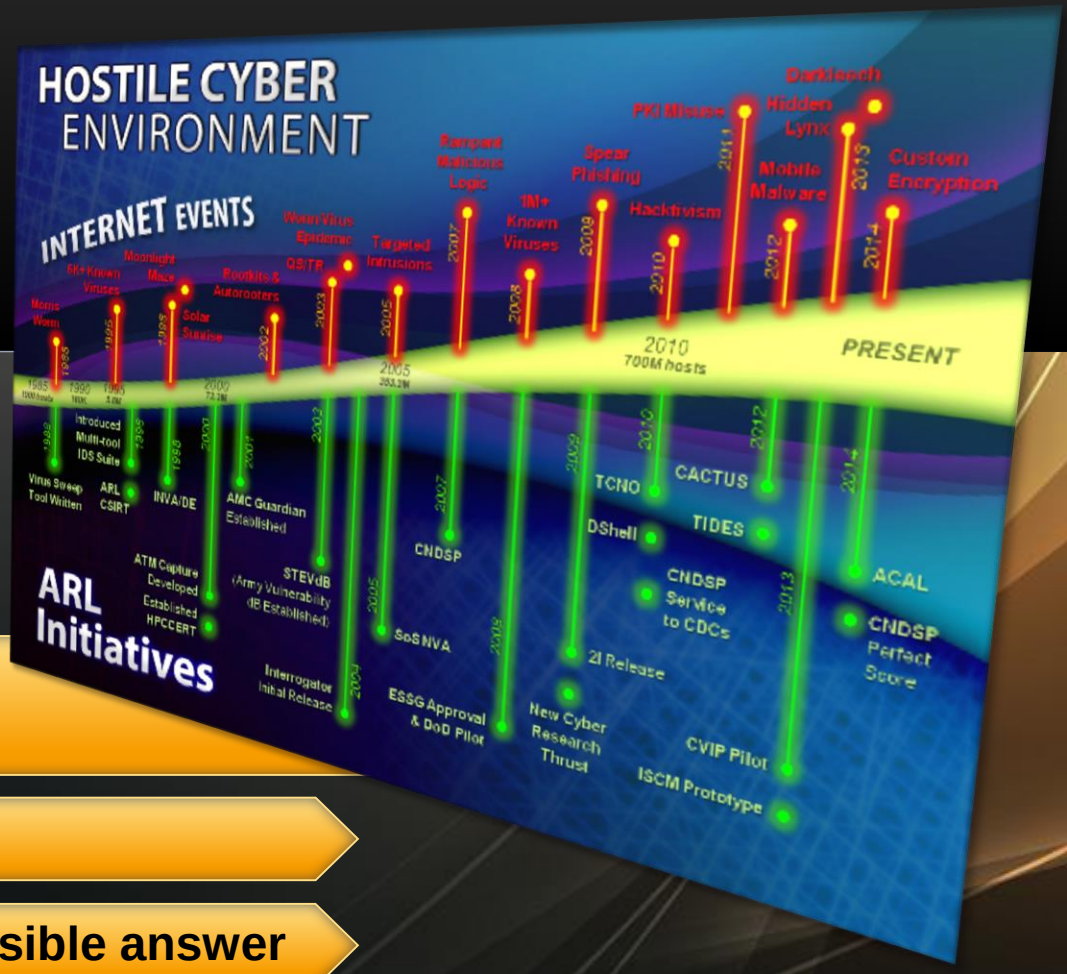
Deception

U.S. ARMY RDECOM

ARL

AI will Fight Cyber Attacks

Intelligent Cyber Agents



The battle of Cyber domain will continue to grow in significance

Offense is stronger than defense

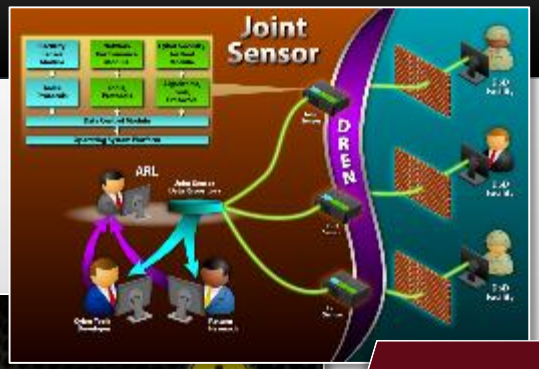
Intelligent cyber agents are a possible answer

