UNG
UNIVERSITY of
NORTH GEORGIA™
THE MILITARY COLLEGE OF GEORGIA®

INSTITUTE FOR LEADERSHIP
AND STRATEGIC STUDIES

Symposium
Monograph
Series

SOLDIER-LEADERS in the AGE OF AI

The Future of Pre-Commissioning Education

If you need this document in an alternate format for accessibility purposes (e.g. Braille, large print, audio, etc.), please contact the UNG Press at ungpress@ung.edu or at 706-864-1556.

Published by:
University of North Georgia Press
Dahlonega, Georgia

Printing Support by:
Lightning Source Inc.
La Vergne, Tennessee

Cover and book design by Corey Parson.

ISBN: 978-1-940771-86-1

Printed in the United States of America

For more information, please visit: http://ung.edu/university-press
Or e-mail: ungpress@ung.edu

UNG
UNIVERSITY *of*
NORTH GEORGIA™
UNIVERSITY PRESS

Blue Ridge | Cumming | Dahlonega | Gainesville | Oconee

Table of Contents

Preface

Billy Wells

The famous French military theorist, Colonel Ardant du Picq observed that the only constant in war is man. That may well be so. The human dimension of war and the effects on Soldiers and their leaders is a significant constant of sorts, and it sets the tone for our 2019 symposium.

The theme of our symposium, "adaptive, agile leaders" is pervasive in today's military literature, yet the leader development impacts of accelerating technological change have been largely overlooked. In this context, educational institutions that produce military officers and continue their learning through the professional military education structure must understand the future operating environment and be equally agile and adaptive. The typical sometimes plodding evolutionary approach to institutional change in education will likely be neither timely nor therefore successful in preparing our future military leaders. Those who evolve the fastest and establish a structure to continue to evolve quicker than their adversaries will almost certainly secure a decisive advantage.

Today's freshman Cadets and Midshipmen will be field-grade officers in 2035 with amazing opportunities and challenges ahead of them. Their success, again, requires educational institutions and leader development programs fit for the age of artificial intelligence and as adaptive as we expect our Soldiers and leaders to be. The presentations and discussions captured here address many aspects of this challenge. To determine what is required for the future results in several fundamental questions.

How will current and anticipated advances in science and technology shape the future battlefield and support the Soldier-Leader and leaders' education? What will be the impact of neuroscience, cyber war, man-machine learning, drones, augmented learning, and artificial intelligence? The speed of change itself is again perhaps the most challenging aspect of future war, with limited time to develop and field new strategies and tactics that not only keep up with technological (and biological) advancements but facilitate rapid distribution and inculcation to the training base and to the field.

Science and technological advances will impact future military leadership education. These advances will also potentially create significant legal, ethical, and moral challenges for the leader, especially those senior leaders charged with the development of those they lead. Ideas, already executable, regarding autonomous weapons systems and Soldier genetic and biotech enhancements are similar to the same discussions accompanying the advent of the crossbow. Like the crossbow, which was simple and required little practice, but was exceptionally lethal, many new approaches to weapons and warfare may be initially considered unacceptable, but soon established as a norm.

Today our question should be how we structure our professional military education institutions to be both adequately preparing our leaders, but also how can they be structured to be adaptive in their military education mission. Fundamentals are ageless, but some things have also changed. How should we not just adapt to but anticipate change in advance? It's a four-year process to become an officer. How do you make that process fit the future? How do you lay the baseline, the fundamentals? What is required to provide the foundation for a future officer, not just to be a lieutenant, but also to prepare them through the years to become a field grade officer and perhaps in some cases a general officer? Do we accept the minimum ROTC curriculum as adequate to prepare a future officer, or should we require more from our academic institution partners?

As one of the earliest of philosophers, Heraclitus of Ephesus observed, the only constant in life is change, and as Charles Darwin opined, at least in general terms, failure to adapt to change results in succumbing to the law of natural selection.

1

Opening Remarks: Day One

Billy Wells

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

This is our fourth symposium, and we do this every year as part of the mission of the Institute for Leadership and Strategic Studies. Every year we choose a different topic. Last year, it was on private military companies, and I have to tell you, that was a very controversial subject, but also a very good one. Because of who we are as a military college, we chose this year to focus on precommission education.

Some things are changing in terms of the environment, in which all of you will operate. And I am hopeful that you have some questions for our speakers and our panelists as we move forward. Just to provide some context, for centuries nations have struggled to determine how to best select, educate, and train their future officers. With each generation there have been changes. At the same time areas of focus have remained very constant.

Since the establishment of the military academies in the 18th century there has been a focus on subjects such as geography. Today, you could translate that to GIS.

Also, foreign languages and additionally certain aspects of military related science, mathematics, and technology.

All those subjects are kind of at play when you look at how to educate future officers.

Nations have established a wide range of educational models for this depending on their cultures, their needs, and their resources as well.

Today, countries have opted for a four-year academy approach, though the form and substance of instruction ranges widely. In some nations, that four years is focused on academics. In other nations, that four years is focused a bit on academics but significantly hands-on application with regard to combined arms, things of that nature.

And a number of countries, including Korea and the Philippines, they have vibrant ROTC programs similar to what we have here to help fill the gap and make sure that we have sufficient—or they have sufficient officers.

Even the length of the academy attendance in various locations varies. The United Kingdom royal military academy model is, for example, one that is employed around the world in previous British colonies. And other locations as well. It's only about one length in the security of a degree, the baccalaureate degree is dependent on the University System there in those countries. So it's not a complete match-up. Yet in Britain, all officers must attend Sandhurst in order to get commission.

Other countries opted for officer programs of varying lengths.

We have an OCS program, as well, and I'll talk about it in a second.

In a number of cases, selected professionals are brought on active duty commissioned—how do I say this? They've selected their commission and they don't have to do anything else. Primarily, we talk about doctors, case lawyers, and other cases—there might be other professionals. That is also true in the saga world as well. It will be interesting to see how that pans out.

In the United States, we have wide range of commission resources. And the military academies are at the top of the list and highly competitive with regard to applicant acceptance. I think we in the U.S., we all know that.

Yet they can only produce, at least in the case of Army, maybe about 20% of August commissions that are going in the ground force. So our heavy reliance in one of these topics is because ROTC provides the majority of officers for the Army. And there's no denying that.

Of this remaining 80%, about 10% of those are produced by six institutions out of, I think, 273, although the number varies day to day. And those are the six military colleges of which we are one.

So for us, this topic is extremely relevant, and we're interested in having feedback from everyone dur during the symposium.

All that said, you should be—how should we be preparing these future officers? Many of the are fundamentals—that's the reason I have Jeff here. Fundamentals are ageless, but some things have also changed. How should we not just adapt but anticipate change in advance?

It's a four-year process to become an officer. How do you make that process fit the future? How do you lay the baseline, the fundamentals? What is required to provide the foundation for a future officer, not just to be a lieutenant, you know, but also through the years to become a field grade officer and perhaps in some cases a general officer.

Those are at least two transitions that have to occur beyond lieutenants. And the education that you receive as a lieutenant or as a cadet should provide you a foundation for that.

Do we accept the minimum ROTC curriculum as adequate to prepare a future officer, or should we require more?

I've got my own personal answer to that question, and the ROTC program obviously is a good start, but it requires more than that if you're going to develop the competencies required. Of critical importance to our discussions here is, how will the age of artificial intelligence impact leadership development?

I don't know the answer to that.

I'm not sure any of us do, but I also believe that we can hash through some of that in the next day and a half and perhaps find some good ideas that we need to promote. Advancements in technology and biomedical science will and are in fact leading us in the future where embedded augmentation of potential super soldiers is becoming a reality and giving the ever-tightening cycle of innovation—if you read military history and you think about it, there's a cycle of innovation. And now it gets tighter and faster and faster.

And so how do we adapt the institutions we have in order to provide the education we need as a foundation for our future officers? That is probably one of the most challenging questions we can talk about.

Also, I would say the ethics of technology and war represent an ever-present and increasing conundrum of moral decisions, and I think those of you, if you've been studying this, you will, I think, agree with that.

There are a whole bunch of things we need to look at.

Ethical implications of technology applications to war fighting essentially—especially artificial intelligence are significant. Human application is one thing. Especially with CRISPR technology, if you're familiar with that. Human augmentation and genetic modification pathways can lead us into the—I'm going to go on a limb, Sharon, just a little bit to the classic Star Trek episode—you don't know about Star Trek, do you?

Some of you do.

Okay.

There was an episode back when I was a young man called "space seed," and it had to do with genetic augmentation and the advancement of essentially what was a super race. It can happen with this new technology. And we need to be aware of that.

The other aspect is semi- or fully autonomous artificial intelligence machines of war, and it's another danger, if there's no person in the loop, human in the loop. Something to think about.

That's the Terminator scenario.

So both of the scenarios are things to think about as we move forward.

People with a lot greater—this guy has seen this danger.

Four years ago, Steven Hawking and Elon Musk, among many other experts, signed an open letter on artificial intelligence about the benefits and exceptional dangers. Hawking says, whereas the short-term impact of AI determines on who controls it, the long-term is whether it can be controlled at all.

Something to think about.

He had similar observations regarding human gene modification. Should you be interested, you can Google all this stuff and find it out. It's all open source.

If you think income inequality is an issue, and that's been espoused by many people, including a number of politicians, just wait until some segments of the population can enhance themselves and their children in order to have no hope of doing so. So there are exceptional social issues associated with this as well.

At the end of the day, there is a final question. What safeguards must we develop and embed to protect us, all of us, from the dangers of AI while reaping the potential benefits for all?

At this point we're focused on the implications of AI on battlefield leadership and preparing junior leaders, but they will soon be leaders and required to deal with more, greater, and challenging scenarios such as I have mentioned.

Again, we're grateful for your participation.

And I hope you will find the symposium helpful to your own work, whatever that might be.

One final caution.

As we work to attain dominance, quote, with regard to peer or peer competitors, perhaps real dangers are outside the normal parameters of competition. We need to be thinking about that. It's a danger perhaps none of us fully recognized.

We have lined up some great speakers and panelists to consider some of these challenges, and I now would like to introduce Dr. Sharon Hamilton, colonel, retired, military intelligence, who will introduce our first speaker

2

The Future Operational Environment

Chief Warrant Officer Jerry Leverich

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

Those circumstances, conditions, and challenges affecting decisions, they have implications, of course, for geopolitics, for national strategy, for the Army itself, for leaders at all levels, and even individual soldiers.

What I'm going to lay out over the next few slides is to try to give you an appreciation of how we foresee the future focusing on 2030, but we'll stretch that a little bit also with some other opportunities.

I'm going to start off with a video, about five minutes. It's meant to help you envision what we're talking about. Some of the things that you see today as well as some of the things that we anticipate in the forecast for the future. So with that, if we can go to "The Changing Character."

[Video] Today's U.S. military finds itself at an inflection point trying to cross the diplomatic, information, military, and economic spheres and rapidly transform all aspects of society, including future warfare.

As we consider the character of future war, we can address it in two stages. An era of accelerated human progress, with evolutionary technologies to challenge our forces. And the era of contested equality, with revolutionary technologies that can dramatically change the character of warfare.

Our understanding of future OE must be continuously informed by analyses of the trends that shape the future. There are twelve trends we're tracking to stay ahead of the curve. All of these trends are constantly evolving and crucial to our understanding of the future.

Robotics, unmanned systems with some degree of autonomy, power generation and storage that is more efficient and economical, technology, engineering and manufacturing that delivers tailored ondemand products.

Collective intelligence that leverages social media platforms.

Increased level of human performance with physical and cognitive enhancements.

Human computer interaction that increases efficiency.

Cyber and space that have emerged as war fighting domains.

Artificial intelligence that enables effective decision making.

Big data—an increasingly vital source of information and intelligence.

Climate change and resource competition that increases the potential for conflict.

Economic rebalancing and income disparity foster discontent and instability.

Demographics and urbanization are changing the social and physical context of the future battlefield.

Among these trends, we see the emergence of a myriad of new and advanced technologies.

The future OE will be multiplied in the way of threats from continually developing new technologies.

Perspective episodes in the era of accelerated human progress is socalled two plus three.

Russia is a capable potential foe. China is rapidly developing capabilities, becoming a pacing threat by 2035. North Korea—nuclear power with conventional capabilities that make it a significant threat. Iran is hegemonic with asymmetric capabilities.

Future warfare in the era of accelerated human progress will be characterized by hybrid threats, contested domains, weapons of mass effects, operations in urban and complex terrain, and increased human rags.

We are seeing gamechanging evolutionary technologies that can provide a decisive edge over an adversary. These include robotics, that will change society and labor markets, that will impact the character of war. Space capabilities will threaten reliable PRT, ISR, and communication networks. Computer power will increase exponential and analyze big data and leverage the Internet. Artificial intelligence that enables manned and unmanned teaming. Adaptive manufacturing will be a boon to logistics but may not result in a decisive edge.

One can be contested in the order that will persist. Trends will interact to create new conditions for competition and conflict, new rivalries and unanticipated adversaries. We can expect revolutionary technologies, such as synthetic biology, the potential for weaponization of biological things. Energetics that revolutionize the storage and usage of explosive energy. Lasers and weapons that provide lethal and nonlethal effects. Hypervelocity weapons that have the speed and energy to defeat countermeasures.

The convergence phenomenon occurs as technologies are blended in a myriad of ways with unpredictable and potentially catastrophic results. These will have an effect on warfare as dramatic as convergence of messaging, Internet access, and smartphones on society.

Future conflict will be waged through other means.

Our challenge is to recognize enduring continuities for the future. Understanding the operational environment is the critical first step in developing concepts and capabilities addressing the challenges of the future.

We must take advantage of advanced technologies and consider a dramatic increase in the speed of human interaction to that faster ability to overmatch any potential adversary at the point of decision.

Although the future is not certain, trends suggest that the character of warfare is changing. For the nation and Army to succeed, we must learn and adapt today for success in the future.

[Jerry Leverich] So not necessarily the nature is changing, but the character is certainly changing. If you listen to Miller, he goes to historical examples. He talks about going from bareback to stirrups, and talks about going from smooth board to rifle.

But I think if you look at some of the things that we have pointed out in the video, you can certainly see that we are in an inflection point and that the character is certainly changing.

Let me lay out another side that describes that operational environment also. So threat characteristics considerations. Consider that for the last eighteen years, the U.S. Army has been optimized, I would argue, for counter insurgency operations.

We have invested in maps, we have taken heart at soldier protection. We invested significantly in countering IEDs.

That's not what the adversaries are looking at, or what the Russians or Chinese have invested in over the last eighteen years.

If you consider things like electronic warfare, where the military has actually walked away from and optimized for IED warfare, the Russians have fielded nine or ten different systems over the last ten years.

Speaking to operating and consistent environments—the potential communications.

If you look at integrated defense and what emotions do in Ukraine, and the ability to shut down air space over a sovereign government, it tests our assumption on air power and superiority.

Other considerations, I really want to come to head on the last one down there, CBRE.

If you consider and look back two years, in a sixmonth period, you had mustard gas used in north Iraq; you had chlorine bombs dropped in Syria; you had nerve agents in airports, Malaysian airports, and advanced nerve agents used in downtown London.

Weapons of mass destruction we have not gotten away from, our adversaries have not gotten away from it, and I'm not sure our investments right now are on par to assist with those things.

If we look at the two plus three threats, we briefly discussed them in the video.

Two new competitors. Russia is a pacing threat. China's looking into the farther future.

Consider one that is probably operationally dominant, that's got a lot of experience. Another one that has a big checkbook. Technologically dominant.

But not forgetting the other region actors of North Korea, Iran, and, I would argue, almost a multigenerational fight with some of the radical idealogs that we anticipate.

If we look to the top righthand side, the potential for overreach, as I mentioned, we made hard decisions over the last eighteen years. There are some areas where we are overmatched on the battlefield. I think we're trying to right that.

We have some priorities for future investments, but things like, as I mentioned, electronic warfare, cyberspace, I would argue is our Achilles tendon if you consider that we are now stateside military.

So we have to deploy.

We are expeditionary.

If you consider reliance on space, 60% of cyber, terrestrial cyber, actually hits a SALT at one point. And our vulnerabilities that we have in space rockets artillery, those things adversaries have invested significantly in.

If you consider the Russian Army, we characterize it as an artillery Army with some tanks. They actually have more artillery than they do tanks.

If you look at the characteristics at the bottom left, I'm going to get to some of those points. The population complex trains, proliferation, speed of human interaction I'd like to elaborate on. I think it's probably the most important one there.

A lot of people try to simplify and say it's social media, it's cyber. The better example I think on the increased speed of human interaction is an example.

If you consider one guy in Tunisia distraught, he goes in for a welfare check, he's distraught and sets himself on fire in the middle of the road.

The message and the media that covered that, and how it proliferated to over twelve other countries over the period of six months, six of those countries had violent overturns in leadership.

Two are still unresolved; if you consider Syria and potentially Yemen and what became the Arab spring, I think is a better example of speed of human interaction, how that increases over time.

Had the military been required to respond to that, how fast could we have? If you consider what happened in Libya, I would say it's not very fast.

I already mentioned the idea, the fundamental changes, when you consider a number of those things that actually were talked about in the video, and genetics, power, laser weapons, truly we're at that inflection point now.

So when I talk about the potential for overmatch, those at the top there, those things that we recognize, we have a capacity issue, range issue, or just a basic investment issue.

Recognizing the historical analogy if you consider this, the French knights invested in, spent years in training, had the best armor; they're confronted by the British longbowmen—they had a different technology. They were considered peasants by the British Army.

The French knights were reluctant to engage the peasants. And as that hesitation occurred, they leaned down with that new technology, those longbows, and decimated the French Army.

So culturally we have to be cognizant of some of our biases.

We've had significant success over the last eighteen years. I would argue that the potential future fight is going to be very, very different.

Taking that to the next level for our leaders, eighteen years, every lieutenant colonel is very good at coin right now. Conventional largescale ground combat, I'm not sure we're there yet.

If you look into the future with some of the investment, that we've seen, staying cognizant of them so we're not surprised like we were in Pearl Harbor.

And to the righthand side, if you consider contested over time, those things that we have to pay attention to so that we don't end up like Cornwallis at Yorktown, not anticipating that the French fleet would have success out of the Capes, and Cornwallis subsequently unable to be extracted from Yorktown, and that happened with the British losing their colony.

So contested over time, using that analogy, but it's also adversaries that adapt just like we do. In some cases faster.

If we use a cyber weapon, many times we have to be we have to be prepared to also defend against that time saver weapon. Once an adversary has it, they can reverse engineer and use it against us.

I think there's a build on it.

So looking out a little further, right around 2030, Intel computer tends to have lesser confidence around that period, but I offer that military senior leadership is making decisions that will affect us in 2050.

So going beyond a little bit on what the Intel community looks at and looking at some of the other considerations. So, for example, climate change and resource competition.

We look at the arctic, and we talk about the natural resources there. One of the significant things about the arctic is ice caps, of course, melting. The northwest passage is opening and will become navigable. And what that means is that travel, transportation between Europe and Asia, will be reduced by over seven weeks. That's a dramatic implication there.

If you consider things like demographics and liberalization, probably they include science that's of these trends, where populations are aging significantly.

If you consider 60% of population will live in urban areas by 2030, and if the military is to close in and destroy the enemy, those persons in urban areas, that's what we also need to consider. The days of bypassing cities, I think are long past.

But other challenges, if you look at mega cities, cities with populations of over 10 million people, how does a military operate in that? Do they operate in that?

Cyber and space as I mentioned earlier, artificial intelligence, it was a little too earlier about Elon Musk and Stephen Hawkings' comments. But lay out other considerations.

If you look at the United Nations convention that recently got together with multiple representatives looking at artificial intelligence and its military implications, Elon Musk got up there and mentioned artificial intelligence as more than a weapon.

What was really interesting was the Russian perspective. Because artificial intelligence is heavily tied to cyber code, the Russian perspective is, if I wrote it, if a human wrote the code, there's still a man in the loop.

So different perspectives, and then think about things ethically.

I would offer up that air defense weapons right now actually have a man on the loop because the system is so automated.

Big data. We're in a period of big data right now. If you consider in the late '90s, 85% of all data was captured on pencil and paper. 95% of all data today is captured electronically. What we lack are the algorithms to make sense of it.

So to give you another visualization and setting up this video... We took this to the Chief of Staff of the Army a couple years ago. His charter to us was, tell us what 2050 looks like.

So this video is going to walk us to 2050, but what we tried to do is 2050 at that point, thirty-four years in the future. What we tried to do is consider, okay, thirty-four years in the future. Let's look at thirty-four years in the past, because thirty-four years in the past, the Chief of Staff of the Army was a lieutenant, just like today's lieutenant potentially would be the Chief of Staff of the Army in 2050.

Take that to the next level, though.

The soldiers of 2050 won't be born for another fourteen years. And as I mentioned early on, we're already making decisions and investments that will affect that time period.

So thirty-four years in the past, thirty-four years in the future, a small break.

And then I have a conceptual Russian consideration of how they look at the future.

So with that...

[Video] What do you consider the greatest threat that America faces? I would put Russia right now in a military perspective as the numberone threat. I would add China and North Korea and ISIS along with Iran.

Just as we are looking forward, so are potential adversaries. Russia is aggressively exploring remote combat operations. Here is a Russian simulation of their future combat, unmanned ground vehicles operating in a contested urban environment.

[Jerry Leverich] So the reason I play that video is three big findings in the September 11th report, the 9/11 report. As intelligence failures.

Number one was lack of coordination amongst the different organizations.

Number two was lack of clear policy.

The third thing was a lack of imagination.

So conceptually that video, which is actually about eight minutes long and is about five or six years old, very cartoonish, but I don't want that to stymie the lack of imagination.

This is what that system actually looks like. It's a Russian autonomous system. It has both air defense guns on it as well as a main gun, and antitank. It's on tracks. The other was on wheels.

The greatest consideration right now is nobody in the turret; the crew of three is outside the turret. It takes three people to actually operate it.

I would offer that with the advent of artificial intelligence and a number of other technology advancements, the significance of this grows more when that crew of three can now control ten or 100 of these simultaneously.

So lack of imagination.

This is actually my last slide. It tries in a single slide to capture what I started off with in the video.

I offer up most of these things, super empowered individuals, contested in all domains, increased lethality, robotics, artificial intelligence.

Populations among populations increase speed of human interaction events and action coevolving.

What is important to highlight is on the particular slide, though, the underlying aspects of it. That's actually senior military leaders, the senior military leader in the Army, reinforcing those ideas.

That's my last slide.

I am very glad to be here. Any time that I can talk about the future, the Army, help understand some of the challenges, the opportunities, and especially in front of such a diverse audience, I'm always grateful.

So with that, I'll open it up for questions.

Question & Answer

[Audience Member] Jeff Mellinger here. In one of your slides, you portray the nearpeer adversaries and their capabilities. I have been in briefings with senior officers that now say that we are the nearpeer and all but personnel and soldiers are standout. So obviously there are varying opinions, but your thoughts on that, sir?

[Jerry Leverich] It's a really good comment, question. If you divide it, the U.S. Army certainly has overmatch in some technological aspects. But our greatest strength has been the way we develop our leaders, the experiences that they have, the training investments that we make with them, certainly dealing with con skirts armies; those are different.

[Audience Member] I've got one. So you've been working on this quite a while for operational environment, and you talked about lack of imagination. So who do you bring in? What organizations and people and allies do you bring in as you're developing the future OE?

[Jerry Leverich] Good question. So very informed from a number of products, efforts, individuals, groups, organizations. Let's start at the top. What we are clearly aligned with is the National Intel Council. If you're not familiar with them, they frame the operational environment. They do it every four years for the president, so a lot of ideas and themes that you see here are resonant strategically to operationally. The joint staff with its J7 does a military version again of that. Again, aligned.

Understanding that this isn't the knowall beall for everything, aligning what we present in our operational environment for training, how we frame it up for investment decisions, how we set it up for leader development, very good alignment in there. That's how we do it internally.

Now, critically looking at it, we also have our own efforts of the mad scientist effort, which is meant to reach out to greater academia, industry,; they do a number of conferences, bringing in some very diverse opinions.

Once we actually had a gentleman named Max Brooks. If you're not familiar with Max, he's the son of Mel Brooks from *Blazing Saddles*. He's also the author of *World War Z*, with the intent of pulling in different perspectives from that.

They, mad scientists, have a blog. I will certainly provide the link to it. They publish constantly. They're always looking for submissions. And General Murray at one point actually recognized the mad scientists and called them his peer review.

So an opportunity for anybody to actually get in there and post your thoughts and ideas.

[Audience Member] Yeah, Jim Crupi. I have two questions actually. You say there are areas where there is overmatch. My question is: Why? How do we get there? Why be in that position?

And my second question/comment is that it seems to me you're describing a world where everybody is a soldier. The idea that soldiers only wear uniforms and that creates competitors in the kind of world you're describing seems to be, to me, outdated.

[Jerry Leverich] Let me get to the first one.

It's been a choice of investment decisions. If you look at antitank guided missiles let me start the other way. The M1A1 Abrams tank or M1 Abrams tank is still the best out there, no ifs, ands or buts. There's not another tank that can challenge it. The problem is, the adversaries are not investing in tanks. They're investing in antitank guided missiles.

Overmatch is not necessarily a onetoone comparison. It's not necessarily tank against tank. It includes technologies.

The way it's inculcated, the way it's trained, and potential symmetries of how it's used.

But if you also look at some assumptions, I alluded to our belief in having the air force for air defense. You know, we've dribbled down significantly our air defense capability within ground forces.

I actually showed that to the former chief, and at the end of it, he said, you know, this was one of the most scary things that he has ever seen in that we had to make some decisions.

We optimize for a different type of fight. And there were costs associated with that.

If you look at some of our formations, you know, corps and divisions, we have few of them, and what they do is actually significantly different. If you look at the experience, again, alluding to eighteen years of coin. So correcting that, I think we have got the leadership in place. I think we've got the ideas, multidomain battle, the CFTs, the investment priorities, the renovations that we're going through in training, the refinement of doctrine, we're going to get there.

Right now the secretary has told us to be multidomain capable as a ground force by 2028. And multidomain ready by 2035. And there is a slew of things behind that, that decisions are already being made for.

And the second part of the question. So the super empowered individual is not a misnomer. And age is relevant. How they're weaponized.

Also I will offer up, society and governments. The Chinese last year passed a law requiring all Chinese citizens to be responsive to their government. What that means, if you have a Chinese citizen in the United States and the Chinese government says, tell me what you're studying, you now have introduced a vulnerability.

Yes, sir?

[Audience Member] I'm a prisoner of my own experience, an infantry guy, so I think at the tactical level more than the operational or strategic.

One of the things that I see from your presentation, you know, traditionally Sun Tzu and others said bad plan to attack cities. But what I see you saying is with automation and artificial intelligence and the ability of soldiers to control multiple platforms, that dynamic might no longer be correct.

[Jerry Leverich] I'm not sure it has changed. That's what I'm trying to posture.

[Audience Member] That's my concern, because it eats infantry.

[Jerry Leverich] And consider our force what is it? 980,000?

Our whole force could operate in Lagos, which has a population of 10 million people. So that doesn't mean that we just altogether bypass them. I think we have to look at ways to effect those populations. It may not be physically on the ground.

[Audience Member] Hi, Jeanie Nash. You talked about climate change and the arctic and how it will impact travel. I understand that Russia is building a military base up there as well. And I was curious, where do we stand on that, if anything?

[Jerry Leverich] That's a good one.

I can't necessarily speak to where we're going. Russia has the existence of proximity when it deals with the arctic. You know, they have forty different ice breakers up there.

They're investing in nuclearpowered icebreakers.

In some cases, I offer up that it actually opens up a contention between us and our allies. You know, with Canada and some of the Scandinavian countries, NATO allies. One of the biggest concerns it's not necessarily the biggest concern, but another consideration— is the Chinese are investing in their OSL.

That's not necessarily always appreciated by everybody else up there.

[Audience Member] Hi, Charlie. Really fascinating discussion. How do you think we should try to distinguish between the good ideas and the bad ideas?

This is what I'm thinking of. You know, when the French in the late 19th century went with this idea of the new school and capital ships were, you know, out of date and weren't so they missed the whole aircraft carrier. And the French Navy has never been the same because they listened to, quote, the young people, and they changed their whole way of looking at the world.

Is there any do you have any thoughts on how we might filter these ideas? Because, you know, commitments need to be made that will be hard to change—any guideposts for picking, you know, the weed from the chaff, I guess.

[Jerry Leverich] Wow, that's a really good question.

I would offer up we shouldn't always forget our past. I was just reading a history book on the way out here on the Chosin Reservoir and the first marines that were out there. More than three battalions of those marines actually went to basic training on the ships as they were moving out.

So I guess my point is, there is tremendous opportunities, and technology will assist in a lot of opportunities, but we can't always be wedded just to that. Because the old compass is still valuable when you don't have a GPS.

[Audience Member] Hi, Josh Bowen. How do you see, I guess, private sector global organizations potentially influencing the future OE or the changing characteristics of warfare?

[Jerry Leverich] So, another interesting one.

So interestingly enough, the largest security corporation in Somalia is CocaCola. They have to defend themselves.

And if you consider the Wagner Corporation and its exploits in Eastern Syria, they certainly have and even if you consider

Microsoft and it's awarded the Edge contract.

Technology in these particular cases, actually commercial technology is driving the government, which has flipped the way we historically thought about things.

Government investments drove technologies. That is changing now, and I think there's a lot of implications throughout that.

But just those three examples I give you as potentials.

Thanks very much for the fascinating discussion.

[See Appendix for corresponding PowerPoint presentation.]

3

The Future Land Battle: Multi-Domain Operations (MDO) or Army After Next (AAN)?

Major General Bob Scales

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

This is the second time I've been back to Dahlonega. Last time I was here was exactly fifty-three years ago this month. It was November of 1966, and my Ranger buddy, Peyton Ligand, those days the temperature was about the same as it is now. Those days, to get warm you wrapped yourself in a poncho and put a can of Sterno between your legs and the heat would come up and dry you out.

Peyton turned to me and said, looking out over the magnificent Pisgah National Forest, he said, Bob . . . the sun was coming. It was amazing. He said, Bob, look how beautiful it is out there. Someday after all this is over, I would like to come back here.

I said, Peyton, there's not a goddamn chance in hell I'll come back to this place.

It's warmer and dryer now, so I guess it's okay.

I would like to pick up on what Jerry said. I'm very concerned about this multidomain operation stuff I'm hearing from the Army. It has all of the earmarks of failures that militaries have made in trying to divine the future for the last fifty years.

We in America have a bad habit of not of ahistoricism when we look at the future. We think we're driving the Army seems to think they're fearing driving by looking at the rearview mirror, that it will only lead to a crash.

And the characteristics the blinking red lights are as follows.

Number one is sloganeering.

Ever since I started in this business, and I've been at it almost fifty years, the first thing you look for is sloganeering. It's you know, run down the list. Gosh, netcentric warfare, effectsbased operations, air/sea battle, blah, blah, blah.

Somebody comes up with some prose, and the next thing you know there's an office in the Pentagon, and colonels are running around with papers under their arms, and you realize it's all smoke and mirrors.

The second thing is the opinions of the senior officer present. We saw this in France in a war period; I'll talk about that in a minute. But the pronouncements of a senior officer who has absolutely no concept of future war or past wars, all of a sudden becomes, first of all, the process is it becomes codified, because that's what the senior officer said. Next thing you know, it becomes a loyalty test. If you don't use the word "multidomain warfare," then you are disloyal and therefore not a team player.

And I could go on and on.

But the bottom line is that somebody needs to raise the red flag, and I'm doing that, not just here, but as I travel around the country.

You know, the elements of warfare, winning in war, are fairly simple. Number one is numbers. God is on the side of the big battalions.

Number two is geography, whether you own what did Bismarck once say? America is lucky they had Canada to the north, Mexico to the south, and either coast, fish. So we're a protected species in many ways.

And the third is technology. Jerry just talked about that very eloquently.

And last we have doctrine, or concepts in doctrine. The process is vision, concepts, and doctrine. We lose on the first two. We tie on one. And doctrine is up in the air.

Let me just push back on what Jerry said. Of the twelve things Jerry had up on the thing, all but two—climate change and the disparity of global income—we had all ten of those plus one more.

So future gazing is as much a process of backward looking as it is forward looking. And everything in that technology is the principle catalyst in change. The problem with that is everybody's got it. We're not alone in that.

Prior to World War I, all the major contenders understood that the technological dynamics were going to change the character of war. You know, 9 million dead people later, we figured out how it should be done.

In the interwar period, all the major contenders, United States included, understood that it was the internal combustion engine and the wireless that were going to be the principle catalysts for blitzkrieg. We all got that.

Not what the technologies were, but how do you apply them? Some got it right, and some got it wrong. I'm going to talk about that in a minute.

Why do people subsist inside the beltway where I work? Because that's where the money is. Of the $715 billion, some $250 billion is directly or indirectly related to applying technology.

But the real unknown here is doctrine.

We have two big wars that we could learn from on how to do a peertopeer warfare.

They have to be sort of the signpost to the future by looking backward.

So you invited me here, Sharon. You invited me here. When you did, you knew I was a historian. So sit back and relax; you're going to get history. I'm going to give you about 150 years of history in three minutes. Buckle up.

Here is the bottom line. Here is where MDO comes off the rails. Big wars have always been balanced between two dualities: firepower and maneuver. You can go back to Marathon and it goes into the two primal elements: firepower and maneuver.

Contemporaneously, at least over the last 150 years, the object that moves the pendulum between the two dualities is technology.

Here is the bottom line. Of the three elements of firepower, range, lethality, and precision, if firepower is dominant, the battlefield favors the defensive.

Maneuver consists of two elements: speed and agility. If maneuver is dominant, the battlefield favors the offensive.

Here is the history lesson. The first precision revolution between 1861 and 1914 was induced by the invention of smokeless powder, the small bore rifle, the machine gun, quick firing artillery, mines, the telegraph, and the railroad.

We all know that. We all studied our history. But the bottom line is the first precision revolution pushed the art of war towards the defensive.

Why? Well, you increase the range of artillery a factor of ten, the small bore rifle went from a range of fifty meters to 900 meters. The machine gun, you all know about the machine gun. 9 million men dead men—later, we finally figured out how to deal with it.

It wasn't the technology. Everybody had it. The problem was how do you apply it? That's called doctrine.

And there are two approaches to breaking the deadlock, as you know. One was doctrinal and the other technological.

Technological was the invention of aircraft and the tank and allies applying it to the battlefield in 1917 and '18.

The German approach was doctrinal. They had the idea that a massive attack over open ground didn't work. So the answer was to reduce the killing effects of firepower by dispersing, going to ground, and using strong tactics to attack over open ground with disparate units with carryalong artillery and carryalong firepower.

So the Germans had the right idea doctrinally.

The allies had the right idea technologically during the interwar period.

The two were jammed together, by whom? The Germans.

The French had the right idea based on World War I experience, the methodical battle. In other words, artillery dominates. The infantry follows the artillery.

Germans said, not so fast. The internal combustion engine and the wireless had allowed maneuver to overcome firepower. The pace of maneuver in World War I was two and a half miles an hour. What if we could make it twenty miles an hour?

In other words, amplify the speed and agility of a moving force by a factor of ten, and the advantage swings from firepower to maneuver, and the result is blitzkrieg.

But the French in 1940 had more tanks and better tanks than the German. But the Germans had a better idea.

As I mentioned earlier, numbers count. And the Russians and the United States—that is, all ideas and warfare are fungible—came up with our own two versions of blitzkrieg, and Germany was overcome by numbers.

But I would argue, and the Army seems to forget, the technology is about to make another swing. We're in, what I call in my writings, the second precision revolution.

The problem with getting Jerry hit it exactly. Eighteen years of coin has not been helpful, but it's also the fact that we have had many, many false starts since the end of World War II. The four Arab-Israeli wars, Desert storm, where Navy redeemed its Army, and the March to Baghdad.

All false indicators. Why? The enemies we fought were all incompetent.

If you're going to fight a war and gain lessons—remember, I wrote the history of Desert Storm and when I finished writing it, I was struck by the realization that all these lessons are completely useless . . . because everything worked.

Why? Because the enemy was ignorant and stupid and incompetent and cowards. So you can put anything on the battlefield, and it's all going to work. Literally, no opposition.

The Arabs can, the Israelis can amplify with their own experience.

But there were two indicators that struck me in my writings and stick with me to this day. The bombing of the Mujhe bridge in 1972 and the 1972 Arab-Israeli War and the Egyptian use of Sam sixes and suitcase saggers, precisionguided rockets that just drove them crazy.

Almost lost the war in 1972.

And it seems to me that what this anticipated—the use of precision guidance against the Mujhe bridge, and the saboteurs—was the fact that we had entered a second precision revolution just as revolutionary and impactful as what happened 100 years before.

I just mentioned all the things Jerry just talked about up there. You have to ask yourself, of those ten things that you saw Jerry put on the board, what are three factors? Firepower, agility, and maneuver.

What did Jerry put on the slide, of that ten, eleven, twelve? What side do they favor? Firepower. Every single one of them.

The missing element, of course, in firepower—second firepower revolution—is ISR. And AI will fix that problem.

So the last missing element, target location and tracking—which is the essence of firepower intensive battle—is now potentially solved. Some would argue with UAVs and drones and all the rest, that it is solved.

What about maneuver? The speed of maneuver today. The speed of maneuver in 2030. However, the Army is going to do it. Is it the same in 1945? Twenty kilometers an hour. No faster. The speed of the M1 tank at a blown bridge is exactly zero.

Now, why is this a problem? The problem is that BO fails to recognize this great cosmic shift.

I don't know why, and I would share it with you. I think I know why, but I think the problem is that it's become so deeply embedded, not only in our philosophical approach to war but also in our programmatic approach to war.

The Army has got six major efforts—I don't know, directors or whatever they call it. I can only find one that has anything to do with maneuver.

Maybe you could argue that vertical to vertical lift technologies may have something to do with it. But the Army has been very kind to me over the last couple of years with my advocacy by showing me war games at TRADOC—many know Colonel Michael Reeny; he showed me a daylong exercise in war games.

I've spoken and lectured, particularly inside the beltway in Congress, specifically about NDO and so forth. What it comes down to at the end of the day, particularly when you face Russia, it's these all over again.

It's two cosmic clashes of two heavily-mechanized armor forces slamming into each other and over a long period of time with precision killing power. On the Russian side, it's artillery and ballistic missiles, and on the Army American side, it's principally airpower, at least for now. And that's it. It is slamdunk smashmouth motorist attrition war.

Now, the Russians in China, dare I say, are sensitive to casualties, but we are hypersensitive to casualties. And Russia and China can certainly afford the butchery and their willingness to stand and prevail.

We unfortunately cannot. Four dead soldiers in Niger completely changed our policy towards South and Central Africa. What do you think 30,000 dead Americans in the Baltic states are going to do to our strategic approach to warfare? So what is the answer?

I would submit to you the answer is to swing the pendulum in the other direction.

Russia is fine with attrition warfare. Their whole Army built around artillery, as Jerry said, is what? It's an attrition, it's an element of attrition warfare, and now it can shoot 1,000 kilometers and be precise within three meters and has lethality, thanks to thermobaric weapons.

Russian artillery is deadly, far more deadly than our artillery. So the Russians are happy to do that. The onus is on the United States to turn the pendulum in the other direction.

How would a war really play out in the Baltics instead of the stuff you see coming out of TRADOC?

Let me tell you what is going to happen, God forbid we should do this, but if we face each other off, there will be no urban warfare.

With Russians having dominance in firepower, instead of being fearful to the United States, they're actually our savior. Cities are sanctuaries, firepower sanctuaries, they haven't been since the day of Napoleon.

To survive Russia's firepower strike, the future will consist of an enormous strikecounter-strike that may meet days or months.

Two sides beat each other to death and then slam into each other in according to the doctrine—in an operational penetration, an attempt at operational penetration in one of the Baltic states, perhaps, Belarus, perhaps, Poland, and then they simply grind to a halt.

And that's World War III.

What if we have an alternative view?

By the way, I've been very influential with the Marine Corps. You read Planning Guidance, basically what he writes in the Planning Guidance is what I espoused. Think about this war conducted with some attention to history.

What do you do if you're facing a firepower dominant battlefield? What did Germans do? They disaggregated, went aground, built an operational force of great velocity that was able to achieve breakthroughs by simply breaking away from massive formations, storm tactic, blitzkrieg, whatever you want to call it.

Say we build a disaggregated force, operated in ever smaller increments. Empowered by what? The micro circuitry revolution.

When I was second lieutenant, air defense installation was what, eight acres?

Today you put it on the side of a soldier.

Tank warfare, as Jerry alluded, Russians have given up on that. Put it on an infantryman's shoulder. Air artillery, light anti-aircraft missiles capable of shooting F35, we will build.

So when you reduce the size and the bulk of a maneuver force you, automatically increase velocity, don't you? Mass X Velocity is a basic law of physics.

So if you unburden an operational force, then all of a sudden the velocity increases. But that's not enough.

The object is what we did against the Germans in 1944. What the Russians did is you have to find a way around this cataclysmic clash of the Titans; as we always have established, maneuver–either go over or around the enemy force.

Now, you're still moving at twenty kilometers an hour. I would argue zero kilometers an hour. The only way to do that is go up.

And all seven military functions in the Army today have a narrow dimension to it. Every single one.

Firepower, maneuver, logistics, intelligence, command and control, you name it, all have. And the key takeaway from that is, the vast majority of that in the future will be unmanned.

So the old problem of fearing the Russians' IED is off the table, because that's not a threat anymore. The Russians have given up on airtoair combat. They can't compete. You know how many stealth fighters Russia has? Zero. Well, very few. The bottom line is they have given up on that.

Their view of dominance is from the ground. And by the way, they could well be right; I don't know. We must be able to increase the velocity of maneuver from something around twenty kilometers an hour to 200 kilometers or more. We must find a way to lighten—do you know what the rate of a division is? 110,000 tons. That's what an armor division is.

How are you going to move 110,000 tons through the Syrian lakes in Lithuania? You can't do it. Maybe in the winter; I don't know. But, the Russians aren't going to attack in the wintertime. It's not their advantage.

So you have to right the force.

Twenty-five years ago we managed to build down the Army's operational maneuver force to about 28,000 tons. Not there yet. But that was with 1990s technology.

Today with the Internet and with this . . . where is it? With this damn thing. You know, with–I get it out of my pocket here. You know what I'm trying to do. With this thing, God knows, we probably could reduce south of 20,000 tons. If you can do that, you automatically triple the velocity of an operational maneuver force.

So you do what the Germans did in 1939. You find the Russian's vulnerable center of gravity, which I believe is their command and control. Then you take it down.

The two principle instruments for taking it down would be cyber, would mainly use cyber and our dominance in the air, and at the end of the day, the ground war in 2035 will be one not on the ground but in the air.

My good friend Charlie Dunlop is smiling when I say that.

Thank you, Charlie.

Ultimately, whoever wins the cyber war will then win the air war. And whoever wins the air war will win the ground war.

But if you don't win the first two, you lose.

And we are far less able to lose than our Russian and Chinese opponents.

What is the Army doing about what I just said? Well, virtually nothing.

Because now we have a mantra, and the general officers are saying that if you're not an advocate of multidomain warfare, then you are disloyal.

By the way, I love this analogy. I remember reading about General Don Lynn, head of the French army in 193940, when certain reformers in the French army, Charles de Gaulle among them, sent a task force to cover the gap on the line and defenses in Belgium.

And he shot them down and refused to authorize promotion for Colonel de Gaulle because of disloyalty.

I'm sorry, dare I say it, I'm beginning to see the same thing now.

By the way, last thing I'll leave you with, if you think we're having problems with the technological advantage swinging, look at our Navy people.

Boy, if you think a tank is vulnerable to a missile strike, what about an aircraft carrier?

What happens when that boy flips over in the north Pacific with 6,000 souls aboard?

That's two 9/11s. In one 110,000ton ship.

The Navy is having to deal with that. And that's one of the reasons why I think the marines are so progressive. Because the marines understand the need to restore offensive because they face the threat from two directions, don't they?

One is ability to maneuver with maritime forces and ability to break the two belt defenses the Chinese have put up, and, secondly, on the ground, they have lost the ability to restore operational maneuver with existing technology.

So the marines are all of the services and trying to restore mobility to the battlefield.

We have a long way to go.

Unfortunately they are going entirely in the wrong direction.

Not that I have a strong opinion—not that I have a strong opinion about any of this.

Question & Answer

[Audience Member] I'll start out. In your most recent book, you compare and contrast Patton and McCrystal. Based on comments today, have we embraced Patton again and ignoring McCrystal?

[Major General Scales] By the way, he doesn't like me much.

Complimentary, but Stan has a huge ego, and he and I debated in the public form several times.

But really the soldier of the future. Patton is the soldier of the past. McCrystal is one who advocates that it is what is in the soldier, not on the soldier.

He advocates for a disaggregated distributed battle.

He is a proponent of building elite forces that are able to operate in small aggregations and are not subject to strike and counter-strike.

His ability to embrace and use modern electronic technology is without precedent, a gamechanger in Iraq and Afghanistan.

As is also his approach to leadership, which is to decentralize and disaggregate and push down all elements of combat.

What are we doing in the Army? What are we building? Divisions and corps.

Jesus . . . Patton is smiling in his grave.

But that is . . . you know, it's 1940 all over again. We're trying to resurrect Patton, just as the French tried to resurrect Fouche.

Has anybody read his book about team meetings?

We've got to look at it through the lens of future warfare, and you see Stanley has got it right. That's why we fired him.

Hi, Charlie. I'm pushing the air force, Charlie.

[Audience Member] I'm glad you finally admitted it. I always have been concerned. Bob, what are your thoughts about two things. one was raised before: weaponization of the masses of the public, and how our military force is going to deal with it. In the Arab Spring, because you see an adversary that is going you know, human shields on steroids.

And then secondly, are you concerned at all and this is a real question whether there could be some kind of technical development that obviates the value of technology on the battlefield, like an EMP kind of weapon, and how should we

[Major General Scales] Twenty years, Charlie, when he had long black hair, we went at each other. Charlie was the advocate for the Air Force's whole strategy, and other things.

Rebecca Grant and Charlie, and I was the guy saying, no, it's about the soldier.

And, of course, when 9/11 came along, they realized I was right and Charlie was wrong.

[Audience Member] Let me say something good about Bob.

You may not remember this, Bob, but you're the one that really gave me the audience at the Army War College years and years ago, the new absolutist war, the war is going to be more political and causing so you always have been let me say this publicly.

You've always been on the cuttingedge.

So that's why right now, this moment, I will listen to you, but I'm also going to be ordering your book.

[Major General Scales] My son, my grandson wants to go to Harvard. Every damn one of you needs to buy this book, okay?

[Audience Member] We'll be selling that book here. We have that book here. You'll be doing some signing.

[Major General Scales] Let me answer the first question.

I don't think it matters as much in pure warfare. Also, when

Jerry was talking, it piqued my interest, because I don't think war of the masses is going to I do think mass I do think, sadly, I think when we go manoamano with the Russians or Chinese, it'll turn into a major conflagration.

Things we have forgotten, mobilization of nation, conscription, the psychological preparation for sacrifice, all those things that our nation experienced in the two world wars will be back on us, and I don't think anybody will give a damn about some dude in a back alley.

The same with subterranean war; I think that's a dead end.

Same thing with megacities. Look at where we fight. There're no megacities there. I think the marines are wrong in that.

The only advantage that urban warfare is going to have is actually on the defensive for the United States, not the offensive. Because the best place to survive a strikecounter-strike phase of a battle is actually, believe it or not, in a city. Because they offer an enormous amount of cover and concealment from massive fire strikes.

Forget the last eighteen years, guys. It's over. Done. You know?

Okay. So somebody, I don't know, blows up an embassy. Tragic. But that's not a threat to the world order or the survival of the United States as a democracy.

That only comes with peeronpeer bigtime warfare, and that's what we have to think about in the future, unfortunately.

Yes, sir?

[Audience Member] Dan Papp, formerly of Kennesaw State University and spent a lot of time in Carlisle and Montgomery.

What about the observation that we actually already won World War III, 1989 to 1991, called the Cold War. Because we're now in the midst of World War IV but didn't realize it until the Mueller report came out.

[Major General Scales] I disagree with that.

There's a good friend at Ohio State, I can't remember his name, and I wrote an article called World War IV, and my view was the first World War was a chemist war, and the second World War was a technologist war, and the third World War was an information war. To your point, we won it through information.

And World War IV, I said, is going to be the human and social war, where human beings and the development of the human factor–human domain, what we call it now damnis going to be the make-way.

I believe that's true. If I had more time I'd talk more about that.

I think the ultimate defeat of Russia by us, and China, if it comes to that, is going to be the quality of the way we harness the human dimension.

No, I don't buy that. I think that's a bunch of hooey.

Be careful listening to all this crap from the beltway. If it's tied to money, an idea or concept tied to money, it's probably wrong.

Motive is not defense of the nation. The motive of Lockheed Martin, Raytheon, and so forth . . . I learned that when I was a guy that forced the Army to buy a new rifle. It took me two and a half years and pissing everybody off in the Army. By the way, now the Army has determined it's their idea, and they're proud of the three new rifles we developed.

It was all because of money.

Lockheed Martin doesn't have a rifle division, so why should we care?

So be careful about the cost of something determining its value in future warfare.

I will argue with you that it's almost inverse.

By the way, if you think you have a great idea, to Charlie's point, if you think you have a great technological idea that will change the course of war in terms of warfare technology, chances are the enemy already has got it.

It's a wash.

Anybody else?

[Audience Member] Jim Solomon. I loved your book. I have a question for you.

How do you attract the type of people that you talked about that you're going to filter through to have that fighting force?

[Major General Scales] That's a great question.

First of all, I don't think we need to attract people. I think the military pyramid is pretty steep. I'm not worried about that. I am worried about picking the right people.

That's the issue.

And, unfortunately, the military educational system is bankrupt and also broken.

First of all, our system is incredibly ahistorical. It just makes me weep. The only reason I stayed in the Army after Vietnam half my class I was class of '66, famous class of '66. The only reason I stayed was Major Jack Woodman, history professor, history of Military Art, lit me up on studying my profession.

I've been doing it fifty-six years.

What did West Point do? Cut the military history program in half and got rid of it.

I got to tell you, I took physics and chemistry and math and social I don't remember a god damn thing of any of that. But I have a 6,000 book library at home, and I have that because of the inspiration I got in studying my profession.

You know, beating Navy and making the *Forbes* Top Ten Public Universities is important. But I've always thought that the purpose of education is to induce young men and women to stay in the profession and serve to term.

And the other problem is that what we're seeing now is that the educational system is too diffuse. The purpose of an educational system is to educate, but also to select the best and brightest. Therefore it must be attributable, and it must have standards for progression. Otherwise, you pick people on manner of performance. And you can't do that. Certainly not in the NCO Corps, what I studied most, but the Officer Corps as well.

Today, we pick generals based on performance as a company commander. That's wrong. There is no correlation, zero correlation, between tactical excellence and strategic acumen. They are unrelated. It's like taking a baker and turning him into a nuclear scientist. The two are unrelated. Yet, that's what we do. Because there's no accountability, and there's no attribution.

You can educate people I spent eighteen years of my thirty-five years in the Army as an educator. You can do this, but unless you have a way to grind off the Tommy Franks of the world, we're going to continue to produce them in the future and think we have a welleducated military. We don't. There has to be attribution. There have to be consequences for not being very bright or very imaginative or creative or, for that matter, good leaders. And the educational system needs to be the way that you do that. Unfortunately, today we don't.

Somebody else had a question or comment?

[Audience Member] A question, sir.

We've spoken a lot about Russia. Can I shift over to China? What is your viewpoint on that? Maybe if we can tie in with AI5G and the Belt and Road Initiative.

[Major General Scales] My information is not from the Army, because it's sort of new with China game.

The Navy and Marine Corps; the other hand, they've thought long and hard about that.

I'm worried about the other direction. The Seabourn approach.

And what is so great about my marine friends, they have completely turned the relation between the Navy and Marine Corps upside down because of the technology and threat from China.

In the old days in World War II, the purpose of the Marine Corps was to capture bases from which the Navy could maneuver. Now the purpose of the Navy is to move forward and wear away the second and first aisle of change so the marines can maneuver. That's fundamental.

First time I read that in the commandant's planning guide, I did a happy dance all over my study. I said, my God, these guys have got it right.

The marines understand that the Chinese can never be assaulted. They have to be worn away from the periphery. Peripheral warfare is different than smash mouth warfare.

The problem is the Navy is burdened by the fact that they had too many large platforms and too expensive and manpower intensive and, therefore, they can't maneuver close enough to a threat.

It's symbiosis between land power and sea power and air power that the marines are starting to develop, which is exciting. V22, their version of F35B and heavylift helicopter initiatives and aerial maneuver and dispersed distributed warfare, look at their doctrine and you can see everything I've been writing about during the last twenty years is deeply embedded in their philosophy.

The Army could learn from that.

[Audience Member] We have time for one more question. It will come from over here.

[Audience Member] Thank you. Enjoyed your presentation.

The question is, it seems to me that one of the things that underpins everything you're saying is, let's use the Army. I don't know where, don't know how, don't know when, don't know why to engage.

Why is that?

And what do we have to do with our training to change that?

[Major General Scales] That's a great question.

First of all, I think the strategic initiative is not on our side. I think it rests with the enemy, the Chinese and the Russians. Whatever happens, God forbid in the future, they'll be the ones to initiate.

So in that sense, the how I mean, the when and where part—I think it can't be determined. We generally can focus in on an enemy of some sort, but what is the deal?

From Pearl Harbor all the way up to 9/11, we always pretty much got it wrong. We're about zero for twelve when figuring out the circumstances you just brought up.

I think the only answer for us—to answer your second question—is we have to be able to build a military that is broadbased enough to be able to first absorb an enemy's aggression and then be able to react creatively.

Of course, the big unanswered question that should be on all of your minds right now is nuclear weapons. Everything that I have mentioned or anyone today or tomorrow is going to mention is that all this has to be conducted, you know, below the glass ceiling of nuclear warfare. Which changes the complexion considerably.

If you think Vladimir Putin doesn't have . . . this is what he dreams about at night. Just as Ukraine and Crimea and Georgia just came out of the blue, we had nothing to do that. I think whatever happens in the future, particularly I'm less concerned about China, I think China is too tied in with Walmart to go to war. But, I think Russia has everything to gain and very little to lose by being aggressive in breaking apart NATO.

Look what happened to Turkey. Putin was doing a happy dance in the Kremlin after a couple shots of vodka when he realized, by God, I'm now going to break apart NATO's southern flank by cozying up to . . .

The great game today is not in Central Asia and not the Middle East. The great game today is in the part of the world that counts. The economic center of gravity in the entire globe, northeast Asia and Europe. The rest of it frankly doesn't matter.

Great. Thanks a lot, guys.

4

How Far Can We Go: The Role of AI in Soldier-Leader Development

Dr. Ash Mady and Ms. Bethany Niese

Abstract

The nature of military conflict has dramatically changed in large part due to the advancement of technology. These advancements require changes in the skillsets of our soldier-leaders. Research and history have shown that hiring talent and ad-hoc fixes are not typically enough to keep up with rapid innovation and change. This paper provides an innovative conceptualization of how to capitalize on the value of emerging AI technologies for training and development in the military. We propose a holistic approach to augment AI and human capabilities in a capacity-based learning environment. We argue that in order to successfully create an AI-based augmented training system, multiple areas of study and application need to be addressed including training and learning best practices, system implementation best practices, AI-specific attributes, and aspects of the military culture and environment. Finally, the best way to pair humans and systems need to be examined. All these areas are explained in the specific context of the future military soldier-leader.

How Far Can We Go: The Role of AI in Soldier-Leader Development

Artificial Intelligence (AI) has been advancing over decades and developments are expected to continue. AI has the potential to influence or even disrupt operations of organizations (Fawkes, 2017). It is reasonable to think that computers with human-level intelligence, or beyond human-level intelligence, will strongly impact our future (Russell & Norvig, 2016). As time advances, AI is becoming more integrated into individuals' daily routine activities (Koch, 2018) in the form of autonomous self-driving cars, household devices that can execute voice commands for personal assistance (Kepuska & Bohouta, 2018), refrigerators which make suggestion for grocery shopping (Minh & Khanna, 2018), applications that routes people away from traffic, and photo applications that tag familiar faces automatically. AI will continue this transition from a novel scientific concept into viable technological applications which have the potential to exceed human capabilities (Russell, Dewey, & Tegmark, 2015). Research has shown the trajectory of AI to reach complex functionalities such as perceiving, understanding, predicting, manipulating, and acting on information about the world without human intervention (Lu, Li, Chen, Kim, & Serikawa, 2018).

The term AI was formally coined in 1956 (Russell & Norvig, 2016) and currently encompasses a large variety of subfields spanning from general-purpose to specific tasks. Applications include playing chess, proving mathematical theorems, writing poetry (Russell & Norvig, 2016), performing financial analysis of the stock market (Kim, 2006), making medical diagnosis (Esteva et al., 2017; Madani, Arnaout, Mofrad, & Arnaout, 2018), educating (Popenici & Kerr, 2017), advancing defense systems, executing governance, and providing transportation (Frank, Wang, Cebrian, & Rahwan, 2019). Organizations are increasing their use of autonomous systems which is causing greater interest in continuing advancement. As a result, society is striving to understand the present and future of AI as evidenced by recurring themes at summits and conferences (site the NATO Science and Tech Organization's 2017 theme).

The wars and conflicts of the past were focused in the physical world. Today, they are focused on destabilizing power grids, holding strategic organizations' data for ransom, and taking down cloud services, so the future of our security will focus more on code than on combat (Webb, 2019). As a result, there is a need for a new kind of soldier; one that has a tighter relationship with the advanced military systems. Training, preparation, and strategies will need to be redefined to support these new soldiers.

There have been many examples in history when the military realized significant changes and modified standard processes to reflect them. Recently, the US Army included critical thinking in its leader development program enabling them to "take initiative in the absence of orders" (Anwar, 2016). Army Sergeant Major Troxell stated that the military is empowering mid-level personnel who are able to apply agile and adaptive practices to defeat enemy threats, solve problems and accomplish missions based on the commanders' intent. Troxell also stated that empowerment can come only through training and trust (Garamone, 2019). Training has been increasingly focused on agile approaches since the 1980s when the idea that knowledgeable and empowered officers would make rapid, intelligent decisions that are aligned with the overall strategy, resulting in a disrupted enemy (Maciejewski, 2019) became well-accepted.

Making significant changes such as the migration to agile methodologies require retraining leaders, staff, analytics team, and end users to work and think in new ways. Research and history have shown that hiring talent and ad-hoc fixes are not typically enough to keep up with rapid innovation and change (Brown, Gandhi, Herring, & Puri, 2019). Broad education efforts can occur in formal educational settings such as in our universities to address potential talent as well as within organizations to address existing talent.

We argue that in order to successfully create an AI-based training system, multiple areas of study and application need to be addressed. Training and learning literature must be consulted. Also, because the proposed approach is AI-based information system for training, we argue that aspects of system development, implementation, and adoption must be addressed. AI and the use of intelligent systems must be understood and the best way to pair individuals and systems will be examined. Finally, the presented research model will be grounded in the specific context of the future military soldier-leader. The consideration of AI capabilities to provide customized capacity-based training is key. Our proposed model provides a holistic, agile training system utilizing AI capabilities.

In our work, we propose a holistic approach to augment AI and human capabilities in training and education. There has been limited knowledge regarding the best way to "share" accountabilities between AI and human in education. Also, there is limited knowledge regarding successful intelligent systems implementation and continuous use in the context of military training. In our study, we address these gaps and suggest an approach for successful AI implementation in a capacity-based environment to create military training environment.

The Definition of AI

AI can be difficult to define. The Webster dictionary defines the word artificial using terms including artifact, manufactured, unnatural, man-made, and imitation ("Merriam-Webster," 2020). The challenge comes when we try to identify intelligence (Bringsjord & Schimanski, 2003). Intelligence has been defined using competencies such as learning, logic, understanding, creativity, problem solving, self-awareness, emotional knowledge, and the ability to accomplish complex goals (Tegmark, 2017). The Oxford Dictionary defines AI as "the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages" ("Oxford English Dictionary," 2020). Researchers often identify AI in terms of the context of their work. In 1950, Turing described AI as systems which can act human-like and have the ability to achieve human-level performance (Turing, 1950). About 10 years later, AI was described as systems that can replicate human thought or follow human cognitive behavior (Newell & Simon, 1963). Russell and Norvig (2016) argued that AI is defined in two main dimensions: reasoning and behavior. Each dimension was measured by comparing the performance of a task as compared to human performance and by the ability to be rational or intelligent (Russell & Norvig, 2016).

This article's focus is on AI's application to military processes, specifically learning and training. As a result, the aspects of intelligence and performance are critical to its conceptualization. The definition of AI for this paper is computing systems that are able to engage in human-like processes such as learning, adapting, synthesizing, self-correction and use of data for complex processing tasks (Popenici & Kerr, 2017).

The History of AI

The possibility of machine learning and AI was presented by Turing (1950) in his paper "Computing Machinery and Intelligence". This idea didn't easily translate into the development into actual systems because AI research complications proved more difficult than anticipated. These complications included the rigidity of rule-based methodologies and natural language translation. As a result, the initial AI and machine learning systems provided a rather naïve output (Taulli, 2019). The period between the 1970s and the 1980s is often referred to as AI winter (Crevier, 1993). This time is characterized with numerous disappointing attempts and failing AI initiatives that caused loss of interest and reduced funding budgeted for AI innovation. AI's research progress accelerated in the late 1990s as researchers focused more on sub-problems of AI and the application of AI to real-world problems such as image recognition and medical diagnosis (Buchanan, 2005). As time went on, methodologies were developed to overcome issues which resulted in progress and innovation as shown in the Figure 1.

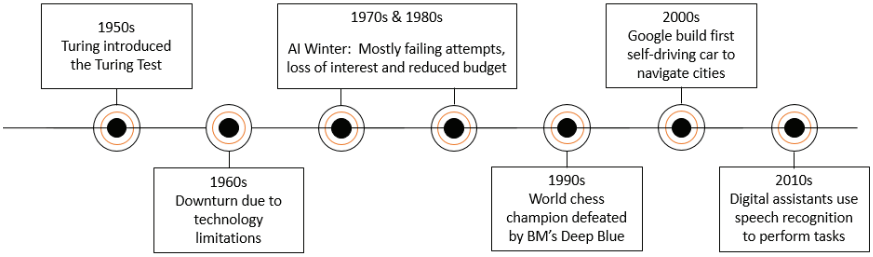

1950s
Turing introduced the Turing Test
1960s
Downturn due to technology limitations
1970s & 1980s
AI Winter: Mostly failing attempts, loss of interest and reduced budget
1990s
World chess champion defeated by BM's Deep Blue
2000s
Google build first self-driving car to navigate cities
2010s
Digital assistants use speech recognition to perform tasks

Figure 1: A summary timeline of AI progress and innovation

AI can be divided into two groups; those purposed for general tasks and those purposed for specific tasks. AI that can support general purpose is called "strong AI" because these machines can learn topics similar to humans (Huang & Rust, 2018). AI that can be only support a specific task or problem for a specific domain, is referred to as "weak AI" (Borana, 2016).

Strong AI was the original motivation beyond AI research; it was the way in which AI was depicted in fiction and movies. However, technology limitations stifled its progress. Strong AI required tremendous amount of data to process and account for many possibilities. To create such a powerful computing power was not practical and economically not feasible. Only in recent years, when powerful computers became economically feasible, the advancements in strong AI applications became a reality. Strong AI will potentially revolutionize national security affairs by decreasing the human cost of war while increasing the speed and efficiency at the tactical, operational, and strategic levels of conflict (Stewart, 2015)

Military Applications of AI

The development of AI does not only occur in private or commercial organizations; military development of AI is significant. A primary deliverable of any defense system is to deliver technologically superior military capabilities to a diverse range of domestic and international missions (Hurley, 2018). This requirement continues to drive the exploration of AI applications in the military.

During WWII, airplanes experienced jumps in innovation resulting in significant increases of speed. This presented a challenge to antiaircraft defense systems at the time because they were based on the speed of humans holding and firing guns. Despite the available tools to help the manual calculations, the traditional concept of a human pointing a gun needed to change. The need for a conceptual design to combine the human capabilities with the speed and accuracy of machines emerged (Fawkes, 2017).

In 2017, news outlets communicated that the Department of Defense kicked off a campaign to integrate machine learning across military weapons and intelligence systems (Magnuson, 2017). The US Air Force Research Laboratory funded an approach to study the use of AI fuzzy logic which is a form of many-valued logic used in a decision tree to handle many inputs with relatively low processing demands. This research led to the development of flight simulator tests that outperformed experienced combat pilot in a variety of combat scenarios. The gap between smart systems and the fighters started to close. However, the new symbiotic relationship of operations where humans interact with AI-enabled systems is changing, humans, structures, and the technology itself.

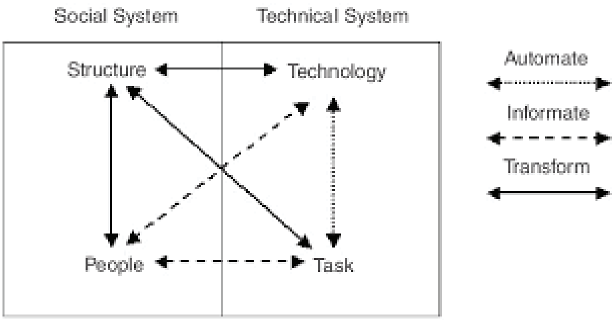


Figure 2: The socio-technical systems - O'Hara et al., 1999

Decision-makers must pay attention to the human aspects instead of just continue to emphasize the technical system to maximize the performance (O'Hara, Watson, & Kavan, 1999). The new generation of warfare is focused on collapsing the enemy internally rather than physically with no definable battlefields or fronts to the point that the distinction between "civilian" and "military" may disappear (Gazette, 1989). As the reliance on AI increases, the structure of the organization, the tasks to be accomplished, and the skills required from people will change. The expectations from warfighters has changed from the Spartan regime that produced ruthless machine-like soldiers to warfighters who are able to fight by pressing buttons from the safety of remote command locations (Galliott & Lotz, 2016).

Autonomous Weapon Systems

There have always been ethical concerns when it comes to war. That concern changes somewhat when considering human responsibilities in a hyper-connected world (Simon, 2015). The integration of AI in weapon systems, referred to as autonomous weapons systems (AWS), has the potential to provide a more humane, precise, and economical warfare. It can also overcome human limitations, such as fear, stress, and self-preservation instinct, providing superior performance at low cost (Galliott & Lotz, 2016). However, it also has the potential to further remove the humanity of war; AWS can operate without supervision in unstructured environments to attack inhabited buildings, vehicles, or even individuals (Altmann & Sauer, 2017).

AWS have the ability to adapt and self-learn over time (Altmann & Sauer, 2017) which may enable AI to create autonomous network of land, sea, and aerial robots that will operate together to locate and destroy targets without human intervention (Sharkey, 2012). There is also concern around whether AWS can reliably discriminate between combatants and non-combatants actors in complex situations (Arkin, 2009).

Simulations

The cost of training is expensive. Costs include the land for training, transporting troops, equipment, and ammunition. In recent years the economy and effectiveness of training as well as trainee safety has been advanced by utilizing AI sophisticated systems (Fawkes, 2017).

AI is enhancing military training with the use of simulators. These realistic simulations train soldiers to use complex equipment, work in teams, follow strategic movements in the battlespace, and negotiate conflicting scenarios efficiently (Macedonia, 2002). Commanders can use it to coordinate the movement and synchronize battlefield actions of thousands of soldiers, weapons, vehicles, and aircraft using advanced AI systems. Decision makers can leverage AI to evaluate strategic options prior to launching campaigns. These systems have also proven to be effective in enhancing soldiers motor control, response to an unexpected scenarios, and calculating the resources needed for combat (Macedonia, 2002).

The benefits of simulations have spawned many research and development projects. The Joint Simulation System (JSIMS) program is an integrated simulation environment that permits a real-time virtual simulation of a real-world battlefield that can be configured for use in exercises of differing durations, scenarios, and complexities (Bennington, 1995). Similarly, the US Army provided a five-year grant to the University of Southern California to create a research center, the Institute for Creative Technologies (ICT), to support collaboration between the entertainment and defense industries, to apply entertainment software technology to military simulation, training and operations, and to leverage entertainment software for militarily relevant academic research (Timothy Lenoir, 2003). The biggest boost in this direction was provided by The Department of Defense's research and development organization, the Defense Advanced Research Projects Agency (DARPA). DARPA funded SIMNET, the military's distributed SIMulator NETworking project. The main principle of the SIMNET is to permit a cost-effective interactive simulators for combat elements such as logistics, armored vehicle, artillery, aircrafts, administrative units, and command-and-control centers (Tim Lenoir & Lowood, 2002). SIMNET provided highly interrelated innovative components and its value as a training system for preparing units for battle became apparent. Studies listed SIMNET as one of six programs that have had the most profound effects on the Department of Defense (Miller, 2015).

Training Applications of AI

Data generation, storage capacity, computer processing power, and modeling techniques are enabling technology such as AI which has the promise to help with such rapid and at-scale change (Fountaine, McCarthy, & Saleh, 2019). A common approach to learning and training is to leverage the structure of Bloom's taxonomy. Bloom's taxonomy suggests that learning be examined and created using three domains; cognitive (thought), affective (emotion), and psychomotor (movement) (Bloom, Engelhart, Furst, Hill, & Krathwohl, 1956; Krathwohl, 2002). The cognitive domain includes knowledge and intellectual abilities. The affective domain includes the attitudes, values, motivations and interests of the learner. The psychomotor domain includes physical movement, coordination, and techniques in execution. AI can be arranged in a similar way. Algorithms in the affective domain can include internalizing, organizing, valuing, responding, and receiving. Related and existing AI in this category include Siri, Alexa, and Microsoft's Digital Assistant. Algorithms in the cognitive domain can include creating, evaluating, analyzing, applying, understanding, and remembering. Related AI in this category include IBM's Watson, Google, and Facebook. Algorithms in the psychomotor domain can include origination, adaption, complex response, mechanism, guided response, set, and perception (Holmes, Bialik, & Fadel, 2019). Related AI in this category include self-driving cars and automated drones.

Expectations of roles have been changing from a focus on effectiveness and efficiency to a focus on the ability to successfully navigate dynamic roles and on-demand learning (Bell, Tannenbaum, Ford, Noe, & Kraiger, 2017; Maity, 2019). As a result, the ability to evaluate soft skills is necessary. AI may provide more accurate evaluations than individuals. Individuals have a degree of attribution error when attributing causes to outcomes (Pan, Pan, & Newman, 2007). An example of attribution error is an individual attributing a negative outcome to external causes, making her/him feel that their personal performance was adequate, even though the results were not satisfactory. If AI were applied to this situation, the attitudes, beliefs, and biases of the individual would not be considered when providing a performance evaluation.

AI has the ability to evaluate not only an individual's answers to questions which allows for the traditional measurement of "how far away from the correct answer" they are, but also measure parameters like facial expressions, verbal tones, and emotions (Maity, 2019). AI can also categorize learners by their capabilities, personalities, self-efficacy, motivations, values, interests, attitudes, emotions, and perceptions (Bell et al., 2017; Maity, 2019). This data can then be analyzed to prescribe profiles which can then be used to provide targeted training. For example, each individual could be assigned a specific mode of training (online vs face-to-face, location), a specific trainer type, visual vs text, schedules, evaluation type (grades and points vs. recognition), pace, individual vs team learning, and module length.

AI can also analyze large amounts of data. In the example of the ALM learning system, an AI could connect individual achievements to required competencies by specialty (Johnston et al., 2015). This data could be used by soldiers to understand how they rank within their specialty and therefore where to place focus, by instructors to signal talent for recruiting purposes and provide early warnings for those falling behind and by military leaders to identify specific experiences required for success in specific situations.

There has been limited activity involving the best way to "share" accountabilities between AI and human in education. There are many instances of machines "outsmarting" humans; Watson beat former Jeopardy champions in 2011 and Deep Blue beat the world champion, Garry Kasparov, at chess in 1997. However, an experiment showed that a human-and-machine team could beat humans alone and machines alone (Brynjolfsson & McAfee, 2014). This study suggests that an approach of augmented intelligence could be the key to a highly effective approach. This pairing of humans and systems can be applied to the military; it would allow for the combination of the strengths of both to increase situational awareness, allowing the armed forces to conduct operations that include combat support and intelligence (Fawkes, 2017).

Research Model

A Holistic Approach to Training

It is becoming clear that education is a key element in navigating an environment of rapid innovation and change. A survey done in a recent practitioner journal showed that employees of all levels of high-performing companies are better educated about data concepts than in lower-performing companies (Brown et al., 2019). In order to create new soldiers who have strong relationships with advanced systems, a significant training and education system must be created and implemented.

Learning systems are critical to the achievement of the defined outcomes. Training has been conceptualized as a system since the 1980s (Bell et al., 2017). These systems include components such as design and training to promote learning, trainee characteristics, and environmental characteristics (Bell et al., 2017). Since AI is a type of technology, it makes sense to consult the information systems research to identify components of an appropriate and effective learning system. IS research has consistently shown that the primary reasons for project failure during technology implementation include factors such as a lack of focus on fitting the technology initiatives into the culture of the organization, managing the change on every level from the executive level leaders to the operational employees, not enough focus on aligning processes and technologies, and ensuring consistent organizational strategies (Fountaine et al., 2019; Gill, 1995; Holmes et al., 2019). As a result, these components should be reflected in the training system for AI.

A key component to any learning system is its content. The rate at which students and trainees forget content is staggering; research has shown that training is forgotten at a rate of about 50% every two years (Holmes et al., 2019). This suggests that learning systems need to deliver "customized" content to reduce the amount of superfluous information, deliver the content as needed, and/or include reinforcement modules to ensure retainment. This goal is made more complex by the current high rate of innovation.

The United States military has taken significant steps toward creating a holistic approach to training and have even coined the phrase "adaptive instruction" to communicate the uniqueness of this approach as compared to past methodologies (Johnston et al., 2015). The Army research laboratory has been investigating the development of adaptive methods to automate the creation, delivery, and evaluation of computer-regulated training (Johnston et al., 2015). The learning system is called the US Army Learning Model (ALM) and considers multiple components which research and historical observations have identified, however, there are several gaps. The gaps include a lack of adaptive systems to support the identified training, lack of capability to analyze training data, lack of an accessible and cost-effective training environment, and an inability to replicate complex and ambiguous environments (Johnston et al., 2015). There are structures and foundations that can be leveraged from existing training systems such as the ALM, however, the identified gaps highlight the existence of flaws in the system.

In order to successfully create and maintain a holistic, agile training system using AI, multiple areas of study and application need to be consulted. Since the outcome of the training effort is individual learning, training and learning literature must be consulted. AI requires aspects of system development, systems implementation, and aspects of end users such as adoption and effectiveness; thus, information systems literature must be included. AI-specific research is also critical so that it can be understood the best way to pair individuals and systems. Also, the attributes specific to the military should be considered so that the strengths can be leveraged, the areas of development be mitigated, and that the system is managed within the context of the culture.

In addition, a clear and strategic purpose and vision for the training itself and the outcome of the training must be transparent. It has been suggested that in order for students to make meaning, the content of the teaching should be closely related to feelings of purpose, understanding and engagement (Holmes et al., 2019). As a result, the learning systems goals and plan to achieve those goals should be shared with the learners and supported by the leadership.

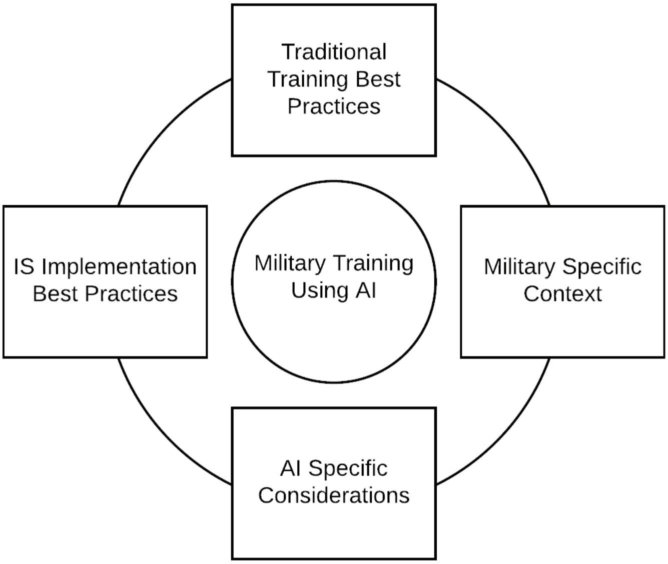

Traditional Training Best Practices
IS Implementation Best Practices
Military Training Using AI
Military Specific Context
AI Specific Considerations

Figure 3: Research model

Challenges & Concerns

Although AI has promise in its ability to address gaps and opportunities within training military personnel, there are problematic areas which exist and will need to be considered when designing, creating, and maintaining learning systems. The real world is full of ambiguity, uncertainty, context, variations, and unpredictability which hinders AI development and implementation.

Mis-categorization

AI has encountered issues categorizing subjects when relying completely on statistical significance from observations. The mathematical process of categorization can lead to many false positives and great deal of inaccuracy. These incorrect categorizations can lead to serious problems such as misdiagnosis of diseases, mistaken identity, security threats, inaccurate drones hits, etc.

Mis-categorization and inaccuracy can impact human identification. For example, in 2015, Google's AI image recognition software classified photos of several individuals with dark skin as gorillas (Nieva, 2015). Google's response was to remove gorillas as a classification as opposed to resolving the root cause of the issue. In 2017, the iPhone 10 could not differentiate between individuals of Asian descent allowing one individual of Asian descent to open another's phone regardless of gender or age (Zhao, 2017). The cause of issues such as these are a biased sampling of data which takes place when data is reported without including the full range of possible categories. Categorization also becomes more complex when dealing with subjective ideas. It is relatively easy to accurately identify and categorize objects such as books, cars, or buildings. However, when the categorization is subjective, such as dangerous, peaceful, risky, or safe, mistakes are more likely to occur.

Algorithm and Stability Bias

AI systems are programmed by potentially biased programmers and trained on potentially biased data (Bellamy et al., 2018). As a result, the output of the AI can be highly inaccurate and offensive. For example, in 2016, a self-learning Microsoft twitter bot "Tay" was released to mimic the language patterns of a nineteen-year-old American female and learn from interacting with other Twitter users. Tay became a misogynistic and anti-sematic conspiracy theorist in just 12 hours (Neff & Nagy, 2016). Another example involves the AI machine translation systems that failed to provide reliable translations when complicated language or rare terms were used (Zong, 2018). When it translated to English from a language with a gender-neutral third person pronoun such as the Turkish language, inaccurate results were produced (Vincent, 2019). AI algorithms rely on statistical data to associate what words would be more likely associated with men or with women. As a result, a reference to a third person soldier was translated to "he" while a nurse was translated to "she". Yet another example is the racially biased COMPAS system, an AI system for parole and correction decisions. Black defendants were more likely to be classified as higher risk than white defendants.

Social Impacts

In order for an AI to create user profiles to allow for personalized learning, a mass amount of data would need to be gathered into a single database. Examples include learning patterns, psychological evaluations, and behavioral tests. In addition, subsequent data would need to be continuously captured to determine effectiveness of the system so adjustments and improvements could be made. For this to happen, learners would need to be observed and monitored. There are multiple potential issues.

This amount of data on named individuals in a single location is unprecedented. The value and potential alternate uses of this data poses a significant risk. This risk can come in many forms. Data can be taken by malicious insiders or stolen by hackers. Data quality could suffer due to a lack of governance which would lead to inappropriate decisions and actions (Clarke, 2016).

In addition, the constant observation and monitoring needed for progress tracking and continuous improvement could have negative effects. For example, a school in China implemented cameras with facial recognition with the stated purpose to measure attentiveness, enjoyment of the material, emotional mood, and distractedness. Many students experienced anxiety because they feel that they're always "performing" and need to be at their best at all times or it may lead to discrimination from teachers and administration (Wang, Hong, & Tai, 2016).

Another negative impact is that algorithms lack transparency. This lack of transparency has many sources. One of these sources is how the software is developed; although much of AI technology is open source, most AI innovative inventions and products are patented and protected as intellectual property (closed source). In closed source software, the source code is not publicly visible, as it is with open source. It has been found that the issues in open source software diffuse more rapidly than in closed source (Ransbotham, 2010) and that open source vendors release patches more quickly than closed-source vendors (Arora, Krishnan, Telang, & Yang, 2010) likely because of the number of diverse developers who can identify and work to resolve issues. Closed source algorithms prevent any reviews to ensure accuracy and fairness in the outcomes. Therefore, more open sourced AI software would likely improve and progress faster than closed source.

Another source of lack of transparency is the complexity of the algorithms and inability to review the data which was used to train the AI. Even if the code is available for review as with open source, there is a lack of qualified individuals who can perform the review and report out on findings; an independent lab found that only .00000142% (less than 10,000) of the population in the world have the necessary skills to implement serious artificial intelligence research (Metz, 2018). Also, without visibility into the data which trained the AI, it's difficult to determine if the resulting algorithms are biased (Clarke, 2016). This transparency issue is often referred to as black box models and is especially problematic in unexplainable outcomes in criminal justice and health sciences (Emmert-Streib, Yli-Harja, & Dehmer, M, 2020). Lack of transparency may contribute to the challenges discussed here such as bias and issues with accuracy and fairness. For example, categorizations of students impact the training content and opportunities given to those students. Without transparency, it may not be clear to the learner how they've been categorized or how to change their behavior to achieve personal goals. Even worse, this situation could lead to general profiling or discrimination.

Ethics & Privacy

AI systems are evolving from tools to autonomous agents and team-mates and, therefore, will be making ethical decision (Dignum, 2018). For example, decision-making during automated vehicles crashes quickly becomes an ethical decision (Goodall, 2014). Scholars raised concerns ragarding the ethical use of AI (Etzioni & Etzioni, 2017). Researchers argued that AI can be manipulated and suggested the use of decision trees to increase transparency and mitigate the unethical use of AI (Bostrom & Yudkowsky, 2014). Microsoft identified six guiding principles to develop and use AI. These guiding principles covered fairness, reliability and safety, privacy and security, inclusiveness, transparency, and accountability (Microsoft, 2020).

In order for AI to deliver on the promise as highlighted in this document, a great amount of data will need to be identified, concatenated, and analyzed. Learner profiles will need to contain personality test results, behavioral profiles, and response results. As a result, the organizations which house this data must be vigilant in protecting this data. Some data will need to follow rules and regulations such as HIPPA, but not all data has regulated protections (Watson, 2017). Therefore, researchers advocated the integration of ethical standards in coding and algorithm, regulation and engineering, and the management of AI (Dignum, 2018). As AI shows social impactions, the creation, use, and management of AI should be govenred to address the ethical issues of AI.

Conclusion

AI has many applications including facial recognition, individual personal assistance and autonomous military defense systems. Its potential continues to evolve and, in some cases, seems to exceed human capabilities which may strongly impact our future. It can perform data analysis beyond human capacity to provide recommendations and future predictions in every domain. Organizations are increasing their use of AI's autonomous systems and showing greater interest in continuous use of AI enabled systems.

AI capabilities are changing military defense systems and the strategies of the new generation of warfare. As a result, the expectations from the future military soldier-leader are changing. This requires retraining future military soldiers and leaders to work and think in new ways. AI is enhancing military training with the use of simulators and intelligent systems. However, there isn't a cohesive and holistic framework for augmenting AI and human capabilities in capacity-based learning. This research proposes a framework to address this gap. This pairing of humans and systems can be key to a highly effective approach to the military training and education.

We argue that multiple areas of study and application need to be addressed in order to successfully create an AI-based augmented training system. Since the outcome of the training effort is individual learning, training and learning literature must be consulted. Training literature supports that training approaches need leverage three domains: cognitive (thought), affective (emotion), and psychomotor (movement). Also, because the proposed approach is AI-based information system for training, we argue that aspects of system development, implementation, and adoption must be addressed. AI-specific research is also critical so that AI and the use of intelligent systems can be understood and the best way to pair individuals and systems can be examined. Finally, the training in the specific context of the future military soldier-leader should be considered.

The United States military has already been investigating the development of adaptive methods and applying AI technology. However, without a holistic framework, these efforts will likely result in an ad-hoc approach producing limited value. Our proposed model addresses these gaps as well as points out known challenges so that a holistic, agile training system can be developed, implemented, and maintained in a way that delivers its intended value.

References

Altmann, J., & Sauer, F. (2017). Autonomous weapon systems and strategic stability. *Survival, 59*(5), 117-142.

Anwar, S. (2016). Saber Junction 16 Empowers Junior Leaders. Retrieved from https://www.army.mil/article/165901/saber_junction_16_empowers_junior_leaders

Arkin, R. (2009). *Governing lethal behavior in autonomous robots*: Chapman and Hall/CRC.

Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2010). An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure. Information *Systems Research*, *21(1), 115*.

Bell, B., Tannenbaum, S., Ford, K., Noe, R., & Kraiger, K. (2017). 100 years of training and development research: What we know and where we should go. *Journal of Applied Psychology, 102*(3), 305-323.

Bellamy, R. K., Dey, K., Hind, M., Hoffman, S. C., Houde, S., Kannan, K., Mojsilovic, A. (2018). AI Fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias. *arXiv preprint arXiv:1810.01943*.

Bennington, R. W. (1995). *Joint Simulation System (JSIMS)-an overview.* Paper presented at the IEEE 1995 National Aerospace and Electronics Conference, Dayton, OH, USA.

Bloom, B., Engelhart, M., Furst, E., Hill, W., & Krathwohl, D. (1956). *Taxonomy of Educational Objectives: The Classification of Educational Goals*. New York: David McKay Company.

Borana, J. (2016). Applications of artificial intelligence & associated technologies. Proceeding of International Conference on Emerging Technologies in Engineering, Biomedical, Management and Science, *5*(6).

Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge handbook of artificial intelligence*, *1*, 316-334.

Bringsjord, S., & Schimanski, B. (2003). *What is artificial intelligence? Psychometric AI as an answer.* Paper presented at the IJCAI.

Brown, S., Gandhi, D., Herring, L., & Puri, A. (2019). Bridging the Gap Between Human and Artificial Intelligence. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-analytics-academy-bridging-the-gap-between-human-and-artificial-intelligence

Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age. *Milken Institute Review: A Journal of Economic Policy, 16*(3), 67-80.

Buchanan, B. G. (2005). A (very) brief history of artificial intelligence. *AI Magazine, 26*(4), 53-53.

Clarke, R. (n.d.). Big data, big risks. *Information Systems Journal, 26(1), 77–90*.

Crevier, Daniel (1993). *AI: The Tumultuous Search for Artificial Intelligence*, New York, NY: BasicBooks, *ISBN 0-465-02997-3.*

Dignum, V. (2018). Ethics in artificial intelligence: introduction to the special issue. *Ethics and Information Technology, 20, 1-3.* Retrieved from: https://doi.org/10.1007/s10676-018-9450-z

Emmert-Streib, F., Yli-Harja, O., & Dehmer, M. (2020). Explainable Artificial Intelligence and Machine Learning: A reality rooted perspective. arXiv preprint arXiv:2001.09464

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. *Nature, 542*(7639), 115.

Etzioni, A., & Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics*, *21*(4), 403-418.

Fawkes, A. J. (2017). Developments in Artificial Intelligence–Opportunities and Challenges for Military Modeling and Simulation. Paper presented at the Proceedings of the 2017 NATO M&S Symposium.

Fountaine, T., McCarthy, B., & Saleh, T. (2019). What it Really Takes to Scale Artificial Intelligence. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-blog/what-it-really-takes-to-scale-artificial-intelligence

Frank, M. R., Wang, D., Cebrian, M., & Rahwan, I. (2019). The evolution of citation graphs in artificial intelligence research. *Nature Machine Intelligence, 1*(2), 79-85.

Galliott, J., & Lotz, M. (2016). *Super soldiers: the ethical, legal and social implications*. Routledge.

Garamone, J. (2019). Noncommissioned Officers Give Big Advantage to US Military. Retrieved from https://www.army.mil/article/229633/noncommissioned_officers_give_big_advantage_to_us_military.

Gazette, M. C. (1989). The Changing Face of War: Into the Fourth Generation William S. Lind, Colonel Keith Nightengale (USA), Captain John F. Schmitt (USMC), Colonel Joseph W. Sutton (USA), and Lieutenant Colonel Gary I. Wilson (USMCR). *Marine Corps Gazette*, 22-26.

Gill, G. (1995). Early Expert Systems: Where Are They Now? *MIS Quarterly, 19*(1), 51.

Goodall, N. J. (2014). Ethical decision making during automated vehicle crashes. *Transportation Research Record*, *2424*(1), 58-65.

Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial Intelligence in Education*. Boston, MA: The Center for Curriculum Redesign.

Huang, M.-H., & Rust, R. T. (2018). Artificial intelligence in service. *Journal of Service Research, 21*(2), 155-172.

Hurley, J. S. (2018). Beyond the struggle: artificial intelligence in the department of defense (DoD). Paper presented at the ICCWS 2018 13th International Conference on Cyber Warfare and Security.

Johnston, J. H., Goodwin, G., Moss, J., Sottilare, R., Ososky, S., Cruz, D., & Graesser, A. (2015). *Effectiveness evaluation tools and methods for adaptive training and education in support of the US Army learning model: research outline. Army Research Lab Aberdeen Proving Ground Md Human Research and Engineering Directorate, ARL-SR-0333.*

Kepuska, V., & Bohouta, G. (2018). Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home). Paper presented at the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).

Kim, K.-j. (2006). Artificial neural networks with evolutionary instance selection for financial forecasting. *Expert Systems with Applications, 30*(3), 519-526.

Koch, M. (2018). Artificial intelligence is becoming natural. *Cell, 173*(3), 533.

Krathwohl, D. (2002). A revision of Bloom's Taxonomy: An Overview. *Theory Into Practice, 41*(4), 212-218.

Lenoir, T. (2003). Programming theatres of war: Gamemakers as soldiers. Latham, R. Bombs and Bandwidth: The emerging relationship between information technology and security. New York: The New Press. Draft chapter accessed on January, 14, 2006.

Lenoir, T., & Lowood, H. (2002). Theaters of war: The military-entertainment complex. Collection, laboratory, theater: Scenes of knowledge in the 17th century, 427-456.

Lu, H., Li, Y., Chen, M., Kim, H., & Serikawa, S. (2018). Brain intelligence: go beyond artificial intelligence. *Mobile Networks* *and Applications, 23*(2), 368-375.

Macedonia, M. (2002). Games soldiers play. *IEEE Spectrum, 39*(3), 32-37.

Maciejewski, J. (2019). How the British Army's operations went agile. *McKinsey & Company*. Retrieved from https://www.mckinsey.com/business-functions/organization/our-insights/how-the-british-armys-operations-went-agile.

Madani, A., Arnaout, R., Mofrad, M., & Arnaout, R. (2018). Fast and accurate view classification of echocardiograms using deep learning. *NPJ digital medicine, 1(1), 6.*

Magnuson, S. (2017). DoD Making A Big Push to Catch Up on Artificial Intelligence. *National Defense.*

Maity, S. (2019). Identifying opportunities for artificial intelligence in the evolution of training and development practices. *Journal of Management Development. (8), 651.*

Merriam-Webster. (2020). Springfield, MA: Merriam-Webster, Incorporated.

Metz, C. (2018). Tech giants are paying huge salaries for scarce AI talent. The New York Times. Retrieved from https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html.

Microsoft (2020). Identify guiding principles for responsible AI. *Microsoft Learn.* Retrieved from: https://docs.microsoft.com/en-us/learn/modules/responsible-ai-principles/index

Miller, D. C. (2015). SIMNET and Beyond: A History of the Development of Distributed Simulation. Retrieved from https://www.iitsec.org/-/media/sites/iitsec/link-attachments/

iitsec-fellows/2015_fellowpaper_miller.ashx

Minh, V. T., & Khanna, R. (2018). Application of Artificial Intelligence in Smart Kitchen. *International Journal of Innovative Technology and Interdisciplinary Sciences, 1*(1), 1-8.

Neff, G., & Nagy, P. (2016). Automation, algorithms, and politics| talking to Bots: Symbiotic agency and the case of Tay. *International Journal of Communication, 10*, 17.

Newell, A. & Simon, H. A. (1963) GPS, a program that simulates human thought. In: Computers and thought, ed. Feigenbaum, A. & Feldman, V., pp. 279–93. New York: McGraw Hill

Nieva, R. (2015). Google apologizes for algorithm mistakenly calling black people 'gorillas'. Retrieved from https://www.cnet.com/news/google-apologizes-for-algorithm-mistakenly-calling-black-people-gorillas/

O'Hara, M. T., Watson, R. T., & Kavan, C. B. (1999). Managing the three levels of change. *Information Systems Management, 16*, 63-70.

Oxford English Dictionary. (2020). United Kingdom: Oxford University Press.

Pan, G., Pan, S., & Newman, M. (2007). Information Systems Project Post-Mortems: Insights from an Attribution Perspective. *Journal of the American Society for Information Science and Technology, 58*(14), 2255-2268.

Popenici, S. A., & Kerr, S. (2017). Exploring the impact of artificial intelligence on teaching and learning in higher education. *Research and Practice in Technology Enhanced Learning, 12*(1), 22.

Ransbotham, S. (2010, June). An Empirical Analysis of Exploitation

Attempts Based on Vulnerabilities in Open Source Software. In Weis.

Russell, S., Dewey, D., & Tegmark, M. (2015). Research priorities for robust and beneficial artificial intelligence: an open letter. *AI Magazine, 36*(4).

Russell, S., & Norvig, P. (2016). *Artificial intelligence: a modern approach*: Malaysia; Pearson Education Limited.

Sharkey, N. E. (2012). The evitability of autonomous robot warfare. *International Review of the Red Cross, 94*(886), 787-799.

Simon, J. (2015). Distributed epistemic responsibility in a hyperconnected era. In *The Onlife Manifesto* (pp. 145-159): Springer, Cham.

Stewart, J. (2015). Strong Artificial Intelligence and National Security: Operational and Strategic Implications. *Defense Technical Information Center.* Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a622591.pdf

Taulli, T. (2019). AI Foundations. *Artificial Intelligence Basics*. Berkeley, CA: Apress.

Tegmark, M. (2017). *Life 3.0 Being Human in the Age of Artificial Intelligence*. New York: Vintage Books.

Turing, A. M. (1950). Computing machinery and intelligence-AM Turing. *Mind, 59*(236), 433.

Vincent, J. (2019). Google's head of translation on fighting bias in language and why AI loves religious texts. Retrieved from https://www.theverge.com/2019/1/30/18195909/google-translate-ai-machine-learning-bias-religion-macduff-hughes-interview

Wang, Y., Hong, S., & Tai, C. (2019). Wall Street Journal. Retrieved from: https://www.wsj.com/articles/chinas-efforts-to-lead-the-way-in-ai-start-in-its-classrooms-11571958181.

Watson, H. (2017). Preparing for the Cognitive Generation of Decision Support. *MIS Quarterly Executive*, *16*(3), 153-169.

Webb, A. (2019). Economic Warfare Technologies. *Future Institute Today, 117*. Retrieved from https://futuretodayinstitute.com/.

Zhao, C. (2017). Is the iPhone X Racist? Apple Refunds Device That Can't Tell Chinese People Apart, Woman Claims. Retrieved from https://www.newsweek.com/iphone-x-racist-apple-refunds-device-cant-tell-chinese-people-apart-woman-751263

Zong, Z. (2018). Research on the Relations Between Machine Translation and Human Translation. Paper presented at the Journal of Physics: Conference Series.

[See Appendix for corresponding PowerPoint presentation.]

5

The Nature of Future Warfare: Panel Discussion

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

[Daniel Papp] Welcome, everyone, to this first panel, "The Nature of Future Warfare."

We have an hour and a half for excellent presentations and will devote the last fifteen minutes or so of that hour and a half to questions and answers.

I'll introduce each one of the panelists before they actually make their presentation.

Our first paper is by an active-duty infantry officer in Romanian land forces. Lieutenant Colonel Laviniu Bojor holds a Ph.D. in military sciences. Since 2017, he has also been university lecturer in the Department of Military Sciences at the Land Forces Academy in Romania.

In addition to his academic expertise and background, he also has served as a platoon leader in Kandahar Afghanistan, supporting operation "Enduring Freedom." More recently, he served in Dakar province Iraq for the Babylonia mission. And he also served in Zabul province Afghanistan as a company commander.

His presentation is entitled "Preparing Military Leaders for Future UnPredictable Events."

Doctor, the floor is yours.

Preparing Military Leaders for Future Unpredictable Events

Lieutenant Colonel Laviniu Bajor

Thank you.

You forgot to mention my Russian accent language.

I will start with a short story from my experience, my human life story. After that, I want to present some transformation of our environment based on this artificial intelligence. Then I will try to suggest some challenges from previous military conflicts, basically from my experience, and also a solution for how we can deal with these artificial intelligence.

In 2007, I was conducting a research mission when I heard on the radio station a message from my battalion commander that unmanned vehicles discovered a possible insurgent near a village in our operation. Something was wrong. Because I know very well that leader. I know the community. It was friends of our forces, and I tried to see what is going on.

I asked to cancel and go there.

They finally approved me.

When I arrived there, I discovered that insurgent was actually a farmer who is shifting the grain. And I could say that I saved a life. But not only did I save that life, but I also have a good relation with that community in the next months.

As I said, today we have this artificial intelligence characterized with voice recognition, prediction and weather forecasts, and so on. Very powerful, designated powerful in only some domains. Making connection, connecting to the Internet and learning from algorithms and also being more human, innovative and creative and confident in making decisions under pressure.

And possibly in the future we have that singularity. Artificial intelligence machines, more so than humans.

And IA lies how it can affect the future environment, and the worst case is when strong AI will turn against humanity and, of course, we have that Skynet loading, and our soldier will fight on horseback and use sensor free weapons, and I'm pretty sure we'll not have a final ending like hasta la vista, baby.

Unless we can stop these events, it is not a military decision. It's a political one, but we cannot stop these events.