U.S. ARMY RDECOM

Intelligent Cyber Agents

ARL

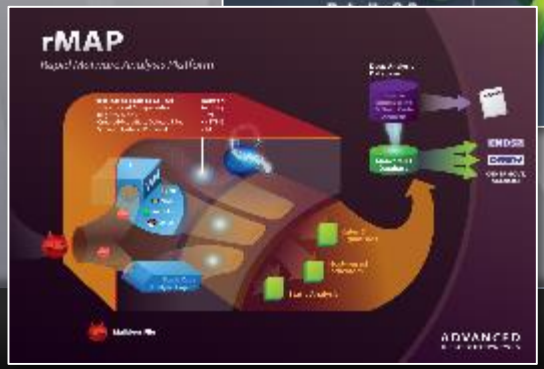
Ways to Defeat the Adversary



Stymie the enemy's cyber intrusions by believable honeypots and honeynets

Fight back by anomaly detection that can highlight unexpected patterns

Use continuous learning process



Large-scale physical fingerprinting

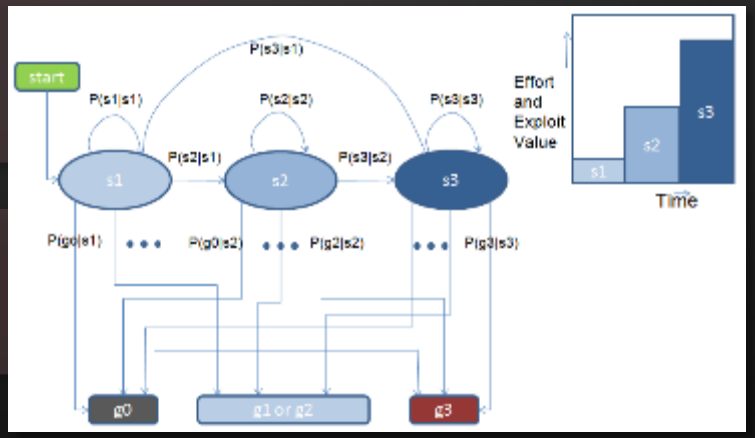
U.S. ARMY RDECOM®

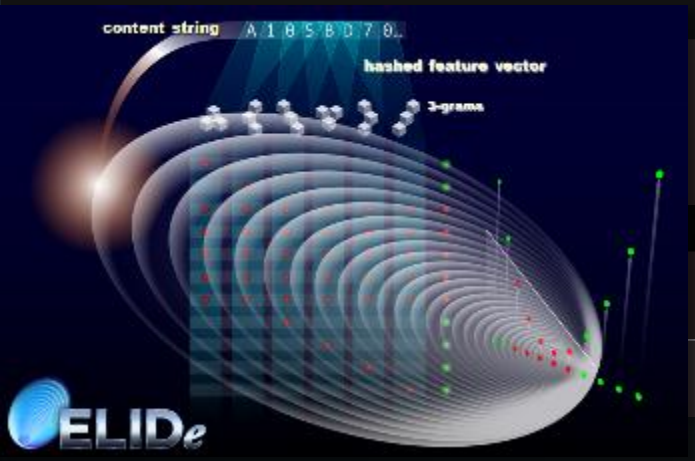
Can We Build Defensive Intelligent Agents?

ARL

Managing a variety of responses is error-prone

Core machine intelligence must reside on-board





ADS is a prototype unified framework for on-board plug-in active defenses

ELIDE is learning-based tool for extremely light, on-board intrusion detection

Chang, Raymond J., Richard E. Harang, and Garrett S. Payer; Extremely Lightweight Intrusion Detection (ELIDe); ARL, 2013

Adversarial Intelligence on Small Devices

AI Must Become Smarter

Hypes & Successes

AI was over-sold many times, but the last 10 years seen impressive achievements

- **Self-driving cars** (DARPA Grand Challenge, 2004 no one finished, in 2005 5 teams finished)
- **Urban Challenge** (2007 follow-up to previous Grand Challenge, 11 teams competed with 6 finishing, 3 in under 6 hour limit)
- **Spectrum Collaboration Challenge Calls for Contenders** (2016)

- **Deep Blue decisively defeats any human chess player** (1996 lost, 1997 won after HW upgrade)
- **Watson defeats *Jeopardy!* Champions** (2011)