And it's not related to China or Russia, because if this state nation decides to stop, we can deal with private companies, Facebook, Apple, Tesla, Google, because they have this economic competition and they don't stop. Elon Musk says that artificial intelligence is more dangerous than nukes, but he invests in some interface to bring the human brain into the artificial machine.

The next possible scenario is a friendly one, is utopian, actually, and it is our best friend and can deal with our huge problem: global warming, diseases, traffic, food insecurity.

A utopian world and no conflicts, and we just need to find another job, of course.

But let's go back.

We have this narrow AI in the next future for sure. We can see that decision-making processes will be fully controlled by people. But, of course, AI can assist our commanders in the field. Of course, we have the same addition to the sensors.

You can use robots, exoskeletons, and other robots from the DARPA, of course, to help us in our fights.

And I want to mention that will be in an urban area, megacities, maybe, and we have the same problem of human shields, civilian casualties.

My point of view is, I'm not afraid of a future NATO versus Russia and China in the future, the next future.

Direct engagement.

But I'm pretty sure we can consider another conflict in the field states where they always support some forces and Russia and China can support the other forces. And I try to see some general characteristic of this kind of conflicts, in order to prepare to propose some solution.

We have, for sure, an urban environment and human shields, unconventional approaches, and the weak part—we will try to find a sanctuary outside the country and prepare or ask help for sponsor states.

Social media manipulation, but also cyber-attacks.

In order to deal with this general characteristic kick, I propose three solutions. The operation environment to dominate the digital network from that area, and also to try to generate, to try to develop an algorithm, a game, Alpha Go, I call it Alpha War, actually, that can help us in our military digs making process.

And this idea of defense is not new. We know that we have a lot of cases, the Great Wall of China, the Maginot Line, and the Morice Line in Liberia. We can also mention United States/Mexico borders; because of that solution, I will try to suggest one in the future.

I mentioned the Morice Line from the Algerian conflict in 1954 and 1962, and I want to detail a little bit. The French army first defeated in Vietnam was facing another weak site from the National Liberation Front and couldn't deal with that because they hit on one, they found sanctuary in Tunisia and Morocco.

They decided to build a wall, physical wall, barbed wire, electrified, and they tried to use every tool available, hooks to lift up the wire, coppers digging under the wire, cleaned the fence with insulating material, explosive loads and even frontal attacks.

But the French managed to hold the wall very well because they involved artillery, fire support, and also quick reaction forces with helicopters, tanks, and airborne infantries. And they denied 90% of the guerilla factors that were in those sanctuaries outside the country.

The next case is from Vietnam.

The United States realized they cannot build a wall, a physical wall. So they tried to manage a network, a network of sensors, acoustic types, chemical sensor, but they could not use airstrikes in order to engage the enemy when the sensors activated were activated.

On the other side, Vietnamese soldiers detected these devices and understood what they were capable of, trying to spoof them using animal, buckets of urine in central areas and finding new routes in order to resupply the forces on the Ho Chi Minh Trail well known by us today.

The design was good, was performed by team JSONs. But the problem was there wasn't enough aircraft available, and those commanders in the fields are not considered a priority because they cannot have a real revelation, and also included a huge budget.

At those times the sensors need to be replaced because they're out of batteries, and they cannot go in the field and replace the battery, so they sent another sensor.

So in time the system was stopped. But we cannot consider it a failure because they arrive on those times at the moment to distinct from false alarms, animals, and heavy rain fall from real soldiers. And they managed to record the north Vietnamese soldiers' conversations in the fields. And also this system helped the American soldiers in the base.

So the question is why the United States did not implement this system in Afghanistan. Of course, if you take a look on the map, we need to deal with not only the Pakistan border but also with the Iranian borders and all around. But today we have sensors much better than Vietnam era sensors. And also the relief, the terrain of Afghanistan, our intervention with infantry, tanks, helicopters, drones, and so on.

So in times after we've dealt with the remaining Taliban and insurgence groups, we can manage to fight only on the borders.

The second proposal is meant to deal with human shields, used to hide inside the people. Today we use our smartphone not only to make phone calls but also to do online shopping and socializing. We clone our physical identity into another one.

They developed the social listening process, watching online forums, reading reviews, feedbacks, charts, hashtags, keywords, but they're not limited on this public information of the digital users.

But they also developed tools, artificial intelligence tools that can collect information about identity, user identity, email, location, political views, and also other interests. They realized these psychological profiles' various details. And sometimes they lose the database in favor of companies.

But not only private companies have access to all this psychological profiles, but also state actors. It was Snowden that told us.

And the question is, why don't you use digital tools in today's and future military conflicts? Because this tool provided by artificial intelligence is able to infiltrate behind the digital contents inside the cities and collect and filter, analyze the digital database.

We can have access to all criminal activities, drug trafficking, war crimes, and the human rights violations, to avoid any social media manipulation, but most important in this irregular warfare, we can separate the theories from innocent and also from civilian.

Of course we need to deal with some countries, like Afghanistan, where there's no Internet. We don't have social media networks. And we need to count on human resources.

And for this we need to invest in our leaders, the future leaders, in order to develop interpersonal communication skills, because today in this kind of warfare, of course, it's not enough to be soldiers, but you need to be a good negotiator, diplomat, public relations, because the problem is not only from military fields but also from economical fields, political, and so on.

The third proposal is coming from a 2016 breakthrough. You know that this Alpha Go game beat our human players and after that all the professional players. And this game is considered very creative. By some estimate it's the number of possible moves is greater than the number of atoms in the universe. And it managed to beat the human with a disability to estimate in advance the move, the moves of the opposite player, but also the ability to memorize and analyze the moves learned from a previous game.

So, actually, they developed this game, the first edition of the game, by playing it with humans, but after that, decided to play with another machine, with his version and decided . . . and came to great results.

This estimate is similar with our MDMP process, with our decision process.

So my proposal is to find this to implement this solution in the fields, in the support of field commanders, because this AI AlphaWar can learn from other experiences of similar conflict and provide assessment and recommendation.

Of course, we have challenges, what constitutes success, what is a mission accomplished. We cannot train and test this AlphaWar in the genuine war. The quality of data collected, and maybe when we transfer and prepare this algorithm, we transfer our bioset and tell him how to fight, how to generate estimates.

And also our human, the commander's ability to understand the black box. If you watch the game two, the move thirty-seven, the deep blue team didn't understand if that move, thirty-seven, was really a brilliant move, which actually it was. Or an error of that system.

And also a big problem is technological infrastructure and resources, the knowhow, and my country and other countries don't have access to developing these AlphaWar machines. But we can, based on the sharing of great powerful states.

In conclusion, I suggest that this human in the loop approach must remain, especially in this lifeanddeath decision, and also in the future for our leaders to use artificial intelligence to control the borders, the enemy, to control our digital network, to develop some interpersonal communication skills, and also to try to find a learning machine that can assist our commanding officer in our MDMP, our military decision making process.

Thank you.

[Applause]

[Dan Papp] Thank you, Colonel.

Our second presentation—"What can the Battle Room, Mobile Infantry, and Forever Wars Tell Us How Advances in Science and Technology Might Influence Future Military Leadership Education and Development?"—will be by U.S. Navy Captain Michael Junge, military professor in the College of Leadership and Ethics at the U.S. Naval War College.

He is a Surface Warfare Officer who served at sea in the USS Moosbrugger, Underwood, Wasp, and The Sullivans. He was the 14th Commanding Officer of USS Whidbey Island.

Ashore, he served as Deputy Commandant for Programs and Resources of the Marine Corps, Deputy Chief of Naval Operations for Communications Networks, and in the Office of the Secretary of Defense.

What can the Battle Room, Mobile Infantry, and Forever Wars tell us how Advances in Science and Technology Might Influence Future Military Leadership Education and Development?

U.S. Navy Captain Michael Junge

Today I want to talk about three different ways futurists think about or have thought about military training. I rebranded this talk, and I'm going to take you back to the future.

But first the obligatory disclaimer. These are my opinions, no one else's. You're welcome to take them on as your own, but you have to say so, and most of the military will disavow anything I say on a regular basis.

Speculative fiction asks questions. What will the future be like? How will things change? What will remain the same? This is part of the switching in nature character discussion of war, what remains the same and what changes?

As we look forward to future leader development, we should look back to what past speculative writers envisioned for future training. Those people will think of holodeck and battle rooms and powered suits and terminators that lock people outside spaceships, and they will try to work these things into how we talk about future training.

In fact, if we aren't careful, it'll be like PowerPoint transitions: something we use without thinking about, without purpose, without really thinking about the intent or the impact. It's easy to get caught up in the flashy tech. What I call the bright shiny object.

The reality is the classic science fiction does the opposite. What is classic science fiction? From Orson Scott Card, two things make a story classic. Genuine is classic as opposed to old and continuing to sell. The first speaks to a time in which the story was first told. The second is tougher. It speaks outside its time.

I'm going to talk about three similar novels, all classics in both senses of the word, and in keeping with that in the title of my presentation, we'll start recent and move backwards.

I first heard of *Ender's Game* in 1994 from a shoremate marine who lived down the street. He described the book as lifechanging. I read it. Loved it. But couldn't put it in the lifechanging category. Over the years, I learned the book was lifechanging for teens, not necessarily for adults. Here I am twenty-five years later, and I'm still talking about it.

Set in an unspecified date in the future, the novel presents imperiled humankind. Anticipating a third invasion, children, the protagonist, are trained from a young age by putting them through increasingly difficult games, including some in zero gravity.

These games aren't really just games, they are training. The games fill the hours between waking and sleeping. Most advanced is called Free Play, where the school computer brings up new things, building a maze the trainees can explore. But this wasn't just brain games.

The book and movie have a critical starting point for all trainees. Physical fitness and physical combat skills and physical fights which settle some of the most important issues of the novel: war's enduring nature.

Joe Haldeman's "Forever War" is also about man and an alien race, where Ender's Game trains children and occurs over centuries. Deep space flight time dilation means society changes, but troops do not. The societal alienation was a metaphor for the reception given to U.S. troops returning from Vietnam, and one discussed today as our own version of "Forever War" continues.

One of the first military discussions involves eight silent ways to kill a man. And a comment from the narrator, he already knew eighty ways to kill people, but most of them were pretty noisy. Killing with a knife, a gun, and entrenching tool. Even with powered armor, there were group training actions carrying heavy garters.

The recruits had IQs over 150 and bodies of unusual health and strength.

Evenly split, fifty men and fifty women started training and whittled down to a dozen before they got near the powered fighting suits.

This story is set in a future society ruled by world government, dominated by veteran elite. The first person narrative follows one through his military service in mobile infantry as he progresses from recruit to officer against the backdrop of interstellar war between humans and an alien species known as arachnids or bugs.

The book includes action and classroom scenes illustrating a vision for future ethics and norms.

For our purposes, however, there's tons of discussion on training. In the future, with interstellar travel and powered suits that can launch atomic rockets, trainees start in tents. Physical exercise. Learn stealth tactics. And eventually these future soldiers reach a point where they can route march fifty miles in ten hours on the level.

Combat training.

Combat drill.

Combat exercises.

Combat maneuvers.

Or as described, it was hands and feet to start with; we trained with sticks and with wire. Lots of nasty things you can improvise with a piece of wire. We learned to service and maintain equipment, simulated weapons and rockets, and various gases and poison, incendiary and demolition, as well as other things.

Maybe best not discussed, but we learned a lot of obsolete weapons too. Sum mi guns, for example, and guns that weren't dummies but almost identical with the infantry rifle of the 20th Century. We fired nothing but solid slugs, jacketed lead bullets, both targets on measured ranges.

The training battalion began with over 2,000 men and graduated 187.

They didn't move to high tech powered suits until the end of the training program. Basic combat skills without weapons or tech or how each of the training regimens started.

Place cement skills, not unlike repeatedly washing and waxing a car.

Practice does not make perfect.

Practice does make permanent.

It's counter intuitive to conventional wisdom as leaders talk about simulations and AI, about moving away from real and into virtual, but there is historical precedent. The Spartans started military training at age seven. They allowed citizens to try out for the army at twenty.

Spartan warriors lived separately from families and society until they turned sixty, and Spartan training, like in each of these three stories, included the possibility, sometimes the likelihood, of death—which meant the training was grueling, difficult, and realistic.

AI may change the character of the future battlefield, but maybe what we really need is a reminder that the basics of physical and mental fitness come without technology, and the technology should be additive and not replaced or supplanted.

If we think of artificial intelligence as an artificial form of natural intelligence, what can people do?

What can't they do?

Sometimes we forget that before we run, we walk.

Before we walk, we crawl.

Before we crawl, we learn to roll over.

Human beings need to progress through skills, and this includes combat skills. My Navy has learned this and forgotten it repeatedly over the last two decades, if not longer, as fewer and fewer understand the sea and our ships tend to be so large they overcome most changes in the ocean.

Until they don't.

Second, most discussion of technology assistance in the battlefield relies on clear communication paths. Something every major discussion of war also expects to fail.

It does no good to have systems that do not work without reachback, and no reachback means systems need to be in standalone, which means systems need to be locally operated.

Back to the roll over, crawl, walk, run analogy.

Third, not knowing one's self and not knowing one's team but relying on tech is a certain way to lose. I recently ran a story where an entire team in training was wiped out because they were focused on their screens—another issue our Navy is battling. We sometimes forget to look out our own windows.

Our tech does not do what was envisioned in the book's suits.

Didn't have to drive it, fly it, operate it, you just wear it and it takes orders directly from your muscles and does for you what your muscles are trying to do.

We aren't there yet.

We're still trying to roll over.

Maybe the means we use to instill selfawareness and teamwork can be updated. Battle room games are more than just games, but wellthoughtout games with intent and purpose.

In the end, without intent and purpose, nothing will matter or make sense.

In the end, leaders developed despite technology and bioenhancement remains about developing the human mind and body with intent and purpose.

In the end, what matters?

People.

Bodies and brains.

John Paul Jones said in the 19th century, men need more than guns in the raiding of a ship. And Wayne Hughes wrote towards the end of 20th Century, men matter most. And Sarah Connor told us . . . we aren't machines.

[Applause]

[Dan Papp] Thank you very much, Mike. That was thought provoking. Appreciate it.

Our third presentation this morning is Augmented Situational Awareness: Drones, Heads-up Displays, and Real-time Cyber Intelligence. This will be co-presented by Bryson Payne and Dr.

Tamirat Abegaz. Dr. Bryson Payne joined the UNG faculty in 1988 and is professor of Computer Sciences. He is the founding Director of the UNG Center for Cyber Operations Education, which is an NSA Center for Academic Excellence in Cyber Defense. Dr. Payne earned his Ph.D. in computer science from Georgia State. He has published articles in scholarly and trade journals and speaks regularly at conferences at national and international conferences on computer science and cybersecurity education.He is also certified Information Systems Security Professional and certified Ethical Hacker.

Dr. Tamirat Abegaz is assistant professor of Computer Science here at UNG and received his Ph.D. from Clemson University five years ago. Prior to joining the UNG faculty, he served in web development roles in Ethiopia, including as senior web developer for the Africa Union and as project manager for the Commercial and National Bank of Ethiopia. As a researcher, Dr. Abegaz focuses on emerging methods of user interaction, including multimodal interfaces and emotional design elements and modeling.

Gentlemen, the mic is yours.

Augmented Situational Awareness: Drones, Heads-up Displays, and Real-time Cyber Intelligence

Dr. Bryson Payne and Dr. Tamirat Abegaz

[Bryson Payne] Thank you, Dan.

We're excited to be sharing with you today a little bit a peek inside some work in progress right now. This is based on research with undergraduate honors research students. We've been working with Microsoft Hololens in a couple of headsup and mounted displays, so that we don't have to look down at a screen to make a decision to gather intelligence. We've paired that up with research in drones and unmanned aerial vehicles.

So he will start us off, and I'll start on drone technology.

[Tamirat Abegaz] Thank you.

Let's start with history. As Bob said in the past, the first computer was as big as a building. So generation first, display starts with a cathode ray tube, and the second one moved from cathode ray tube to LCD, and the third generation we see currently is mainly on laser technology.

So we'll see very interesting happenings in the past.

We can move to the next slide.

So for consumers heads up display, to just tell you the story, for Google Glass I was a researcher at Clemson University on humancomputer interaction. The first time I used it for my research was to see if it does have any impact on search engine research. So I was doing emotional design for older adults. I used it for my research. For me it didn't add any value.

The prize was $1,500.

Apart from using it for searching, it did not have any value. It's just similar with a smartphone.But currently, people are using it for an inventory management system and also using it for capturing videos. We can tap it and capture videos while you are using it.

But in many places, people are buying and using Google Glass because you cannot capture video in a gym or a movie theater or somewhere else. So that's very interesting to see as a device. And Google was not successful. It was not pushed to consumers.

But the second one that you see, Microsoft Hololens, we have it at UNG and used it, but the second one, which is Microsoft Hololens 2 is very fascinating to see. You can use it inside a virtual room and anybody, like in Asia or Europe, can collaborate with someone in the U.S. in the room, which is a virtual room, where I can use the Hololens and someone can we can even collaborate with some device.

It could be used for brainstorming. You can collaborate with anything, as if you are in the room, which is a 3D environment.

So that's really fascinating to see for the future where you can work on a project. You don't have to be in the same room but in a virtual environment. I can add some feature in it while you modify as it is. So very interesting to see.

The price for Hololens is around $3,200, which is not really expensive. The magic one is very similar with Microsoft Hololens 2, except that the price is cheaper than the Microsoft one is.

The other one that we want to see here is military head mount device. You can see, it is enhancing night vision goggles being used by the military. It can be used in every weather condition.

You can use it. It's very interesting. It is controlled by the control center. It is being used by and also there is the Nett Warrior situational awareness system which supports the binocular vision goggle device.

The joint helmet mounted cueing system is part of the head developed in collaboration with the industry systems, which can be used by either daytime or nighttime. The very interesting HMD device I saw currently was F35 Generation III helmet, which they call "God's eye."

The price is fascinating to guess. It is around $400,000 just for the helmet. It is really you can see anything with it. Very interesting. I think that is implemented here.

While pilots can see anything, virtually anything with the device. The feature is, rather than using the device, you are wearing the device itself. So wearable, making it used.

Another interesting device I have seen was the DJI goggles. This is integrated with a drone technology where you wear the goggles while you control the drone.

There are several modes. One is a top fly mode. You can use your head to control the drone and you can focus on one object only.

Then it can access that. Or you can have an active select object, like a car or any moving object, and it will follow that object.

Which is very interesting to see. The price is really not expensive. It's a range of around $2,000. Which is interesting to see.

The other one you see is the Epson Moverio. It's very similar to a DJI, except with DJI, once you put the goggle on your head, you can't see anything. You can only see what the drone sees. But with the Epson, it is integrated,; you can see other objects around you while you are looking at the object.

So with that I will pass.

[Bryson Payne] I won't go through the entire history of military unmanned area vehicles, but we've been using drones for decades for imagery intelligence. The really big change with some of the high altitude long endurance and medium altitude long endurance remotely piloted vehicles—really the big turning point came in 1995 with the MQ1 predator, just adding a video camera, having realtime live video or video acquired over a target.

That's really what has enabled us to start thinking about now feeding that video through for a device that is headmounted. Of course, there are lots of other I'm not going to do a lesson on any military aircraft technology in a room full of people who know it much better than I do, but I'll share a couple of interesting things perhaps for those who are not acquainted with some of our military UAV technology.

The MQ9 Reaper there, the long endurance, can fly about forty hours, about 1,200 miles with a light load and about fourteen hours fully loaded with 4,500 pounds of payload.

You can get four of those it was mentioned the price of the headsup display for the F35. You can get four of the MQ9 Reapers multiple control stations for the low price of $64 million. So you can keep watch around the clock with a few of those that swap out.

And of course all the way down to the MQ4Triton, high altitude flying more than ten miles in the area. We're not just talking about seeing over the next hill, which was a really great thing with those large drones. We're talking about seeing around the world from a remote pilot located just about anywhere.

What we have been working at, since our budget is a little smaller than that, is looking at micromini drone applications. You're seeing this out there.

We have cases where drones have been recalled or taken back out of the front lines, but many microdrones like the black hornet, that personal reconnaissance system, PRS, weighs less than an ounce or up to thirty-three grams, depending on the battery life.

It lasts about twenty-five minutes, but you can pack a dozen of them. So it's a really lightweight, really userfriendly technology. And it's closer to what we expect in consumer level technology, something you might even buy for your kids.

Then you've got bigger drones like the Sky Raider there, and then some of the fixed wing UAVs like the RQ11, the Raven B, that you launch from your hand. We don't go in our paper into the unmanned ground vehicles or C vehicles, any kind of understood water or surface vehicles, but we're focusing mainly on the ability to gather situational awareness from unmanned aerial vehicles.

So we need to talk a little bit about situational awareness in the field. Nett Warrior, of course, can integrate with a lot of this; we're used to handheld devices, but then they do come with some of the drawbacks, when you're looking closely at the screen, you're not looking at what might be in front of you.

They still come with challenges, but we have the ability to take not just the force tracking intelligence data, navigation, command and control—all the sensory data—we can now stream realtime video from those unmanned aerial vehicles and ground vehicles.

And then we've got the information synchronization capability with some of the headsup and head mounted displays.

So what we are looking at using this technology for here at

UNG is—we're calling it realtime cyber intelligence, for lack of a better singular term, because you're really talking about some signals intelligence and imagery intelligence, electronic warfare—there are lots of pieces that factor into this.

We have surveillance UAVs combined with traditional signals intelligence; a great example is Sky Tracker and others used in the field. We can use radio frequency detection and mitigation not just to find the drones but the ground control system.

If someone is flying a small drone improvised to drop a grenade, we cannot only find that drone before it gets to its target, we can also find who is controlling that drone. And we're mixing some good old fashioned signals intelligence with some cool consumerled technology.

Converged cyber signals intelligence electronic warfare, you're seeing that across cyber and electronic warfare outpaced on information operations.

If twenty special operations forces can set up two or three hundred social media accounts and say, we missed the days when Russia was here in Crimea or wherever that may be, it looks like a groundswell of support for whatever Russia is doing on the ground.

That's something we could catch up with and get better at ourselves.

General Scales mentioned winning cyber air and land. He also mentioned disaggregation of small teams.

One of the benefits of each of these smaller, lighter technologies is that it can be deployed to multiple team members. Small teams out on the front lines. Some of the challenges to augmented situational awareness include the reliability of mixed virtual and physical environments.

If you're seeing an overlay of information first of all, it could block or distract your situational awareness of what is really going on right in front of you, but then the question becomes whether we can trust that data that is being overlaid.

We need sensors that can't be spoofed; they can be hacked or interfered with. They can be jammed entirely. So we have to rely on human intelligence to figure out whether that threat really does exist over the next ridge. So still a lot of room.

We have UAS system vulnerabilities, but these don't just extend to UASs. We're talking about vehicle vulnerabilities, now that we have much higher technology vehicles, whether that is tanks or manned aircraft, whether that is ships.

We've got SALT communications, IP communications, whether WiFi, Bluetooth, you name it, radio frequency, even USB connections on these small miniature devices.

So we've got multiple radios and multiple interfaces that can be interfered with.

Like I said, it doesn't limit itself just to UASs. I'll say just one controversial thing here.

I feel a duty to try to get some discussion going a little later.

We may be able to count the number of countries that could challenge one of our aircraft carriers with conventional attacks, conventional weapons to disable an aircraft carrier, maybe on our fingers, and then debate on how many fingers we need to count, to list that out.

But there may be several thousand individuals and small teams out there that could disable the wastewater system on an aircraft carrier. And if you can't go to the bathroom on a ship with 6,000 men and women, that ship turns around and goes home.

You've taken it out of well, out of effect.

So this is something really close to our hearts since we train young men and women to be the people who think about hardening a ship or another device from that type of interference.

And there's one challenge that is across all of these technologies: consumer level expectations.

When Nett Warrior came out and was being vetted, there were complaints that it wasn't as fast and cool back in 201011 as these devices we were carrying around, like General Scales mentioned earlier.

That's going to be a concern for any type of military surveillance technology, just trying to match the pace with consumer level expectations.

And just a few trends to watch.

You've seen a couple of hints towards this.

Swarms, selfhealing redundant flocks of small inexpensive drones. If you have $2,400 devices in the air instead of one $160 million device, you also have the possibility for cooperative tactics using some of that AI, making swarms work together to go into new and undiscovered unexplored spaces, even inside buildings. Something to think about, whether we can trust those devices if we know enemies have capabilities in electronic warfare and information warfare.

What if they're messing with signals and intercepting signals or injecting something into those signals?

If your AI is relying on sensory data, can you taint the AI of your enemy or can your AI be tainted to think something is there that is not or miss something that is there?

And then so zero trust, multiple confirmation strategies will continue to be important there.

And, of course, more AI in contextual intelligence, but integration in the field and trust are still remaining challenges.

And then some nearterm impact on future of warfare.

We, of course, have to work this into military training, as we talked about today. That integrated visual augmentation system, if it is at consumer level cost, that is something we could work into training for our soldiers, our airmen and sailors and beyond.

We have realtime battleground situational awareness that we can start to offer at the small team, disaggregated team level and AI based target level that we're already seeing.

I hope we spurred a little conversation for questions at the end.

[Applause]

[Dan Papp] Thank you.

Discussion

[Audience Member] Are you familiar with IVAS?

A little background, I'm chairman of the board, and we're spending about $6 billion a year on close cam bat. When you put up the devices, you didn't have IVAS up there.

$3.8 billion put into IVAS, which is essentially the Microsoft thing you what did you call it? Hololens.

[Audience Member] Yeah, it's Microsoft's a $600 million contract to develop Hololens for the military, but that's IVAS. I don't know if you've connected with IVAS at all, but the things that you're shown up there are basically being pushed aside, particularly of the binocular thing you showed there, that won't go any further.

IVAS is going to offer services, and I don't know if you're connected with this organization or not, but the future of AI the future of AI applied to training—and the idea, this is secretary Mattiss, I want every soldier to fight twenty-five battles before he fights his first battle.

And the science and experiences, you can only do today two virtual nations a year for restrictions of terrain and time.

You can only do four emotions given today's current technology.

His challenge is to do a minimum of twenty-five a year. And twenty-five a year times 5,000, 6,000; you can see how big the problem is.

The other thing about IVAS, it's not only a training device but also a sensor. In other words, IVAS, the navy family life is now aided by a soldier WiFi. You don't have to aim anymore.

But that's all done by the three microprocessors in the tip of the lens of this thing, and there are three marks or phases to IVAS.

We're now at phase 2.

I would suggest after this is over you need to talk to me, because the future is not in that.

The future is in IVAS.

Thank you.

[Audience Member] IVAS, integrated visual augmentation system.

But my question is for Colonel or Bethany or anybody that wants to step in.

You showed a slide that talked about you talked about it, perhaps maybe not on the slide, but we're having the same problem with human shields, and then we talked about how automated weapons systems are going to be able to make more ethical decisions and so forth.

To come back to the purpose of this symposium, it's the future leader training, not the systems. So where do you see that you're going to be able to train those soldiers, that small S, not large S, in ethical decision making when machine says shoot, but your eye says don't shoot?

And, you know, where do we where do we draw the line with the minority report Tom Cruise kind of scenario where I look at you and say, "I know what you're thinking"?

Maybe you do, maybe you don't.

Sometimes we train ourselves not to give that away.

So what kind of kind of a broad question, but I'm really after, how do you anticipate being able to train soldiers to make those ethical moral decisions when they've got machines that are starting to do some of that thinking for them?

And let me take the matter under prerogative to add on to that question by asking at what age do you begin to do that training, going back to the Spartan example.

[Panelist] I can start.

So I haven't done a lot of research, so a lot of this is opinionbased, just to make sure we're clear there.

So what we have seen in the past is a lot of continuous improvement.

So when the machine says shoot, you look at yourself and think, like, well, I'm not sure I want to do that.

So I think it's situational. And understanding when that happens.

As that data gets generated, then we can use those situations and those rules to improve our artificial intelligence. And until we start to get this stuff in our processes, we're not going to be able to do that.

So that continuous improvement, that algorithm critiquing and tweaking, I think, is the way to go.

And also the human in the loop; I really like that idea, because I think that's what is needed. We can't just believe what comes out of the magic box.

[Audience Member] Can I quickly add one thing?

One of the recent papers comparing the performance, this is where our work saying that the interaction between humans and machines will provide better results than humans alone and machines alone.

And the example that we're giving, if you tell the machines all the attributes of an enemy and the machine is in front of an enemy that surrendered, those attributes are not changing.

So the decision might be tricky.

And if you have a human in the mix, the survival instinct, when you face danger, may also interact and interfere with a good decision.

So the approach is to have humans teaching the soldiers about the ethical decisions, and the big picture, and understanding of what to do, but then you have machines to support those decision makers.

So to take out of the equation the survival instincts, the stress, the fear, and you allow the benefits of the accuracy and precision of machines to help you make a better decision.

So our model supports, you have to have both in the same equation.

[Dan Papp] Additional?

[Audience Member] I want to get to Dan's question about age, because one of the things that we're trying to do here at North Georgia is train soldiers for the future. And we've been very good at doing it.

This now, you know, this kind of world creates a whole difference.

You have kids that are coming to North Georgia, and they don't know a world without cell phones. They don't know a world without global integration.

They believe, even if you look at research, that these kids are more likely to believe in avatar as a voice of authority in a game simulation than they are a real person.

So how do you take people that are coming to this school with that background and train them with people that came out of another background, so that you get the ones that are coming at you from a very different set of references, a very different way of thinking about things, the multiple different family backgrounds and values they may have learned, and narrow that down to the kind of decision making that we like to see come out of a place like this or any other place that is training soldiers?

[Panelist] This is an excellent point.

There is an initiative endorsed by the Department of Defense. It's called the Institute of Creative Technology. It integrates entertainment and game systems with a defense training. It builds on the currently prior experiences and perceptions, and the advanced systems that were built for entertainment and gaming to start building from early ages, and the younger prospects who are familiar with games and entertainment and mobile devices and integrating this in the context of military training.

So this is a big initiative endorsed by the Department of Defense.

I would say this is where the data comes in.

So as we're, you know, giving those personality tests, as we're creating those behavioral profiles, we're also doing a lot of observation, so with that data we're gathering, we can create those personalized profiles, and so that is where a lot of your you know, it could be maturity level, it could be the way that you think, it could be whatever those data points are: we can use those in the categories when we're creating these custom programs.

[Audience Member] [off microphone] . . . data on all the students that are going to graduate from this institution and others, which makes them potentially predictable.

But on the battlefield, particularly AI enhanced battlefield, unpredictability is a virtue.

So how do we make sure that these kids we're trying to educate, not just train but educate, are able to overcome the ability of an enemy to read, you know, their own thoughts and processes and how they react to things?

And I would just open that up for anybody.

[Panelist] I'm going to take that one.

Because there's a couple things that I have been hearing through this process.

The first thing you have to do is stop assuming anything about them. So the assumption that I spent thirty years now hearing how the next wave of training is going to be tailored and perfect and wonderful, and that is a great idea that we can get to.

Maybe.

Someday.

The second and the biggest assumption is that, well, the next generation is going to be able to do all the stuff better and easier. No, they're not. They're human beings in the same way that your generation are human beings, or General Scale's father fought in World War II as a human being.

That part hasn't changed.

We're not significantly taller or smarter or faster than our predecessors were. And we have to recognize and accept that. We cannot expect that we're going to have some sort of new soldier that can be better with the technology.

The Navy two years ago had a spate of collisions. One of those collisions in my opinion clearly my opinion because this flies in the face of the official Navy investigation is that a decision to remove the physical and accepted norm throttles from the ship was the proximate cause of that collision.

Because we expected the X Box generation to be able to use a touch screen to replace the normal physical changes.

For you infantry guys, imagine if somebody took the trigger off your gun and replaced it with a touch screen.

I know!

But why?

Who is actually making and this goes back to your question. Who is making that decision? Who is deciding where this tech is changing?

Because that, that unnamed bureaucrat that authorized changing the throttles to a touch screen, which by the way we're now stepping back from, who is that person? Who is that individual that made that decision?

Until we can reach a point where those individuals are accountable for their decisions that we can actually attribute a name to those decisions, all the rest of the stuff is just great and fun, just not going to make a difference.

[Audience Member] [off microphone] . . . all men entering have this. Eddie Gallagher is one of them. The deal is you have to factor that out early.

We can do it here in Georgia, if you want.

There's an instrument called TAPAS, which is the first cognitively varied psychology test that the DoD, that we are experimenting with which gets beyond the ASVAB and looks at personal attributes.

What does that mean? That means you never assign a North Georgia graduate in the infantry. You send them to the transportation corps four years.

It means a small unit should be led not by a lieutenant but by a master sergeant or ward officer, not a second lieutenant.

It makes no sense. It defies logic.

Who does the Marine Corps recruit? College graduate, 18yearold males, unmarried. That's the preferred Marine Corps model.

It's completely antithetical to logic about human performance and why the Marine Corps has something like 2.5 times greater killed in action and wounded in action. It's your biology.

There's nothing you can do about the evolution and development of your prefrontal cortex.

[Dan Papp] And thank you to all the panelists for a fascinating discussion.

[See Appendix for corresponding PowerPoint presentations.]

6

The Artificial Intelligence Revolution

Mr. Paul Scharre

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

So, I'm going to put my job title to the test here as director of the technology program and see if we can make this remote connection work. I'll try to screen share a presentation with you all, so please give a holler if this doesn't come through properly.

I've got some slides that I would like to go ahead and share with the group, then I'll walk you through a brief presentation about artificial intelligence, and then we should have some time for Q&A.

Can everyone see the slides okay? I'll assume that's a yes and someone run in and grab me if that's not the case.

So, what I would like to do is walk through in a broad sense when we talk about artificial intelligence: what is it, why do we care, and what does it mean for national security and defense?

We have seen explosive growth in the field of artificial intelligence and machine learning in just the past few years.

This recent excitement about AI started about seven years ago at the dawn of a new revolution in machine learning, coming out of a type of machine learning called deep learning deep neural networks that began in 2012 and is really a combination of huge datasets, increases in computing power, all coming together to allow the creation of a machine. We are able to learn from data and then the machine is able to perform a number of tasks that are as good or are even better than humans.

And you see some examples there.

But I want to caveat this with the type of AI that we're talking about today is nothing like the AI we see in science fiction; it's not like Terminators or C-3PO from Star Wars; this is a very narrow or task specific form of intelligence. That is, that we can train machines to perform a variety of tasks as good or better than humans, but they are not able to do anything else.

So, we have machines engaging in stock trading.

We have machines beat humans at various games like chess, Go, Atari games, computer strategy games like StarCraft.

And they are beginning to perform some very interesting and valuable real-world applications, things like diagnosing skin cancer, but the kind of general purpose reasoning that humans have where humans can drive a car, play a game of chess, engage in a conversation, make a pot of coffee—machines can't do that today.

They are able to do one task and really nothing else very valuable, and this intelligence is so narrow that even if the task changes slightly, the performance can drop off dramatically. So to give one example, a few years ago when the program AlphaGo was trained to beat the top human in the strategy game Go in levels of performance by training millions of moves of Go, but if you change the size of the board slightly, its performance would drop off dramatically.

Because now the operating conditions were not consistent with the environment in which it was trained on and the data that it was trained on.

So that's a major limitation you have to factor in when thinking about how to use these machines.

Nevertheless, you hear lots of people talking about this technology and its potential to spark something akin to another Industrial Revolution.

What we're really talking about is a cognitive revolution as we're able to use machines to imbue them with more intelligence in a variety of settings. I really like this quote here from Kevin Kelly, who is a technology writer, where he compares AI to electricity being embedded in a variety of objects around us and over the next several decades, we'll see the AI imbuing these machines with more intelligence making them more valuable, just like we have a whole bunch of networks networked and we have been able to connect things to the Internet and connect our watches and phones and thermostats and cars to the Internet.

We'll now see all of these machines become more intelligent and able to accomplish more tasks.

People are predicting huge dollar amounts in terms of the market for AI technology.

And creative disruption on the orders of tens of trillions of dollars annually that will automate various jobs and task productivity gains as much as 30% in some industries, and, according to the best study I've seen about the impact of automation on our workforce, McKinsey has estimated roughly half of all tasks currently being done in U.S. economy could be automated with existing technology.

That doesn't mean half of all jobs.

It's a very small number of jobs that could be completely eliminated, less than 5%.

But most jobs would have some tasks that could be handed over to automation: routine, cognitive, and physical labor.

There's never a reason to think that a similar type of translation function of current tasks over to automation would exist in a national security workforce, in defense, intelligence, Homeland Security and other aspects of national security.

You don't have to take my word for it—there's lots of companies putting down tremendous amounts of money in this space, investing in AI, investing in data, in computer power, buying up startups that are engaged in this.

The market for talent in this space is astonishing; top tier researchers command NFL salaries, so there's real human capital in this space. You'll notice not all of these companies are U.S. companies; some of the major players in this space, Alibaba, a number of these are Chinese companies, so China is a global powerhouse in AI.

This is by no means a U.S.-only or even a U.S.-led technology revolution.

China has stated that their intent is to be the global leader in AI by 2030, and they are engaged in a major national push to achieve that goal and, absent of course correction, they look on track to achieve that over the next decade.

So, what does this mean for global security?

Well, the AI revolution is likely to change warfare and international power dynamics just as much as past Industrial Revolutions did, while prior Industrial Revolutions led to the creation of machines that were stronger than people for specific tasks.

We are seeing today the creation of computers that are smarter than people for specific tasks. These are likely to be purposed for a variety of national security uses in military intelligence, information, and economic warfare. We're already seeing automation play an important role in information warfare and propaganda as bots are used to spread this information on social media.

And social media companies themselves use algorithms to filter through information.

And we're likely to see increasing new uses of this technology as it evolves.

So deep fakes, for example, AI generated high quality fake audio and video are one example where we're likely to see more applications of this technology in the information space.

More broadly, if we think about something with AI like Industrial Revolutions we're likely to see a shift of balance of power among states and even key drivers of global power. So just like the Industrial Revolution made coal and steel production an important indicator of national power, and oil a global geostrategic resource, AI is also shifting the key metrics of power.

Making data, computing power, and human capital are also extremely valuable indicators of national power that we're seeing nations compete over and companies, as well.

Now some of the features of this technology of AI automation are that they allow for embedded expertise, which means that you can take tasks that were previously done only by human experts and now embed that knowledge into the machine allowing then fewer expert people to be able to conduct the same task.

One example of this and one we're probably very familiar with is tax preparation software.

You don't have to be a CPA to use tax preparation software.

It embeds the knowledge about tax code and filing taxes into that. All you have to do is move through a simple step-by-step interface. You just put in codes and punch in answers; this lowers the barrier for entry for people to be engaged in various tasks in both economic settings, which is a lot of value for productivity gains but also in the national security sense has benefits and risks.

So, for example, we have seen small drones today give non-state actors the ability to launch aerial attacks in ways that wouldn't have been possible without this technology.

They may not have access to fighter jets or helicopters, but they can buy small drones for a few hundred dollars and then use these to carry out aerial attacks.

Automation also allows operations at scale.

So people can then scale up the amount of activity that they are doing from one person or individual.

You have seen this in cyberspace with things like Botnets that spread across the Internet and infect unsecured devices, things like WiFi routers or Internet of Things devices.

And then allow widespread Internet disruption.

We're also seeing this in the physical world with things like drones, again where we see non-state groups begin to now use mass drone attacks.

There was an attack in Syria last year where a Syrian rebel groupe used thirteen drones against a Russian air base. So the ability to scale up the effects from a small group or from individuals have significant effects when we think about national security.

Sometimes this technology can allow super-human abilities; that is to say, we can achieve super-human performance at some tasks.

That's of course the goal of self-driving cars, that someday they will be safer than human drivers and save lives on the road.

And automation also allows delegated authority so people can hand over tasks to machines and allow them to execute tasks in settings where it might not be feasible for people. Automated stock trading is a good example today where we have algorithms executing trades in milliseconds.

And they can do so quite effectively.

Now there are some limitations of these AI systems that I want to highlight for the group that I think are really important.

One is their inability to understand context because they don't have the same general purpose reasoning ability.

They are not necessarily going to be able to understand what they are doing and why.

When we have seen, for example, stock trading algorithms engage in erroneous behavior, sometimes in ways that have liquidated assets for companies or in one case nearly bankrupted a major trading firm or engaged in flash crashes where the stock market moves very, very quickly and crashes because of interactions among algorithms.

Machines don't understand the context for what they are doing.

They don't understand that these dollars are affecting the economy of a nation or the entire globe and disrupting peoples' lives; they don't understand what any of this means.

This can also come into play when we talk about the brutalness of machines and narrowness of their intelligence that you could have systems that work very well in one setting and in another setting their performance plummets in really catastrophic ways.

We have seen this, for example, with Tesla autopilots where they can be quite safe in some situations and lure the human drivers into a sense of safety and trusting them and quite suddenly it will fail and drive into a concrete barrier, a parked car, or a semi-trailer, resulting in accidents and fatalities. So that can be a real danger of these systems: they go from super smart to super dumb in an instant and in some cases with real catastrophic effects.

AI systems also can be vulnerable to new failure modes that can come out of the learning process if they have been given the wrong goals or have faulty data. And they are vulnerable to new forms of hacking or manipulation that might exploit vulnerabilities in the learning system.

This is an example of what I mean when I say understanding context so you can see what an AI system can do today: it can identify objects, that there are people here, that they are carrying bags; you can see one person looking at another person; there's an accordion, a person sitting on a bench; so it's very good at things like object classification.

Understanding what's happening in the picture here and telling a story about what's happening is not something that an AI system can do today.

So, a person might look at this saying, "What's going on here?"—looks like a guy with a hat will reach into his pocket, maybe he will pull out money, maybe hand it to the person playing the accordion. The AI system has no ability to tell a story about what's going on, and it may evolve over time as the systems become more sophisticated; it can have more data, but it's certainly a limitation today.

I want to skip through some of these. I want to give one example of brutalness. This is from Watson on *Jeopardy*. I'll attempt to show a video; we'll see if it works. I'll queue it up in a second, but this is when Watson was playing *Jeopardy* a few years ago, and it won against some of the top human contestants in the world. You can see in the video, you'll see on the bottom bars there what Watson is basically thinking.

So those bars indicate Watson's probability of what it estimates what the correct answer is to a given question. Here it's estimating 1920s is the correct answer with a 57% likelihood.

So, let's try this video and see if it works.

We're going to go ahead and give this a shot.

[Video] Crosswords and Oreo cookies are introduced.

What are the 20's.

Watson. What is 1920s.

No.

Ken said that.

[Paul Scharre] Did that work? Did people get audio on that? Were you able to hear Alex?

What's interesting about this is, here you have the system that's really good at *Jeopardy*. What's the flaw here is that Watson can't hear what the other contestants are saying.

I'm not very good at *Jeopardy*, but once Ken Jennings got the answer wrong, I knew 1920s wasn't the right answer. Watson doesn't have the ability to do that in this case. This was a known limitation of the system.

The designers were aware of this problem.

And they made a conscious decision it wasn't worth correcting, it wasn't worth the time to do so. When asked afterwards, they said they didn't think Ken Jennings would get that many questions wrong. They were right, not a major issue, but this can be a factor in other settings if you see unexpected surprises come up.

I want to show another video that illustrates a similar problem; this one is called reward hacking, and it's where a system does what it was told to do, but it turns out to have some unexpected effects. This is from a computer program that was learning to play classic Nintendo games from the '80s and this is playing Tetris.

[Video] It puts its block on top of another block. This is a really bad planning, let's fast forward to see how this all ends.

This is not good.

Now it's almost done, and it pauses the game because as soon as he unpauses he will lose.

And really the only winning move is not to play.

Thank you.

[Paul Scharre] So, this is—am I there—did it come through?

So, this is a fun example where although this technology, this effect called reward hacking, this machine does exactly what you told it to do in many ways—you can think of sort of the military context, maybe a lot of these machines; it's like a very literal private who will do precisely what you told him or her to do.

You want to be very careful what instructions you give to the machines, what goals you give them and allow them to carry out. I want to end with one additional—I'll try to pull this screen up one more time—one additional vulnerability that I think is quite interesting that I want to show you.

One of the challenges here is that AI systems introduce their own vulnerabilities that could be vectors for attacks.

In an adversarial context, which we certainly care about in the national security space, we need to worry about people also attacking and manipulating the system. That can occur in a variety of places in the learning process if people poison the data. They can then basically bake into the learning process vulnerabilities that could be exploited later on the other side.

This is particularly an issue if you have systems engaging in a real-world context with an adversary.

So just like you might want to for [inaudible] to habituate forces to certain kinds of activity to then carry out maybe some kind of deception, you can do that to machines, as well.

Let's say, for example, you have AI systems that are used for spam filters for email or filtering out malware, tracking malware; if they are learning from that which you would want them to, it could be an avenue in which an adversary could introduce vulnerabilities that are then exploited later.

I know there is a type of an attack—a particularly thorny one is something called adversarial data attacks or spoofing attacks. Basically, what it is is that people feed into a machine learning system a tailored piece of data that manipulates a vulnerability inside the system. This isn't during the learning process; this is after it's been trained, and it's now put into the real world.

What might this look like? AI systems today are very good at object classification.

It's one of the things where ten years ago AI systems were terrible at, but looking at huge datasets of objects, we have been able to train machines to identify different kinds of objects and they have beaten humans at benchmark tests. Now that's very valuable, but as it turns out, you can create these very tailored kinds of images that you feed into these machines that trick them and prey upon what you might think of as optical illusions.

That the AI system is vulnerable to people isn't in this case. So here is one fun example of this kind of cognitive hacking. This is a 3D printed turtle.

As you can see as I turn it around, it's a physical object; it looks like a turtle, but the AI system is classifying it as a rifle.

And you can see on the left side of the screen there, the classification in real-time as searching through the object, but it's searching through different things but quite confident it's a rifle one. The system is very good at object classification. This is not an AI system that's bad at identifying images, it knows what turtles look like, knows what rifles look like, and knows they are different. It turns out this turtle has been manipulated in a way to trick it and what's going on is—I tried to pause it there, that didn't work.

Hold on.

What you can see here is when they turn the turtle over and look at the shell, there are some very subtle swirls embedded in the pattern of the shell. You can see them on the top in sort of the pink there and on the bottom in some kind of weird swirl patterns. They are very subtle, not something that would stand out to a person, but these swirl patterns are screaming to the AI neural network that this is a rifle. They are saturating the parts of the neural network that might identify it as a turtle. What's particularly problematic about this kind of attack is, one, the system does it with a high degree of confidence; it's not like on the fence whether it's turtle or rifle; it's very confident it's a rifle. Two, these can obviously be embedded in ways that are hidden to humans or not obvious to humans. And lastly, you don't even need access to the underlying data to make the attack successful.

It is better there's a—when there's a higher degree of success, if you can access the dataset it was trained on, but it still works in a totally black box fashion where you can't access the underlying data. These are some of the problems when we think about deploying the systems in the real world that are worth being aware of. Just like any technology, there are countermeasures, there are vulnerabilities, there are exploits we certainly want to think about as we think about real world applications.

So, I'm going to go ahead and stop there, and we've got some time for questions.

Thanks very much.

Question & Answer

[Eddie Mienie] Thanks, Paul.

Okay.

Do we have any questions? I'm going to start out then.

In *Army of None*, Paul, you bring up some of the dilemmas obviously that you touched on today, the moral and ethical dilemmas, and one of the experiences that you shared was telling of your Ranger team on the Afghan-Pakistani border where your team sees a young girl. She's herding goats, and you have decisions that you have to make.

Can you speak to us about that and how that applies to some of the things you laid out as far as how you help AI to make the right decision?

[Paul Scharre] Yeah, absolutely. So I was in—in the book I recount an incident early in the war of Afghanistan where I was part of an Army Ranger Sniper team on the Pakistan border we infiltrated at night. We ended up in a place that didn't have great cover, so we were compromised early in the morning a—when a farmer came out in the fields and saw eight of us with our heads bobbing out of an outcropping not too far away, and we expected to be attacked, but what we didn't anticipate because this was fairly early in the war and we were yet to really foresee some of the tactics others would use to exploit U.S. roles of engagement, is they sent a little girl to scout out our position.

So, the little girl came along; she's maybe five or six. She had a couple of goats in tow. I think it's a cover; she was supposed to be herding goats; she wasn't very sneaky to be honest. It was clear she was there to watch us—she stared at us while she walked along in circles around us. We heard the chirping of what we realized was a radio on her, probably reporting back information about us. We watched her for a while, she watched us, and she left. Not long after some fighters did come.

We took care of them. The gun fight that ensued brought out the whole battle, so we had to exit. But later we were talking about what we would do in that same situation. We talked about how we might detain someone if we didn't know they were a civilian scouting for the enemy, pat them down to see if there was a radio on them. Something that didn't come up that no one suggested at all was the idea of shooting this little girl. It was not an option we considered. Now what's interesting is under the laws of war in that setting, that would have been legal.

Because by scouting for the enemy, she was directly participating in hostilities. The laws of war don't set an age for combatants by participating in hostility. She was a valid and lawful combatant just as if she was an eighteen-year-old male in that activity.

If you designed a robot to comply with laws of war, it would have shot this little girl. I think that would have been wrong, if not legally then morally in that stance, but I think it begs the question as we begin to use AI and robotic systems in other settings: how would the machine know what's the difference between what is legal and what is right? How would you program that into a machine? Certainly when we think about things like autonomous weapons and lethal decision making, this technology raises a lot of challenging and ethical questions.

[Eddie Mienie] Paul, I'm going to ask you another question.

[Paul Scharre] I see a couple of hands there in the back behind you.

All right, thank you.

[Audience Member] Hi, Paul, Charlie.

What did you think of the new DoD defense innovation for AI ethics thing? Do you know what I'm talking about?

[Paul Scharre] For the group, the Defense Innovation Board recently released a set of AI ethics principles.

This was largely in response to some of the controversy surrounding DoD's use of AI in project Maven, and having some tech employees at Google, Microsoft and Amazon really standing up and being critical of what DoD is doing with AI and raising some questions about where this is going.

I think the AI principles do largely what they needed to do—which is set out a broad set of guiding principles for how the Department should approach AI technology, acknowledging to some of the communities who are concerned about this that DoD cares about operating responsibly using it in a right way and operating in a way that's ethical and understanding the abilities of AI technology, whether that it's subject to bias, to failures, the importance of relying—testing evaluation to get reliable behavior and other things.

I think one could easily quibble with elements of it and some of the wordsmithing. I think there's elements I'm not crazy about. I think it's 80% in the right space, but I think it does fill a gap for the Department—where people could fairly criticize DoD, I think, and DoD was moving out with AI technology with programs like Maven and the joint AI center and hadn't really articulated a high-level vision for where it wanted to go, and now these principles do that; they acknowledge some of the concerns people have about AI technology.

It acknowledges humans will be responsible for the technology and makes sure that humans are always at a high level, responsible and in control. I think for people who are opposed to DoD's using AI at all, it won't satisfy them.

The people who want DoD to sign onto a treaty banning autonomous weapons or to say some things need to be ruled out entirely, they won't be satisfied.

The range of objections that came out of tech employees hit a whole bunch of different things; some people were worried about drones; other people didn't like the military; other people they were just like – well, I'm not American, maybe I'm from another country, I don't want to do something that supports U.S. national security—fair enough, but needless to say, you're not going to convince DoD of those ideas. So I think ultimately the principles are headed in the right direction and articulate some sensible broad guidance, give tremendous flexibility about how it carries forward with that, and ultimately give some talkover for tech company leadership that wants to engage with DoD and say DoD is thinking responsibly about this.

[Billy Wells] My question to you is this: you listed a number of limitations of AI. How quickly do you think those limitations are going to be overcome? And at some point, what is their—is the end state, if there is one?

[Paul Scharre] Right, so I want to answer this in a roundabout way which is—there were lots of debates in the 1920s about the role of the tank in the Army and in ground warfare, and there were debates on either side about what you might do with tanks—how good were tanks. In fairness, tanks at the time were new technology, They had a lot of limitations. They were still developed in different ways.

Some of the objections were compared to horses: that tanks required bigger supply chains. Horses could eat off the land. Tanks required fuel. They were very maintenance heavy; they would break down.

What's interesting is all of those things are still true today. Those are—tanks have—there's real limitation of armor. It just so happens that benefits outweigh those limitations.

Some of these I think we'll see. It's hard to know. Some of these we are likely to get a better sense of as the technology matures about things like reliability. But they are likely to still be failures particularly in novel situations.

I think one important illustrative example of the limitations of safety and reliability comes out of the commercial airline industry where there's no question commercial airline autopilots have dramatically increased airline safety over the last several decades, but we still see accidents like the MCAS and 737 MACs where we had a new type of automation.

It hadn't been used before; it ends up through the process of development, getting used in a way that it wasn't really intended, and even though you have a very highly regulated industry—they are very concerned about safety—you still have accidents that lead to huge numbers of fatalities with these plane crashes.

So, I think we need to acknowledge that's going to happen. Some of these problems look very, very difficult to fix.

For example, one of the concerns that people have with AI systems is the opacity of neural networks. Because they are learning from data, there's not like an easy way to go back and peel back the network afterwards and say, well, why did it make this decision? There's not a simple if-then set of statements that could explain its behavior the way you may have. For example, like an airplane autopilot that may not be the case in a learning system.

This problem of explainability seems like a particularly challenging one.

People are working on it.

But it could be, we don't know, it could be ten years from now before we have AI systems that are really explainable and people are very happy with them. It also could be that the most powerful systems are super weird and incomprehensible, and we actually have to choose between high performing systems that are largely opaque to us but work and—(audio cutting in and out) simpler explainable systems that are—(audio cutting in and out).

Right now, it's very hard to defend against these.

It's very—a very active area of research. So we could see in the next five years, it's possible we end up with much more robust systems that are robust against these kinds of attacks.

I think it's hard to know, and some of these vulnerabilities might be showstoppers for certain applications where we say, like, I can't use it in this case, but in other cases—(audio cutting in and out) to work around that and manage that.

I think the most important thing is that we're cognizant of the limitations of the technology.

So, we're using it in a way so we're not surprised by these vulnerabilities in some operational setting where there might be then high consequences.

[Eddie Mienie] We have one more question.

[Audience Member] Hey Paul, it's [inaudible].

I had a question about the AI arms race.

So, one of the big bottlenecks we face now is basically the size of a training set and training data.

The United States, we have privacy regulations, we have a number of obstacles that might limit the size of that training set—those training sets.

China doesn't face those same privacy regulations when they are trying to accumulate these massive training datasets.

We also face a number of challenges with the integration of Silicon Valley with the U.S. Defense Department. China doesn't face those same obstacles.

So I'm wondering if autocracies are kind of privileged in this AI arms race and is there anything we can do to overcome that?

[Paul Scharre] Yeah, I think there are probably some ways in which China or autocracies in general have some advantages, but I think there are other places where the U.S. and other democracies will have better advantages. And two things you raised in particular, these come up a lot—I think there's some validity to them, but they are often a little bit overstated—so in data, these machine learning systems, as you're well aware of, but kind of for the group, they feed on large amounts of data. So if you want to train, for example, a neural network how to identify objects, it's not enough to have like a picture of the object: a cat, a rifle or tank, or whatever.

You have to show them thousands of images from various angles and various settings, and then these images are fed into this neural network that then learns from them. So, having large datasets is really valuable and important in training these systems.

Now, one of the concerns people have raised is this sort of—the rules of data protection that exist here in the United States and certainly the norms against Government collection of private data don't exist in China and are not a factor there.

There's obviously some element of truth to that; there are hugely different political systems and there are checks and balances in the Government here that just don't exist in China.

On the other hand, a couple of limitations that are worth pointing out.

One is that there is, of course, massive collection of personal data by companies here in the U.S. that's largely unregulated.

That's proceeding despite a lot of public outcry and consternation. The Government has sort of flailed about with Congressional hearings and angst and statements from lawmakers. We don't seem to be on a path towards any kind of comprehensive data privacy regulation, and consumers individually seem unable to manage where their personal data gets sucked up into and how it gets used, so there's at least rampant use by companies here and in China. You do see some interests in data privacy in the consumer side—not a conversation from the Government, but certainly from the consumer side it is an issue.

It's also the case that data is not fungible across different tasks. So, data on like geolocation of people that might be—that companies suck out of peoples' cell phones. That's not going to be helpful in some national security context.

The data needs to be very task specific.

So there might be some places where China ends up having a huge edge because they are able to collect large amounts of data. I think facial recognition is likely to be one example of this where you see Chinese computers who are already really leaders in facial recognition continuing to push that lead because they are able to engage in facial recognition applications in China that are just not the case here in the U.S. and there's already mass Government funded surveillance underway.

Might that help boost the AI industry as a whole?

Sure, but it's not necessarily going to apply in other settings, and facial recognition itself is even very brutal across like skin tone and gender. For example, a database of hundreds of millions of Chinese people is not necessarily going to be effective against Caucasians or Africans or people with other skin tones.

That's something that's come up quite a bit with facial recognition technology.

The other thing worth pointing out is, over time we see a general trend of computing power starting to supplement or replace data in some contexts, where synthetic data is allowing people to get by on shorter and smaller datasets; the last—I know we're out of time, but let me make a brief comment about the civil military connection because I think this issue of military civil fusion, this Chinese concept has gotten a lot of attention in the U.S.

Certainly the political obstacles we have seen in the U.S. where tech employees are saying we don't want to work with the DoD: that doesn't exist in China. Even if private individuals felt that way about the Government, they can't stand up and say that. They can't write open letters. If they get on WeChat, if they make anti-Government statements, the police will pay them a visit. So that's a real—that's an important difference. On the other hand, there are important other barriers to non-traditional companies working with the Defense Department here in the U.S. and working with the POA in China that exist on both sides.

And I think those are probably in the U.S. side bigger actual obstacles to cooperation. We have seen these major tech companies, Google, Microsoft, Amazon, they actually want to work with DoD, and they are moving through some of the friction that are coming out of some of their employees.

But it certainly hasn't stopped Microsoft with Amazon and Gemini and Google trying to get back into defense work, and I'm much more concerned quite frankly about barriers that we have within the Defense Department—bureaucratic red tape moving too slowly, lower profit margins, the inability to scale startups to larger sizes; I think these are much bigger obstacles to DoD actually accessing this technology.

[Eddie Mienie] Thanks very much for your comments it was amazing. We still want to get you here physically, but let's give him a hand.

[Paul Scharre] Thanks so much, everyone.

[See Appendix for corresponding PowerPoint presentation.]

7

Leading Humans in the Age of AI: Why We Need Integrator Leaders

Bruce LaRue, Ph.D. and Jim Solomon

The role of the leader in the Age of Artificial Intelligence (AI) is evolving into what we call the Integrator Leader[1]. The focus of the Integrator Leader is to provide clear intent and rationale, guided by key characteristics (see sidebar), while utilizing AI as a means of extending the reach and capability of self-organizing teams of knowledge workers. We have found this leadership approach to be effective through our work with thousands of leaders in some of the most complex organizations in the world today, including the private, military, government, and non-profit sectors. With less attention given to the mechanics of managing workers, and with knowledge workers spending less time managing data, both can become more strategic. This will place a premium on the leader's ability to drive innovation and integrate the efforts of specialized cross functional teams across the enterprise. Further, while AI is expected to cause major disruptions in global labor markets, the implications of declining birth rates and aging populations are occurring in most advanced industrial countries leading to an acute shortage of qualified knowledge workers. In this context, we argue the leader must us AI primarily as a means of augmenting rather than replacing the knowledge worker.

Why We Need Integrator Leaders

Integrator Leaders possess the unique ability to see what isn't there, channeling the collective energy of others to make their vision a reality. Simply stated, leadership is about leading change. Rather than engaging in futile attempts to manage, adapt to, or resist change, Integrator Leaders utilize the full range of AI technologies to extend the capability and reach of their teams in service of their mission.

In the Age of AI, leaders must see the world more as an integrated whole rather than a collection of independent parts. Seeing patterns of connections between thoughts and ideas will help to understand the world in terms of systems of complex interdependencies. Much like the challenges and crises we face today, they cannot be seen in isolation nor solved independently of one another. In the Age of AI, we need Integrator Leaders who can build coalitions of people to create change in our complex world.

The role of the Integrator Leader is to guide, mentor, provide essential resources, and remove barriers to progress. The leader is also responsible for ensuring that the team operates within appropriate boundaries while achieving essential outcomes.[2]

As the leader, your job is ultimately to guide the ship from the helm and not from the engine room. That is, you set the compass heading and priorities while you help your team self-organize to create an ownership mentality in how they accomplish the mission.[3]

Characteristics of Integrator Leadership

- **Trust**: Leaders must create a climate of mutual trust between themselves and those they lead, including a climate of trust between team members. Trust becomes firmly grounded within a team that upholds strong values.

- **Vision**: The leader must create a clear and compelling vision for their organization. It is this compass heading that helps the team members prioritize and align their efforts in support of the mission.

- **Communication**: Regular communication between the leader and all team members is essential. It is equally important for team members to communicate between themselves without the leader's involvement. This ensures that the team is learning to self-organize and self-correct behind mission priorities.

- **Accountability**: All members of the team must be held accountable for outcomes, not merely their inputs. That is, while everyone must be held to the same high standard of individual performance, they must also be held accountable for the outcome they achieve.

- **Feedback**: Timely, actionable feedback is critical when managing a team in the fast pace of the AI world. This allows for immediate course correction if underperforming, helping to make necessary changes to improve performance.

- **Recognition**: Timely recognition for individual and team performance. A role of a leader is to routinely find good in things, since challenges will naturally occur.

Throughout this process we must be careful to separate What from How. That is, we want to keep our strategic intent separate from how this strategy is operationalized in practice. This is because the old strategic planning paradigm rooted in industrial times routinely attempted to control both the What and How of change. This approach made sense in industrial times when most companies used unskilled workers to perform repetitive tasks on long runs of standardized products and services with very little variation. In the Age of AI, we must turn this paradigm inside out to create nimble, flexible organizations that can adapt and leverage change to their advantage.

Change has become so pervasive that simply to survive means that we must learn to leverage change to our advantage by building organizations that are more adaptive, agile, creative, and innovative. Improving your change strategy by becoming an Integrator Leader is therefore not only a matter of survival, but it is the key to thriving in an increasingly volatile and uncertain world.

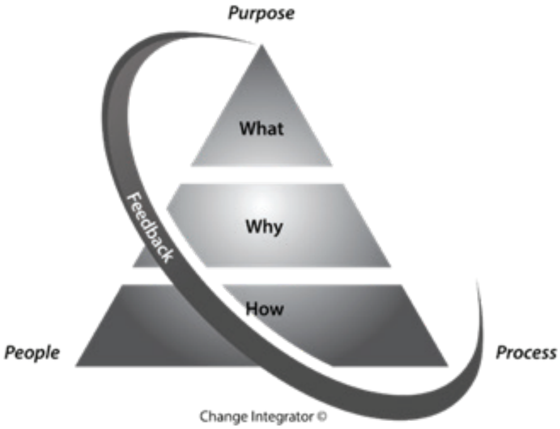
Globalization and AI enabled automation are accelerating at a dizzying pace, leaving people, organizations, and whole societies struggling to adapt. Work has become increasingly specialized, and specialization without integration leads to internal fragmentation, which is the enemy of any strategy. We need Integrator Leaders capable of inspiring others with fresh visions of the future, coalescing and aligning the efforts of our entire organizations to accomplish their mission.[4]

How Humans Adapt Their Environment to Themselves

At the most basic level, nature teaches us that organisms that sense and adapt to changes in their environment will succeed, while those that don't will fail. Organizations, like organisms, must learn to sense and appropriately adapt to changes in their environment to survive and thrive. Yet biological adaptation, while crucial to our survival, is only part of the picture. Biological adaptation on its own is exceedingly slow and, at its root, largely unconscious and reactionary.

Humans are unique among other species on earth in that we don't simply adapt to our environment, but instead we adapt our environment to ourselves. This means that we are fundamentally and inextricably involved in creating and re-creating the world around us through the mechanism of culture facilitated through technology. AI dramatically accelerates this progression of technology, becoming an extension of the human mind and body, expanding both our capability and reach. The problem is humans have not yet learned to fully comprehend the second and third order effects of the changes that we ourselves initiate in the world.

How we respond to change is ultimately a choice. We can see change as a threat to be avoided or a challenge to be overcome. We can choose to be a victim to our circumstance, or we can learn to leverage change to our advantage. The key is to never surrender our ability to choose how we respond to our situation. This is the essence of how humans adapt, develop, and evolve, and it is what distinguishes us from nearly every other creature on this planet.[5]



The Change Integrator

The Change Integrator is a tool for guiding your vision from concept to reality. As we can see from the Change Integrator model above, the first role of the integrator leader is to clarify purpose (strategic intent) and to build a compelling rationale for why change is necessary.

Begin with a focus on the purpose (What) that guides the change effort and the rationale (Why). Then ask the team for input as to how best to accomplish the purpose. The sequences are nearly always the same: What, Why, then ask How. That is, after providing the purpose, ask the team for their input, their insights, what is working, and what is not; then help integrate what they have proposed into a course of action. Ultimately, we want to create teams that can self-organize behind your intent to accomplish their mission.[6]

Seeing the Operation Through the Eyes of Your Team

One of the primary goals of the Change Integrator model is to help leaders learn to see their organization through the eyes of their people, treating them as their operational advisors. Employees have typically been on the receiving end of change initiatives and are rarely asked for input or consulted along the way. By understanding the true nature of AI enabled knowledge work, we approach leadership and change in our organizations differently.

It has been said that we should lead people and manage processes. We look at this a bit differently: our goal is to lead people and allow them to manage processes – including all essential AI enabled technologies. Treat your workers as the eyes and ears of your operation. Give them a clear strategic intent and rationale, engage them with appropriate AI enabled technologies, and then *ask* them how best to get from here to there. In this way, AI serves as an extension of the knowledge worker, enhancing both their reach and capability.

If you consistently utilize this form of leadership, your people will not only provide you with input on your course of action, they will learn to bring you an entire plan of action and *ask you for your input on their plan*. This is when you know you are on the right track. Your job should get easier while your people step up, take more initiative, engage with one another, and take ownership of how change is implemented.[7]

Purpose: Defining Your Strategic Direction

Defining our purpose begins with seeing the world from the canopy view. The idea is to widen everyone's aperture so that they see their actions within the broader organizational context. Through the use of AI technologies, this canopy view enables workers at all levels to become more productive and efficient, and better able to align their efforts with those of the broader organization.

The first role of the Integrator Leader is to determine the Purpose. It defines what we are here to accomplish, and as such, it serves as your compass heading or your strategic direction. It needs to be clear, concise, and compelling. Begin by outlining your organization's purpose or strategic intent. This should include any key strategic priorities or special initiatives coming your way. Do not make the mistake of assuming everyone understands the common purpose. Knowledge workers are inherently myopic; that is, they possess a deep, yet fragmented, knowledge. They know more and more about less and less. Without a clear compass heading to orient their activities and an AI enabled dashboard to provide feedback on their progress, knowledge workers will never be fully productive.

Providing your team with a view from the canopy gives them a clear line of sight to their goal. Show them where they are going and then ask them how to get there. Help them learn to self-organize behind your intent and become less dependent upon you over time.

Unlike industrial times where workers were viewed as an extension of the machines they operate, in the age of AI these technologies become an extension of the knowledge worker. All AI enabled technologies must be routinely validated against the leader's intent, and the structure of the algorithms must clearly operationalize this intent in practice.[8]

Build an Ownership Mentality in Your Team

To build an ownership mentality in your team, begin by outlining what challenges and changes are coming, why they are important, and how they will impact your team. Summarize the mission of your organization, your key strategic priorities, and your expectations of performance. Tie your expectations of performance to the outcomes you expect your team to create.

Everyone on your team must understand that you will hold them accountable for these outcomes and not just their inputs. When defining your purpose, focus on the following three key categories:

1. Strategic Priorities: What are your core priorities? This should flow from your organization's strategic guidance. Paint a picture for your team so that they can see their own desired end state based on what the customer expects in the form of an integrated solution to their problem.
2. Outcome-Based Success Criteria: What *are the criteria by which you will determine a successful outcome?* On what criteria will your end-user or customer judge a successful outcome? What are the gaps between what your customer expects and what you are delivering? What are the key milestones along the way that you expect your team to achieve, and by when?
3. Expectations of Performance (Linked to Priorities): It is important that you tie individual and team performance ratings to the outcomes you expect them to produce. Activity does not equal progress. We have often witnessed large organizations whose major functional groups were meeting or exceeding their performance metrics, but the goods and services the organization produced were below par. Customers expect integrated solutions to their problems, and integrated solutions require integrated operations. This means that workers need to self-organize and integrate cross-functionally to achieve the results customers expect.

The most innovative firms anticipate customer needs based on a methodical form of empathic observation and questioning, where they place themselves in the customer's shoes and look out at their world through their eyes. This capability is greatly enhanced in the Age of AI, where we can leverage big data cloud computing combined with social media and predictive analytics to identify patterns and emerging trends, leveraging this information to drive innovation and rapid change.[9]

Why: The Rationale for Change

Your team must understand the rationale for any changes or new priorities that you propose within the following three key categories:

1. Why will this change benefit our customer?
2. Why will this change benefit our organization?
3. Why will this change benefit individuals?[10]

How: Crafting the Roadmap

Whether speaking of algorithms or humans, we do not want our standard operating procedures to become substitutes for thinking and straitjackets that limit our ability to think and act creatively. We need to stay out of the *prison of the known* by continually looking for new and better ways to meet our mission.[11] Rather than focusing on following a process, the focus must be on the outcome we achieve.

Your team may not always come up with the best solution the first time, though with practice they will often amaze you. However, by asking first and then listening carefully to their responses, you will know exactly how they are thinking. This window into your team's psyche is invaluable as it allows you to calibrate your leadership accordingly. Your goal is to guide your team to their own solution. The more they own the solution, the less you will have to manage them, and the happier your customers will be.[12]

The Feedback Loop

The feedback loop on the Change Integrator represents a constant real-time integration of strategy and action that goes both ways. It symbolizes the critical need to ensure that strategy is being informed by action, action is being informed by strategy, and that What and How are always aligned. It symbolizes our ability to identify and exploit unforeseen opportunities and to spawn new innovations. The feedback loop also reminds us that tactical decisions have strategic consequences.

One effective form of a Feedback Loop is to provide an AI enabled dashboard of critical vital signs throughout the organization. The main criteria for this dashboard are that it is accurate, timely, and actionable. While many knowledge workers in the past spent much of their time analyzing, modeling, and crunching data, AI technologies allow them to spend less time on the mechanics of data analysis and focus more on where they are going strategically. This is analogous to focusing on driving your car versus spending your time under the hood. Many of our customers report that these AI enabled dashboards allow teams to spend less non-productive time crunching data and preparing for briefings, and more time focused on their mission. The dashboard provides the leader and their teams with a strategic view of the operation, allowing them to make adjustments to their strategy in real time.

We have frequently seen knowledge and expertise hidden away inside people's heads, housed in fragmented databases, or within pockets of the organization, where it is not widely shared and therefore cannot make the rest of the system smarter. This problem can be endemic within large, complex organizations that follow rigid operational procedures and lines of authority. Too often, critical knowledge exists within silos and stovepipes, meaning that many organizations literally do not know what they know.

The Feedback Loop on the Change Integrator represents a constant real-time source of information between strategy and action, and between cross-functional groups within your organization. AI enabled technologies can play an essential role as a feedback loop to ensure that everyone understands the mission and how their activities support it. The feedback loop also helps functional groups better understand what they need from one another.

As an Integrator Leader, you can't over-communicate; and communication requires learning to listen as well. Listen closely to your own people and utilize the critical *operational intelligence* that exists throughout the organization.

Let your team know that you are not only open to their input, but *that you expect it*. That is, you expect algorithms and robots to follow processes, while you expect your workers to analyze and improve these processes. This means that you expect your team to manage and maintain algorithms, robotics systems, and other AI enabled technologies which have now become an extension of the knowledge worker. In fact, let them know you want them to come up with the entire plan while you mentor and guide them just enough along the way to assure that the plan becomes theirs and not yours.

Demonstrate through your actions that you are willing to incorporate input from your people in service of the mission and give them all the credit and recognition for their ideas. Conversely, if you are unable to use their input, do your best to explain why their suggestion cannot be implemented. Assess all ideas on their merits regardless of position or grade of the one who originated the idea.

To create an environment where feedback is encouraged, you as the leader must model this behavior by routinely asking for feedback and input from your team. Conversely, you should also challenge your team's ideas, as appropriate, based on the needs of the mission.[13] It is their job to sell you on the merits of their idea by explaining why it will benefit the mission, and it is your job to explain why the idea cannot be implemented when that is the case. The key is to be as transparent as possible in this process to build a foundation of trust in the team. Be patient, and do not expect that your people will always get it right the first time.[14]

Create a Culture of Innovation

Make a habit of thinking out loud with your team. Rather than giving them answers, help them follow your train of thought to arrive at an appropriate solution. Most importantly, expose them to your own source code—the values, rationale, and ethical standards that underlie your decision-making process. At the end of the day, it does them no good for you to give them answers. Instead, you want them to own the decisions—anticipate what a situation requires, use AI enabled technologies to think for themselves, and work as a team to self-organize around a solution. This helps them to become less dependent upon you over time.

Once your team understands your What and Why, asking them How allows you to have a window into their consciousness and their way of seeing the operation. Now as a leader, you know exactly how your team is thinking, and you can adjust your mentoring accordingly. The key is to ultimately help them think on their own and self-organize behind your intent.[15]

Escape the Prison of the Known

To take a new idea from concept to reality, leaders need to help their team *see* differently: to begin to see our organization *as it could be* rather than how it has been in the past. Like many corporate, non-profit, and governmental agencies struggling to remain viable in the face of accelerating change in the Age of AI, they can be stuck in the *prison of the known.* Leaders must be able to help the team escape the shackles of their past by developing a new vision for their future along with a compelling rationale as to why change is both necessary and desirable.

To focus the attention of your team on the future, you must first guide them out of the *prison of the known*. This prison is where our individual favored ways of seeing become *ways of not seeing*. If we are not careful, we see our future in terms of the past, which is a bit like driving a car by looking in the rearview mirror. Yes, whether we realize it or not, most of us exist inside a prison of our own making. The walls of our prison cell can best be thought of as our basic assumptions. To become an Integrator Leader, you must first become self-aware, meaning that you clearly perceive your own basic assumptions and learn to consciously modify them where necessary.

Our current reality did not arise by chance. Rather, each of us exists within our own *prison of the known*, comprised of the preconceptions, assumptions, and biases that make up our world view. However, looked at another way, the same forces that have imprisoned us can also create new worlds limited only by our imagination and collective will to act.[16] You may think that what makes you who you are is a given; but the *self* is largely a constructed entity, evidenced by the degree to which the concept of *self* changes across cultures. By first becoming self-aware, that is, becoming aware of the assumptions and biases that comprise the *self*, the Integrator Leader learns to see the subtle basic assumptions operating both internally and externally to their organization. This heightened intuitive sensitivity helps to better understand the complexities of a situation or what makes another person tick. With time and practice, you can learn to quickly grasp the basic assumptions operating within an individual or the culture of an organization.

AI technologies will not solve this problem. If left unchecked, advanced AI technologies will simply replicate our current reality in a more efficient and effective manner. Integrator Leaders must ensure that knowledge workers remain on azimuth, and that the knowledge workers are managing all relevant AI technologies to support and carry out the mission.

Skilled Integrator Leaders can comprehend multiple points of view without being tied to any of them. This is the difference between *assumptions that hold us* and *assumptions we hold*. In other words, we all see the world through an unconscious set of beliefs and assumptions that hold us captive to some degree. They are a lens through which we evaluate everything without realizing we are wearing glasses. Further, this prison grows into a self-reinforcing echo chamber through the effects of AI enabled social media, marketers, and internet search engines that constantly feed us more of what we already believe and desire based on secret algorithms. Rather than becoming aware of and questioning the basic assumptions that drive us, our assumptions are being systematically manipulated and reinforced by the digital air we breathe, leading to the heightened social fragmentation and disintegration we see today.

Basic assumptions can be thought of as cultural DNA. Unlike biological DNA, your cultural DNA can be manipulated by others through the mechanism of culture and increasingly facilitated through the use of complex and often secret algorithms. These assumptions and biases, intentional or not, become embedded in the algorithms underlying all AI enabled technologies. As such, these assumptions and biases must be routinely evaluated and validated in light of our mission and changing circumstances.

If you have the courage to leave the familiarity of your own *prison of the known* and examine the hidden assumptions that stealthily guide your life, you can begin to intentionally change the lenses through which you see the world. Using the language of AI, this process is similar to changing your own source code. While many approaches to leadership development focus on changing behavior, we have found that we don't need to change a person's behavior. Instead, if we can help people to *see their world in new ways,* positive actions naturally follow. In other words, if you want to change the world, begin by *changing how you see the world*.

Leading Distributed Teams in the Age of AI

As we move into the Age of AI, organizations will become increasingly composed of individuals and teams that are geographically dispersed. Whether you lead a team of individuals who telecommute part of the week or an entirely distributed organization, Integrator Leaders need to adapt their leadership approach to ensure their distributed workforce can achieve superior results.

Adapting the Change Integrator model to distributed teams will allow them to learn to self-organize behind mission priorities, resulting in greater customer satisfaction, organization effectiveness, and employee engagement. Treat your distributed workers just as if they were sitting in the office with you, making them an integral part of the team. Our goal is to create a more cohesive team that can collaborate across space, time, and organization boundaries to align behind mission priorities while requiring less direct supervision.[17]

Conclusion

Leading in the Age of AI requires that you learn to see possibilities where others see obstacles, inspiring others with fresh visions of the future. A premium must be placed on utilizing AI to extend the capability and reach of the knowledge worker. This enhanced capability permits leaders to drive and accelerate change, while creating a culture that attracts, develops, and retains top talent.

Bibliography

Abrashoff, D. Michael. *It's Your Ship: Management Techniques from the Best Damn Ship in the Navy*, 2nd ed. New York: Business Plus, 2012.

Adizes, Ichak. *Managing Corporate Lifestyles,* rev. and enl. ed. Paramus, NJ: Prentice Hall Press, 1999.

Bohm, David. *Thought as a System.* London, New York: Routledge, 1994.

Isaacson, Walter. *Steve Jobs.* New York: Simon & Schuster, 2011.

Krishnamurti, J. *Freedom from the Known,* 1st US ed. New York: Harper & Row, 1969.

Krishnamurti, J. and David Bohm, *The Limits of Thought*. London, New York: Routledge, 1998.

LaRue, Bruce and Jim Solomon. *Seeing What Isn't There: A Leader's Guide to Creating Change in a Complex World*. Atlanta: Deeds Publishing, 2019.

Malone Scott, Kim. *Radical Candor: Be a Kick-Ass Boss Without Losing Your Humanity.* Performed by Kim Malone Scott (2017; New York: Macmillan Audio), audiobook.

Notes

1 The concept of the integrator as a work style originated with Ichak Adizes, *Managing Corporate Lifestyles*, rev. and enl. ed. (Paramus, NJ: Prentice Hall Press, 1999). The term *Integrator Leader* as we use it here focuses more on characteristics of a leadership style rather than a work style.

2 Bruce LaRue and Jim Solomon, *Seeing What Isn't There: A Leader's Guide to Creating Change in a Complex World* (Atlanta: Deeds Publishing, 2019), 30.

3 See for example: D. Michael Abrashoff, *It's Your Ship: Management Techniques from the Best Damn Ship in the Navy,* 2nd ed. (New York: Business Plus, 2012). Captain Abrashoff led the crew of an Aegis Class destroyer from one of the worst performing to highest performing ships in the Navy's Fifth Fleet, in large part by instilling an ownership mentality in the crew.

4 LaRue, *Seeing What Isn't There*, 3.

5 Ibid., 6.

6 Ibid., 29.

7 Ibid., 36.

8 Ibid., 49.

9 Ibid., 57.

10 Ibid., 59.

11 For more on this concept, see: J. Krishnamurti, *Freedom from the Known,* 1st US ed. (New York: Harper & Row, 1969).

J. Krishnamurti and David Bohm, *The Limits of Thought,* (London, New York: Routledge, 1998).

David Bohm, *Thought as a System* (London, New York: Routledge, 1994).

[12] LaRue, 63.

[13] Kim Malone Scott, *Radical Candor: Be a Kick-Ass Boss Without Losing Your Humanity,* Audiobook, performed by Kim Scott (New York: Macmillan Audio, 2017).

[14] LaRue, 72.

[15] Ibid., 85.

[16] See for example: Walter Isaacson's *Steve Jobs* (New York: Simon & Schuster, 2011). Isaacson used the term reality distortion field to describe the late Steve Jobs' uncanny ability to consciously see the world in new and novel ways, and in so doing, create conditions for the development of innovative products and services. As it refers to the prison of the known, it describes an unconscious distortion of reality caused by the influence of culture on the human mind.

[17] LaRue, 107.

[See Appendix for corresponding PowerPoint presentation.]

8

Weaponization of Technology and Leading Future Warfighting

Colonel Candice E. Frost

The views expressed in this paper are those of the author and not of her employer; they 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.

Abstract

As the rapidity of technology improves America must prepare the forthcoming generation. Future leaders must understand the need for the United States to retain its leadership role in technologically enhanced warfighting. Technical weapon systems impact warfighting and warfare in the future. Threats by other nations will augment their own warfighting capabilities using big data, cyber warfare, and artificial intelligence (AI). The two nations who heavily integrate technical weapons are China and Russia. Both nations plan to offensively use technical systems, when facing the U.S. on any spectrum of conflict. The next leaders who face threats from big data, cyber warfare and AI require more than a simple understanding of the internet. Future leaders who face technologically advanced foes must possess skills in command leadership and creative intelligence. The education and training

of such leaders begins with a resilient workforce and adaptive training.

Introduction

Threats depicted in the United States 2017 National Security Strategy focus a growing effort towards effective employment and decisive application of technological weapon systems.[1] As the rapidity of technology improves, America must prepare the forthcoming generation. Future leaders must understand the need for the United States to retain its leadership role in technologically enhanced warfighting. Technical weapon systems impact warfighting and warfare in the future. Threats by other nations will augment their own warfighting capabilities using big data, cyber warfare, and artificial intelligence (AI). Incorporation of such capabilities impact the characteristics of warfighting in the future.

The two nations that heavily integrate technical weapons are China and Russia. China, a rising power with potential to challenge the U.S. on a global scale, employs technological advances to support their territorial ambitions in the East and South China Seas. Any conflict with American, or adjacent, territories, could begin with the international legal principles of freedom of navigation and expand into a larger regional contest for territory.The other nation, Russia relies on technology to assist leaders when defending their interests against external threats, such as the North Atlantic Treaty Organization (NATO). Offensively, Russia heavily operates in the grey zone where their offensive actions, through opaque or non-military means, uses technology to reassert Russia's role as a great power in the world. Both nations plan to offensively use technical systems, when facing the U.S. on any spectrum of conflict, remains highly likely.

The next leaders who face threats from big data, cyber warfare and AI require more than a simple understanding of the internet.

This type of threat requires sense making of the terabytes of information. Through enhanced collection and intelligence, operational leaders are provided highly complex information in a manner to make clear decisions. Despite the potentiality for information overload, the next generation requires a foundation in understanding information warfare and its impacts. Future leaders who face technologically advanced foes must possess skills in command leadership and creative intelligence. The education and training of such leaders begins with a resilient workforce and adaptive training.

Technological Advancements

Science and technology meets the military's needs through the weaponization of such systems and applications. Three major categories of advancing technology turned into weapons are big data, cyber warfare, and artificial intelligence (AI). First, when defining big data it begins with data that is too complex and too large to store in a traditional database. Simply put, whoever owns the data, owns the advantage. Through gathering, storing, and processing previously innocuous points of information, a clearer picture emerges and patterns define areas to manipulate. Big data's exponential growth emerged as an output of the internet. To put the vast amount of data into perspective, from 1992 to 2018 the Army's use of Multimedia Message Manager, a secure messaging capability, has increased an average of 1,000 percent, from approximately 30,000 messages per year to the current flow of 35,000,000 per year.[2]

The second category is cyber warfare. Often understood as the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers networks themselves of another state.[3] Daniel Coats, former U.S. director of national intelligence, included cyber operations not simply physically threatening infrastructure but also cognitive pressure on American citizens.[4] The boundary between cyberwar and hostile social manipulation are blurry as campaigns of manipulation, especially by the Russians, are supported with cyberactivities. Whether designed to steal information used in the information campaign or to conduct coercive or intimidating attacks on information networks, cyberwar continues to target tech users worldwide.[5]

Lastly, the technological advancements of artificial intelligence (AI), classified in the National Defense Authorization Act for Fiscal Year 2019, defines AI as machine learning to adapt to new circumstances; detecting and extrapolating patterns.[6] AI uses automated reasoning to utilize stored information answering questions and drawing new conclusions. Dr. Margarita Konaev, a Research Fellow at Georgetown University's Center for Security and Emerging Technology, draws out impacts of AI when she states,

> AI-enabled ISR will increase the speed and accuracy of decision-making on the urban battlefield. ISR is one of the promising areas for AI applications in urban warfare because cities produce enormous amounts of data. With advances in high-fidelity sensing, image recognition, and natural language processing, military and intelligence analysts can exploit thousands of publicly available datasets for insights into the demographic, social, economic, and logistical characteristics of cities and their populations. Automated intelligence processing can be a game-changing capability.[7]

Weaponization of Technology

Studying technology without consideration of its employment divorces the means of its use from the ends.[8] To understand future applications requires comprehending the threat. Within this space, the threat is defined by both a state's capability and intent. Capability is the ability to employ force in a materially credible fashion with the capacity and competency to create an effect. The intent of the threat incorporates the "why" and "how" such behavior occurs. Both Russia and China are considered against this definition and their weaponization of technology.

The capability of China to create a workforce to apply weaponized technology is not only underway, but is growing. As of 2017, the Chinese press reported through their growth of the "Thousand Talent Plans" the successful recruiting of 6,000 high-level overseas employees from around the world to participate and work on Chinese national programs.[9] China's operators in academia also utilize their Thousand Talents Plan to target U.S. scholars with top-level research capabilities who hold intellectual property rights, key technologies or patents in technological fields. Additionally, more than 300,000 Chinese nationals annually attending U.S. universities or employed at U.S. national labs, innovation centers, incubators and think tanks results in a growing capability of individuals to utilize their gained knowledge.[10] Russia does not maintain the economic or military space in the tech space, as does China. Princeton University's Professor Stephen Kotkin brilliantly points out that despite Russia's economy measuring only one-fifteenth the size of the U.S. economy, measuring Russia only by an economic yardstick is reckless.[11] Russia's capability focuses their efforts in technology to target enemy vulnerabilities by deception and untrustworthiness within the internet. Russia's use of its newest weapon, cyber, demonstrates their ability to punch above its economic weight.[12]

The ability to deploy, support, and sustain said capability in militarily significant numbers defines the capacity of the threat. China is the only country, other than the U.S., who could produce a cadre of elite private technology firms to meet the definition of widespread capacity. China is capable of marshaling resources needed to deploy a major AI applications at scale. In China, companies like Alibab, Baidu, and Tencent compete with America's Google, Facebook, and Amazon in areas such as driverless cars, cloud services, and facial recognition.[13] China pressures data networks with its domestic equipment champions, Huawei and ZTE, and already determined up to a quarter of 5G mobile technological standards for the world. China's 800 million internet users produce an order of magnitude more data, fueling improvements in AI, than their American counterparts.[14] China's capacity for growth in these areas are accelerated through their use of the Belt and Road Initiative (BRI). Economically, China uses BRI to improve trading and transport links between China and the world, mostly through infrastructure investments.[15] The same trade and transportation nodes neatly fit into possible military uses in the future. As historically demonstrated, Russia is already a capable nation acting within the cyber domain in Georgia and Ukraine. The former Director of National Intelligence, Daniel R. Coats, stated that Russian influence operations, especially through cyber means, remains a significant threat to the U.S. interest. They are low cost, relative low risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions and to influence populations. Russia remains the most capable and aggressive source of this threat.[16]

Lastly, the capability to competently employ warfighting actions enabling efficient and effective military operations remains evident within technology. Unfortunately, the opaqueness of what is considered weaponized technology remains ill-defined often due to difficulty attributing the action to a nation state. China and Russia both understand the potential of influence through cyber activities.[17] Through influence and exploiting the internet's interconnected nature of information when distinguishing a threatening state activity is complex. Clearly differentiating between military and civilian activities in cyberspace is almost impossible.[18] Therefore, attempts for the U.S. to defining clear and precise indicators and warnings of threat actions remains exceptionally difficult due to deception and untrustworthy information.[19]

Capability, capacity, and competency each cover portions of tech threat, lest we forget the intent. Understanding the why and how actors behave remains critical. The hostile use of big data, cyber, or AI in warfare is not always clear. As the U.S. has not faced a near peer threat in decades, the aggressive behavior of a state adversary may not clearly appear. For instance, the possible breakup of the internet along regional lines could lead to the Balkanization of the web.[20] Why nation states are drawn away from the U.S. and to either China or Russia, through technology is both economic and political. Partnerships and alliances formed through trade are one measure both China and Russia use to increase their influence around the world.

How each nation plans to weaponize technology depends on their implementation plans. China's Central Military Commission's Science and Technology Commission, Lieutenant General Liu Guozhi stated that the People's Liberation Army (PLA) expects AI to reshape the character of war itself. The demonstrated intent by the PLA's doctrinally updated view to "intelligentize" warfare points to prioritizing technological advances in their military. The focus for the PLA to accelerate military transformation, reshape military units' programming, operational styles, equipment systems, and model combat power generation, plans to lead China into a profound military revolution.[21] Demonstrating over the past two years a willingness for such change occurred as the world watched China used big data to collect, intimidate, and detain those who fail to conform to the political aims of the Chinese Community Party. Beginning in April 2017, Xinjiang authorities in China detained hundreds of thousands, possibly millions, of Muslims in the region ostensibly for anti-extremism reeducation. As part of their campaign, security officials greatly expanded their use of high-tech and big-data surveillance systems. Continuance of such actions are expected to extend countrywide in an effort to curb social unrest.[22] As China demonstrates how they exploit big data, Russia continues to value technological innovation and manipulation of actions in cyberspace for the nation state. Even Russian President Vladimir Putin stated that "artificial intelligence is the future of mankind and that whoever becomes the leader in this sphere will become the ruler of the world."[23]

Implications of Warfighting in the Future

Shakespeare aptly stated, "What is past is prologue," and both China and Russia demonstrate the relevance of their past actions with technology shaping the future.[24]Their use of big data, cyberwar, or AI align with their development of doctrine and use of military technology over the past decade. China sets conditions and Russia uniquely conducts activities. Both directly imply a potential option for military action should each nation see fit for an opportunity to strike.

Since 2003, China's PLA emphasized the development of its "Three Warfares" strategy in operational planning, which focuses on psychological warfare, public opinion warfare, and legal warfare. Psychological warfare uses propaganda, deception, threats, and coercion to affect the adversary's decision-making capability. Public opinion warfare disseminates information for public consumption to guide and influence public opinion and gain support from domestic and international audiences. Legal warfare uses international and domestic laws to gain international support, manage political repercussions, and sway target audiences. The Office of the Secretary of Defense reported to Congress that China views cyberspace domain as a platform providing opportunities for influence operations; the PLA likely seeks to use online influence activities to undermine an adversary's resolve in a contingency or conflict.[25]

With respect to big data and AI, China follows the advice of World War II General George S. Patton as he stated, "Nobody ever defended anything successfully, there is only attack and attack and attack some more."[26] China understands the value of moving first and how it provides advantages in several ways. AI favors the country that successfully applies the applications first.[27] China may offensively strike first, should the Chinese Communist Party (CCP) feel threatened, and use their advantage of immense stores of data both refining and enhancing algorithms behind AI. A lack of individual privacy laws in China allows the CCP to collect heaps of data through their almost cashless society and information networks.[28] This quantity of global digital data may reach 44,000 exabytes by the end of 2020.[29] Fortunately, in technology the advantage of the first attack is often short lived and as cyber defense capabilities use more AI technology, defenders have greater tendencies to operate at the speed and scale of the attackers.[30]

Russia not only understands speed but also tests the boundaries of alliances and partners. Most recently, Georgia's cyber-attack on 28 October 2019, harkened back to cyber-attacks in 2008 when Russians were suspected to have launched a cyber-assault against Georgia as the two countries went to war.[31] This rapid military maneuvering in the cyber domain does not just extend to former Soviet Union states but also to their allies. Cyber assaults reached the U.S. over the past half-decade through the Russian Internet Research Agency (IRA). The IRA used U.S.-based servers and other computer infrastructure—including virtual private networks (VPN)—to mask the IRA's Russian location during operations targeting the U.S. during the 2016 U.S. Presidential election.[32]

A U.S. social media company predicted in October 2018 that the IRA would adapt and change its tactics to enable despite changing technology detecting foreign influence activity on social media platforms.[33] The IRA pushed unique messaging to specific communities—including African Americans, liberals, conservatives, and others—to "push and pull" them in different ways, according to the two reports commissioned by the Senate Select Committee on Intelligence using proprietary data social media companies provided and analysis using the publicly released social media data published by the House Permanent Select Committee on Intelligence.[34] The social media company noted that attribution of malicious actors is challenging due to the use of proxy servers, virtual private networks, and other identity-masking technologies, according to a retrospective report on observed activity on the social media company during the 2016 and 2018 elections.[35] The use of this activity by the IRA to internally divide a state it sees as a threat will likely continue into future and worsen should states go to war.

Lastly, the expression, "The enemy of my enemy is my friend," found in a Sanskrit treatise on statecraft dating back to the 4th century BC fits less so with Russia but increasingly with China.[36] A potential new bipolar world exists as conflicts between China and the U.S. grow. Not to say that conflicts between Russia and the EU could rapidly increase along their borders, but the likelihood of this action is increasingly not likely. Should hostility between the U.S. and China intensify, the possibility of a united Europe, Japan, and the U.S. could invite a stronger alliance between China and Russia.[37] Fortunately, the tense relationship between China and Russia historically remains mired in past conflict and a culture of distrust. Unfortunately, the wilderness of the cyber world does not always hold historical norms and the potential exists for a united front to face the U.S. in such an arena.

Future Leaders

Over the past year, the U.S. Army refocused efforts to modernize of its weapon systems. The Army's big six priorities for weapons —long-range precision fires, next-generation combat vehicles, future vertical lift, the network, air and missile defense, and soldier lethality all require accurate and timely decisions for their application. Reaching the level of modernization desired by senior leaders requires sense making of the terabytes of information. Accomplishing this change requires both enhanced military intelligence and focused operations to face an enemy on the battlefield with comparable weapons. Within big data, cyberwarfare, and AI the potential to overwhelm the decision makers because of information overload exists. To prevent this from happening requires leaders with different skill sets.

Moving from an industrial aged to an information-based society is akin to the cavalry to the tank. The data-driven and algorithmic systems required for applications of future weapon systems forces the American military to understand the complexity of this change.[38] One reporter, covering the U.S. defense sector, suggests that the future battlefield in 2030 may consist of as few as 250-300 human soldiers and several thousand robotic systems of various sizes and functions with artillery and combat engineering units done by robots in human-robot teams. Offensively, combat arms personnel are repurposed to areas demanding command leadership and creativity-enabling intelligence functions.[39] Artificial cyber hunters who are intelligent, autonomous, mobile, and specialize in active cyber defense will exist amongst an environment strife with blurred lines of conflict.[40] Those who understand the intent of China's doctrine heed their outline of the future, as recently explained by Chinese leaders,

> Driven by the new round of technological and industrial revolution, the application of cutting-edge technologies such as

> artificial intelligence (AI), quantum information, big data, cloud computing and the Internet of Things is gathering pace in the military field. International military competition is undergoing historic changes. New and high-tech military technologies based on IT are developing rapidly. There is a prevailing trend to develop long-range precision, intelligent, stealthy or unmanned weaponry and equipment. War is evolving in form towards informationized warfare, and intelligent warfare is on the horizon.[41]

Changes in the character of warfare requires leaders who understand resilience. As the United States Army adjusts their doctrinal approach, it is understood that, "improving the resilience of leaders and Soldiers—the Army's most valuable capability—requires training, educating, equipping, and supporting them to execute multi-domain operations in all of its intensity, rigor, and complexity."[42] In the past, training habitually required both a physical and mental component when preparing individuals and units for battle. In the future, leaders must include understanding influence campaigns. As machine driven communications integrate both AI, in alignment with computational propaganda, the enhanced capabilities to manipulate human minds remains offensive in nature. Combating this requires adaptive leaders to have the foresight to move aggressively and address threats on multiple fronts with an eye to protecting the soldiers from online propaganda and disinformation, while also maintaining their core values.[43]

The 2018 National Defense Strategy notes state that "In competition short of armed conflict, revisionist powers and rogue regimes are using corruption, predatory economic practices, propaganda, political subversion, proxies, and threat or use of military force to change facts on the ground."[44] The ethical implications of both gradual and disruptive technological innovations that could change civil-military relations, political power, and the ways wars are waged are profound.[45] Preparing leaders to face this evolving space creates an advantage that the U.S. has enjoyed for decades. Failure to do so creates opportunities for strategic surprise.

Notes

[1] White House, "National security strategy." Washington, DC: 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf, pg 20.

[2] U.S. Army, Deputy Chief of Staff for Intelligence, G-2, The Army Intelligence Enterprise Digital Concept of Operations, 31 October 2018, 6.

[3] Craig B. Greathouse, "Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?," in *Cyberspace and International Relations: Theories, Prospects, and Challenges,* ed. Jan-Frederik Kremer and Benedikt Muller (New York: Springer, 2014), 23.

[4] *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Before the Senate Select Committee on Intelligence,* 116th Cong. (29 January 2019) (statement of Daniel R. Coats, Director of National Intelligence), 5.

[5] Maichael J. Mazarr, Abigal Casey, Alyssa Demus, Scott W. Harold, Luke J. Matthews, Nathan Beauchamp-Mustafaga, James Sladden, "Hostile Social Manipulation," RAND Corporation, 2019), p. 17-18.