- **Apple's Siri** (2011), **Google Now** (2012), **Microsoft's Cortana** (2014)
- AI personal assistants with voice recognition

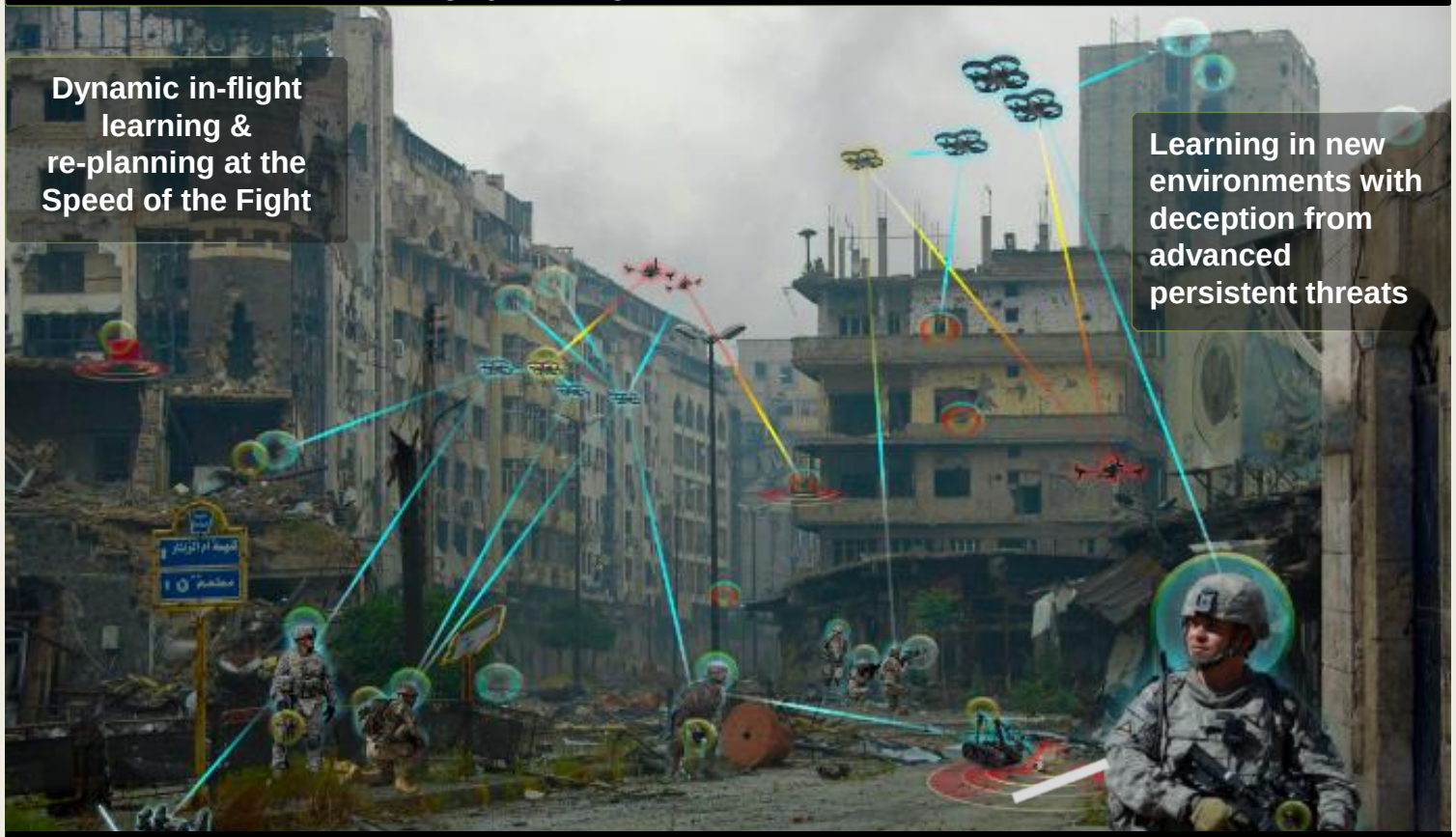
Skype can translate your conversation in real-time (2015)

Google's DeepMind defeats reigning AlphaGo Champion (2016)

Many products of AI research are so common they no longer perceived as AI by the users: route planning on Google Maps; Google Translate; facial recognition products; automated customer service; video games; etc.