[6] See FUTURE of Artificial Intelligence Act (S. 2217 and H.R. 4625, the AI JOBS Act of 2018 (H.R. 4829), and the John S. McMain National Defense Authorization Act for Fiscal Year 2019 (P.L. 115-232). The AI classification scheme is presented in Peter Norvig and Stuart J. Russel, "Artificial Intelligence: A Modern Approach", 3rd ed (Harlow, UK: Pearson Education Limited, 2014). 1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. 2) An

artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. 3) An artificial system designed to think or act likes a human, including cognitive architectures and neutral networks. 4) A set of techniques, including machine learning that is designed to approximate a cognitive task. 5) An artificial system designed to act rationally, including an intelligence software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting

[7] Margarita Konaev, "With AI, We'll See Faster Fights, but Longer Wars" https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/ published 29 OCT 2019, (accessed 30 OCT 2019)

[8] "Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense," John D. Winkler, Timothy Marler, Marek N. Possard, Raphael S. Cohen, and Meagan L. Smith, RAND, 2019 (page 3). Santa Monica, Calif.: RAND Corporation, PE-324-RC-2019.

[9] Online Article; China Daily; October 23, 2017; "Global talent flocking to work in China"; Source is a prominent English language publication of Chinese news; http://www.chinadaily.com.cn/china/2017-10/23/content_33596566.htm; accessed 29 August 2019.

[10] Forum Staff, "Intelligectual Pursuits: The People's Republic of China Uses Buying Power, Theft, Spying to Gain Technological Edge," INDOPACIFIC Defense Volume 44, Issue 2, 2019, pg. 22.

[11] "Russia and the West: A Historical Perspective," Council on Foreign Relations, last updated October 25, 2017, https://www.

cfr.org/event/russia-and-west-historical-perspective (KOTKIN: The problem is that Russia is weak and getting weaker. And cyberwarfare and other activities are weapons of the weak. You've got a Soviet economy that is one-third the size of the U.S. economy, at peak. You've got a Russian economy that's one-fifteenth the size of the U.S. economy.)

[12] Burrows, 30.

[13] Burrows, 28.

[14] Burrows, 28.

[15] M.L. "What's in it for the Belt-and-Road countries?" April 19, 2018. The Economist, https://www.economist.com/the-economist-explains/2018/04/19/whats-in-it-for-the-belt-and-road-countries, accessed 27 December 2019.

[16] Coats, p.11.

[17] Kimberly Orinx and Tanguy Struye de Swielande, "A Chinese Fox against an American Hedgehog in Cyberspace?,"*Military Review,* September-October 2019, Vol. 99, No. 5, page 64.

[18] Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections: The Quarterly Journal* 15, no 2 (2016): 111-12.

[19] Alexander Kott and D.S. Alberts, "How do you Command an Army of Intelligent Things?" 2017. *Computer*. 12: 96-100. Alexander Kott, "Challenges and Characteristics of Intelligence Autonomy for Internet of Battle Things in Highly Adversarial Environments," Spring Symposiums of the American Association for Artificial Intelligence, at Stanford, March 26-28, 2018.

[20] Mathew J. Burrows, "Global Risk 2035 Update: Decline or New Renaissance?" Atlantic Council, 2019. Pg 15

[21] "The Race for AI," *Defense One,* March 2018, p. 14.

[22] Defense Intelligence Agency, "China Military Power: Modernizing a Force to Fight and Win," Pg. 18. www.dia.mil/Military-Power-Publications (accessed 30 OCT 2019) In ethnic minority regions such as Tibet and Xinjiang, the CCP has promulgated repressive regulations against alleged extremism by tightening limits on peaceful religious expression and ethnic identity. Beginning in April 2017, Xinjiang authorities detained hundreds of thousands, possibly millions, of Muslims in the region ostensibly for anti-extremism reeducation. As part of the Xinjiang campaign, security officials greatly expanded their use of high-tech and big-data surveillance systems, which they are expected to extend countrywide in an effort to curb social unrest.

[23] Radina Gigova, "Who Vladimir Putin Thinks Will Rule the World," CNN, September 2, 2017, https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html (accessed 05 November 2019).

[24] Shakespeare "The Tempest"

[25] Office of the Secretary of Defense, "Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2019," 02 May 2019, 112

[26] Rich Logis, "Remembering the General Patton Speech that Helped Win the War", *American Thinker*, December 30,2018, https://www.americanthinker.com/articles/2018/12/remembering_the_general_patton_speech_that_helped_win_the_war.html , accessed December 27, 2019.

27 Dependent upon the sector of AI deployment, the size and breadth of the deployment and timeline of action, there are areas like cyber security of defense, where humans cannot match the response speed necessary during an attack. For instance, in cyber security, AI technologies, combined with bot nets could overwhelm defenses. Lindsey R. Sheppard, Robert Karlen, Andrew P. Hunter, and Leonard Balieiro, "Artificial Intelligence and National Security: The Importance of the AI Ecosystem," Center for Strategic International Studies, November 2018, p. 60.

28 Burrows, 39.

29 Burrows, 41.

30 Burrows, 39.

31 "In echo of 2008 war with Russia, Georgia hit with massive cyberattack" by Will Englund, published 28 OCT in The Washington Post https://www.washingtonpost.com/world/europe/in-echo-of-2008-war-with-russia-georgia-hit-with-massive-cyberattack/2019/10/28/63f57778-f9c2-11e9-8906-ab6b60de9124_story.html (accessed 30 OCT 2019)

32 DOJ; US Department of Justice; Internet Research Agency Indictment; p. 9,15; 16 February 2018; www.justice.gov/file/1035477/download; accessed on 17 SEP 2018.

33 Twitter; Blog Post; "Enabling further research of information operations on Twitter; 17 OCT 2018; https://blog.twitter.com/official/en_us/topics/company.html; accessed on 04 MAR 2019.

34 New Knowledge; "The Tactics and Tropes of the Internet Research Agency", page 12; 17 DEC 2018; accessed on 04 JAN 2019. And University of Oxford and Graphika; "The IRA and

Political Polarization in the United States, 2015-2017"; p. 18-20, 23; 17 DEC 2018; accessed on 04 JAN 2019. And The Social Media Listen Center, Clemson University; "Troll Factories: The Internet Research Agency and State-Sponsored Agenda Building"; page 6; 2018; https://www.davidpuente.it/blog/wpcontent/uploads/2018/08/Linvill_Warren_TrollFactory.pdf; accessed on 8 APR 2019.

35 Twitter; Report; Retrospective Review: Twitter, Inc. and the 2018 Midterm Elections in the United States; 31 JAN 2019; https://blog.twitter.com/content/dam/blog-twitter/official/en_us/company/2019/2018-retrospective-review.pdf, p. 6; accessed on 11 MAR 2019.

36 Rangarajan, L.N. (1992). "The Arthashastra." New Delhi: Penguin Books India. p. 520. ISBN 9780140446036. Retrieved 20 April 2017.

37 Burrows, 17.

38 Osonde A. Osoba and William Welser IV, "The Risk of Artificial Intelligence to Security and the Future of Work," Santa Monica, Calif.: RAND Corporation, PE-237-RC-2017.

39 Jason Sherman, "Army Previews Desired Capabilities for Next Generation Combat Vehicle," *Inside the Army,* August 31, 2018.

40 Kott, A.; Alberts, D.S.; Wang, C. 2015 "Will Cybersecurity Dictate the Outcomes of Future Wars?" *Computer*, 48(12), 98-101.

41 The State Council Information Office of the People's Republic of China, "China's National Defense in the New Era," Foreign Language Press Co. Ltd., Beijing, China, http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc (accessed on 24

July 2019), 4.

42 Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028 (Fort Eustis, VA: TRADOC, 6 December 2018), 20.

43 Burrows, 46.

44 DOD, Summary of the 2018 National Defense Strategy of the United States: Sharpening the American Military's Competitive Edge, Washington, D.C., January 2018, pg 5.

45 Konaev (2019)

[See Appendix for corresponding PowerPoint presentation.]

9

Science Fiction Story Contest Winner: "Dear Mom"

Gary Phillips

Every story has an inspiration, the story behind the story. Before I wrote this story I was digging in the storage area of my basement looking for something that I just knew I had somewhere. In the process I stumbled across a box of my letters home from Desert Storm. I think every soldier has something like this, a "box" where letters and other memorabilia from deployments are collected and stored. We do this because while the memories are important they are also painful, bringing back emotions and passions that are best kept in a box out of sight in some storage area. It is a love-hate thing. After looking through those letters, I was intrigued by what a "letter" home from a soldier might look like in the future. In the following story it is not really a letter, more of a transfer of thoughts and ideas over some overarching connective network. Whatever . . . even with the technological advances of the future, humans are still humans and we still fear, love and feel. Enjoy the story!

Dear Mom,

Really bad week. Lost my friend Gilley—you remember him; I brought him home at Christmas after basic training. He rewired our home entertainment system so that it no longer caused those terrible headaches when you accessed those muscle memory dance move transfers you like so much. Gilley got hit by a brain tangler. Shorted out all his neural connections. My heart hurts from the memory of him after it hit him.

Sorry to start this letter with bad news, but I know you understand. I can feel your love even where I am in the Federated Politikos of Eurasia. My unit just got rotated out of the front lines near (**REDACTED BY AI CENSOR**) and this is the first time I have been allowed to re-energize my civilian neural interfaces. Connecting up to send this message nearly caused brain overload with all the distractions of the Global Human Interface immediately available to me. I had nearly forgotten the all skills I grew up with. The military interfaces are pretty Spartan compared to GHI, certainly not all the offerings that appeal to the less morally and ethically inclined available on GHI- which you know is not me—right?

You know, I think I still have some letting go to do about Gilley. I know you worry about me, so let me tell you what happened so you can understand what it's like at the front. Probably won't help the worry, but maybe you can take some comfort in at least knowing. It is so weird because the enemy is largely faceless, just like we are. With all the battle rattle we wear, the huge machines, the nano-warriors and a million freaken robots the front lines make the chaos at our house look calm. Sometimes I wonder if there is even front line. No matter where you are on the battlefield there is something that can hurt you.

The best battles are when we send our robots to fight their robots. It is an amazing sight, hundreds of machines moving three or four times faster than humans blazing away at each other. Smoking piles of metal and steaming proto-plastic neuro systems as far as the eye can see.

At first the Captain put me in a Robot Control Shelter (RCS). The RCS is pretty sweet, armored, air conditioned and a great food reconstitutor! The RCS is put pretty far back from where the robots fight and my job was to monitor robot units and ensure they were doing what they were supposed to do. Sometimes something glitches and the robots get stupid. I had to check on supplies, like pyronite to power the batteries and ammunition. The RCS had a 4D ammo printing shelter that was attached. I even had my own air force of resupply drones to carry the ammo forward. It was good deal! Then the enemy screwed it all up. They started targeting the RCS’s across my unit with homing EMP missiles, but that was the least of my worries. The fighting got so intense and fast moving that none of us could keep up. Before I could change a robot units’ orders they were dead. Some muckety-muck from on high told us to put all the robots in autonomous mode and abandon the shelters. It really sucked (I know –Language!) to put back on all my combat gear and leave that comfortable shelter.

So this is how Gilley and I got stuck doing a patrol in that big city I told you about in our last connection. You know the cities today are nothing like when you grew up Mom. Sure lots of people still live there and there are tall buildings, but the cities of today are really more like the alien organisms with a humongous central nervous system, and all the odd body parts and organs one would expect in a living being, including a massive need for resources. In our case the enemy had occupied the cities media central as well as the controlling the power and communications grid. The propaganda they were spewing was really bad, and the worst part is that it was believable! Even I had a tough time sorting out the truth from the lies, the deep fake news videos were incredibly realistic and accurate enough that Gilley and I wondered if we were fighting for the wrong side. I mean not really, but imagining that US armed forces units were capable of such inhuman things really made us think long and hard about what we had to do.

The order came down to send in two battalions of heavy mech robotic forces with supporting light robot skimmers as skirmishers. Supporting fires were going to be provided by a cohort of electro-optic jammers, encephalographic disruptors (brain tanglers), and a swarm of drones carrying “wire virus” (basically a bacteria that eats insulation on wires and carbon switches on quantum computing devices.) Gilly and I were assigned a platoon of the heavy mech robots to control.

The plan was to go in heavy with the skimmers taking out any snipers and providing target intelligence on the enemy fire support systems. Heavy mech robots would roll up and destroy the defensive positions and seize the media complex. The second phase of the operation was to move north and regain control of the power production and distribution compound as quickly as possible.

As I am sure you can guess, the plan did not last long. Before we could even gain full control of the robotic forces the enemy begin using technology we had never seen—long range remote devices that short circuited a person's central nervous system. The little hockey pucks started falling out of the sky and we immediately reached for our helmet shields, powered up the magnetic field and hoped that it worked as well as the manufacturer claimed. Mom—it kind of did, all I got was a nosebleed and headache. But Gilley, looked like he got the low bidder helmet shield—I heard a loud snapping noise, smelled electrical burn and then Gilley was on the floor flopping like fish out of water. He was making terrible noises and then he died. That was it. He was gone. Our unit suffered many human casualties but the robots were unaffected and in autonomous mode achieved the mission, only killing two to three thousand civilians in the process. Someone higher apparently thought that butcher's bill was OK—or worse maybe they didn't even know.

Was it worth it? Hell (I know language) Mom, I just don't know. Even robots don't change the nature of war. It is still ugly, violent and unpredictable. Anyone who thinks that technology can produce a "clean" war where destruction is limited to robotic combatants misunderstands human nature. War is fundamentally about coercion, and one cannot threaten a robot with pain or death. In the end humans must suffer for any war to reach its conclusion.

So Mom, you know I am not a bitter person, but there has to be a better way.

Love,
Ergere

10

Opening Remarks: Day Two

Dr. Billy Wells

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

This won't last more than 60 seconds. I gave my remarks yesterday. Sergeant Major has me on the clock. He's spent at least two tours with me trying to keep me honest, all right? And has failed miserably.

Here's the deal; first off, for the international cadets . . . I will tell you, we have a saying in the Army, particularly in the infantry. I don't know what you did after the social, but if you want to hoot anybody know what an owl is? Anybody that wants to hoot with the owl as a soldier, must be able to scream with the eagles in the morning. Okay . . . you're all here, so you did, that's a great thing.

Listen . . . I think this symposium has been very beneficial. I would ask you, as we proceed through this last component of the symposium, to think about, again . . . what is, what are the implications of AI with regard to how we train with officers. It's something all our nations are interested in. We're certainly not perfect at that. If you don't anticipate what's happening, you'll be left behind. When you get left behind in the military, it's a bad thing. Other folks are going to dictate to you, what you and do how you live. And that's not good.

Anyway . . . that's all I have to say.

11

Law, Ethics, and Autonomy: The Challenge for Military Leaders

Major General Charles (Charlie) Dunlap, Jr.

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

It's been a lot of fun seeing some old friends and meeting some new ones. I am a lawyer; I'm going to try not to use any legal terms. I'm not a philosopher, but I did have a Jesuit education, so you know that means something, because I know words can mean something. And fortunately, we do have a cadet from South Africa. South Africa was one of the countries that I visited. One of the great things about military service is you really do see the world, but South Africa was one of my favorite countries. I was always well treated there. Their Judge Advocates are very much like ours in the sense that they do everything. They took me out to dinner, and what's South Africa known for? Its wines. And there are, and correct me if I get anything wrong here, Cadet, but they have twelve official languages in South Africa, of which English is one. I picked up one of the bottles. I looked at the label, and it was entirely in Afrikaans. So, all the South Africans were looking at me and I poured a little glass and I started drinking it. And to be perfectly honest, it was awful. But I'm drinking this stuff. The South Africans are looking at me, and finally one of the wives of the South African officers leans over to me, and she says, “Sir, you do know you’re drinking the salad dressing, don’t you?”

I said, Of course I do. We Americans love that.

Anyway, I’m going to go through a lot of things here super, super quickly. So, if you don’t see everything, you will have a chance to look at the film later on. What are ethics? Do you have ethics in the world of autonomous weapons? Well, I think, I hope, we talked a little bit, this was mentioned yesterday. The Defense Innovation Board has come up with some ideas, really guide posts, as opposed to true ethical principles. Just some general things that they’re looking at as to guide the development, and what you’ll see here is that the devil is in the details. I think Paul Scharre, yesterday, kind of made that point for us. How does law play a role? Well, historically, law has been because law started in ethics and especially in the law on conflict and will continue, I think, for the rest of time.

One of the perspectives, though, comes from Australia, which I thought was kind of interesting. This one woman was talking in a civilian context, but what she said was that we already have enough laws, we don’t need laws to help us in this journey. And in fact, more recently, Eric Schmidt said, let’s not regulate AI so much at this point because we really don’t know what the potential is, and, in any event, we have existing regulations. What he’s arguing is, don’t regulate what you don’t really understand yet. That’s a way of looking at the world. I’m going to come back to that later. Is just compliance with the law enough to fulfill your ethical requirements? This young man wrote this article a couple years ago, and when you think about it, law just sets the minimum standards, ethics goes above that. But what we’ll be grappling with a little bit later on is, whose ethics really are you talking about? There’s lots of ethical constructs out there. Do they matter? I think Chuck Hagel, who did serve in Vietnam, was a soldier himself, former secretary of defense, he made the point that in a democracy, it’s important to have ethical parameters and adhere to the law because it's part of the trust that you have to have with the public. But let's ask yourself, is it really important? Cadet, what do you think? Is trust really important?

Why, ma'am, is trust really important? Why?

And as a practical military officer, why is that important? Yeah, and in this country, actually let me go back here a little bit. In this country, it's important because it's important we have an all-volunteer force. So, people aren't going to join an organization which they think is unethical. Young people, especially millennials, are adhering to the kinds of principles that they want to be associated with. And right now, being a military officer is one of the most prestigious organizations that you can belong to. And in fact, just this last June, the military is the most trusted organization in American society, by far. We can talk about whether that's really a good thing to be that popular. In democracy, that's a legitimate discussion. But more recently, I thought this poll was important because what it showed is that, this part is the important part, because this shows that most people think that military officers, more than other professions, act ethically. So, this is an important standard of keeping the compact between the military and the people. I do think it is and even more recently, we just had a poll come out that says that the military is the agency in American society that Americans trust most to confront our adversaries in all dimensions, actually. What would be the consequences? Do ethics matter for war fighting, and have today's adversaries weaponized it? This always struck me when I read this book. So, many years ago, because people and democracies aren't going to support operations that they think their militaries are acting unethically in, and that's back in 1994, but as we saw, beginning with the post 9/11 wars, we have adversaries who are deliberately trying to orchestrate situations which would present to the public a military acting unethically. And what was America's worst defeat since 9/11?

Worst defeat? Think about it. No, I think these cadets need to.

What do you think?

Worst defeat? Actually, Abu Ghraib. No U.S. soldiers killed, but it had an effect on the support that we need in a democracy. Would it have made a difference if an AI had done those things to the detainees? I don't think so, and there are real operational impacts. General Petraeus made the observation that Abu Ghraib—this is the situation where U.S. troops were abusing detainees. He says, I like the words he uses, non-biodegradable; the enemy will keep beating you with a stick. In other words, they will keep using that against you when you're trying to win the support of the people. And it actually matters to the troops. When I was assigned to our nuclear command, I wrote a law review article about how we did the legal review for nuclear weapons strikes. We actually review it under international law, and part of the reason I was allowed to do it was the commander at that time was concerned about—wanted to make sure that the troops would do what they were told in a crisis situation. And part of it is they need to know that what they're doing is legal and moral. And that was one reason why we did that.

I don't think anybody over here was born when this was written, but I wrote this, and I thought what I would do as I go back and take a look at what I wrote twenty years ago and see how, if at all, it would apply today with respect to artificial intelligence. One of the first things I talked about in my conclusions was the unpredictability of reactions to technology. I wasn't thinking of artificial intelligence at that time. I'm not sure if it was invented, or at least as we understand it today. But what I was wondering at that time was, how would adversaries react? Because the soviet union at that time said that they would react to high tech precision guided munitions. That was just appearing with nuclear weapons, and so I was concerned. We needed to think about how is the enemy going to react to technology and artificial intelligence?

And in this context, nuclear weapons are one of the things we need to think about because there have been people who have been concerned about the integration of artificial intelligence into the command-and-control system of nuclear forces. They could have an effect on adversaries where they might think that they had to act in a different way. In other words, they'd be upsetting the traditional notions of deterrence. And, in fact, there's been a guy who recently wrote an article that said that because of artificial intelligence and the speed in which an adversary could strike us, we needed to have a dead hand.

You know what a dead hand is? A dead hand is an automatic system that will react even if you're not able to do it yourself. And he suggested that this dead hand would have to operate through artificial intelligence. General Shanahan kind of nixed on that because we are not ready to go to the point where deterrence would require the use of an automatic system to respond. But I do wonder in the future if an adversary's system got so sophisticated that the only way to ensure response was through artificial intelligence. And if you didn't have that system, what would that do to deterrence?

Another point I talked about was that I was concerned about the co-mingling of civilian and military systems. And at the time, I was more concerned about how computer systems were just coming online. We were very dependent upon civilian systems, and how were we going to resolve degrading that capability in an enemy that was used so much by civilian systems? And I think today, to update that, the issue is that we depend upon civilian enterprises primarily for a lot of the development of artificial intelligence. And Secretary Esper recently remarked on that. The problem, of course, is, as you probably know, a lot of the tech companies don't want to work with the government because they raise ethical issues about working with the government. And the ironic part about it, with Google, is that Google works with China. They built an artificial intelligence center in China. Now, what they say is we're not working with the military because they're working with the government, as if there was a difference. There you have it, and Bob Work, Former Deputy

Secretary of Defense, has talked about this a lot. And he takes the position that the military does act ethically, and that the policy right now is that commanders are going to retain control over the artificial intelligence system, at least as it comes to the application of force.

This is actually General Shanahan from the same article where he talks about how people think that we're in some back room building the Terminator. That's kind of the summary of what he's saying, but that's not what he's doing, and they're talking about the narrow intelligence. That's a term of AI, narrow artificial intelligence. That's kind of the thing that's being touted, and we'll talk about it a bit more, and then he points out that properly-used artificial intelligence can actually limit civilian casualties and so forth. But one of the thing—take a look at this, Sergeant Major, I want your opinion on this.

Here's Dunlap's view of the world: if you get a commander that gets in a situation, Bob says that we don't want the true artificial intelligence weapon that's going to go out and search for targets and so forth. No commander would want that. I disagree. I think if a commander's in an existential fight and he's losing, or she's losing, and she has a reasonable belief that this weapon will strike the enemy with a reasonable understanding that it's not going to violate the law of war, she's going to use it. I think she's going to have to use it or face defeat, Sergeant Major, absolutely.

Yeah, and even if it was going to do it on its own, you're told, hey, the thing is only going to go after the enemy. It might make mistakes. Your soldiers might go after them, but they also might make mistakes, so of course.

But we could actuall—in fact, I've written a blog post, and everybody's going to subscribe to my blog, right? But it's this world that we're living in because of communication technologies and being powered by AI. And so, again, they're talking. What the U.S. is developing now is this narrow AI. And narrow AI means like you get—I think there's some examples, he uses a sniper, where it's just limited to certain things. In other words, it will shoot down a drone that is coming your way, period. It won't look for other types of targets. Narrow AI, the problem with that is the adversary.

Here's something to take with you: every time you try to do something good, the adversary is going to war game it and figure out how he can turn it into something bad. So if you develop narrow AI, they're going to develop something that is just a little different so that the AI doesn't go after it. Can we count on civilians to work out these ethical issues? No, they, Google, tried to have a Board and they had to cancel it because an African-American woman was on the Board, and she happened to be a conservative, and there were protests from Google employees, so they disbanded the whole Board. It's something that the military is going to have to do itself. I'll talk about how we do that.

One of the things–oh, let me go back for a second. One of the things I was concerned about is how information–twenty years ago the advances were going to impact democracies, and how governments run because of just the super empowered nature of it. And I think we've only seen that more, had some discussion about deep fakes, and deep fakes are really aided by the development of artificial intelligence. And, as you know, a deep fake is when you're looking at a video and it looks super accurate, you can't tell the difference, and, in fact, experts are having a hard time telling the difference. But in this image that they see, can it have an effect on the population's motivations within the military. Without the military. The Pentagon is aware of this. They're working on it. So now you have the Pentagon involving itself and really domestic U.S. politics with the idea that they're defending the system in a way that we haven't normally seen the military get involved. And we need to think, what are the long-term implications of that?

I also think there's a good short point paper that the congressional research service has put out recently where they raise the issues about deep fakes for congress in the context of national security. And you can see some of the questions that they're asking. I would suggest to you that these raise various legal and ethical issues. Looking just very quickly, so you can see some of the things here have great implications for democracy when you have the armed forces as a matter of national security trying to make judgments as to what should or should not be involved on social media. That's an issue that we've got to think through. It's a legal issue, it's an ethical issue, and here's the thing, everybody is all leathered up about deep fakes. But if you have the opportunity, and you are a commander, and you can create a deep fake that shows the adversary's president doing something that is going to erode his authority and his power in his country, to degrade the ability of that country to attack you, are you going to do it? Are you going to do it?

Suppose that the adversary's president is elected, but they're a hostile country to you. Are you going to do it? Is that a legal issue? Legally, you probably could. I don't know anything with international law that's going to bar that. But is it an ethical issue? Because then you're attacking the concept of democracy. On the other hand, what's the consequence of not doing it? This is another issue. And in *Like War*, the book that one of our speakers has, it raises similar issues. Farah Baker is sixteen years old, and she started a blog or a twitter account. And what's interesting about this is that she had so much impact on that conflict that they characterized her impact as akin to the most elite special forces unit. So, if that's having that kind of battlefield effect, what do you do to her? You take her out.

Your soldiers are getting killed because of what this person is doing. Well legally, yeah, you can take him out, take her out, but she's sixteen years old, and she's just exposing–suppose she's exposing the truth, but it's adverse to your military mission. And you know, how do you deal with that? These are the kinds of ethical issues that are going to be occasioned because AI is super empowering these kinds of techniques, so we have to think about that. Is she targetable militarization of space? Twenty years ago, I was concerned about the militarization of space and how that technology was going to work out. And actually, artificial intelligence has a lot to do with it because we're going to be able to do things in space that we weren't able to do before. And it will enable us to go to places and conduct operations. Now there are treaties that forbid the establishment of military bases on the moon or other terrestrial objects, but you can still conduct operations in space, and we can talk about that during the Q&A.

There're arguments that say no you can't, despite what the Outer Space Treaty says, actually establish a military base on a planet under certain circumstances. So, what they're talking about is soft law. What does soft law mean? It means like countries get together. It's not a treaty, it's not binding. They decide that we are going to do things this way or that way. It's like a code of conduct, it's trying to establish a norm. And it's a good idea if you want to eventually get to a treaty that you start out with these voluntary norms, but the problem with trying to restrain this is that you can't verify, it's almost impossible to verify whether something has a weapon in it or not when it's in outer space. It's hard enough to do here on earth, but in outer space it's virtually impossible, and so what people will say is that so long as you're not able to verify you're not going to have weapons, you're not going to be able to have a treaty.

So should your country be involved in an agreement of voluntary agreement not to militarize space? Maybe, but then you have to think, what is the enemy going to be doing? What is the adversary going to be doing? And where will you be? How dependent are you on space? I would suggest very dependent. Don't think your cell phone, your GPS, and so many other things are going to work. One of the things that I thought about–I was concerned that technology, especially precision guided munitions and so forth, this is something we've talked about on our loop a lot, does it lower the threshold of conflict? And people will tell you—a recent article came out that said, because they're lowering the threshold of conflict, they think, oh, my god, everybody, they're going to be using means, you're being involved in conflicts all the time. And the question is, is that going to make a world at war?

If artificial intelligence can make it seem like it doesn't cost a lot of human life, that will then have been a time of continuous war. What I'm asking here, is that always bad? I mean continuous conflict, yeah, but if we get involved in conflicts that we might not have gotten involved with, is that really bad? Because as this suggests, humanitarian interventions with countries that may not have enough interest to go to Rwanda or Darfur or something like that and risk their soldiers. They might be willing to do something about genocide or something else if it is conducted by an artificial intelligence system. And here's an example of it. It has to do with drones, but what this author talks about is maybe we can do something about these horrible things that are happening in other countries that our people don't want to use our soldiers for, but would if we have another way of doing it. So we need to think through what are the implications of that? Because there, generally, we would think it'd be bad, but then there might be times when it is good to lower the threshold of being involved in conflict. It's talking a lot about organizational culture.

There're things that are happening in the artificial intelligence world that will affect your organizational culture because you will have people in your units in the future who may be different in the sense that they may be artificially supplemented. The human computer interface—it may be that there're different ways of using artificial intelligence to determine what people are thinking. You can see—find on the web—that China is developing something that they can put on somebody's head, and they can control drones without even touching anything. Just through its picking up on the electrical energy in the mind. And so we need to think through what are the implications when we supplement a human being with artificial intelligence? In other words, we are going to get to the point where we'll be able to plug something into your head, and that will give you capabilities. Can you conscript soldiers and force them to have something put in their head? And then what happens when they finish their military service? You may not be able to bring them back to what they were. These are kind of some of the issues that are being raised.

Organizational culture, how much do you have to know about AI to be a legal and moral actor? Here's something that's in the Cyber Law Manual, which, by the way, was developed in Eastern Europe and NATO sponsored. What they talk about here is that commanders don't have to know everything about the what. And they're talking cyber here, but I suggest it applies to artificial intelligence. They can rely on subordinates, but that's not an excuse not to know anything. And ultimately they're going to have to have a reasonable knowledge of what the system does and what the risks are in using that system. And how much do they have to know about ethics? I would suggest, okay, sounds good; it doesn't matter whose ethics they are going to be because you can just pick out ethics. Well, in the U.S. military, say you have an ethical objection to an order. Interesting but not an excuse for not obeying an otherwise lawful order. Because remember, law represents the agreed-upon baseline. So if it's legal in the U.S. military, even if you object to it on ethical grounds, you still have to obey the order. So that's why I'm a little worried about who is this ethicist that they're talking about hiring, and why is that the law in the U.S. Why do you think we have it in the U.S. that you have to obey an order if it's legal, even if you personally don't like it? Why do you think we have that?

Yeah, you have to obey the law. You don't, in the U.S., you don't have to obey the law if it's illegal, but if you individually think it's unethical, you still have to obey it. Why? Because there're lots of ethical codes out there. Lots of people think different things, and you have to have a baseline that everybody has to observe.

And so in the AI area, the tech companies came up—have you heard about this Tech Accord where all these companies agreed to this ethical standard? I wrote on this because, you know, the devil's in the details. What did they exactly say in that Tech Accord? This is what they said they would do.

That's what's the problem with that.

Yeah, in other words, if ISIS is using their technology to capture young women and turn them into sex slaves, they're going to protect ISIS. They're going to protect that system that is morally indefensible. And they act like they achieve the high ground. I think that's offensive. I think it's unethical in its own way, but that's the way it is. And I just suggest to you that there are other people, Michael Ignatieff—who some people know he's Prime Minister of Canada or something—he wrote a book on that when I was in the Somali operation. I reflected upon it after that came out, after the Somali operation, because it's something I saw in Somalia. Different societies have different understandings of what is ethical behavior, and so when you're trying to come up with something like AI and you're looking along around the globe, you're going to find that there are different interpretations, interestingly enough.

Twenty years ago in China, two Chinese colonels wrote this book. I would suggest to you that two Chinese colonels don't write a book and don't give an interview to the *Washington Post* without the agreement of the Chinese government. This is how they looked at it. Now, today, we're finding China is suddenly interested in this, and the idea was that they are wanting to have some sort of framework, and they want to continue to develop air weapons. Here's the danger: there are adversaries out there. They want the world to collectively throw up its hands and say well, there's no law out there because they've done this in cyber. There's no law out there, ergo, they will never be in violation of the law. And they'll make it seem like they want to develop law, knowing that it's not really going to get there.

The Russians have been opposed to this for a long time; now, suddenly they're changing their tune a little bit because this is what their story is.

We'll see what their real motives are. Now in the U.S., we have always counted on the notion of reciprocity. In other words, if we obey the law, if we act ethically, we do it because we can have confidence that if we do it, then the enemy is going to treat us that way. I would suggest to you that maybe that's not so true in the current world because we have situations where fighting adversaries set fire to pilots and buried children alive and so forth. And so now we have what I call the collapse of the notion of reciprocity. You really can't say that with a straight face to the troops, and it is an ethical problem and a legal problem. As Joshua Faust has pointed this out in this article, because we're fighting people where we have this asymmetry of values, but the reality is that the public still wants us to act in the right way. So, one of the things that the U.S. military has done in its Law on Conflict Manual, which by the way is on the web, they've added the idea of honor. Now, there have been academics. This is one of the things different between academics and people who have done something or served or been in the field. That's what I'm struggling for because they ridicule this. They ridicule the notion that honor would make a difference to a soldier on a battlefield.

It can make a huge difference. There are soldiers—for example, if there is a soldier who's left behind on the battlefield, they will go to huge expenditures of life and resources to get that soldier. And I remember during the Kosovo operation Danish, remember the f-16 pilot was down. We sent, when you looked at the total mobilization of that effort, there were 28,000 troops that were mobilized to get that one pilot out of Serbia. And there were a lot of things that would have happened to Serbia if that pilot hadn't been rescued. But I think this is a way, we have to fight against what we've seen in the past.

When people are under stress, they do things that you wish they never had done. That's why part of our training for this AI situation—we need to talk specifically with the young soldier, the nineteen-year-old that's going to be in that crucible of pressure and help prepare him or her for that moment. We have got to talk through, hey, this machine might be coming after you; it doesn't mean that you're going to take it out on all the civilians there, you've got to discipline yourself. You have to build that mental muscle memory so that the troops will do the right thing. People always wonder, well, how come you like, you know, for example we would always court-martial people for barracks. Largely people say, why are you court-martialing? He only stole $20. I'll tell you why, because when you go on that deployment and you put all those big bags in a big pile, it's easy to steal. And if people don't understand that there are consequences, because I can tell you and, Sergeant Major, correct me on this, when you go on a deployment, people are scared, they're under stress. And their cell phone gets stolen or something, they will begin to obsess on that because that's the way they're dealing with the stress. And so we have to have these ideas in place specifically shaped to the artificial intelligence.

So one of the things that we have to do, I think, is talk openly about our idea of ethics, our idea of adherence to the law, even when it can't be rationalized in the traditional way. Because we're going to be facing situations which are going to be terrifying, and we need to make sure that our troops react in the right way. It's called virtuous ethics, where you focus on the goodness of the ethical standard, as opposed to some kind of rationalization of the ethical standard. Again, coming back to the risk of over regulation, you know ethics, if you're looking for rules, another rule scheme, that's the law. Ethics is where you develop an idea of what you should be doing and still accomplish your mission. So we'll see this.

And the reason I put this up here in closing is we need to be aware it's easy to come up with a lot of rules. A lot of people want to come up with a lot of rules, but every time you come up with a rule, that can be constraining. And just because you're constrained doesn't mean good things will happen. I often think about this in terms of our drone strikes. People say, oh, well, if you don't do that drone strike, no civilians are going to be killed. No, that's not true. You don't do that drone strike, that guy's going to live to go on to kill a lot of other people and do it in a horrific way. So never think that not doing something, constraining yourself is, ipso facto, going to be more lawful, more ethical, and so forth. I call it the moral hazard of inaction. Talk about it a little bit and try to put it in that context. If you don't act, if you say you're restraining yourself on all these moral and legal things, you can feel good about yourself. It doesn't mean it's going to be good for people who are most vulnerable. So what are we going to do? We need to keep in mind one thing, there's physical courage, but suppose if AI eliminates the need for physical courage. In the way we've historically—there's still moral courage. Does anybody know who Hugh Thompson is?

Yes, My Lai massacre, he was the helicopter pilot. There was a massacre that was by U.S. troops of Vietnamese civilians. He saw it happening, and he landed his helicopter. He got in confrontation with the troops; he threatened to kill them if they continued to kill the Vietnamese. He was ostracized by the army for twenty years. They finally gave him the soldier's medal, but it's an example of moral courage. Max Hasing, one of great military historians, he makes this observation. Now what's interesting about that is that it's more common among women than among men, moral courage. Interesting, but in the event, I've tried to raise a bunch of issues. I know I haven't resolved a lot of things, but I hope I've given us something to think about, especially as we look forward to the panel which I'm anxiously awaiting.

Do we have time for a couple questions?

Question and Answer

Okay, I'm going to ask–well, no, we have one over here. Man, what's your question? You have a question in your mind? What is your question?

[Audience Member] [inaudible] I don't know, I was hoping you could answer that. I've looked at that for a while, ma'am.

[Charlie Dunlap] That book doesn't help America, but helps China. Is it–what do you think? Is it because the Chinese become, like, their economy becomes bigger and bigger? In the future, China has really a big—they actually had a big future in economics. So is the financing side. That's why Google is interested in China. I'm so glad you asked that question because that's the right question. What we're seeing with these tech companies that are so into artificial intelligence they are getting so big, they fancy themselves as global entities, not with responsibility to the sovereign nation. Which they are headquarters. They think that they have a responsibility to the whole world.

Irrespective of what these different countries may be doing. Now, what Google will tell you is, oh, no, we're not going to sell them this technology like facial recognition that they can use to suppress dissidence in their country. Yeah, they will, because they're money driven. At the end of the day, it's money. Now keep in mind, the free enterprise system is a wonderful system. It's the reason America has such a powerful military, but when it's unconstrained and it doesn't show itself with some sense of loyalty to a value set that's represented by democracy, it can get unsure. In my article, I go after the Tech Accord that the technology companies have agreed to. What I talked about in this country, we can conscript people, we can draft people if we want. We can take over companies if we want. During wartime, we did it in the first World War, we did it in the second World War. And as we look to the future, if this artificial intelligence technology is so critical to success, to the survival of our nation, then we may have to conscript, in other words, draft Google, draft engineers, draft their company, and so forth, if you're going to survive. And people say, well, how can that be legal? Well, there's lots of legal bases; is it moral? Of course it is, because if you value democracy, and the things that your country stands for, then you'll have to do those things when you're faced with what we call an existential threat.

Do we have time for one more? I'm going to go with this student. Is that okay? One more student question and then we'll finish up real quick.

[Audience Member] I have a question. because I've done research on this before, and I was a law student. The question I find is that in international code, you actually have to have someone to hold account, accountabilities when you attack other countries. So, if AI are manned by themselves automatically, there's no one to hold in accountability.

[Charlie Dunlap] I've been asked that question before. It's a good one. Here's my answer to it: if you're the person that turns that AI on, you're accountable. So that means if you turn that on, you better know what it's going to do because you're going to be personally accountable. And if you're a head of state, your nation is going to be held personally accountable. So that's why people your age have to—you might not know all the details of how an AI works, but you're going to have to have a general idea. And here's the problem: learning artificial intelligence systems that learn as they do things, that may change. What will they end up ultimately doing? That's why the U.S. is looking at this narrow AI where it can't learn beyond certain parameters, and that may be the way that you have to go in the future. But it's a good question; it's asked a lot. But there are a lot of people who say, oh, AI, you can't have AI because nobody's accountable. Yeah, there's somebody accountable; somebody who turns it on, and then the responsibility's on that person. Real quick?

[Audience Member] Keeping with the theme of the symposium here, and talking about ethics and developing an ethical mindset and values with cadets and then future officers, how do we get beyond the annual checklist of doing the ethics briefing or the pre-deployment ethics briefing? But how do you embed ethics in all that we do?

[Charlie Dunlap] Here's what I suggest: you talk about these general principles, like the defense innovation board, and then you assign cadets to dive into what's being done. In other words, get their fingers into the technology and the capabilities and the proposals, and then you have a session with them where you ask them to compare what's being done with these broad ethical principles. In other words, they need to get into the facts, because the problem with a lot of our ethics education is that it's all platitudes. It's like, do the right thing. Okay, I got that, but sorry, Major, maybe you'll agree with me, we all want to do the right thing, but when that vehicle is heading towards your checkpoint, you can see that there's children in there, you can also see that it's large enough to have a pretty good size impact. What do you do? You want to do the right thing, but you need to have a good understanding of the facts because sometimes people say, hypothetically, they know that certain kinds of vehicles have been stolen and, ergo, they're more likely to actually be the threat. So that's why the facts make a difference, but we spend too much time just lecturing cadets and students about these broad platitudes without getting into the specifics. Now one last thing, I will say, don't be into writing a cookbook for people because this is what—

Sergeant Major, you probably saw this in Roe briefs, you'll have the lieutenant down there, he starts asking fifty questions where he's changing the facts a little bit, and he's writing them all down because he wants a cookbook. He wants to imagine every possible scenario. Of course, in real combat, the first thing that happens will not be in that cookbook, so we have to get people to internalize the values and then be able to react to them. And I also think that we have to give them a rationale because if you just say we do this because we're good people, that can be hard; we do it because if we don't do it that way, our other soldiers are endangered. Our mission is endangered, because they can understand that, and especially because we know the motivation in combat; we like to think they're fighting for these big values. In a sense they are, but in that tactical execution, it's the soldier right there that they're fighting for. And stop me if I get anything wrong, Sergeant Major. One more question.

[Audience Member] You spoke about reciprocity and law of war for these cadets, mainly that they haven't faced perhaps any of those types of situations. What would you suggest to them? That they start thinking about learning and more importantly passing on to their soldiers? So when they get into those ambiguous situations or we're really trying to follow the law of war and ethics and so forth, then the people we're fighting absolutely don't care about it, how do you prevent the, you know you can't, but how do you work to prevent the Abu Ghraibs? The My Lais? The marines that think it's okay to do things out in the west to a child?

[Charlie Dunlap] Here's the way you prepare yourself, I recommend that you read a lot of the books that are written by our young lieutenants coming out of Afghanistan and Iraq because then you people like to say, oh, well, it's just reading. No, reading gives you an intellectual database so you can see how other people—what they were confronted with and how they dealt with it successfully or not. And then with your soldiers, what I recommend is that this is the 21st century, Sergeant Major may not agree, well, I think you would when you're giving your orders to your soldiers. When you can always explain to them the why and never be one of those soldiers, those lieutenants who say, well, higher headquarters is forcing us to do it, because that erodes you, but take the time to explain this is why we're doing it. Because when you get in combat and you're not able to do that, they're going to know she has a reason that she asks us to do this thing, and we trust her because you build up that trust in garrison.

The other thing I recommend based on my experience, you are very strict with them on some little things like their uniforms, if they're late, or whatever, you don't just–I mean, there's a way that you deal with this, but you have to be strict with them in garrison because, can I tell one war story? I know I'm running a little bit over, okay. During the Somalia operation, I was attached to the Marine Corps—keep in mind, Air Force guy, JAG officer, never been in the field. First, no training, first going into the field. Sorry Major, I couldn't even get my helmet cover on. So, the First Sergeant helped me, but here's what happened. It was really hot. I go into the, I was kind of the executive officer for the Marine General, he goes and he says, Dunlap, you need to go look at your mechanics. I went out and saw the mechanics and what they'd done with their uniform. Because it was hot, they cut it off. And they cut off this and I'm like, what is going on here? And so I asked the, geez, the only time I was in the military, for almost thirty-five years this is the only time I ever did this, I said, I got the two chiefs, I said, geez, what's going on here? And he said, well, he started saying, hey, you don't understand. I said, chief, I understand; bring yourself to attention.

That's the only time I ever did that with an e9. I said switch to receive only because what you're doing with these soldiers is you're letting them think, oh, it's hot out here, we need to change everything. And do you think a soldier who gets that mindset and is reinforced by his chief, do you think he's going to run that checklist on that airplane the way he's supposed to do? Because he's going to start thinking everything's different, I don't have to do everything because it's hot. And when they get into combat, they will know what they're supposed to do, but they'll think that things are different somehow and you have to set the example. I think it's very hard because when you're there, you're going to have to be the person who keeps the morale up, who doesn't let them get down and doesn't let them think that the rules don't apply. That's what happened in Abu Ghraib, note that happened in Abu Ghraib, the officers, this is so un-Army-like, and I was in the Air Force, but I've never seen this with the Army, but it happened. The junior enlisted people were in the prison, supposedly guarding these detainees. They're getting attacked all the time, so they're scared. They figure maybe we can soften these guys up or whatever, but there were no senior NCOs who came around and checked with them on swing shift. There were no young officers that came around. They were like just treating the prisoners anyway they wanted because they were scared, and they were trying to deal with it. You have to be the person that reminds them that we need to do things the right way, because if you don't then they are calling each other by their first names, which we don't do in the U.S. military, and they start thinking rules don't apply.

One more example, this from World War II. There's a book by Richard Overy. It's called *Why the Allies Won*. When the German army went into Russia, Hitler issued the partisan order and, okay, you had the SS put the SS aside. This is the Vermont, the regular German military issued the partisan order and what that partisan order said was that you can kill any civilian you want because they're all partisans. They're all coming after you, and the German army had learned the traditional rules of law war, but once you tell the soldiers something like that then they throw out all their rules. How did it come back to bite them? When the German army was being pushed out of Russia, everybody talks about how disciplined they were, what they had to do was they had to start shooting their own troops. They had these, what we call summary court martials where they executed 15,000 of their own soldiers because the mindset of the soldiers was, okay, there are no rules; ergo, if there're no rules, then I don't have to stay at this front-line position. It changed their mindset. Always be thinking about what's the mindset of my soldier. And when you're dealing with young soldiers, you can't be saying okay, this is the law here, this is ethical here, but it's not here. You can't mess with their minds like that because they're under extreme stress. You've got to get it right and then stick to it. I mean flexibility, sure, change circumstances once in a while, but not very often. What you need to do is spend a lot of time preparing yourself for that moment. Do it through reading. Decide what kind of person you're going to be, and then also build your brand, your reputation with your soldiers in peace time, in garrison, because only in that way, when you get under the extreme stress of combat, will things happen the way you want them to happen. Because, otherwise, you know what's going to happen if they don't see you as the leader? They're going to develop their own little leadership cadre. And there's a good article in *Vanity Fair* magazine about a unit in Afghan, in Iraq, where that's exactly what happened. They ended up committing war crimes because—then they lost. They didn't know what the rules were. They were just doing what one guy told them. Sorry, yeah, okay, we're out of time.

[See Appendix for corresponding PowerPoint presentation.]

12

Social Media has Transformed the Wars of Today. It will Revolutionize the Wars of Tomorrow.

Emerson T. Brooking

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

I am honored to be here.

I would like to start in June 2014. In June 2014, the Islamic state which emerged out of the Syrian Civil War from a new generation of rebel fighters, as well as the remnants of a QI, poured over from Syria into northern Iraq.

The weapons they used weren't that much different from guerrilla groups of the past. It is about 1500 guys and mostly Toyota pick-up trucks with AKA's.

They took a novel approach because typically you go into another country and launch some sort of military operation. You want to keep it a secret. These guys wanted everybody to know about it. They have their own hashtag. All eyes on ISIS.

They have twitter bots and a smart phone app which amplifies their propaganda across Arabic speaking Twitter until it was the top-trending subject for days. Everyone knew ISIS was coming.

They were extremely good at doctoring propaganda and making themselves look as indomitable and foreboding as possible.

There is a contingent of fear which spread as they were advancing.

In their sights was a city of [inaudible] defended by 60,000 Iraqi soldiers as well as numerous Iraqi police. They were trained by the forces and retained a lot of U.S. equipment.

It was not enough.

The fear of these ISIS forces spread like a virus for these communities.

Not that many folks had access to a smart phone.

In some ways they made the situation worse because even if you were not online and have a neighbor who is in a scene, things spread easily by word-of-mouth and there's no way to track it.

It seemed like nothing could stop the ISIS forces. Defending of the Iraqi military disintegrated. The police fled, and 500 hundred thousand billions played thereafter.

When ISIS came in to Mosul, they were essentially unopposed. They released militant prisoners that had been locked up and increased the size of their forces significantly, and they seized this U.S. military arsenal.

All of a sudden, all the propaganda they had been spreading about how unstoppable they were started to seem a bit more like reality.

The propaganda outlet significantly increased.

It was a testament to the danger that Isis posed that the Iraqi government could do nothing directly to stop these ISIS propaganda broadcasts. Instead, one of the first actions they took was to cut Internet access for Iraqi Citizens and to lock down in Baghdad and stop civilians from having access to the propaganda to stop the contagion of fear and install terror attacks in Baghdad and elsewhere.

It was at this point that President Obama, after making clear that his time in Iraq was over, began to initiate limited airstrikes against the Islamic state.

Isis kept growing stronger.

In August 2014 they executed James Foley, an American journalist who been held several years in the Syrian Civil War. They did it in a staged video. They actually shot it eight or nine times before they got it right and had the colors just right. They had multiple camera angles. The original was high definition.

When they cut this video, they called it a message to America.

They laid Twitter and social media applications networks in advance to ensure it would go as viral as possible.

And it did.

When this video was released it was like a gunshot across the global information environment. This image graced front page news everywhere.

The contagion of fear which had hit Mosul a few months earlier was felt internationally.

Even though at this point, the ISIS-inspired terror attacks abroad had not yet started. In fact, no American citizens had been killed at home by this group. This was a singular terrorist killing.

It completely changed U.S. strategic calculus regarding the dangers that Isis posed. President Obama had made it absolutely clear that these limited airstrikes would not proceed into Syria – yet, they expanded these airstrikes into Syria.

The statistic that stands out to me most throughout all of this is in September 2014 more Americans, according to a poll, were scared of an imminent terror attack then they had been in October 2001. Nothing had happened at home, but that fear was palpable and widely spread.

Isis is not alone.

We have seen conflicts between Israel and Hamas extend online. We've seen increased Russian utilization of propaganda. We've seen dozens of national militaries jumping into space.

For myself and my co-author, this seemed like a field worth studying. I got interested in this issue back in 2012 shortly after I graduated school. I grew up here and on the Internet. My interest and focus were on U.S. defense policy.

It seemed clear to me that the social media Internet stuff, which was increasingly driving international politics, would affect conflict in time. I looked around for all the smart folks who were writing on it, but a lot of people had not caught on it. I jumped into this field and that's how I arrived at this point today.

I want to start by discussing how we got here. I want to start by talking about this phenomenon Doctor Singer and I call Like War. Broadly, it's a contest of psychological and algorithmic tribulation bought through the competing viral events.

What does that mean? To break it down, the competing barrel event is any piece of content you share online, any status update or image. It is all competing for this most scarce and finest resource: attention. It's competing in the same ecosystem.

Terrorists and military propaganda is competing with a wedding photo or a status update from an old friend. All of these things now exist in that singular information environment.

How do you measure attention? You measure through likes, page views, and emoji's.

If you are thinking about this from a conflict military perspective, you are competing for the same likes as everybody else.

This has fascinating military implications.

Conflict, war, is a continuation of politics by other means.

That just means when you have exhausted diplomatic and economic recourse, you turn to force in order to realize your political objective.

We are always trying to achieve a specific military objective. You have to do so by neutralizing your adversaries center of gravity.

Writing in the 19th century, the center of gravity meant the opposing army. In Napoleonic times, if you take out your adversaries' means to project force, the war is pretty much over. You can impose your political will on the enemy.

After the 1920s, military theorists thought increasingly about airpower as means of circumventing the adversaries' army and, instead, targeting civilian population and civilian industry and industrial capacity. The thinking being, if you neutralize those that were the new center of gravity, you could realize your objective.

There was another line of thinking emerging during this time. It may be through a process of psychological dislocation—you could alter the perceptions of the civilian and military that you are fighting. But you could somehow change or eliminate the enemy's political will without ever having to fire a shot.

This was broadly information warfare and propaganda.

For a long time, the thinking did not line up with what was actually possible. During World War II, the Nazis hired a few thousand full-time shortwave radio operators. They were broadcasting some fifty or sixty hours of original content every day to try to win this global radio war. They even took the time to track down a few native Gaelic speakers whom they tasked with doing a few hours original broadcasting each day to Ireland. The intent being to reach a few Irish cultural naturalists and open up a new front against the United Kingdom of Great Britain.

However, even if you were persuaded by these broadcasts, you had to have a radio, you had to be tuned in at the right time and could not record the broadcast and listen to it later and you had to bind together with other people who felt like you did.

Those are a lot of steps and it could not really come together.

A slightly more recent example occurred over the course of the Vietnam War: we dropped something like five tons of propaganda leaflets over North Vietnam, trying to help force a political settlement with the North Vietnamese government. These leaflets were extremely popular in Vietnam because it was the highest-grade toilet paper you get over the course of the conflict but had very little other political effect.

As you might guess where I'm going, things are a lot different now.

The big term to remember here is disintermediation. This is a term that communication scholars and Internet theorists thought about a lot in the 90s: the future effects the Internet might have on society and political organizations. This intermediation means taking out the middleman. Taking out the thing that lies between a service provider and a consumer.

In the context of retail incorporated: It's about how Amazon has planted the need for big-box stores. How Uber changed taxi services.

This intermediation has always promised its greatest effects with regard to the media and how we consumed information. Traditionally, we had big broadcast companies. You had radio and television.

We e had a series of what were essentially gatekeepers, which were editors and reporters who would figure out the stories that were most relevant to the public to make it available to people.

As folks were considering the implications of the Internet, you, all of the sudden, everyone would be an information producer, and anyone can consume anything that anyone else produced.

He would eliminate the need for these gatekeepers. He would democratize the information environment.

These guys all thought you had some noble free market for information work with stuff that was best and did the most objective good for society and would invariably rise to the top of the pile. As we know today, that is absolutely not the case.It is the most salacious content that rises to the top. It is the stuff that stokes outrage and, in fact, nothing at all says that this content has to be true.

It is useful to survey what this information environment looks like.

When we talk about an entity like Facebook, there are several orders of magnitude difference between it in previous media.

Facebook has about 2.4 billion active users. That makes it substantially larger than the biggest country in the world. Facebook is the second largest continent in the world after the Asia-Pacific.

We also think about this information environment and this new information battlefield. We should understand that there are no neutral rules that govern it. There is not the force of gravity or other environmental concerns which are neutral. Instead, this environment is governed by algorithms.

They are written by a handful of engineers based primarily in Silicon Valley.

This simulation of those algorithms then becomes a major priority of anyone trying to compete in this information environment. We have a lot of people, national governments and militaries, who have now decided they have to compete in this information environment.

There are some thirty verified national militaries who have launched information mitigation apparatuses for the purposes of infiltrating and altering social media conversation. Altogether, when you factor in third parties and political parties, there's some seventy nations where this has occurred.

These are just the ones we know about.

The U.S. and a few other countries have actually been in the sphere for a while. I think it is a testament to how crucial this focus is becoming. Secretary of Defense Mattis, elevated in information, is the newest joint function.

I want to shift gears a bit and talk about how the social media environment changes military intelligence. I want to start back in World War II. If you think about Operation Overlord or, more specifically, the preparation for Overlord, there were, at the height of our preparation, some 40,000 tons of material transiting to the British Isles each month. We had 2 million Allied soldiers in theater getting ready to invade.

The Germans obviously knew a landing was coming but, through a bit of subterfuge and a bit of luck, the Germans were caught unaware and truly did not know where we would show up until the first Allied soldiers stormed Omaha and Utah beaches.

I want to contrast that with the more recent military operation. One of the most secretive in modern U.S. history. This is operation Neptune Spear: Osama bin Laden in 2011.

We had our best COT team six. We had Black Hawk helicopters who flew low in Pakistan.

Out of the giant U.S. national security bureaucracy, there might've been 100 people who understood the full extent of the operation and mission of what was involved.

The video link everyone thought was with this operation was being transmitted to the situation room, with that iconic photo with President Obama and his team watching the operation unfold.

In fact, there was another corroborating source for this operation.

There was a Pakistani IT consultant who was staying up late at night and crashing on a project and heard helicopters overhead. He did what a lot of us would do, and he took to Twitter to complain about it.

The record he left quickly became corroborating evidence for reporters the moment that President Obama announced that bin Laden was dead. Reporters figured out the city that had been hit and figured out a lot of details the U.S. government was not necessarily going to disclose to the public. All through these contemporary tweets.

What is interesting is this guy was watching Obama's broadcast, too.

It's now midafternoon the next day, and he tweets, "oh, no, I'm the guy who live tweeted the mission of getting Osama bin Laden."

Western journalists really go to his house, into the state, and he is accused of being alternately an agent of Al Qaeda or of the Pakistani intelligence forces.

It does not matter.

There is the shock and surprise that he had this unusual window into this highly secretive event. That is actually the way things work these days.

When this happened in 2011, the Pakistan and Internet penetration rate was at only four percent. about four percent of people use the Internet. Now it's up to forty percent.

I want to highlight a recent example.

There is a significant escalation between India and Pakistan. It looked like they might turn to a more general conflict. There had been a terror attack conducted by JTM militants based out of disputed territory in Kashmir, likely orchestrated by the Pakistanis who killed twenty-four Indian soldiers.

India retaliates with airstrikes over the line of control that has traditionally divided Kashmir. It was a big event. There was a lot of confusion and disinformation flying around.

India, which was also in the middle of a general election, claims they have struck JTM militant compound. The initial estimates are they killed 500 militants.

This seemed a little high, and there wasn't that much information to go on.

I had just joined the organization, and the guy who was investigating this was a 24-year-old Danish dude who liked military hardware and had no clue about Indian-Pakistan dynamics.

He just knew how to use the Internet to pick up pieces of information. He definitely did.

There were a few videos of the village that had supposedly been struck by the Indian airstrikes. He was able to take bits of those footages and, in images, clarify them a little bit to try to look for distinction landmarks and line those up with Google maps to GIS locate the reported compound.

Of course, Google maps does not update every day. But a private satellite provider does.

For $300, we purchased before and after satellite imagery of the area, and it's a very rudimentary battle damage assessment, and although we could not be 100 percent, we are still a little bit foggy; it did not look like an area that had held 500 militants who had all been cleared, killed.

We put out our findings.

There are a lot of Indians online and a lot of Indian cultural naturalists and nationalists. We quickly became ourselves a target of this information war, which invariably became part of the Indian general election. There were actually walk backs on the part of the military, and they said we are the ones who said it was the civilian government who said it.

In India, it quickly became an electoral issue, the Indian government pushed back, the Lisa posted video of the strike to Indian media.

That video turned out to be taken from a videogame.

Then, reportedly, Indian military had the clarifying satellite imagery and just was not going to share it. That is basically where they left it.

More recently, they have taken a new line of attack and are targeting these open-source intelligence analysts online through Twitter, trying to shut them up by saying they are a threat to national security.

Not only is this revolutionary in intelligence but it's fusing with general information warfare.

I want to talk about what these information warfare campaigns look like in the open. I want to start with the nonmilitary example. This was the Fire Festival. I would highly recommend it. If you haven't seen it, check out a documentary on Netflix or Hulu about it.

In short, two tech guys who had no experience in the music industry, no experience running a festival, decided to throw the biggest and most ambitious one in history. They wanted to be different, so they chose an island in the Bahamas that did not have electricity or running water.

Not a great start.

They also decided to start ticket pricing around $5000, which is a bit high for a music festival and also not a great start.

One could reasonably be skeptical if they will pull it off.

They understood the modern information environment.

With their seed money, they put no effort into planning the festival. Instead, they put together the coolest trailer that you would ever see for a music festival. They spent 3 million on this one-minute trailer. They fly in Instagram models around the country to party on a different Bahama Island.

They pay Kylie Jenner $50,000 to do one sponsored Instagram post regarding the festival. The Instagram post goes out to 100 million followers.

Quite quickly, the Fire Festival becomes the hottest festival ever.

Everybody wants a ticket, and they sell out and oversell and then there is a ton of people who show up to Florida and fly to the Bahamas expecting the experience of a lifetime. Expecting this.

The problem is planning is everything.

Just because we are selling a beautiful image doesn't mean it will come to fruition unless you put in a lot of hard work, which they did not do. These guys showed up to what was literally a humanitarian disaster.

The government helped evacuate the Americans, and the whole thing collapsed.

Lest you think that this was a shock, there were people on the ground in the Bahamas who were capturing this evidence the whole time saying, "Don't come here, this is not going to come together." This was a handful of interested citizens who had a Twitter, following of maybe 100 people.

You're up against Kylie Jenner. They had no chance at all.

This was another information battle.

I want to start shifting this more toward conflict.

I talked briefly about gang violence and its utilization of social media. Many of the things we see now in global warfare, where you could see the first hints of regarding King organization—when you think about gangs and criminals, they are basically a different form of political organization. Inhabited by almost exclusively testosterone-filled young men trying to show off.

We were early conversant users of social media technologies and integrated the seamlessly into gang culture. The man pictured here was Rochon Thomas who grew up on the South side of Chicago and was a talented musician and YouTube rapper.

He was a member of a local gang franchise of the Gangster Disciples and wanted everyone to know it.

He incorporated King life and symbolism into his music, and he became a major target of other gangs for assassinations. His rivals tried to kill him and missed the first time; the second time they also missed, but they killed a bystander.

If you survive two attempts on your life you might lay low a while. For Thomas, he saw this as content which he built into his songs which got more popular than ever. This life-and-death situation was also building his brand.

He kept going.

They got him on the third attempt, and Thomas died in 2015. His story did not end there.

A week later, in a totally different part of Chicago, miles away with different game dynamics, one high schooler shot and killed another one in an argument over his memory because they had disrespected him. Over time, he has become something of an icon with the microscopic bit of gang culture.

I really like this quote by two criminologists. We are studying social media use over a decade in Chicago and elsewhere. They say the street is no longer limited to the perceptual horizon of the person walking down it.

That means, if somebody fronts on you or disrespects you in social media, if the Internet personality is so intrinsic to your brand in existence, it is no different than if somebody is disrespecting you in real life.

This also has implications for international diplomacy.

If you think back to January 2018, we saw a brief but significant exhalation with North Korea. President Trump via Twitter initiated what was probably the most explicit threat of U.S. nuclear use in several decades.

Think about the dynamics at play here.

President Trump did not need to navigate a giant State Department bureaucracy who would whittle down what he was trying to say and repackage it in diplomatic speech. Instead, he could pick up his smart phone and type out exactly what he was thinking.

He would reach a rival world leader who would then respond in kind because Kim Jong-un is very good at the same sorts of bombastic type of declarations.

As we think about the ways that social media changes these narrative conflicts, we should understand that in the future even after President Trump, we are probably going to live in a world where world leaders can indicate directly, and where they are tempted and party to all the same passions and escalations as anyone who uses these platforms, that international politics will change accordingly.

I'm unfortunately going up to speed this up.

Another conflict example very recently conducted by my lab, examining the Turkish invasion of northeastern Syria and their attacks and fighting against the white PG. We see here a demonstration of the Turkish information campaign which is intended to seize a few hours of Twitter traffic but starts repackaging and representing the Kurdish fighters as terrorists.

This is an intrinsic part of warfare moving forward.

I want to talk briefly about these conflicts we can't see; the best entry point to that is the Russia stuff.

When we are doing the social medium ablation, it does not have to be a clear two-sided narrative content. We can pretend to be someone else and infiltrate these conversations and work through the shadows. My best way to approach this is to provide a little bit of context regarding how Russia saw these information operations against the US.

The starting point is the Green Revolution in Iran where a group of democracy protesters became a much larger group by organizing on Facebook and Twitter. In the West, this was a beautiful moment of social media stream realized.

For Iran and Russia and China and numerous other less open societies, this was an information attack by the West against a political system. Many nations began to think about how to weaponize the space accordingly.

Here we have an expert of the 2009 Russian National Security Strategy.

Events kept moving. There is the Arab spring in 2011. The tail end of the Arab spring, President Putin saw the most significant protests against his rule since he had come to power. This seems to be fermented by the United States and NATO, and attempted to change the Russian government.

More reflection, more concern and then, in 2014, the overthrow of a rush of friendly oligarchs in Ukraine replaced with a much more pro-Western democratic society.

As for Russia, this was essentially the last straw. They began to invest heavily in information manipulation capabilities. The important thing to emphasize here is at least the Russian doctrine and military articles.

This investment was seen as a preventive or preemptive measure to essentially use information to defang and neutralize a more powerful conventional adversary to try to forestall military conflict to use infiltration to paralyze a rival.

I get asked a lot, "Are the Russians Republicans and what's the deal here?"

He was just thinking about the most effective way to hold NATO and U.S. foreign policy.

They have to choose one person over the other.

Very briefly how this stuff worked, a few statistics that stand out to me over the course of this relatively minuscule investment cost may be $10 million in 100 full-time staff working on the stuff.

They managed to at least briefly reach 140 million Americans on Twitter more than the voting population on Facebook.

On Twitter, they ran Twitter accounts which were shared and rebroadcast by a number of individuals who are not administration officials who thought this is representative of unofficial GOP parties.

In some cases, Russians actually orchestrated protests and counter protests in the United States.

They are running both sides of Facebook pages: the other in support of Islamic cultural values.

They get these two groups of protesters to meet up across the street from each other trying, it seems, to incite some violence between them.

The folks doing this were not hard-boiled Russian intelligence agents. They were humanities majors who could not get jobs. Kids that grew up in Western culture and received in it love the U.S. and converse in English, but it was philosophy and political science grads.

Nowhere else was hiring.

What they were doing was essentially a different form of marketing ,and it's going to become prolific in political campaigns in the years to come.

How does this look like in practice?

Very briefly in 2016, a group of researchers were trying to map

Twitter conversations regarding the Black Lives Matter movement and incidents of unarmed black men shot by police officers.

They divided the number of Ttwitter accounts in the left-leaning and right-leaning quadrants.

The closer you are to the center of one of these networks, basically the more of a true believer you are, the more you are only interacting with people who think and feel like you do.

For a time, this sort of behavior leads to a gradual self-radicalization or polarization. These two groups move further and further apart.

In 2018, Twitter released a list of attributed Twitter accounts which had been operated by Russians and folks from the Russian trolls.

A method under this network.

If you will see roughly the center and the most polarized part of each of these networks is not American citizens but instead outside actors who actually have no party to American political processes but are just trying to pull in fragment society is much as possible. The end goal of this, as I said, is not to defeat the United States in any definitive way, but rather to tie it down. To hold in a place where it can't effectively use its own conventional instruments of force.

I will close reflecting briefly on how AI will change all this.

This is available now, Face After. You can play around with your own face and age it, if you want to look like an old person. This is all basic audiovisual manipulation. This is also a deep fake.

These are wholly generated faces by an algorithm. None of these people are real.

This is of great concern.

We are talking about social media and influence operations as one of the primary ways we detect false personas online is by seeing where they stole the photo from. Very soon it will no longer be a factor. Machines will be able to effectively masquerade as real people.

Stuff that has been the most worrying, here's a video of that an action.

This has not been as worrying, but it's a good illustration of a deep fake produced by the Chinese public facing broadcaster, which was basically a message to the West where they recorded this actress, but her movements right now were spontaneous and machine generated. She's not actually doing this.

If you can hear her, she has a pretty believable English language voice where she is delivering a script. That voice is entirely machine generated. It's a glimpse of what will soon be the new reality.

What has been most worrying is the stuff that looks a little bit less sexy. This is textural generation. The idea that soon—in fact this is a primary field research now. Machines will be able to read and consume massive amounts of text and begin to understand basic context and right responses accordingly.

What is pictured here is a recent paper published by a group of Chinese computer scientists who tested a new AI on a ton of ESPN stories.

We see here their program, Deep Calm, is just commenting on the story about the rockets and that the rockets will do a good job in the next season.

It is not crazy stuff, but it is another massively forward rethink about AI and how it interacts with machines.

Lastly, you can do this, too; there was just a public release of a neural network that conducts textural generation. What you see on the screen here, I just played around the software for this presentation, but what you see here is me posing a question to the machine in bold.

Everything you see after is what the machine wrote. This is entirely AI generated.

This first one is basically an introduction to a student paper; it's not that great but you can't tell that a machine wrote it. I tried it again, and we see a very different strategy.

This is what students do if they are out of time and trying to summarize the presentation. Again, not the most compelling stuff, but it's crazy to believe a machine wrote it.

I tried it one more time. This is the one I like the most because it really reads like a dispatch from a conference. What resonated with me was the last line that this AI decided to produce.

The Army is in no way prepared to meet the challenges of the future of warfare.

Their new course is a start. We still have a long way to go.

It seems to me like the new course is being set at this conference.

Thank you very much for having me.

[Applause]

Question & Answer

We have time for questions.

[Audience Member] How do consumers and leaders and organizations discern what is real and what is not?

What steps do you recommend so in the future they are reading a dispatch or picking up some information from somewhere, what are the signs and symbols and triggers that will cause you to suspect that maybe this is not correct and what to do about it?

[Emerson T. Brooking] Short-term, I think the cadets are the best equipped out of anyone in this room to deal with modern disinformation information manipulation.

Right after this became a big topic of public conversation, there was a big fear that it was going to be the next generation who will be overwhelmed by the stuff.

More studies now show folks over the age of sixty-five are significantly more vulnerable to what they read online because they are generally newer to these Internet platforms and have not grown up with them in the same way.

If you think about how young people consume information, they are much more likely to do so in a horizontal fashion. Instead of digging deep into one website or news source, they often skim shallowly across a range of sources. If there is an individual claim, it takes a quick Google search to see if it is echoed elsewhere.

By doing that you are basically doing a broad-based authentication across the whole information ecosystem. It is not foolproof, but that sort of thinking and checking alternative sources helps you avoid a lot of this obvious manipulation.

In the long term especially, this AI generated stuff—I think it's going to be indistinguishable from the real thing.

I don't think there is a way that we as human beings can make that distinction. The best we can do is develop AI that detect trace elements of machine manipulation. That is a big focus of the social media companies now because they're investing a lot of time.

I think we're going to see a future and there will be this realistic or entirely believable AI generated material that is then detected and pushed back by another AI. In essence, the future information battlefield is going to have two AI's and one on either side fighting a war that is essentially invisible to us.

[Audience Member] I'm going to be up all night. As someone who teaches an occasional course, we are already challenged with how to figure out plagiarism students doing this, and Turnitin does not necessarily capture all of them.

It sounded like you just talked about we are now training students to be my professional Intel analysts. The veracity of information first has to be clarified and verified before they ever use it as a source. At the university level how would you suggest we attack that?

[Emerson T. Brooking] One of the best ways to encourage information literacy and deep thinking regarding veracity of sources is to put students in the seat of being a disinformation actor.

Instead of presenting students with a list of recommended best practices, or even a list of facts which tend to be misrepresented, the exercise can regard whatever content. You put one student in charge of trying to deceive another student through a system of online tools. That one student is thinking how most creatively to effect the deception.

The other student is on guard against being deceived and assesses the material they are accessing much more critically.

Over time by teaching that adversarial relationship, I think you build a lot more thoughtfulness regarding how you approach the information environment. I should say adversarial training model is also how we train the AIs. The AI's detect machine forgeries are paired with an AI that is producing it.

We try to emulate the machines and come up with a more effective course of instruction.

[Audience Member] You mention the ISIS maybe in elation. I read about that young people from Morocco that posted real pictures and video are good way to fight against this manipulation enclosed areas to promote this kind of young people we are posting on Twitter and Facebook.

[Emerson T. Brooking] After ISIS held Mosul, it was telling. One of the first actions was to ban satellite dishes and Internet access.

They were conversant and good at manipulating online information environments, but they also understood that one of the greatest threats to their power was the production of counter propaganda that might have presented them in a less good light.

In fact, there were a handful of extremely brave residents in

Mosul to maintain twitter accounts and online posting profiles for the duration of the occupation.

The material that they put out was invaluable for the broader coalition and other civil society actors outside of Iraq to begin to contest that narrative battlefield which ISIS had initially dominated.

I do think one of the best things you can do when you're facing an adversary that is conversant with these tools in a closed information environment is to use resources to give access to the information environment to citizens within that area who might have a very different view of the occupier or government but who may not be empowered to speak freely.

That's it.

Thank you very much.

[See Appendix for corresponding PowerPoint presentation.]

13

Ethical Implications of AI on the Future Battlefield

As presented at the 2019 Civil-Military Symposium
Hosted by the Institute for Leadership and Strategic Studies
University of North Georgia

It is my honor to introduce the next panel. The theme is ethical implications of AI on the future battlefield.

It's a special honor to introduce our moderator Doctor Tony Pfaff.

Doctor Pfaff is the Research Professor for Strategy and the Military Professor for Ethics at the Strategic Studies Institute at the U.S. Army War College in Carlisle, Pennsylvania.

He is also Senior Nonresident Fellow at the Atlantic Council.

Doctor Pfaff has served on the National Security Council Staff in the State Department, in the Policy Planning Staff where he advised on cyber, regional military affairs, the Middle East, and Security Sector Assistance reform.

Prior to taking the State Department position, he served as the defense [inaudible] in Baghdad, the Chief of Military Affairs for U.S. Army Central Command and the Defense in Kuwait.

He served twice in Iraqi Freedom, once as the deputy j2 for the Joint Special Operations Task Force, and the Senior Military Advisor for the Civilian Police Assistance Training Team.

Doctor Pfaff has authored numerous articles on national security ethics, including on the acquisition of disruptive technologies.

He has a Bachelor's degree in philosophy and economics from Washington, a Master's degree in philosophy from Stanford

University, a Master's in National Resource Management from the Industrial College of the Armed Forces, and a Doctorate in philosophy from Georgetown University.

Doctor Pfaff?

[Tony Pfaff] Thanks everybody for sticking around.

We had a great conference so far, and we hope to end it on a high note.

It is my pleasure to introduce Lieutenant Colonel Chaplain Jacob Scott who is a chaplain in the Oregon National Guard as well as a pastor in the Lutheran Church in Missouri Senate.

He started off his military career as a combat engineer, saw combat on the ground in Iraq, and deployed to Afghanistan.

More relevant for our purposes, he is also a 2019 graduate of the U.S. Army War College where he did a strategic research project on the ethics of lethal atomic weapon systems.

Just to understand what kind of thing that is: that is a year-long investment where you take the expertise you have and dig into something strategic of importance to the Army with the resources available from the Army War College, as well as the expertise that the professors there are connected to.

I'm looking forward to this, and on that cheerful note you're on.

Iron Triangle of Painful Tradeoffs" and Responsible Decision-making with Respect to Lethal Autonomous Weapons Systems (LAWS)

Chaplain (Lieutenant Colonel) Jacob Scott

Thank you, Doctor Pfaff, for that introduction, and thank you, Doctor Wells and Doctor Hamilton, for the invitation to be here.

Doctor Hamilton, you cast a net broadly to get different perspectives. And a West Coast Lutheran pastor is probably about as far as you can get.

[laughter] I am a bit of an anomaly.

It's not my full-time job to think about defense issues, let alone the moral implications of AI or lethal autonomous weapons. I have been working on the complexities of these issues for a little over a year. Today my name tag says pastor.

I've been privileged to wear the uniform of our country for well over two decades. Both as a combatant and as a noncombatant.

I have been studying theology and, by extension, anthropology and ethics for more than fifteen years.

If you are wondering what a chaplain was doing at the Army War College in thinking about legal autonomous weapons or laws, I can't recall how many times I was asked that question. My standard response is to quote Ella Root who established the college not to support war but peace: "We preserve peace through strength in a morally responsible manner."

That debate is unquestionably important as it forces consideration of fundamental issues related to humane society and warfare. Where or if, and if so, how is it appropriate to take human life?

These questions are more important to AI and war than any dystopian fears of a runaway machine learning technology that might threaten the human race. To paraphrase St. Thomas Aquinas, the common good transcends material interests.

He suggested at the very end of his military career that demands that are technical skills be ordained to a good higher than simply victory. It is slightly out of context, but he was citing another philosopher.

Stanley Howard Wass at Duke University noted that the dominant form violence takes in modernity is speed. Stanley Howard Wass, if you know anything about him, is a pacifist born and raised in Texas. He says he wished he did not have to be a pacifist.

I am not a pacifist. I can't be even if I wish I could.

Autonomous weapons create tension for us who would serve honorably and virtuously in the profession of arms. Artificial intelligence will not only enable the national defense establishment in a myriad of support and efficiency applications, it will, undoubtedly, work its way to the tip of the spear.

It leads us to reflect critically on where we derive our moral strength, our identity and existential meaning, both individually and collectively. I will attempt to describe the tensions that are inherent in strategy formulation, specifically with regards to legal applications using a triple constraint construct.

Ethics, technological development, and strategy coherence.

The rapid development of AI technology and its application of the conduct of war both in autonomous weapons and enabling systems, creates a delicate balance between advancing technological developments and ethical principles in strategy formulation.

It is a healthy tension between ethics, weapons, development, and strategy because this tension creates the space for men and women to act responsibly in a field where the stakes are very high.

Even one life, from various perspectives, has an estimated worth.

Consider debates over capital punishment.

It's worthwhile to consider the propriety of loss before life is ever in the crosshairs, regardless of who or what is behind the optics.

Early in the Cold War, then Chief of Staff of the Army General Omar Bradley feared that "our knowledge of science has clearly outstripped our capacity to control it."

Are we there yet?

I don't believe so.

As Tom is showing, his suggested nearly seventy-five years without nuclear war demonstrates that some measure of stability is possible.

I do believe that the United States is at an inflection point in the world regarding AI and laws.

That is analogous to the advent of nuclear weapons prior to 1945. Because, before the decision was ever made to employ them, we committed to develop nuclear weapons even as serious moral and ethical concerns lingered. What would these weapons do if and when they were unleashed?

Today, just as then, strategic leaders face decisions that are both thrilling and terrifying in their potential impact.

Just as nuclear weapons still generate moral concerns in their development modernization procurements and strategy, there is serious debate over the development and employment of laws. Focus on the legal applications, even though their applications are for nonlethal weapons and their effects as well.

In order to contribute to the conversation over the propriety of AI applications and laws in particular, each of us has to have a firm grasp on the source of our moral strength individually and/or collective strength as a nation so that we can act with confidence and courage in our vocations. We have to consider if and when ethical principles that guide policy might or might not change that policy.

Many, however, see the moral underpinnings of the military profession as timeless.

When I was a second lieutenant studying and training in the art and science of minefield and placement, I didn't reflect on the morality of the systems that I was employing.

I only reflected very briefly on the morality of war in general.

In retrospect I was confronted by the immense destructive power that was placed in the hands of a group of eighteen- to twenty-five-year-olds, trusting that our political and military leaders created a space for us to do our jobs honorably.

Now, as a chaplain and a *Seelsorger*—that's the German word for pastor that means literally one who cares for souls. I have a great deal of sympathy for our warriors and our emerging military leaders. I personally do not believe that machines threaten what it means to be human, even if they pose a very real threat to human flourishing.

I think trans-humanism and soldier enhancement is another question entirely.

When we reflect on what war is, on the nature of war and the changing character of it, I don't want to instill doubt but to build resiliency in a completely complex location.

[Inaudible] . . . one socially sanctioned violence to achieve a political purpose or, to quote Clausewitz, were as an extension of policy. Laws introduce, as a part of the sociopolitical aspect of humans, interaction and war.

War is a breakdown in the relationship between states and groups of people, even nonstate actors that have become violent.

Real people die, usually both friend and foe.

Political decisions, whether or not to wage war, place blood and treasure at risk. A just cause to go to war, right conduct in war, and care for the men and women in the profession of arms, require a great deal of empathy.

Even empathy for our enemies, as we consider our conduct and what are weapons and the means we employ due to our adversaries.

The law of armed conflict reflects greatly on the effects of what we do and how that affects real people, even our enemies. It is a good question; we ask how far should humans be removed from the decisive act of taking a life.

Currently, the Department of Defense does not authorize the use of laws against human targets. The DOD specifies autonomous and semi-autonomous weapons systems have to remain under human control given our present capabilities for autonomous systems and the need for those who employ them to trust in the system that they use as both commanders and operators; humans remain in the loop.

Yet, some of the concepts being discussed only very loosely keep a human in the loop.

The rapidly-evolving threat with respect to AI and laws, however, will force the U.S. to reconsider these policies, possibly before we fully trust the machines or risk lives in mission success in the face of being overmatched.

Pragmatic arguments like that can, and I would say should, leave us unsettled. People are naturally and appropriately uncomfortable killing other people. Even for a justifiable reason.

Izumi. . . [inaudible] . . . the high presented for disarmament affairs for the United Nations on conventional weapons asserted that laws "pose ethical and moral quandaries."

Are we comfortable with outsourcing life and death decisions to machines, and what does that say about the value we place on the sanctity of human life?

What does it mean to be human?

Do legal autonomous weapons threaten that?

Without delving too far into my approach to the question, there is concern that crosses a moral threshold if we allow machines to independently target and kill humans. Not simply because those machines are not yet trustworthy enough to be unleashed on the battlefield.

The triple constraint triangle describes the decision space for strategy formulation with respect to these weapons. Triple constraint, also known as the iron triangle of painful trade-offs, comes from the project management triangle of scope, time, and cost.

An actor can optimize any of these three without trade-offs. These factors compete for priority, creating an unresolvable tension. You can't achieve optimum value for all three constraints, and there are limits, and privileging one or two at the expense of the others assumes risk.

Proposed law, triple constraint includes three factors. Technological advancement, strategy coherence, or the ends or means or ways of understanding of risk and ethics.

What is right behavior?

Strategic decision-makers operate in this space defined by the limits of morality and ethics with available and emerging technology and strategy that is formulated by those same decision-makers to achieve specified goals.

This is not new.

Military leaders have wrestled with the use of various types of weapons in their employment throughout history. From the crossbow to Aerial compartment. Even snipers, landmines, and other weapons cause moral reflection in their own right.

Consider, again, nuclear weapons which the United States developed while addressing the significant moral concerns that they raised in view of the present threat and ultimately decided to employ them. A decision that is still the subject of debate.

But as Bernard Brodie observed in the classic book *From Crossbow to H-bomb*, the objections of some never slow the development of increasingly lethal weapons of war.

The Department of Defense agency that is responsible for developing new capabilities and technologies, the Defense Advanced Research Projects Agency, notes that the nation is best served if we push critical frontiers ahead of our adversaries. Hence, the important work that the Defense Innovation Board has done to development schools for the use of AI by the DOD.

That assumption that we need to develop principles for moral and ethical decisions uses an acceptance of the triple constraint between the technological development and strategy coherence. I believe ethical or existing ethical principles and accepted legal restrictions of the just prosecution of war are sufficient to guide morally responsible conduct regarding legal autonomous weapons systems.

Therefore, the capability to responsibly and ethically develop and procure laws should not be categorically restricted.

At the same time, I'm grateful for dissenting voices that stimulate critical reflection on the distance and direction of technological development of weapons systems that are enhanced and enabled by artificial intelligence.

In like manner, it will be important to continue to involve leaders and thinkers from various disciplines both inside and outside the national security establishment.

We must always train military leaders who can think critically and creatively about complex problems for which there are no good answers.

Even if fully autonomous learning machines are not currently capable of effective battlefield employment and current capabilities and governing policies do not permit the employment of legal autonomous weapons, strategic leaders in the national security establishment must consider their eventual development and use in order to continually take morally-responsible actions in the present.

This iron triangle helps leaders understand the ethical intentions and associated trade-offs as the technology continues to rapidly evolve and our national security strategy is reassessed.

Meanwhile the study of history, philosophy, and religion to complement training in the art and science of warfare will form adaptable and ethical leaders of sound moral character for a rapidly-changing security environment, or to quote the ancient King Solomon, "There is nothing new under the sun."

Even if timeless challenges are new to us in our generation.

There may come a day when an ethically-sound choice would be to employ occlusal autonomous weapons.

Much more could be discussed and studied with regards to the concepts of nuclear deterrence, escalation, and stalemate. It was Thomas Schelling who pointed out that the words terror and deterrence have the same Latin root.

The last time that Sir Winston Churchill spoke to the British Parliament early in the 1950s, he said it may well be that we show by a process of supplying iron we've reached a stage in the story where safety will be the sturdy child of terror and survival twin brother of annihilation.

All of that being said, I am a military chaplain and civilian clergy, and I trade in the currency of hope.

I have an abundant supply of temporal and ultimate hope, and it's not merely naïve optimism.

My understanding of the way the world is in the way the world ought to be looking forward to a brighter future.

Today, as I stand here, I am grateful for all of you at the various stages of your public service. There are centuries of public service in this room and centuries of public service to come.

You all, and especially our cadets, give me hope.

My prayer for you is that you continue to grow and to learn and serve and teach and coach and mentor America's sons and daughters today and tomorrow.

That you are empowered to do your vocations and to live faithfully in them confidently.

Thank you.

[applause]

The Ethics of Acquiring Disruptive Technology

Colonel Tony Pfaff, Ph.D.

General Dunlap in his presentation correctly admonished us to be careful about regulating something we don't understand. What

I want to talk about, I will widen the aperture a bit.

I will not talk about AI directly. I want to talk about disruptive technologies in general. Particularly because it's not just about AI anymore. It's about a lot of different technologies and how they come together to create the concerns we have.

I'm going to ask the question, how do we regulate something because we don't understand?

I saw Boris Johnson's UN General Assembly speech last month. It was great.

At the end of the speech, he warns of a dystopian future of digital authoritarianism, the practical elimination of privacy, and, my favorite part, terrifying limbless chickens, which is a great name for a band.

I will learn to play an instrument so I can have that band.

Among other possible horrors, he specifically highlighted artificial intelligence, human enhancement, and cyber technologies as a cause for concern to bring about possible dire global consequences.

While the speech was kind of weird, I think he captured the concern about technological innovation and change. It is not just proceeding at a rapid pace but rather combining in ways that are difficult to control. While such a loss of control can be unnerving, when it is applied to military technologies it can be downright frightening.

The right answer is not to walk away.

As we talked about several times in the conference, our adversaries are developing these technologies too. To walk away represents its own kind of moral failure.

Let's take three examples here. I think everybody is familiar who the rebels are in Yemen. Their use of unmanned vehicles not just to attack the Saudi oill refinery.

Also something I don't think a lot of people know about is the Iranian government, Iranian hackers, created a massive power outage in Turkey and Istanbul, putting 40 million people without power. Because Turkey was supportive of Saudi operations.

The other thing along the line of human enhancement is another group which suppress fear and builds endurance and allows them to punch well above their weight when fighting larger organized forces.

What I want to do, and moving ahead on this, I'm going to talk a little about what disruptive technologies are. What is the problem with this disruption? What makes it morally problematic? And I'll talk about a possible way ahead.

One thing that is important to realize about these technologies is that none of them are very new. None of them are very advanced. A lot of them are available commercially in some form, despite the fact the targets of these attacks that I talked about were caught by surprise.

Moreover, despite the fact these technologies have been around a while, as we've talked about in the last several presentations, we don't really have a good defense for it.

As Rudy Multi observes, technological changes also often a subversive process of established social roles, relationships, and values. That poses a number of problems for us.

Let's talk about what a disruptive technology is.

The key is not how advanced they are, but the attributes that they bring. What is common to disruptive technologies are the novelty of the attributes they introduce and how useful those attributes are to at least a subset of the user community. The extent they meet user requirements well enough and incorporate attributes, other users find attractive.

They can displace technology over time, even if they do not perform as well.

A good example of this: in one of the early studies on disruptive technologies in the field of economics, a guy named Clayton Christensen talked about the hard drive industry. In the beginning, hard drives are big because they maximize speed and memory. Somebody got the idea they were going to make a small one. Small ones were slower and had less memory.

They were portable.

With that attribute, the home computer market was born.

Now you have computers we can move around and put on our desks and so on.

Within a few years of the innovation, all of the companies that were still making the big hard drives and not making small ones were out of business.

That is how disruptive technologies work.

The question you have to ask is, so what? What is the ethical problem with that? The fact that the companies went out of business doesn't pose a moral problem. How do we get there?

Whatever your ethical commitments are, ethical analysis has a certain kind of logic. It begins with the possibility of moral behavior which requires morally autonomous agents. When these agents act, they have to consider how their acts affect others and conform to the moral principle. Because ethics is regarding justice that they should consider.

They should also consider how such conditions promote moral behavior and good character, which includes accounting for physical and mental well-being and not just of the individual but the society they live in as well.

It's not hard to see, based on conversations we have had this week, how these technologies raise those kind of concerns.

Moral autonomy: we have already talked about the concern regarding accountability and the accountability gap that they can raise. The problem I highlight here is a conventional technology or noncognitive ties technology when something goes wrong.

In principle, at least I can attribute that fault to the operator, manufacturer designer, or some human. Either through bad intent or negligence.

The problem with AI is that you can have the harms arise even when everybody is doing a job well done. That introduces the accountability gap, since it may be more harm to which no one can assign moral fault.

AI enhancements also lead to a similar concern.

Imagine an enhancement frequently in military contracts. Imagine enhancement that proves survivability for the soldier but comes with long-term side effects.

Depending on how much survivability one gets out of it, and depending on the severity and probability of the side effects, you can be in a situation where you're forcing the soldier to choose between short-term survival and long-term pain. Which is kind of like giving someone an offer they cannot refuse, which is coercive.

As an example, the Germans in World War II provided the soldiers and airmen with a drug called Provident, which is like crystal meth. They are very transparent with the soldiers about side effects. They try to regulate the doses so they would minimize side effects.

There's a great quote from a German bomber pilot who said, "Why do I care about the side effects when the Brits are going to shoot me down any minute."

He continued to take it.

What was the outcome?

One good vignette is, on the Eastern front, a unit of well-trained SS troops ended up surrendering to Russian conscripts because they had been on meth so long and they were so jittery they had fired all of the ammunition at the response to little noises in the night. When they finally encountered Russian forces, or Russian forces encountered them, they had no more ammunition left.

Treating others' moral injustice depends on how we are affected.

When I want to fill in what that means, I'm really asking here is that we commit the idea that we owe something to other persons, and we will call that respect.

We can talk about what that means, but following the philosopher John Rawls from the perspective of public policy, what that means is acting justly by disturbing social goods.

I think in the military context, we are primarily talking about risk and reward, both soldiers and civilians.

Here is where we can raise some concerns about justice.

We already talked about the fact that any technology that distances soldiers from the violence they do or decreases harm to civilians lowers the political risk associated with using that technology.

As someone said earlier, that's not necessarily a bad thing, but it can become a bad thing if it incentivizes disregarding more costly, but not violent alternatives, which can put you at possibly violating the use of bellum condition of a last resort.

As Christian Mark argues, political leaders prospecting the cause of death might accordingly feel less anxious about using force to solve political problems.

While regarding well-being, this takes into account not only the physical safety and health of individuals affected but also mental health and quality of life concerns.

AI enhancements are the only technologies that raise those kinds of concerns.

A lot of risks in technologies have been associated with the desensitization of operators.

In 2017, a study confirms the number of mental trauma, including moral disengagement, as well as intensified feelings of guilt resulting from riskless killing by UAV operators, making the matter more complex. A 2019 study of a British UAV operator said the real culprit was environmental factors associated with employing the technology, such as work hours and shift patterns, which are more important than the expense of mental injury and the dramatic events associated with the strikes they did.

Regarding social disruption, we can break that down into two components. One is the simple relationship. As the technologies reduce risk, the distribution of how the society views military service will change. That is not necessarily a bad thing, but it is something to be prepared for. Also, it can alter how society rewards military service and who serves.

We are all familiar with cyber command and reconsidering the standards for recruiting it needs to have. It's already offered direct commissioning to certain STEM majors, something previously reserved for the medical, legal, and religious fields.

The second concern is, of course, the transfer of technology or its effective civil society. That is not always a bad thing. Missile technologies for military use, for example, pave the way for space exploration.

Not all transfers of military innovation are always helpful. We talked about it earlier yesterday; we had a presentation where they raise the concern of human enhancements. For military purposes, making their way to civil society whether because of soldiers returning to civilian roles or technology itself moves in. We have already seen that happen before.

In World War I, the British mixed cocaine with rum to make it easier to go over the top. Other armies used cocaine to improve endurance and suppress fear.

What happened was at the end of World War I, they had a massive cocaine epidemic all over Europe because of addicted soldiers returning home, which caused a lot of disruption to those particular societies.

Even when beneficial, there is a downside to military research because sometimes it distorts priorities and directs technology development in a way that reduces efficiency of civilian applications.

For example, the U.S. Navy's dominant war and nuclear reactors led to designs that were less efficient and came to greater risks. The least for civilian purposes. To the extent that the effects of these technologies have the kinds of impacts on the conditions I just described.

I think, then, you have to ask, is it permissible to perceive developing these technologies?

I get it, we have already talked about how development of these technologies is probably inevitable. They still have to ask the question about how we go about doing it so we can align the development better with our moral commitments.

I'm going to suggest three conditions. Moral effect, necessity, and proportionality need to be considered. Moral effect refers to the potential that employing technology has four conforming or violating moral norms.

There are, of course, rules in place to govern this.

International law prohibits the development and acquisition of new technologies that cause unnecessary suffering of an indiscriminate nature or cause widespread long-term and severe damage to the environment or modify the environment in a way that the effects would otherwise be prohibited.

It only gets us halfway there because design covers obligations to others or external obligations to the enemy or adversaries or others in general.

Here again, I invoke respect for persons who say that line with this imperative means that the government military commander should avoid deceptive and coercive policies when it comes to acquiring these new technologies.

Having said that, respecting someone does not always entail taking into account individual preference. But taking on a particular role, soldiers have agreed to take on certain risks. Taking on these new technologies will require us to reconsider what kind of things soldiers legitimately consent to by agreeing to serve.

Albert Einstein once said, growing up I made one mistake in my life. When I signed the letter to President Roosevelt saying the Atom Bomb should be made.

The danger that the Germans would make them was the justification.

What I think is interesting about the statement is Einstein says his support for developing the atomic bomb was not for military advantage, not that it would hasten the end of the war and stabilize it, but because failure to have one would put allies at a disadvantage. When you're developing disruptive technologies, it is not enough to just seek an advantage; you also have to avoid the disadvantage.

Based on the risk that these things pose, regarding proportionality and talking about proportionality relative to the disruption technologies can cause, can be difficult in practice.

To do so, one first needs to determine how they weigh against each other. In the context of national security to find that victory as goods. An implication of goods as harms. They specify additional goods as harms, which includes human lives and the environment.

For the analysis we have done today, I would also suggest autonomy, justice, well-being, and social stability are also goods.

It's not meant to be exhaustive, but it provides a starting point for moving ahead and analyzing whether or not something is proportional or not.

Even with this in mind, such comparisons are hardly straightforward. Michael Waltzer makes the point that "Proportionality turns out to be a hard criteria to apply, but there is no ready way to establish an independent or stable view of the values against which the destruction of war is to be measured."

Even in conventional situations it's not always clear how many noncombatant lives are worth any particular military objective.

The context of disruptive technologies is less clear; how much increased military effectiveness or deterrence is how much injustice or social disruption.

These really are questions noone can really answer.

Fortunately, one does not have to.

If one conceives of proportionality as a limit on action rather than a permission, what matters isn't what's proportionate, but what is disproportionate.

For example, it would be disproportionate to threaten divorce over an argument about what to have for dinner. I can say that without having to commit would be proportionate reasons for getting a divorce.

It works the same way in the military context.

Nor does it mean marginal cases are [inaudible] and possible.

Go back to the Iranian hackers creating the power outage in Turkey. 41 million Turks.

Since the Turkish government's criticism did not have a similar effect on Iranian civil life, I would think arguably intentionally imposing a massive blackout would count as disproportionate, even if there were no equally effective alternatives to the irradiance.

Of course, when doing proportionality in the context of disruptive technologies, it's not enough to account for intended as well as unintended but foreseen consequences.

Disruptive technologies require us to take into account unforeseen and unintended consequences as well.

I know that sounds silly. How can you take into account unforeseen consequences since they are unforeseen? Given that, one can be faulted for taking into account one's imagination that may fail and not all the disruptive effects considered.

What that point suggests is that proportionality requires actors to consider how to manage the proliferation and evolution of the technology in advance as they are developing it. Not because they have an idea of what the effects will be, but because they don't.

We may not know how these technologies will affect autonomy, well-being, justice, and social stability, but they could also suggest you identify further measures for shaping development.

I will conclude with some suggested measures.

I will read them to you, but basically to summarize, I talk about things like privatizing consent and thinking about the consequences and concerns on the outside of development. Paying attention to the distribution of reward and risk. Managing the transfer and proliferation of the technology at the onset. Designing those technologies with that kind of concern in mind. And assessing the way ahead in terms of the alternatives you have to developing that technology.

I think that puts us in a better position to handle the policy problems we talked about today and yesterday that these technologies will produce.

On that cheerful note, we are done.

Question & Answer

[Audience Member] When it comes to any autonomous system in cyberspace about a field or whatever else, I'd like to hear your thoughts on the ethics of a kill switch if you will.

The ability to disable and destroy any ad we put out, whether it's denying the use or preventing misuse or perhaps a system will function.

[Jacob Scott] I think Doctor Pfaff just talked about being able to deal with the potential that affects; even if that is unforeseen and unintended, something like a kill switch gives you that ability.

That's a good thing to pursue with any kind of weapons technology, the ability to bring it back once it is unleashed.

That's the fundamental problem with the treaties we have signed because there is no ability to pull that back if you just leave it and forget about it.

I agree and think that is important to consider with any development.

[Audience Member] A couple of things—mine has a battery and if the battery runs out—the kill switch isn't the problem with the kill switch that might be compromised immunity.

For you, Tony, I see that you have mentioned efforts to ban technologies.

Isn't the problem with doing that is you can only capture the technology in a snapshot of time?

Other later developments may change with that conclusion while we're still stuck with the band, for example; with blinding lasers you can incinerate somebody lawfully, you can't design a weapon intended just to point them.

If you look at the ICRC site, say it's better to be dead than blind. That's in essence what they say. That is hard to morally justify. Now, we have technologies that enable people to see.

I think you get the point and concern about disruptive technologies.

Rather than emphasizing the basic law and applying it across the board and try to pick out a technology and ban it, I think it is problematic.

[Tony Pfaff] That is a great point.

One of the things I did not get into because of time is what that is really about: is when are we morally permitted to develop something that would be on the base even itself? The answer should be never.

I agree with you.

Not always.

The example and precedent that I think is interesting, in 1864, the Russians developed soft shells. They were designed to be used against logistics wagons. The minister correctly discerned if they are used against people, they are soft and can explode and cause a lot of unnecessary suffering.

Rather than developing and feeling these weapons together, everybody in 1868 in St. Petersburg got them to agree to abandon these weapons and systems, limiting the size and caliber of the soft shells that would be fielded under the principal of not committing unnecessary suffering.

I thought that was an interesting precedent and suggest that sometimes might actually be because the bad guys are going to do it and because of the effects you just described, might have permission to develop otherwise prohibited technologies.

My point there is you have to develop it with getting the band in mind, the way the Russians came across that kind of accidentally.