Real-world is Still Too Hard for AI

Highly-dispersed team of human & robot agents accessing highly heterogeneous information sources



The Army AI and ML problems involve unique challenges: unstructured, unstable, rapidly changing, chaotic, rubble-filled adversarial environments; learning in real-time, under extreme time constraints, with only a few observations that are potentially erroneous, of uncertain accuracy and meaning, or even intentionally misleading and deceptive.

Gaps

Vision: **Artificially intelligent agents (heterogeneous & distributed) that rapidly learn, adapt, reason & act in contested, austere & congested environments**

Gaps

→ AI & ML with small samples, dirty data, high clutter → AI & ML with highly heterogeneous data → Adversarial AI & ML in contested, deceptive environment	**Learning in Complex Data Environments**
→ Distributed AI & ML with limited communications → AI & ML computing with extremely low size, weight, and power, time available (SWaPT)	**Resource-constrained AI Processing at the Point-of-Need**
→ Explainability & programmability for AI & ML → AI & ML with integrated quantitative models	**Generalizable & Predictable AI**

Humans and AI will Team

Challenges of Teaming

A key challenge is to enable Intelligent Things and Soldiers to effectively and naturally interact across a broad range of warfighting functions, with trust and transparency, common understanding of shared perceptions, and human-agent dialog and collaboration.

Teams Train

AI will be a key technology for building, realistic, intelligent entities in immersive training simulations. These should include realistic sociocultural interactions between trainees and simulated intelligent agents.

Summary

- Warfare will be by the distributed society of humans and intelligent things
- This forces will be far more fluid and self-adaptive than today's
- Proliferation of intelligent things invites predation of malicious cyber agents
- As well as great increase in overall complexity of warfare
- Humans will be both sources of vulnerability and resilience
- AI both invites cyber-attacks, and enables their defeat
- AI will have to close gaps: adversity, complexity, resource constraints, explainability
- New forms of human-agent teaming will emerge
- Humans and Intelligent Things bring complementary strengths
- Humans will learn to partner with Intelligent Things

References

REFERENCES

Stytz, Martin R., Dale E. Lichtblau, and Sheila B. Banks. *Toward using intelligent agents to detect, assess, and counter cyberattacks in a network-centric environment*. INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA, 2005.

Rasch, Robert, Alexander Kott, and Kenneth D. Forbus. "AI on the battlefield: An experimental exploration." *AAAI/IAAI*. 2002.

Kott, Alexander, David S. Alberts, and Cliff Wang. "Will Cybersecurity Dictate the Outcome of Future Wars?." Computer 48.12 (2015): 98-101.

Kott, Alexander, Ananthram Swami, and Bruce J. West. "The internet of battle things." Computer 49.12 (2016): 70-75.

Paul Theron , Alexander Kott, Martin Drašar, Krzysztof Rzadca, Benoît LeBlanc, Mauno Pihelgas, Luigi Mancini, Agostino Panico, "Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture," In Proceedings of the ICMCIS Conference, Warsaw, Poland, May 2018

Kott, A., Swami, A., and West, B., "The Fog of War in Cyberspace," IEEE Computer, November 2016

Wampler, Jason A., et al. "Heterogeneous information sharing of sensor information in contested environments." *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII*. Vol. 10190. 2017

References

REFERENCES

Chang, Raymond J., Richard E. Harang, and Garrett S. Payer; Extremely Lightweight Intrusion Detection (ELIDe); ARL, 2013

Kott, A., Singh, R., McEneaney, W. M., & Milks, W. (2011). Hypothesis-driven information fusion in adversarial, deceptive environments. *Information Fusion*, *12*(2), 131-144.

Young, S., & Kott, A. (2009). *Control of small robot squads in complex adversarial environments: A review*. ARMY RESEARCH LAB ADELPHI MD.

Kott, A., Alberts, D., Zalman, A., Shakarian, P., Maymi, F., Wang, C., & Qu, G. (2015). *Visualizing the tactical ground battlefield in the year 2050: Workshop report* (No. ARL-SR-0327). ARMY RESEARCH LAB ADELPHI MD COMPUTATIONAL AND INFORMATION SCIENCES DIRECTORATE.

Kott, A., & Alberts, D. S. (2017). How Do You Command an Army of Intelligent Things?. *Computer*, *50*(12), 96-100.