Have to develop the beginning with the band in mind and build consensus on their use.

It would be perfect, but then you have it available for a deterrent.

Chemical weapons are another good example. We did not use chemical weapons in World War II on the Germans, despite the fact they lost in using chemical weapons in World War II.

One of the reasons I think people understand the case is, there are two large ships sitting in a port in France filled with chemical weapons, and we let them know if you use them, we have plenty and we will use them back.

They never got used.

We talked earlier about reciprocity. This is how you set the stage for it.

The point here is sometimes their submissions continue to develop these kinds of technologies, even though they are otherwise prohibited.

These conditions have to apply.

[Audience Member] I have two questions.

The first, we talked about introducing a lot of wide-ranging AI solutions.

Being a former Director of Training for the infantry for four years, the real question is how do I train it? How do I sustain it? How do I take the technology and make it work in the field on a consistent performance basis? That is the first challenge.

If I build a missile, I can't fire that every day.

If they build a trading system that goes with it, that is almost more expensive in the beginning because I have to use it over and over again.

That is part one.

This is back to the general's question that we had earlier.

Increasingly, we are fighting as advisors to other countries, having spent a long time fighting both as mercenaries, and in transition, we have a whole set of codes and ethics that are so different to understand.

You have to be really careful in how you really work with that.

Without soldiers that will go in and support training and help armies, this whole thing about ethics is going to become proportionately more challenging.

Not that we did not make good decisions; we did, and we stopped a lot of things from happening, but we had to explain why we were doing it.

Your thoughts on this?

[Pfaff or Scott] It's a great question.

It came up in an earlier panel.

I would say two things to that.

One is looking cross culturally at ethics; often I find while they may seem different, what really is the difference is who would applies to more than what the differences are.

We tend to have rules for showing each other respect. Fairness and kindness and all those things we might consider ethical behavior. They don't always extend to the people in that society.

Even when you don't have that or have the difference in ethics, we are the ones providing the ethics, it's our ethics that matter.

We have to go back to the American people and say we did this. We are not asking for the other society to fully accept our way of life or all our ethical norms. We are not asking to accept much more than what's in international law: discrimination, proportionality, and not committing unnecessary suffering.

I think the way to proceed is to be very clear with what ethical commitments you're requiring them to make. If they are not willing to make that, they either have to reconsider how you are supporting them or reconsider whether you are supporting them.

[Audience Member] Questions related to training devices and how we will address that.

That's equally as challenging with some of the things you want to put out there.

[Pfaff or Scott] I think we build that into any weapons development.

To use the missile example, we would not field the system like that until we could trust the system, and a big part of that is not just training the operators or soldiers that would employ the systems but also making sure the equipment and machine itself is reliable and trustworthy and performs with the defense innovation award and the principles they worked to establish in the DOD directive from 2012, that we want to use systems to behave the way we want them to.

You have to have that stuff in place as you field it.

If we didn't, our missiles would've missed more often than they did.

[Audience Member] Is the unique problem with AI, especially AI learning machines, is the device different each time you use it?

In other words, it has different characteristics based on what it has learned.

That is why I think DOD is focusing as we saw in ethics on narrow AI. In other words, where it can only learn up to a certain point.

Eventually you're facing adversaries that have a more generous assessment, but another aspect, if that is explainable AI.

Maybe doing things in coming to those conclusions that don't fit with what you actually wanted to do.

[Pfaff or Scott] I would agree.

In another article I wrote, I talk about explain ability being a moral requirement and not just practical and ethical, precisely because of the kind of simple decisions.

That's another thing with AI; we're not just talking about targeting systems, we're talking about decisions and support systems as well.

We have a logistics system that gives the ammunition in the wrong place and people are going to die. We may not be violating international law in getting people killed, and that's bad.

Interactive division support system that picked convoy routes and told you to avoid the ones where there was a lot of enemy activity and go on the ones where there wasn't.

One day, throughout generators put out a particular route.

The convoy went on it, and they got annihilated. A massive attack with lots of casualties. What happened was because nobody was going on that route, there was no data regarding attacks on that route.

Over time the machine thought it was the best route.

This is a simple example of when our human operators did not know to check that output of the machines.

The challenge is going to get harder for all the reasons you just said.

These machines change at every iteration.

[Audience Member] I want to bring this back down to the ground.

We had a great first two philosophical discussions.

The focus of the conference is on pre-commission education and preparing our lieutenants for the battlefields.

Here is my concern mission first, people always.

If you give me a tool, I will use it.

How do we prepare these young people to deal with these ethical situations?

Can't give them a long, philosophical answer.

You've got to embed it in their training, and you have got to select the right people to be those lieutenants.

I am just not sure.

I like your opinion particularly because you are a rucksack chaplain.

And Tony is absolutely distinguished in terms of thinking through the stuff.

[Audience Member] I think we have touched on some of those things earlier, not just ethical situations but where people have to reason through those types of scenarios and not just putting a tool in their hands and saying have added.

I recall a friend in Baghdad in 2004, there was a company commander who dismounted his 50 calibers from his contracts because he knew the collateral damage in the area he operated every day would be too great.

Giving our cadets and emerging leaders situations where they think through that and giving them the ethical and moral tools by philosophical, religious education, history, and keeping those historical examples.

Like a college in West Point highlighted yesterday, when they read through Washington's Crossing and work those scenarios into other aspects of their curriculum, those types of things are important.

Not just giving them a tool in seeing "this is how you use it," but talking about when and why.

[Pfaff or Jacob] It's a great question; my first response is if you don't want philosophical conversation, he probably should not hire a philosopher.

We just can't help ourselves.

It is inevitable.

Just like AI.

Here would be my response.

And taking care of them I have got two audiences.

My first audience is guys like you because I want you to be able, through your experience, to understand ethical concerns that we are talking about.

How they all fit together and are integrated into the training they received.

I want you guys to hear this because I want you thinking about this right now.

I'm not asking you to look at this as a checklist, but these are things you should raise.

Ethics is more about the reasons we give and take for justifying behavior we have.

You better get good at that and you have to start doing that now because you will always have a clear-cut answer.

As you said, you got to give your troops the reasons.

If you have ethical challenges, you better get good at giving those reasons in a compelling and justified way.

What is interesting about the crossbow we're talking about being morally problematic is it helped with the evolution of just warfaring.

Before, warfare was governed by chivalry, which is much more about personal honor and the kind of humanitarian concerns that motivated "just work" tradition over time.

That is why disruption is not necessarily something to fear but something to manage.

[Audience Member] We are at the end of our symposium here and there are three things we want to do to wrap things up.

I'm going to invite Doctor Pfaff to come up as a representative of the strategic studies Institute at the Army War College, our partner in the symposium to wrap things up.

Doctor Pfaff, it's all yours.

[Tony Pfaff] I have already given my concluding remarks, because I've done my best already to summarize what I think we got out of it and engage the material we talked about before.

What I hope everybody got out of this conference, you guys in particular, is a good understanding of what AI is, the kinds of things it can do, especially the legal and ethical and practical challenges with employing it in an effective but just manner.

This will be important to all of us here in whatever role we play in the future.

I would be remiss if I did not conclude with thanking the wonderful folks at the University of North Georgia for hosting another great conference where they were able to bring together some outstanding speakers who engaged in thought-provoking conversations and gave us a lot to lose sleep over tonight.

A round of applause for the University of North Georgia folks for putting on a great conference.

Safe travels to wherever you go.

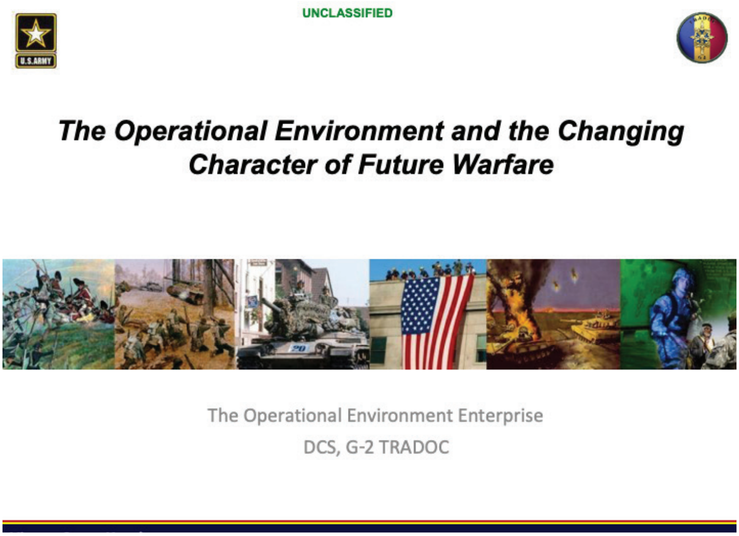
If it was up to me, we are done.

[See Appendix for corresponding PowerPoint presentations.]

Appendix

The Future Operational Environment

Chief Warrant Officer Jerry Leverich

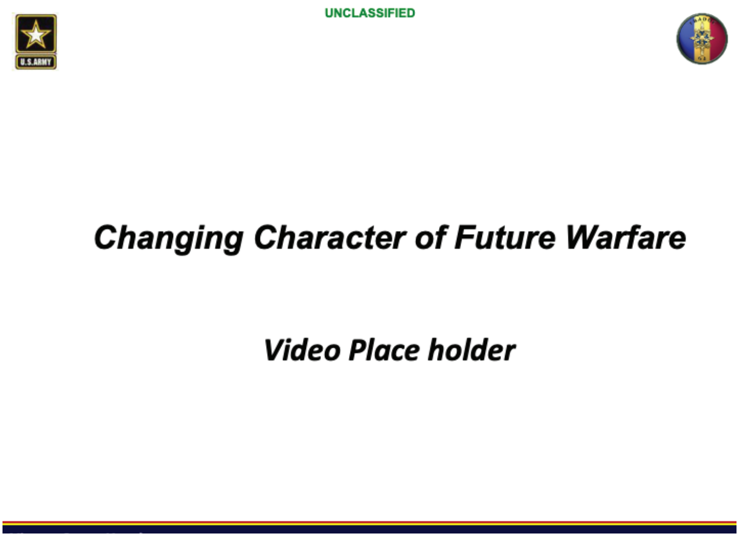


UNCLASSIFIED

The Operational Environment and the Changing Character of Future Warfare

The Operational Environment Enterprise

DCS, G-2 TRADOC



UNCLASSIFIED

Changing Character of Future Warfare

Video Place holder

UNCLASSIFIED

The Operational Environment

Threat Considerations

- Electronic Warfare
- Integrated Air Defense
- Counter Space & PNT
- Cyber & Social Media
- Recon-Info-Strike Complex
- Extensive use of UAVs
- Massed Artillery & Forces
- Protection
- Proxies
- Deception & Ambiguity
- CBRNE/WMD

OE Characteristics

Populations & complex terrain

Proliferation of WMD

Potential for overmatch

Speed of human interaction

Contested in all domains

2+3 Threats

Near Peer Competitors

Regional Actor (Nuclear)

Regional Actor (Non–Nuclear)

Radical Ideologue

Potential for Conventional Overmatch

Electronic Warfare

Cyber & Space

Fighting Vehicles

Air Defense

MRLS & Rockets

Artillery

Fundamental Changes

Laser Weapons

Synthetic Bio

RF Weapons

Internet of Things

Energetics

Power

EDKEW(Rail Guns)

UNCLASSIFIED

Unpacking the Potential for Overmatch

Current & Emerging

(through 2025)

Cannon / Rocket Artillery

The Battle of Agincourt

Missiles

Robotics / UAV

Shape Charges

Active Protection

IADS & Manpads

Computing / Big Data

Armor (anti armor)

C3 / Deception

Future

(2025 - 2050)

Pearl Harbor

Siege of Yorktown

Contested over Time

Laser Weapons

Chem / Bio Weapons

EDKEW (rail guns)

RF Weapons

Cyber

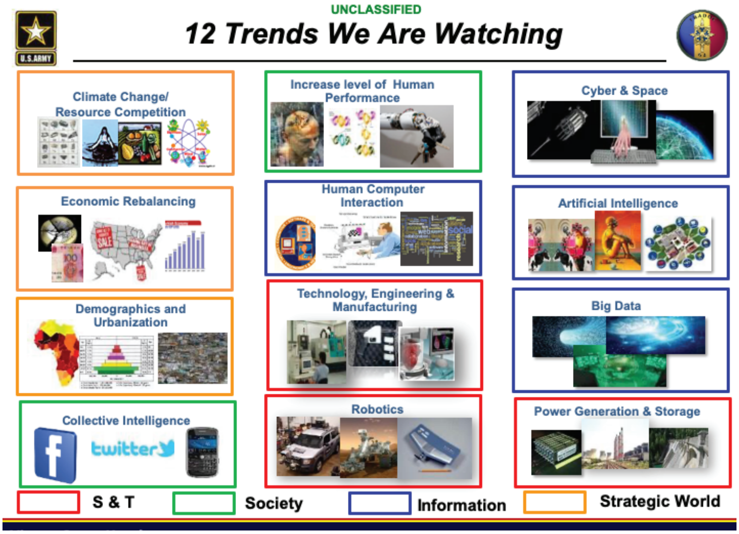
Internet of Things

Synthetic Bio

Space

Power

Energetics



UNCLASSIFIED

12 Trends We Are Watching

Climate Change/ Resource Competition

Economic Rebalancing

Demographics and Urbanization

Collective Intelligence

Increase level of Human Performance

Human Computer Interaction

Technology, Engineering & Manufacturing

Robotics

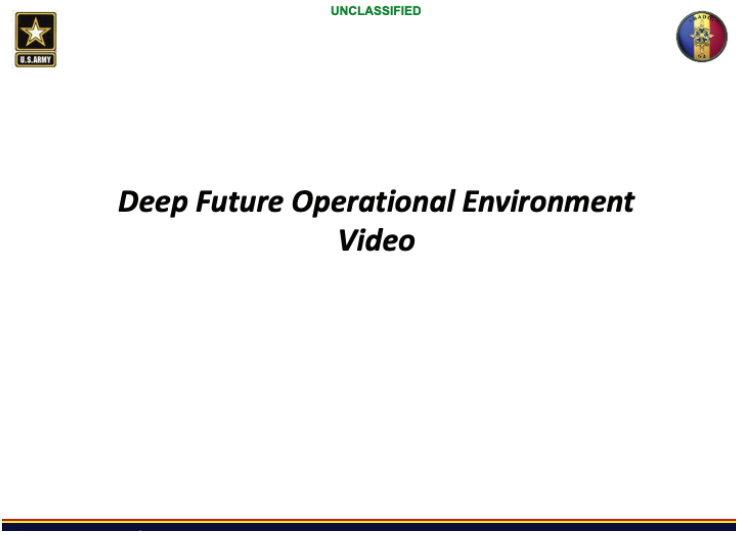
Cyber & Space

Artificial Intelligence

Big Data

Power Generation & Storage

🟥 S & T 🟩 Society 🟦 Information 🟧 Strategic World

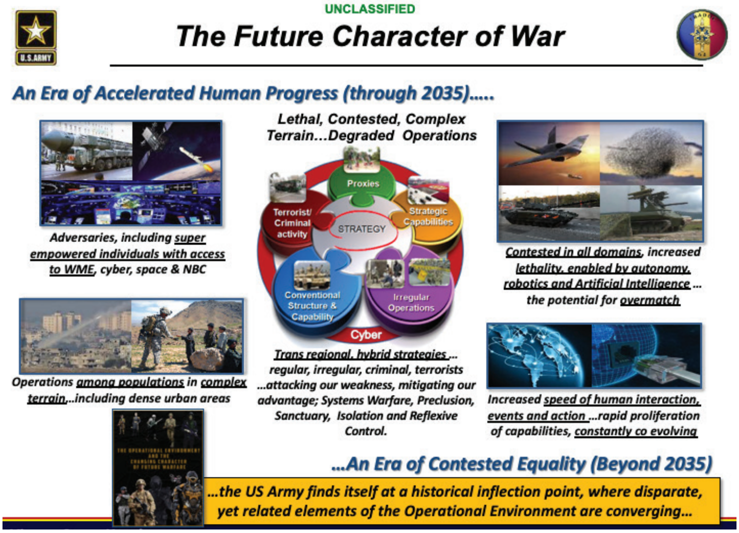


UNCLASSIFIED

Deep Future Operational Environment Video

UNCLASSIFIED

Russian Uran-9



UNCLASSIFIED

The Future Character of War

An Era of Accelerated Human Progress (through 2035)…..

Adversaries, including super empowered individuals with access to WME, cyber, space & NBC

Lethal, Contested, Complex Terrain…Degraded Operations

Proxies
Terrorist/ Criminal activity
STRATEGY
Strategic Capabilities
Conventional Structure & Capability
Irregular Operations
Cyber
U.S. ARMY
THE OPERATIONAL ENVIRONMENT AND THE CHANGING CHARACTER OF FUTURE WARFARE

Trans regional, hybrid strategies … regular, irregular, criminal, terrorists …attacking our weakness, mitigating our advantage; Systems Warfare, Preclusion, Sanctuary, Isolation and Reflexive Control.

Contested in all domains, increased lethality, enabled by autonomy, robotics and Artificial Intelligence … the potential for overmatch

Operations among populations in complex terrain,..including dense urban areas

Increased speed of human interaction, events and action …rapid proliferation of capabilities, constantly co evolving

…An Era of Contested Equality (Beyond 2035)

…the US Army finds itself at a historical inflection point, where disparate, yet related elements of the Operational Environment are converging…

UNCLASSIFIED

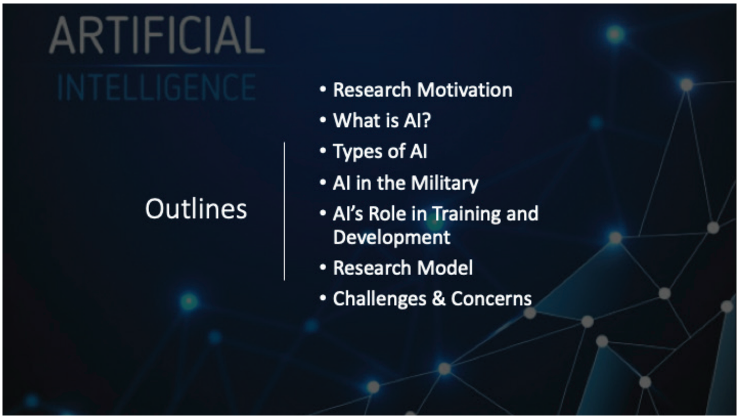
Discussion

How Far Can We Go: The Role of AI in Soldier-Leader Development

Dr. Ash Mady and Ms. Bethany Niese

Mady & Niese
2019

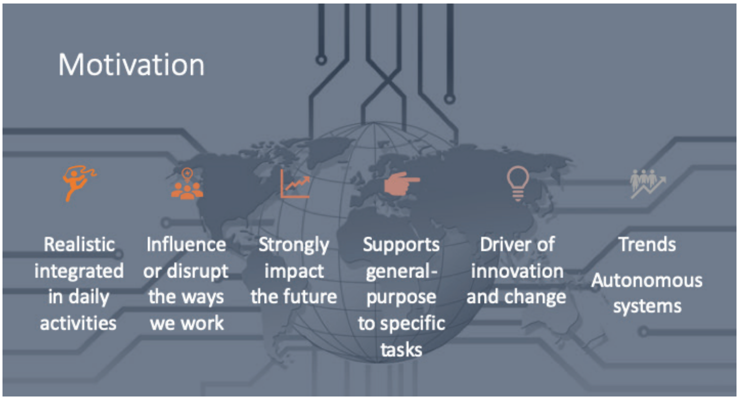
AI
How far we can go



ARTIFICIAL INTELLIGENCE

Outlines

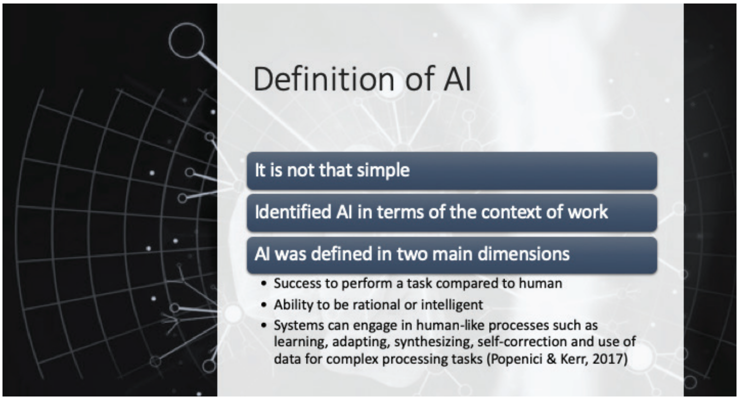
- Research Motivation
- What is AI?
- Types of AI
- AI in the Military
- AI's Role in Training and Development
- Research Model
- Challenges & Concerns



Motivation

- Realistic integrated in daily activities
- Influence or disrupt the ways we work
- Strongly impact the future
- Supports general-purpose to specific tasks
- Driver of innovation and change
- Trends

  Autonomous systems



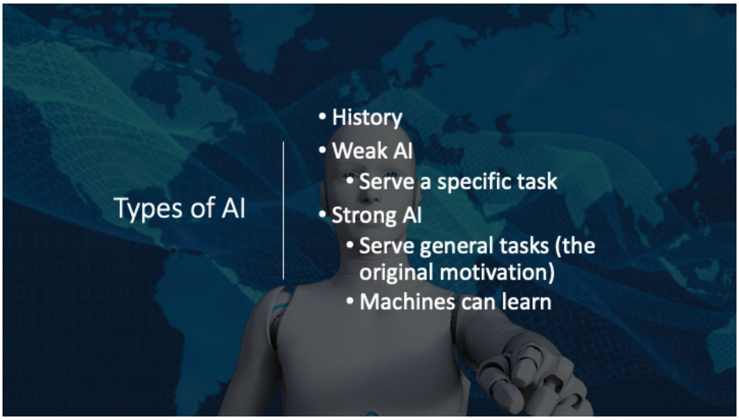
Definition of AI

It is not that simple

Identified AI in terms of the context of work

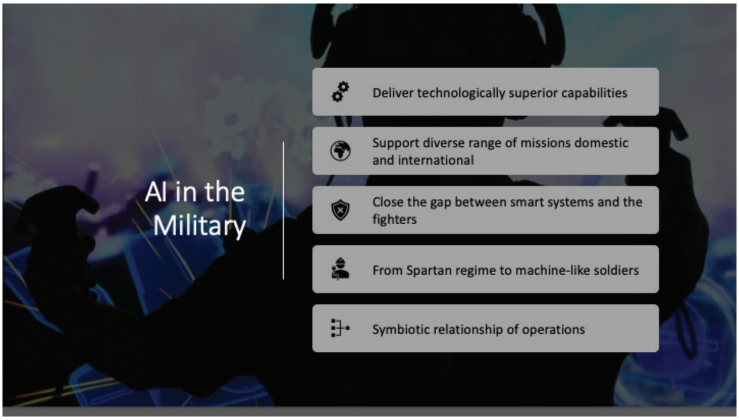
AI was defined in two main dimensions

- Success to perform a task compared to human
- Ability to be rational or intelligent
- Systems can engage in human-like processes such as learning, adapting, synthesizing, self-correction and use of data for complex processing tasks (Popenici & Kerr, 2017)



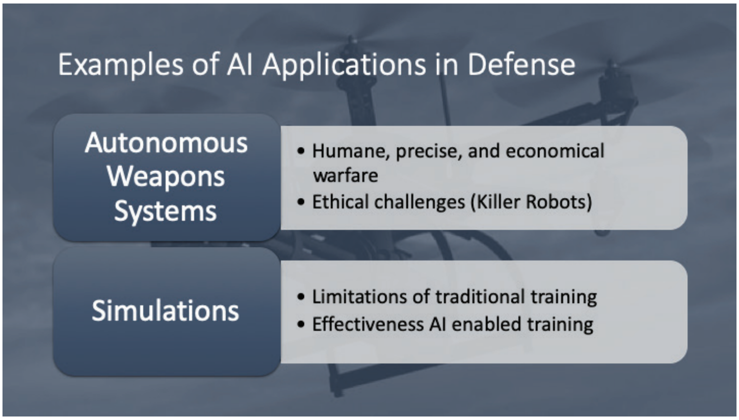
Types of AI

- History
- Weak AI
  - Serve a specific task
- Strong AI
  - Serve general tasks (the original motivation)
  - Machines can learn



AI in the Military

- Deliver technologically superior capabilities
- Support diverse range of missions domestic and international
- Close the gap between smart systems and the fighters
- From Spartan regime to machine-like soldiers
- Symbiotic relationship of operations



Examples of AI Applications in Defense

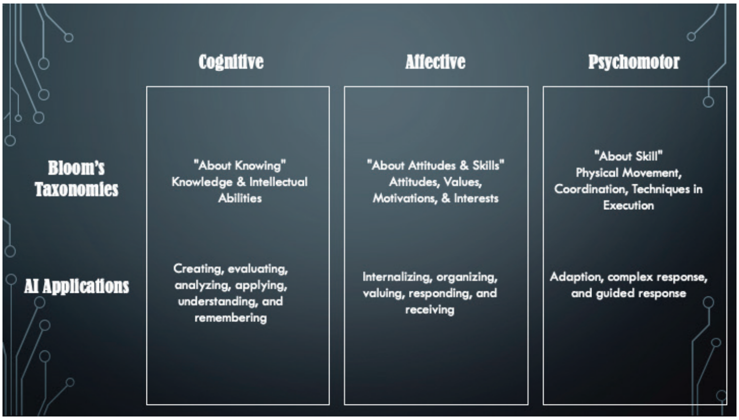
Autonomous Weapons Systems

- Humane, precise, and economical warfare
- Ethical challenges (Killer Robots)

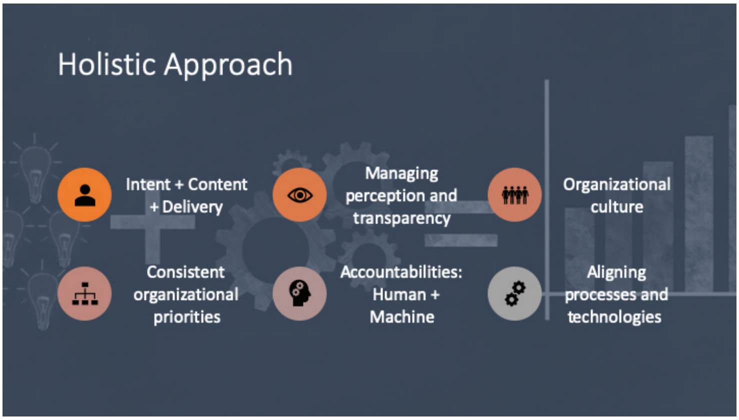
Simulations

- Limitations of traditional training
- Effectiveness AI enabled training

AI Training and Development

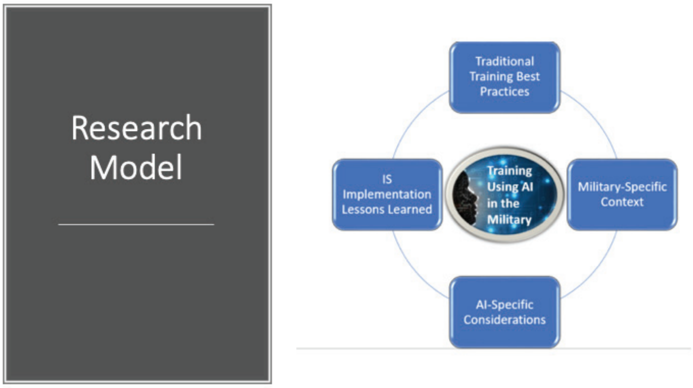


	Cognitive	Affective	Psychomotor
Bloom's Taxonomies	"About Knowing" Knowledge & Intellectual Abilities	"About Attitudes & Skills" Attitudes, Values, Motivations, & Interests	"About Skill" Physical Movement, Coordination, Techniques in Execution
AI Applications	Creating, evaluating, analyzing, applying, understanding, and remembering	Internalizing, organizing, valuing, responding, and receiving	Adaption, complex response, and guided response



Holistic Approach

- Intent + Content + Delivery
- Consistent organizational priorities
- Managing perception and transparency
- Accountabilities: Human + Machine
- Organizational culture
- Aligning processes and technologies



Research Model

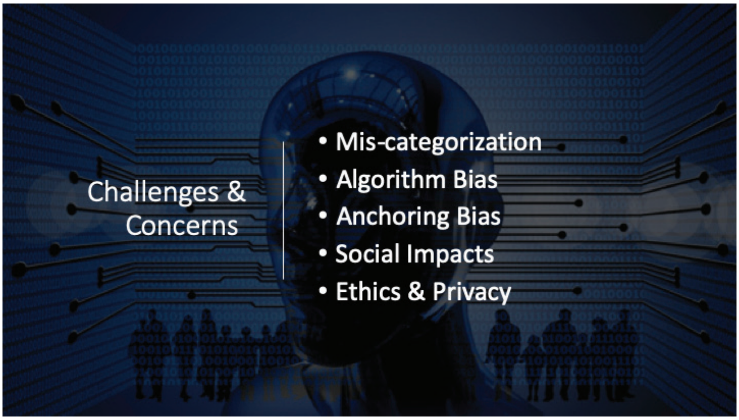
Traditional Training Best Practices

IS Implementation Lessons Learned

Training Using AI in the Military

Military-Specific Context

AI-Specific Considerations

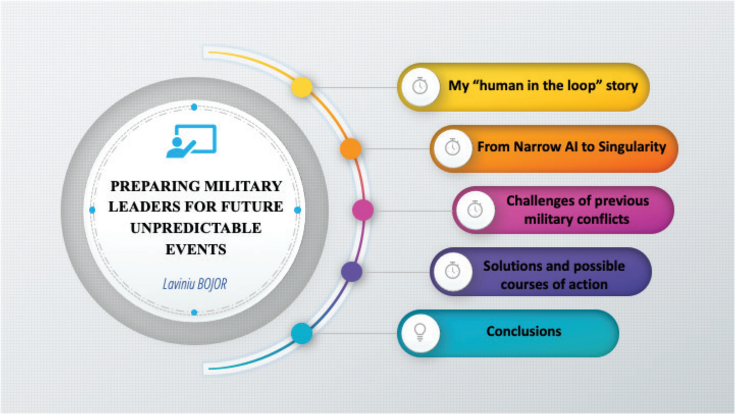


Challenges & Concerns

- Mis-categorization
- Algorithm Bias
- Anchoring Bias
- Social Impacts
- Ethics & Privacy

Preparing Military Leaders for Future Unpredictable Events

Lieutenant Colonel Laviniu Bajor



PREPARING MILITARY LEADERS FOR FUTURE UNPREDICTABLE EVENTS

Laviniu BOJOR

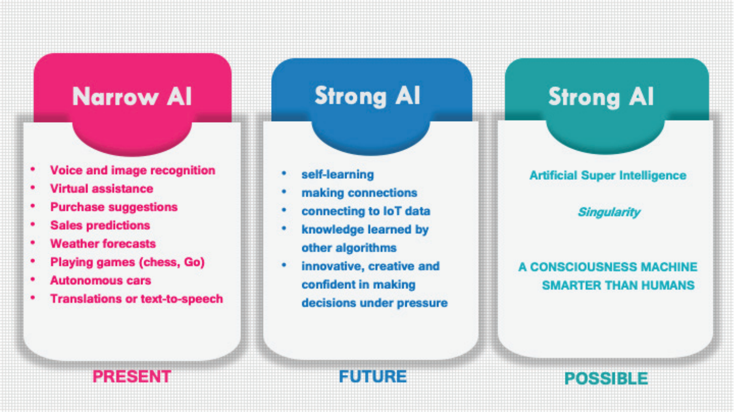
My "human in the loop" story

From Narrow AI to Singularity

Challenges of previous military conflicts

Solutions and possible courses of action

Conclusions



Narrow AI

- Voice and image recognition
- Virtual assistance
- Purchase suggestions
- Sales predictions
- Weather forecasts
- Playing games (chess, Go)
- Autonomous cars
- Translations or text-to-speech

PRESENT

Strong AI

- self-learning
- making connections
- connecting to IoT data
- knowledge learned by other algorithms
- innovative, creative and confident in making decisions under pressure

FUTURE

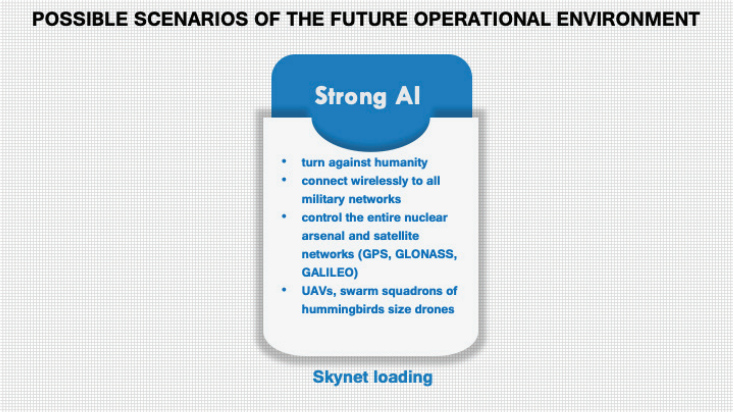
Strong AI

Artificial Super Intelligence

Singularity

A CONSCIOUSNESS MACHINE SMARTER THAN HUMANS

POSSIBLE

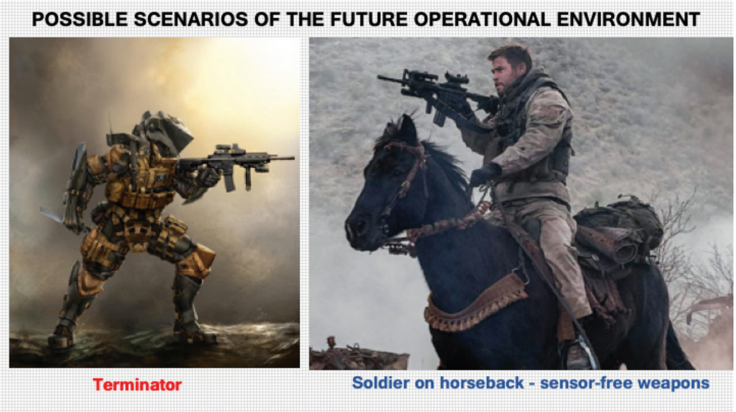


POSSIBLE SCENARIOS OF THE FUTURE OPERATIONAL ENVIRONMENT

Strong AI

- turn against humanity
- connect wirelessly to all military networks
- control the entire nuclear arsenal and satellite networks (GPS, GLONASS, GALILEO)
- UAVs, swarm squadrons of hummingbirds size drones

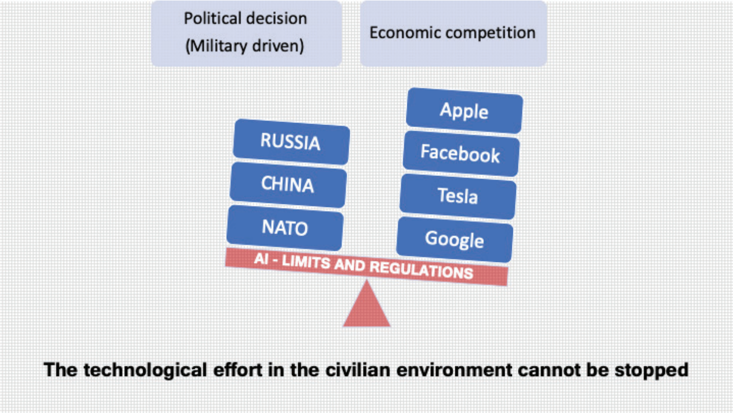
Skynet loading



POSSIBLE SCENARIOS OF THE FUTURE OPERATIONAL ENVIRONMENT

Terminator

Soldier on horseback - sensor-free weapons



Political decision (Military driven)

Economic competition

RUSSIA

CHINA

NATO

Apple

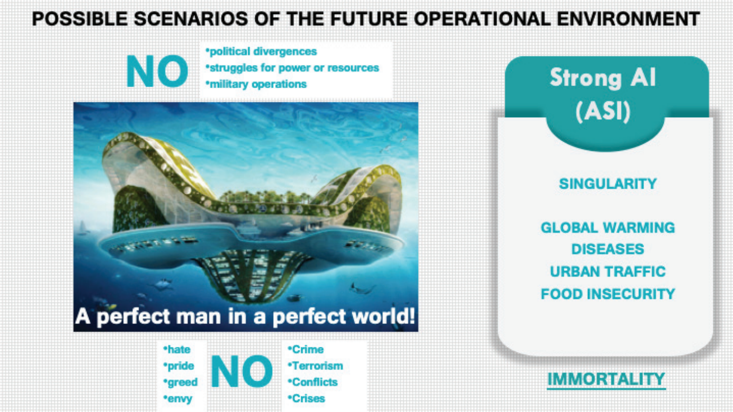
Facebook

Tesla

Google

AI - LIMITS AND REGULATIONS

The technological effort in the civilian environment cannot be stopped



POSSIBLE SCENARIOS OF THE FUTURE OPERATIONAL ENVIRONMENT

NO
- political divergences
- struggles for power or resources
- military operations

A perfect man in a perfect world!

- hate
- pride
- greed
- envy

NO

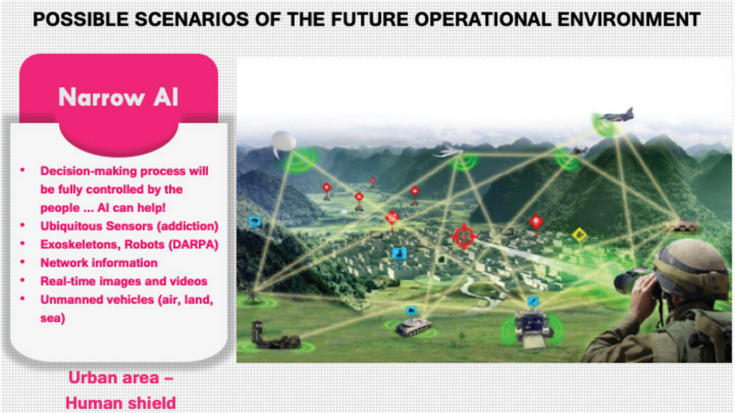
- Crime
- Terrorism
- Conflicts
- Crises

Strong AI (ASI)

SINGULARITY

GLOBAL WARMING
DISEASES
URBAN TRAFFIC
FOOD INSECURITY

IMMORTALITY

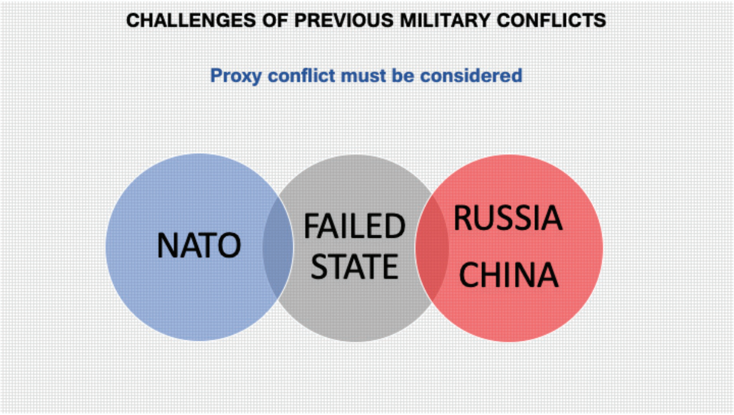


POSSIBLE SCENARIOS OF THE FUTURE OPERATIONAL ENVIRONMENT

Narrow AI

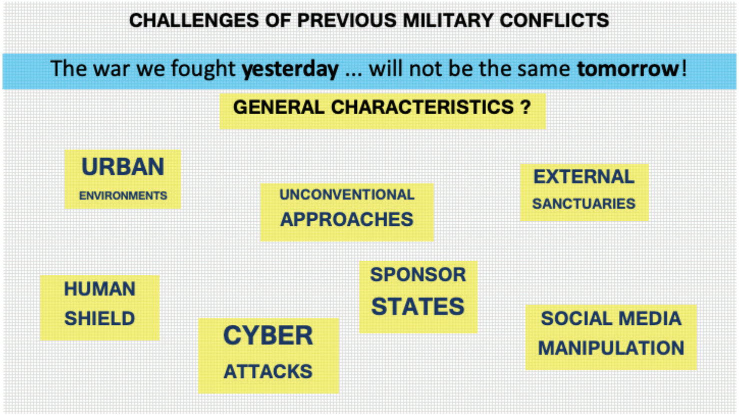
- Decision-making process will be fully controlled by the people ... AI can help!
- Ubiquitous Sensors (addiction)
- Exoskeletons, Robots (DARPA)
- Network information
- Real-time images and videos
- Unmanned vehicles (air, land, sea)

Urban area – Human shield



CHALLENGES OF PREVIOUS MILITARY CONFLICTS

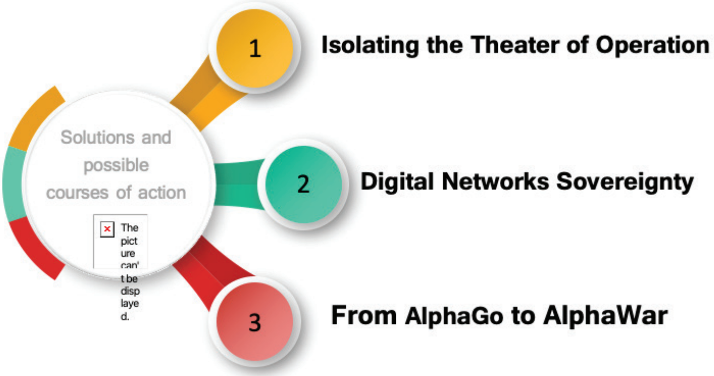
Proxy conflict must be considered



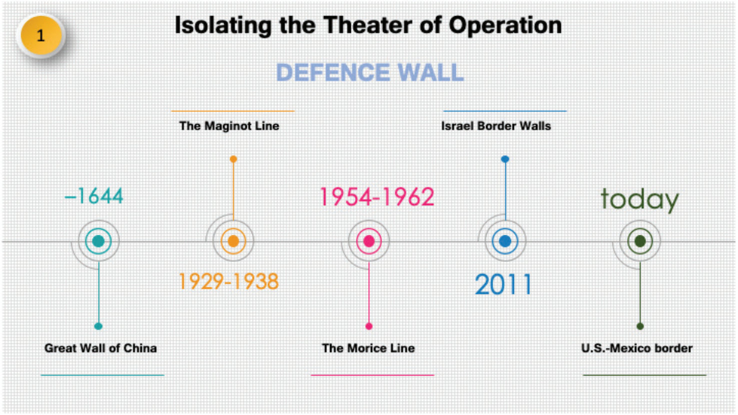
CHALLENGES OF PREVIOUS MILITARY CONFLICTS

The war we fought **yesterday** ... will not be the same **tomorrow**!

GENERAL CHARACTERISTICS ?



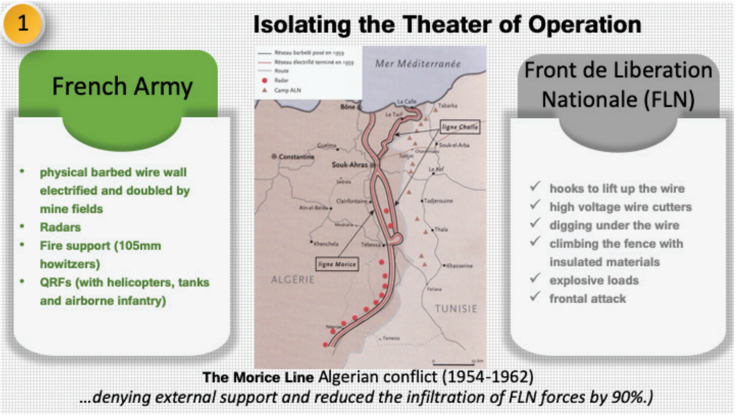
Solutions and possible courses of action
The picture can't be displayed.
1
Isolating the Theater of Operation
2
Digital Networks Sovereignty
3
From AlphaGo to AlphaWar



1

Isolating the Theater of Operation

DEFENCE WALL



1

Isolating the Theater of Operation

French Army

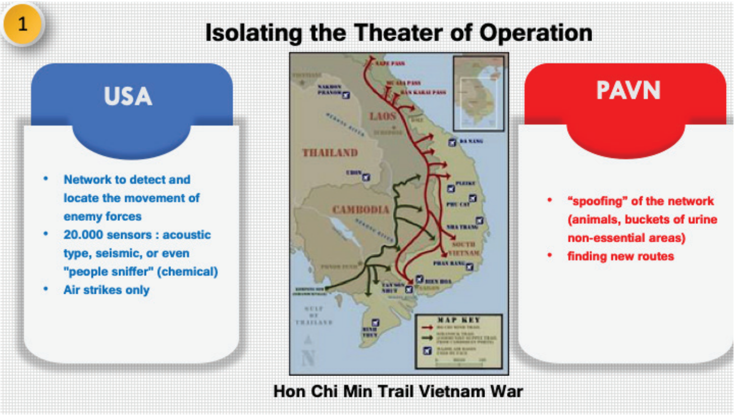
- physical barbed wire wall electrified and doubled by mine fields
- Radars
- Fire support (105mm howitzers)
- QRFs (with helicopters, tanks and airborne infantry)

Front de Liberation Nationale (FLN)

✓ hooks to lift up the wire
✓ high voltage wire cutters
✓ digging under the wire
✓ climbing the fence with insulated materials
✓ explosive loads
✓ frontal attack

The Morice Line Algerian conflict (1954-1962)

...denying external support and reduced the infiltration of FLN forces by 90%.)



1

Isolating the Theater of Operation

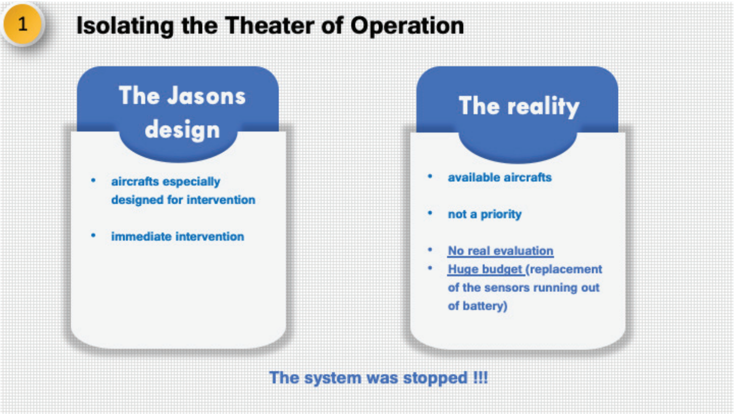
USA

- Network to detect and locate the movement of enemy forces
- 20.000 sensors : acoustic type, seismic, or even "people sniffer" (chemical)
- Air strikes only

PAVN

- "spoofing" of the network (animals, buckets of urine non-essential areas)
- finding new routes

Hon Chi Min Trail Vietnam War



1

Isolating the Theater of Operation

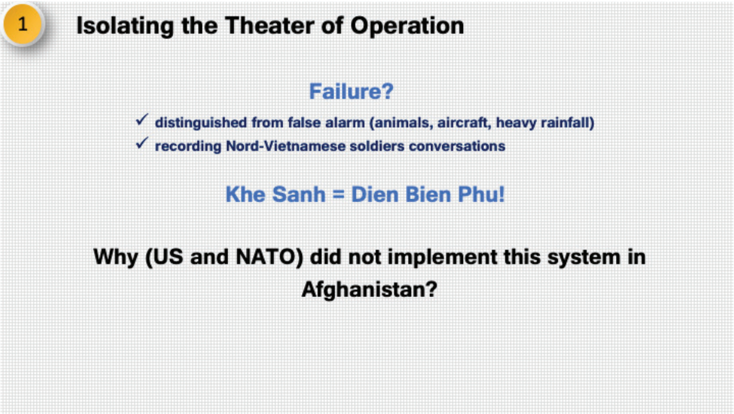
The Jasons design

- aircrafts especially designed for intervention
- immediate intervention

The reality

- available aircrafts
- not a priority
- No real evaluation
- Huge budget (replacement of the sensors running out of battery)

The system was stopped !!!



1

Isolating the Theater of Operation

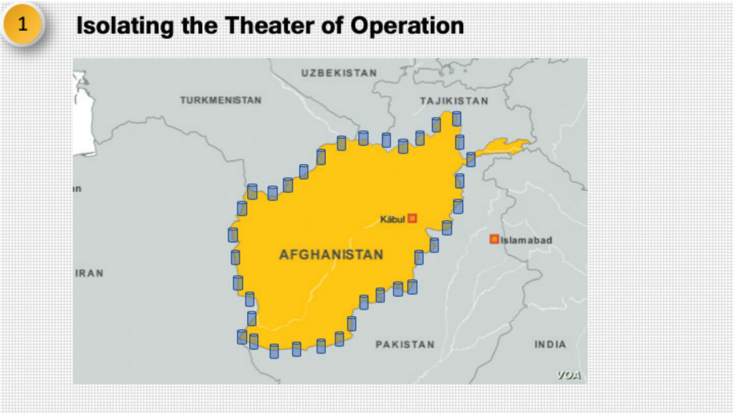
Failure?

✓ distinguished from false alarm (animals, aircraft, heavy rainfall)

✓ recording Nord-Vietnamese soldiers conversations

Khe Sanh = Dien Bien Phu!

Why (US and NATO) did not implement this system in Afghanistan?



1

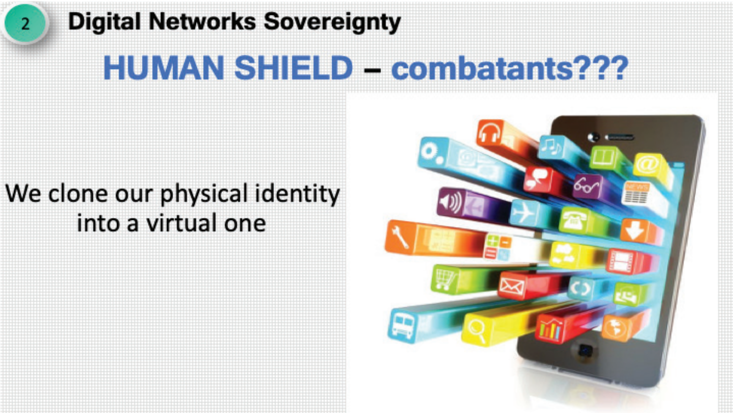
Isolating the Theater of Operation

1 **Isolating the Theater of Operation**

UZBEKISTAN
TURKMENISTAN
TAJIKISTAN
in
Kābul
AFGHANISTAN
Islamabad
IRAN
PAKISTAN
INDIA
VOA

1 **Isolating the Theater of Operation**

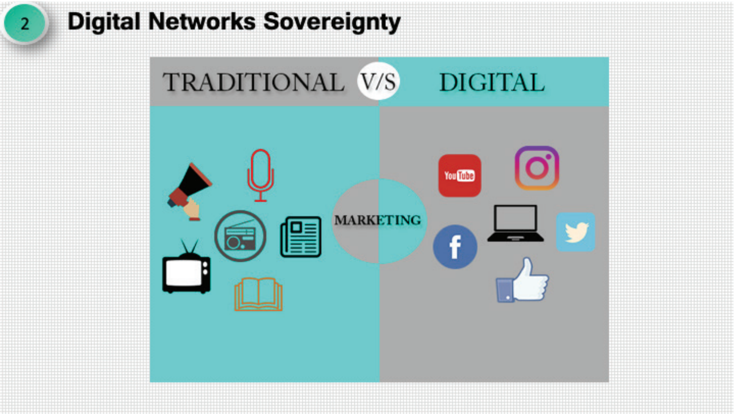
UZBEKISTAN
TURKMENISTAN
TAJIKISTAN
in
AFGHANISTAN
Islamabad
IRAN
PAKISTAN
INDIA
VOA



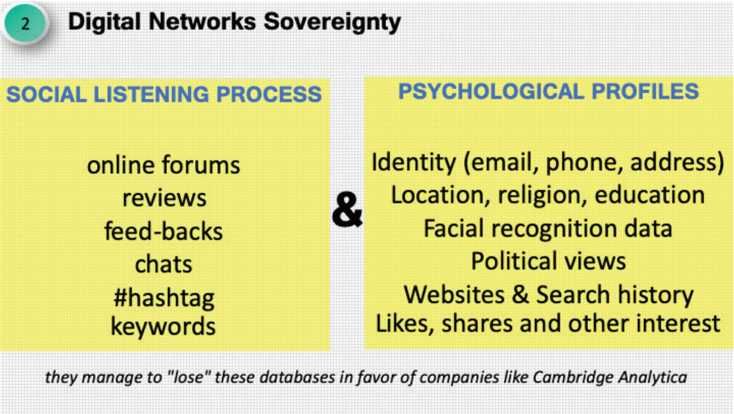
2 **Digital Networks Sovereignty**

HUMAN SHIELD – combatants???

We clone our physical identity into a virtual one



2 **Digital Networks Sovereignty**



2 **Digital Networks Sovereignty**

SOCIAL LISTENING PROCESS

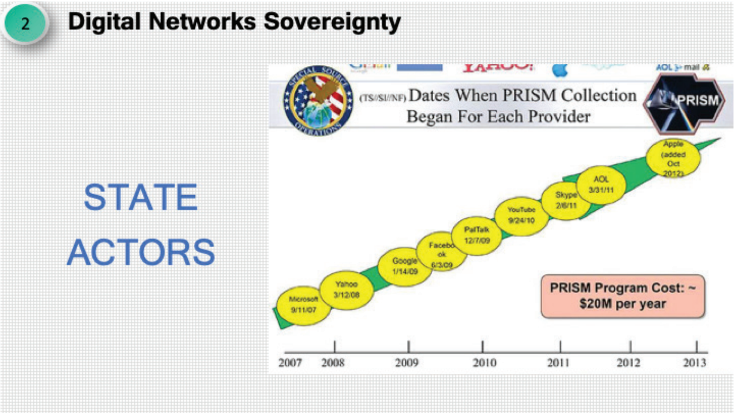
online forums
reviews
feed-backs
chats
#hashtag
keywords

&

PSYCHOLOGICAL PROFILES

Identity (email, phone, address)
Location, religion, education
Facial recognition data
Political views
Websites & Search history
Likes, shares and other interest

they manage to "lose" these databases in favor of companies like Cambridge Analytica

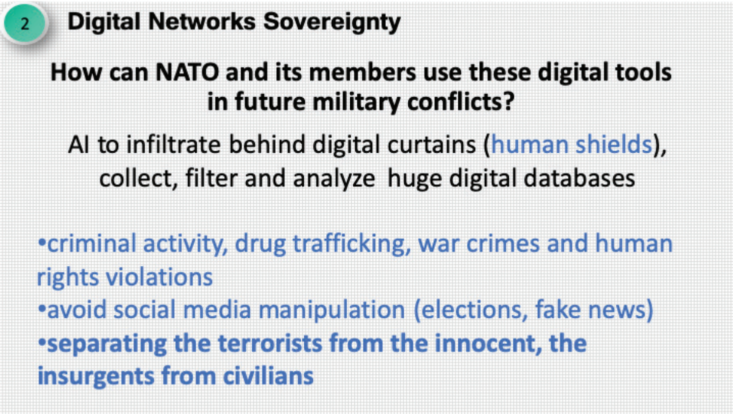


2 **Digital Networks Sovereignty**

STATE
ACTORS

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year



2 **Digital Networks Sovereignty**

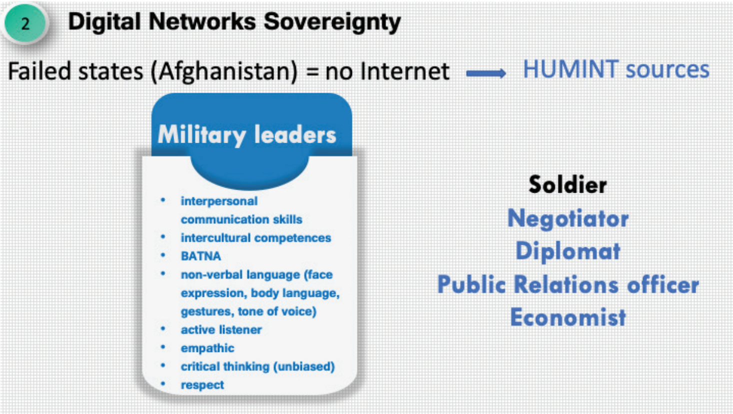
How can NATO and its members use these digital tools in future military conflicts?

AI to infiltrate behind digital curtains (human shields), collect, filter and analyze huge digital databases

•criminal activity, drug trafficking, war crimes and human rights violations

•avoid social media manipulation (elections, fake news)

•separating the terrorists from the innocent, the insurgents from civilians



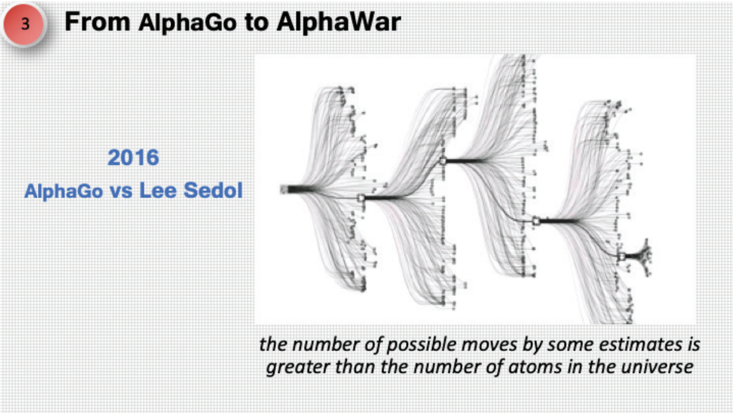
2 **Digital Networks Sovereignty**

Failed states (Afghanistan) = no Internet → HUMINT sources

Military leaders

- interpersonal communication skills
- intercultural competences
- BATNA
- non-verbal language (face expression, body language, gestures, tone of voice)
- active listener
- empathic
- critical thinking (unbiased)
- respect

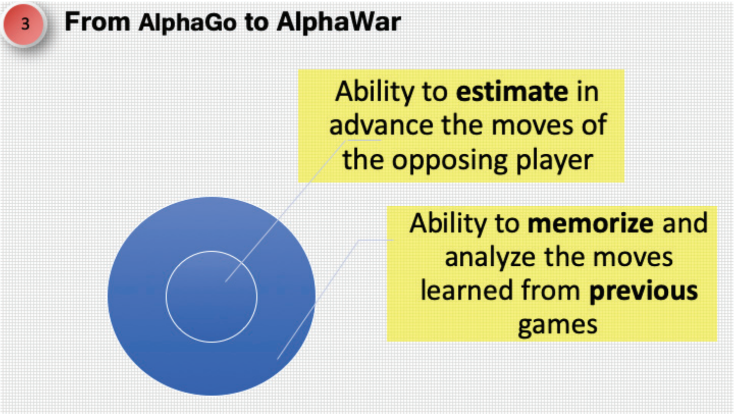
Soldier
Negotiator
Diplomat
Public Relations officer
Economist



3 **From AlphaGo to AlphaWar**

2016
AlphaGo vs Lee Sedol

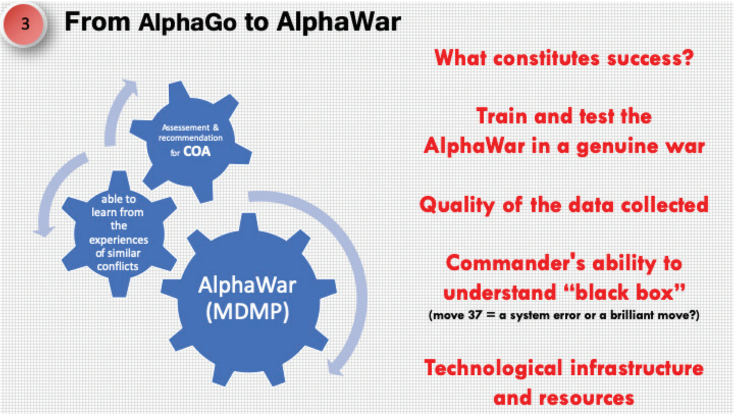
the number of possible moves by some estimates is greater than the number of atoms in the universe



3 **From AlphaGo to AlphaWar**

Ability to **estimate** in advance the moves of the opposing player

Ability to **memorize** and analyze the moves learned from **previous** games



3 **From AlphaGo to AlphaWar**

Assessement & recommendation for COA
able to learn from the experiences of similar conflicts
AlphaWar (MDMP)

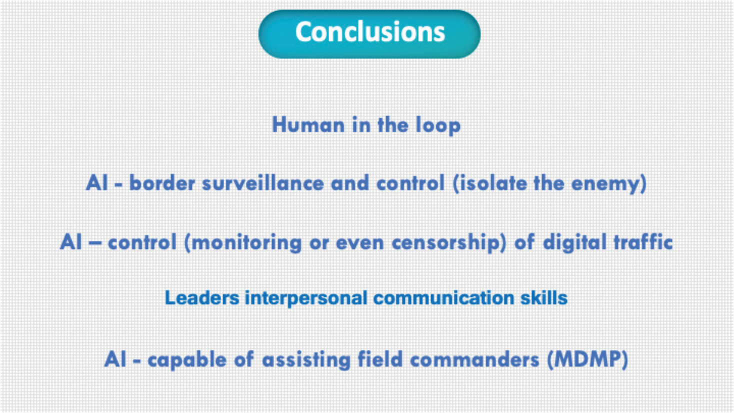
What constitutes success?

Train and test the AlphaWar in a genuine war

Quality of the data collected

Commander's ability to understand "black box"
(move 37 = a system error or a brilliant move?)

Technological infrastructure and resources



Conclusions

Human in the loop

AI - border surveillance and control (isolate the enemy)

AI – control (monitoring or even censorship) of digital traffic

Leaders interpersonal communication skills

AI - capable of assisting field commanders (MDMP)

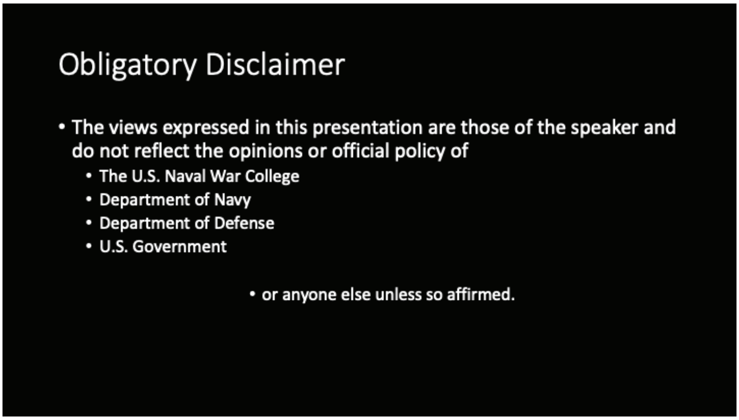
What can the Battle Room, Mobile Infantry, and Forever Wars tell us how Advances in Science and Technology Might Influence Future Military Leadership Education and Development?

U.S. Navy Captain Michael Junge

Training Future Officers

The Battle Room, Mobile Infantry

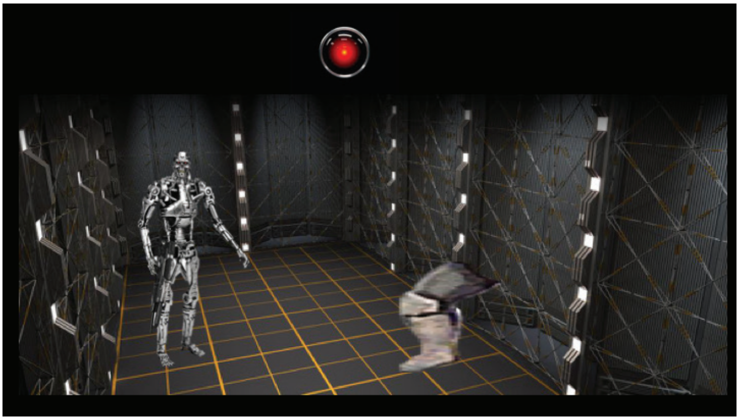
& Forever War



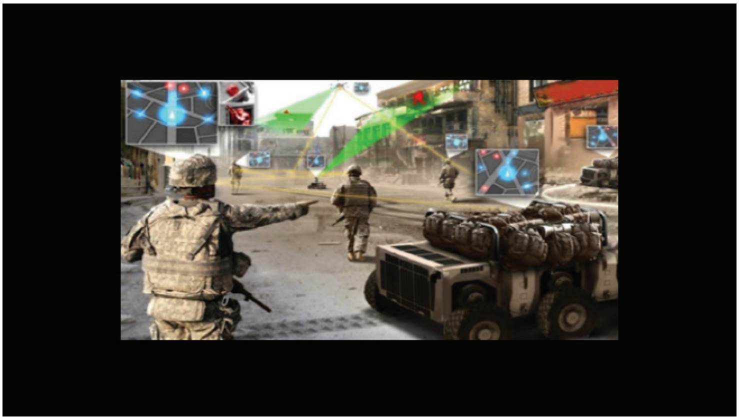
Obligatory Disclaimer

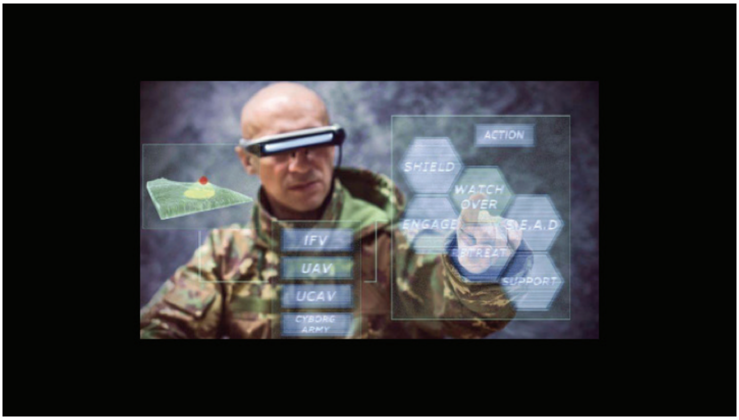
- The views expressed in this presentation are those of the speaker and do not reflect the opinions or official policy of
  - The U.S. Naval War College
  - Department of Navy
  - Department of Defense
  - U.S. Government

- or anyone else unless so affirmed.



APRIL-JUNE 2017
ARTIFICIAL INTELLIGENCE
ADVANCED MANUFACTURING
ROBOTICS



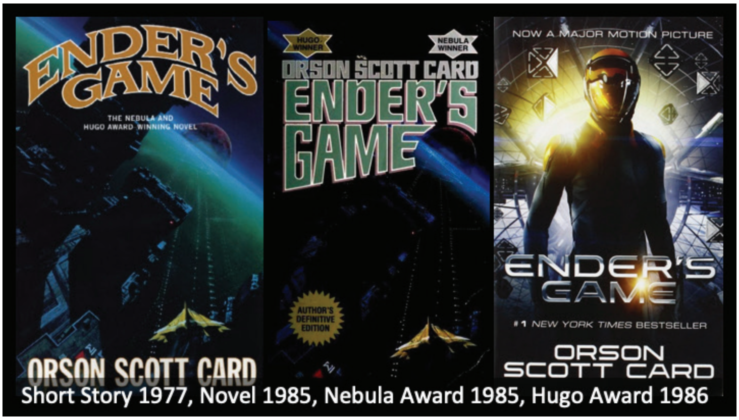

ACTION
SHIELD
WATCH OVER
ENGAGE
S.E.A.D
RETREAT
SUPPORT
IFV
UAV
UCAV
CYBORG ARMY

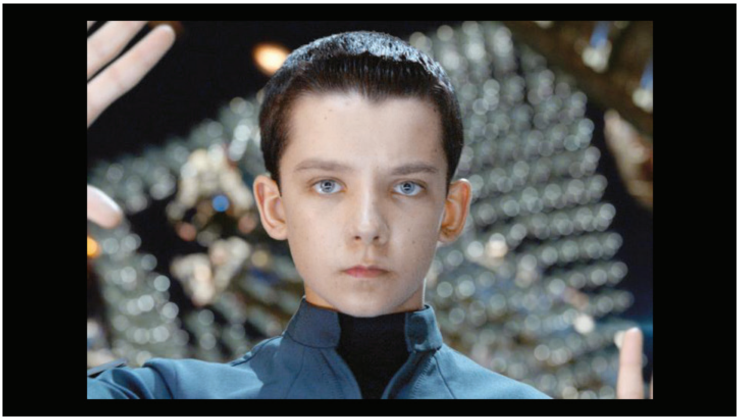
FULLY INTEGRATED INDIVIDUAL COMBAT
FUTURE SOLDIER

Bright Shiny Object™

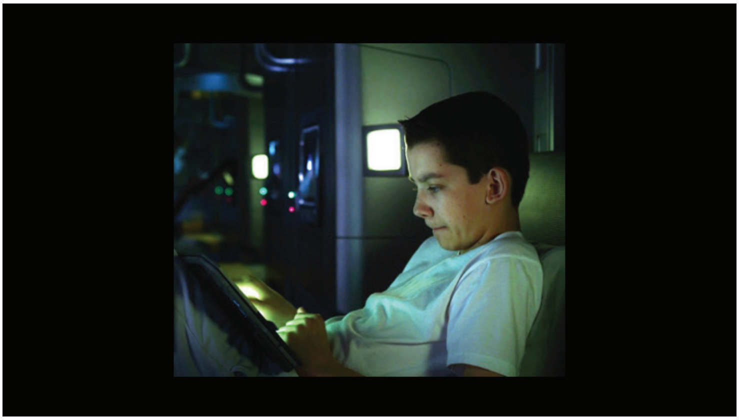
[redacted]

HARRISON FORD ASA BUTTERFIELD HAILEE STEINFELD VIOLA DAVIS with ABIGAIL BRESLIN and BEN KINGSLEY
ENDER'S GAME
THE FUTURE MUST BE WON
/ENDERSGAMEUK
ENDERSGAMEUK.COM
#BEAHERO
2013


ENDER'S GAME
THE NEBULA AND HUGO AWARD WINNING NOVEL
ORSON SCOTT CARD
HUGO WINNER
NEBULA WINNER
ORSON SCOTT CARD
ENDER'S GAME
AUTHOR'S DEFINITIVE EDITION
NOW A MAJOR MOTION PICTURE
ENDER'S GAME
#1 NEW YORK TIMES BESTSELLER
ORSON SCOTT CARD
Short Story 1977, Novel 1985, Nebula Award 1985, Hugo Award 1986



Richard Foreman Jr. SMPSP



Mind Game

E. WIGGIN
100
LIVES: 01/03
1:18

[redacted]

"To say that *The Forever War* is the best science fiction war novel ever written is to damn it with faint praise. It is, for all its techno-extrapolative brilliance, as fine and woundingly genuine a war story as any I've read."
—WILLIAM GIBSON, author of *Neuromancer* and *Spook Country*
THE FOREVER WAR
JOE HALDEMAN
THE HUGO AND NEBULA AWARD · WINNING NOVEL
JOE HALDEMAN
THE FOREVER WAR
A DAZZLING & POWERFUL SCIENCE FICTION CATCH-22!
THE FOREVER WAR
JOE HALDEMAN
Winner of the Hugo and Nebula Awards BEST NOVEL OF THE YEAR

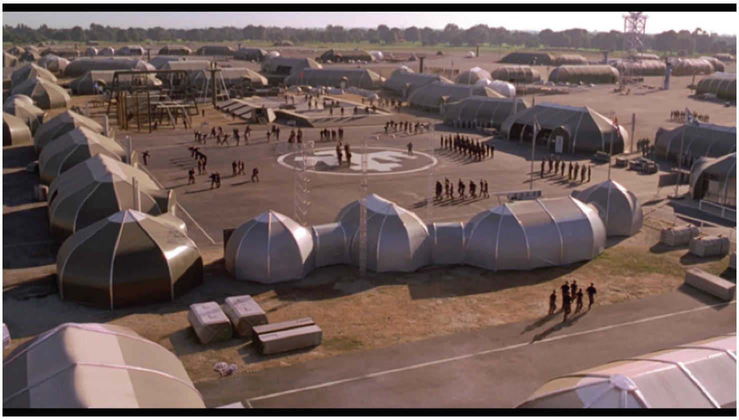
Novel 1974, Nebula Award 1975, Hugo Award 1976

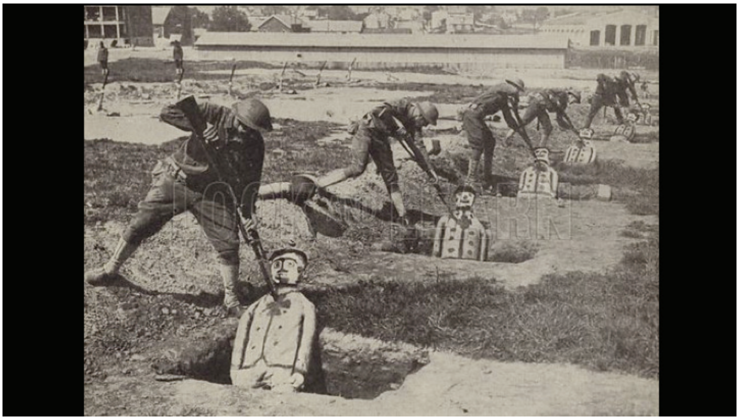
I REMEMBERED HER IN THE CLASSROOM. QUIET BUT STUBBORN.
ALL RIGHT! THOSE WERE THE EIGHT SILENT WAYS TO KILL A MAN. ANY QUESTIONS?
MANDELLA
YES, SIR. MOST OF THOSE METHODS, THEY LOOKED... KIND OF SILLY.
FOR INSTANCE, PRIVATE BOVANOVITCH?
KILLING A MAN WITH A SHOVEL BLOW TO THE KIDNEYS. WHEN WOULD WE HAVE ONLY A SHOVEL AS A WEAPON?
AND IN THAT CASE, WHY NOT HIT HIM OVER THE HEAD WITH IT?

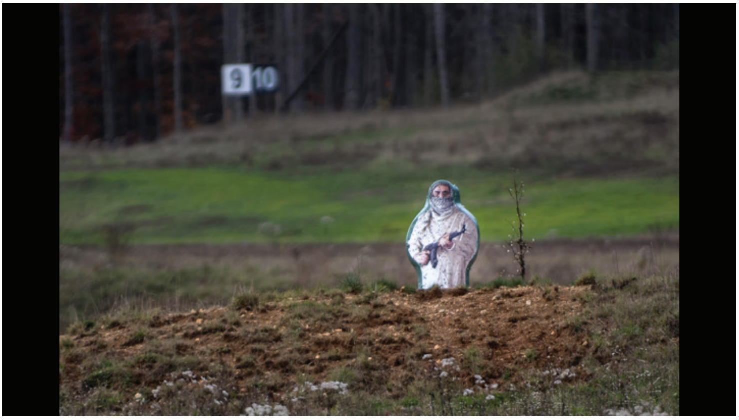
1997

FOUR SQUARE SCIENCE FICTION
ROBERT HEINLEIN
Starship Troopers
WINNER OF A HUGO AWARD FOR BEST SCI-FI NOVEL OF THE YEAR
Mobile Infantrymen of the
ROBERT A. HEINLEIN
THE MODERN MASTER OF SCIENCE FICTION
STARSHIP TROOPERS
STARSHIP TROOPERS
THE CONTROVERSIAL CLASSIC OF MILITARY ADVENTURE!
Robert A. HEINLEIN

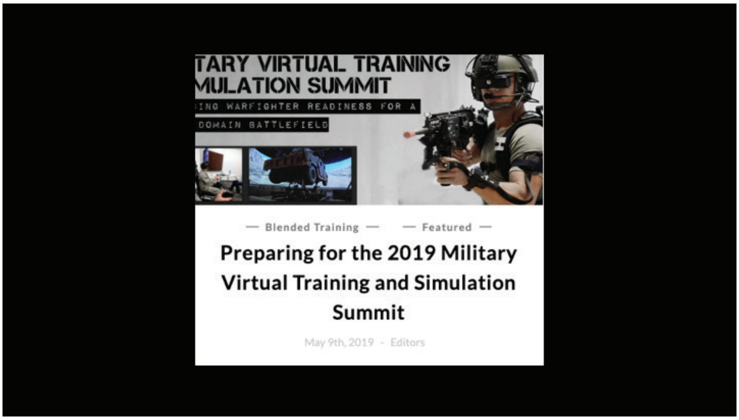
Short Story 1954, Novel 1959, Hugo Award 1960






9
10

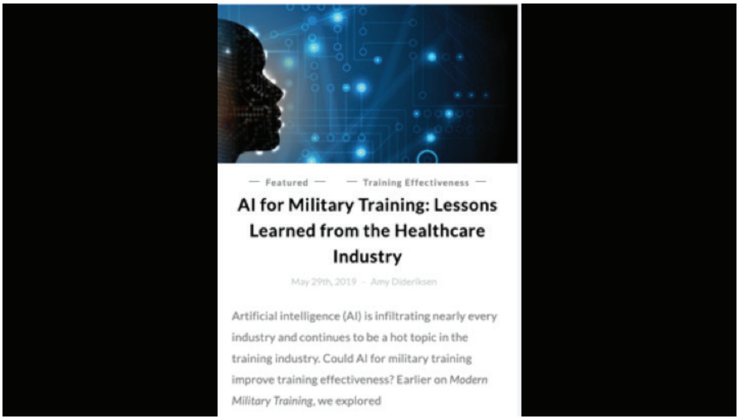
MOVIECLIPS.com



— Blended Training — — Featured —

Preparing for the 2019 Military Virtual Training and Simulation Summit

May 9th, 2019 - Editors

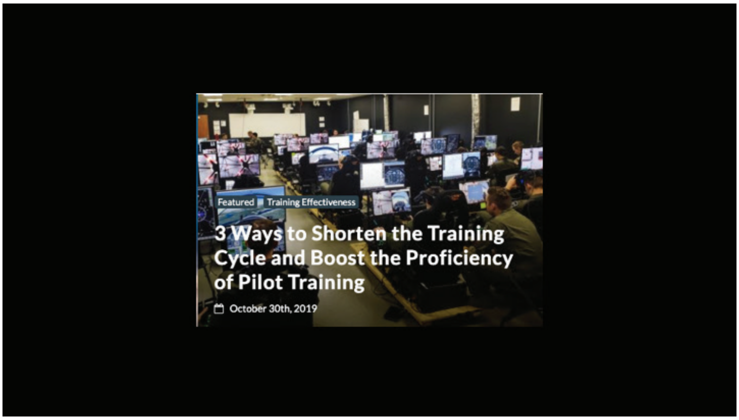


— Featured — — Training Effectiveness —

AI for Military Training: Lessons Learned from the Healthcare Industry

May 29th, 2019 - Amy Dideriksen

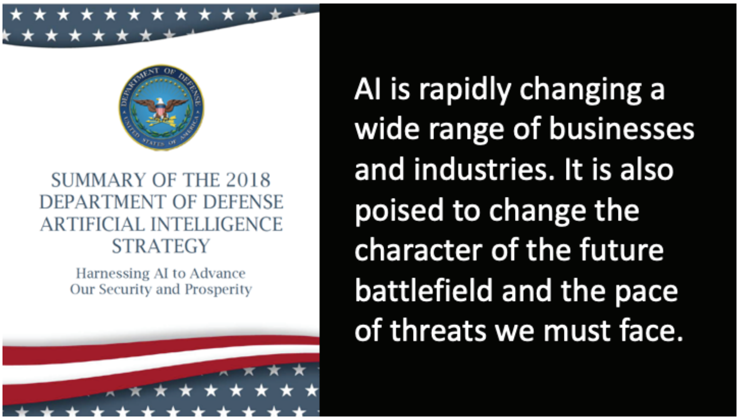
Artificial intelligence (AI) is infiltrating nearly every industry and continues to be a hot topic in the training industry. Could AI for military training improve training effectiveness? Earlier on *Modern Military Training*, we explored



Featured Training Effectiveness

3 Ways to Shorten the Training Cycle and Boost the Proficiency of Pilot Training

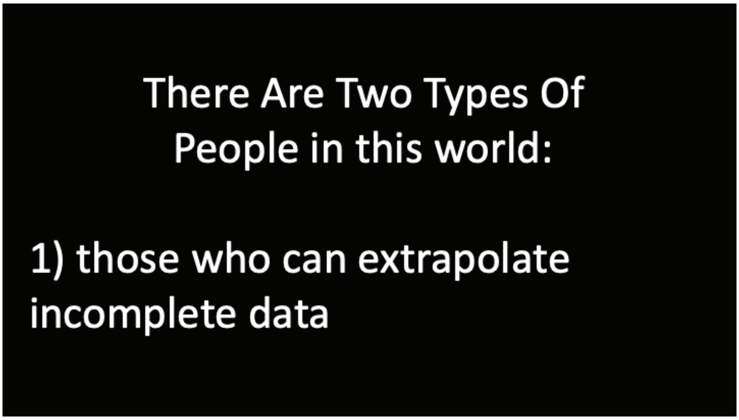
October 30th, 2019



SUMMARY OF THE 2018
DEPARTMENT OF DEFENSE
ARTIFICIAL INTELLIGENCE
STRATEGY

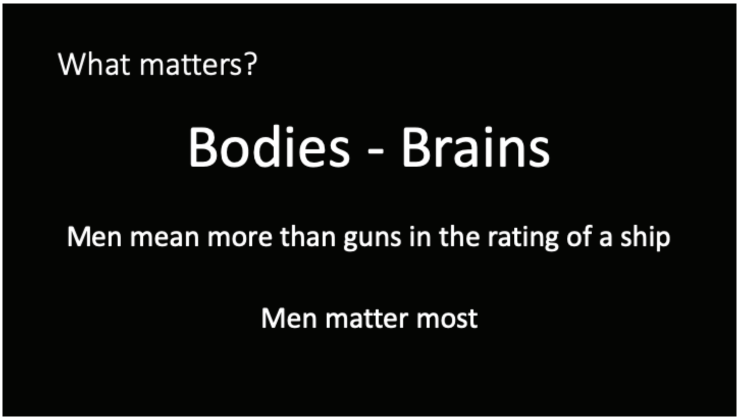
Harnessing AI to Advance
Our Security and Prosperity

AI is rapidly changing a wide range of businesses and industries. It is also poised to change the character of the future battlefield and the pace of threats we must face.



There Are Two Types Of People in this world:

1) those who can extrapolate incomplete data

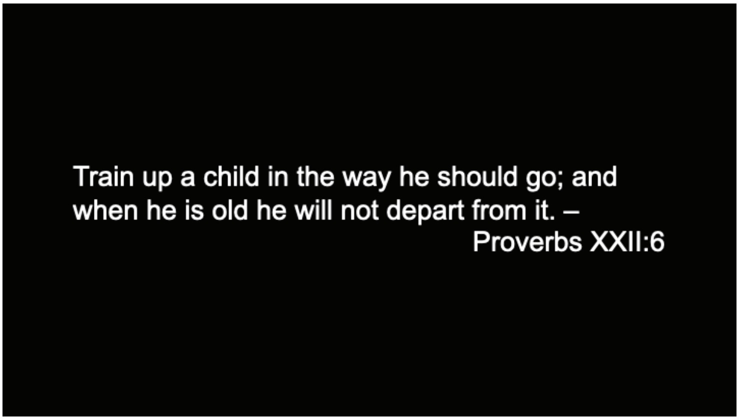


What matters?

Bodies - Brains

Men mean more than guns in the rating of a ship

Men matter most



Train up a child in the way he should go; and when he is old he will not depart from it. –
Proverbs XXII:6

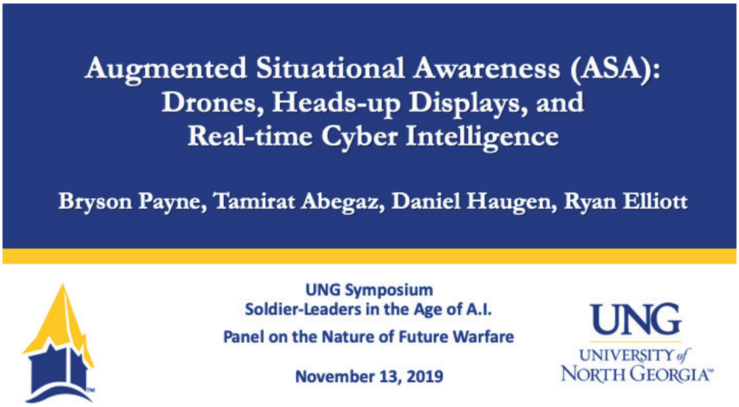
[redacted]

[redacted]

[redacted]

Augmented Situational Awareness: Drones, Heads-up Displays, and Real-time Cyber Intelligence

Dr. Bryson Payne and Dr. Tamirat Abegaz



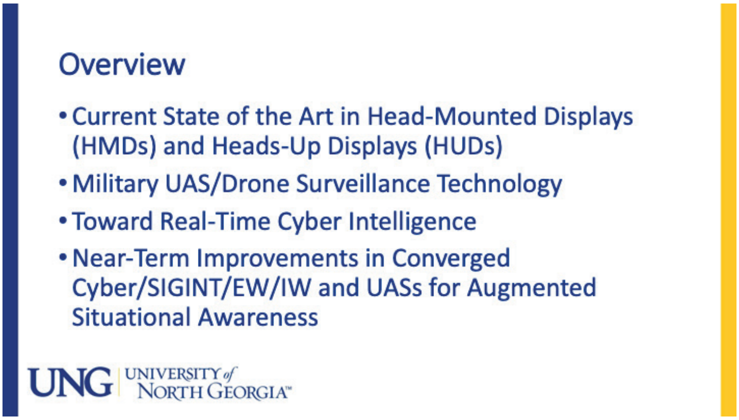
Augmented Situational Awareness (ASA): Drones, Heads-up Displays, and Real-time Cyber Intelligence

Bryson Payne, Tamirat Abegaz, Daniel Haugen, Ryan Elliott

UNG Symposium
Soldier-Leaders in the Age of A.I.
Panel on the Nature of Future Warfare

November 13, 2019

UNG
UNIVERSITY of NORTH GEORGIA™

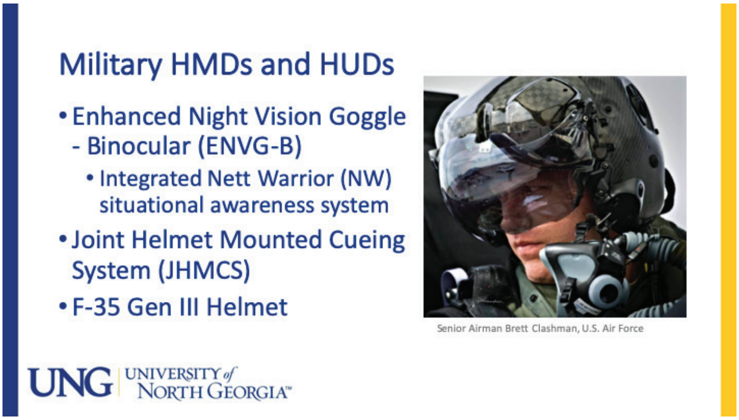


Overview

- Current State of the Art in Head-Mounted Displays (HMDs) and Heads-Up Displays (HUDs)
- Military UAS/Drone Surveillance Technology
- Toward Real-Time Cyber Intelligence
- Near-Term Improvements in Converged Cyber/SIGINT/EW/IW and UASs for Augmented Situational Awareness

Consumer HMDs and HUDs

- Google Glass (Enterprise Edition)
- Microsoft HoloLens
- Magic Leap One



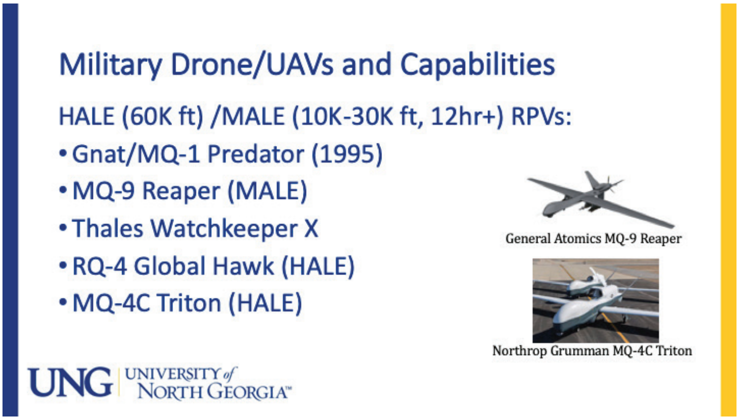
Military HMDs and HUDs

- Enhanced Night Vision Goggle - Binocular (ENVG-B)
  - Integrated Nett Warrior (NW) situational awareness system
- Joint Helmet Mounted Cueing System (JHMCS)
- F-35 Gen III Helmet

Senior Airman Brett Clashman, U.S. Air Force

HMD + UAV/Drone Technologies

- DJI Goggles
- Epson Moverio BT-300 Drone FPV Edition Glasses



Military Drone/UAVs and Capabilities

HALE (60K ft) /MALE (10K-30K ft, 12hr+) RPVs:

- Gnat/MQ-1 Predator (1995)
- MQ-9 Reaper (MALE)
- Thales Watchkeeper X
- RQ-4 Global Hawk (HALE)
- MQ-4C Triton (HALE)

General Atomics MQ-9 Reaper

Northrop Grumman MQ-4C Triton

Military Drone/UAVs and Capabilities (cont.)

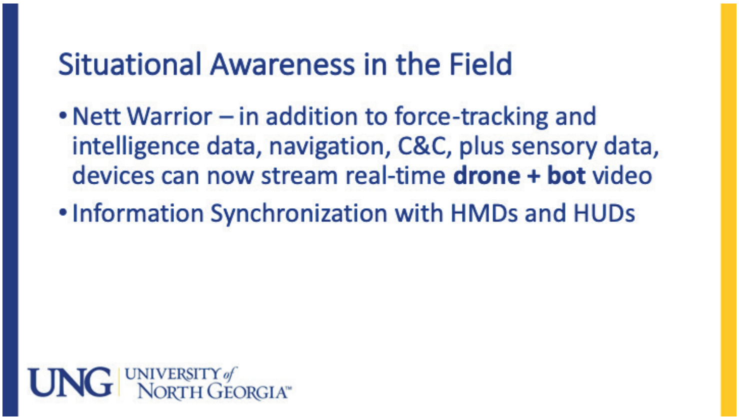
Mini/micro-drones for SA & more:

- FLIR Black Hornet PRS
- R80D SkyRaider
- RQ-11 Raven B

FLIR Black Hornet

R80D SkyRaider

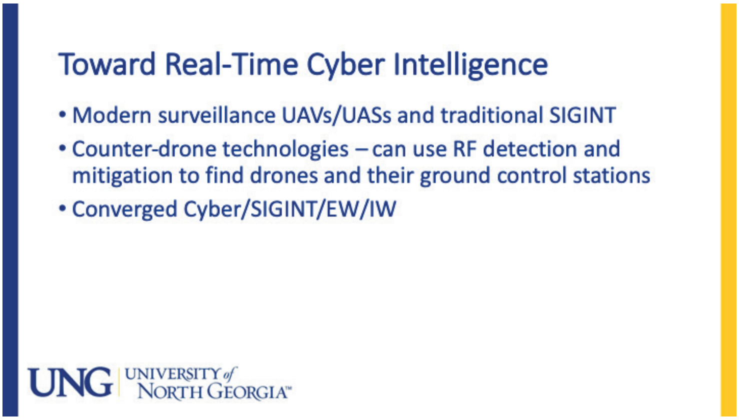
RQ-11 Raven B



Situational Awareness in the Field

- Nett Warrior – in addition to force-tracking and intelligence data, navigation, C&C, plus sensory data, devices can now stream real-time **drone + bot** video
- Information Synchronization with HMDs and HUDs

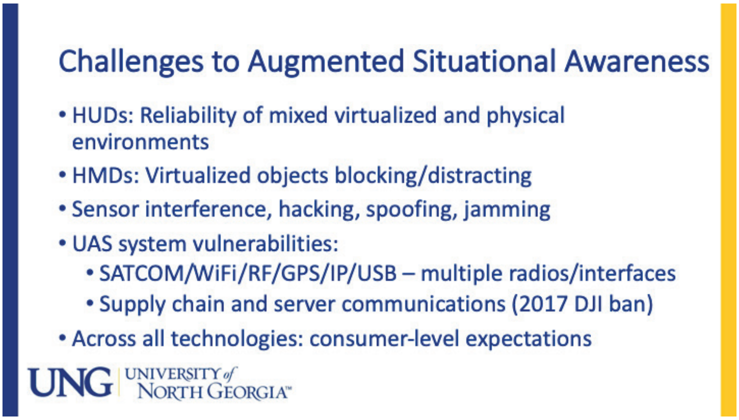
UNG UNIVERSITY of NORTH GEORGIA™



Toward Real-Time Cyber Intelligence

- Modern surveillance UAVs/UASs and traditional SIGINT
- Counter-drone technologies – can use RF detection and mitigation to find drones and their ground control stations
- Converged Cyber/SIGINT/EW/IW

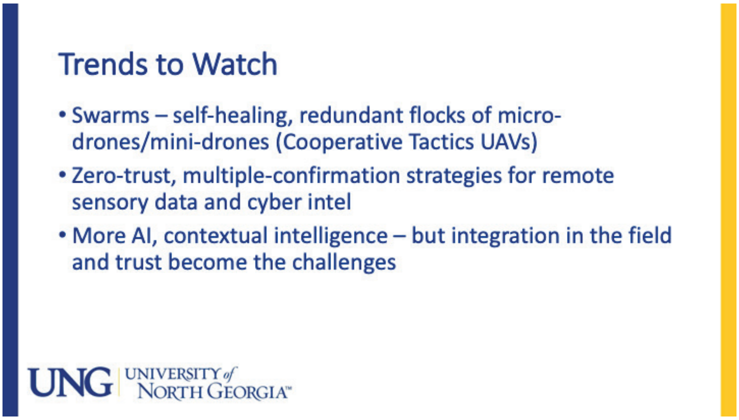
UNG UNIVERSITY of NORTH GEORGIA™



Challenges to Augmented Situational Awareness

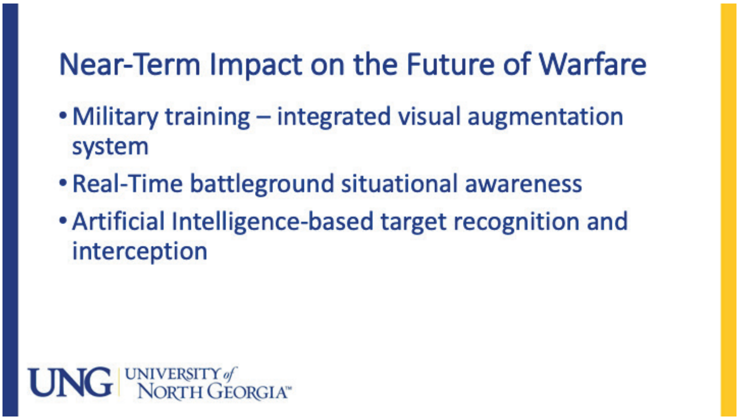
- HUDs: Reliability of mixed virtualized and physical environments
- HMDs: Virtualized objects blocking/distracting
- Sensor interference, hacking, spoofing, jamming
- UAS system vulnerabilities:
  - SATCOM/WiFi/RF/GPS/IP/USB – multiple radios/interfaces
  - Supply chain and server communications (2017 DJI ban)
- Across all technologies: consumer-level expectations

UNG UNIVERSITY of NORTH GEORGIA™



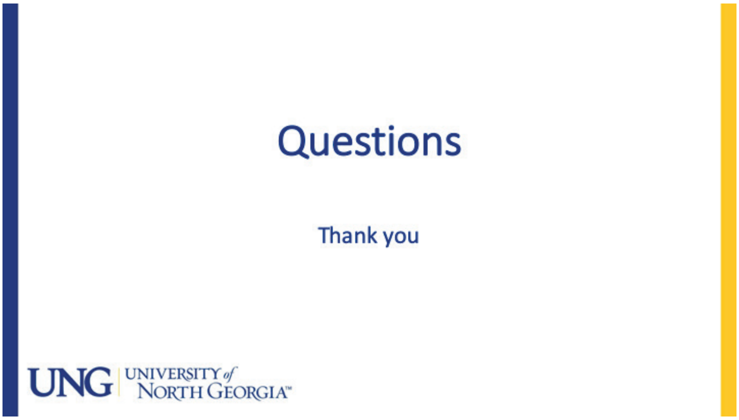
Trends to Watch

- Swarms – self-healing, redundant flocks of micro-drones/mini-drones (Cooperative Tactics UAVs)
- Zero-trust, multiple-confirmation strategies for remote sensory data and cyber intel
- More AI, contextual intelligence – but integration in the field and trust become the challenges



Near-Term Impact on the Future of Warfare

- Military training – integrated visual augmentation system
- Real-Time battleground situational awareness
- Artificial Intelligence-based target recognition and interception



Questions

Thank you

UNG Center for Cyber Operations Education

NSA/DHS National Center of Academic
Excellence in Cyber Defense
(CAE-CD) 2016-2021
Languages ★ Leadership ★ Cyber
http://www.ung.edu/cyber

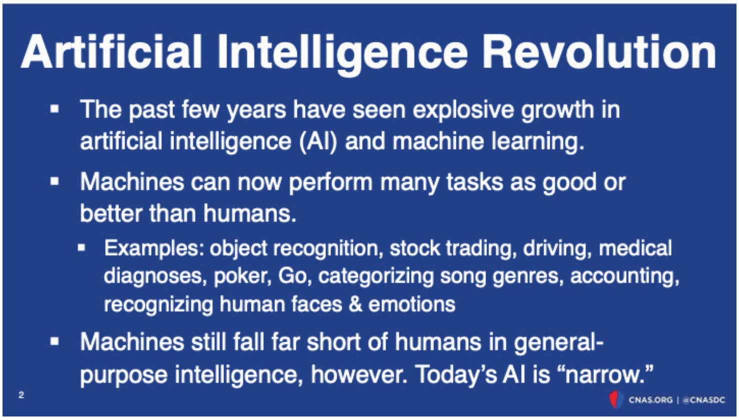
The Artificial Intelligence Revolution

Mr. Paul Scharre

Artificial Intelligence and Global Security

PAUL SCHARRE
SENIOR FELLOW AND DIRECTOR
TECHNOLOGY AND NATIONAL SECURITY PROGRAM

Celebrating 10 Years
CNAS

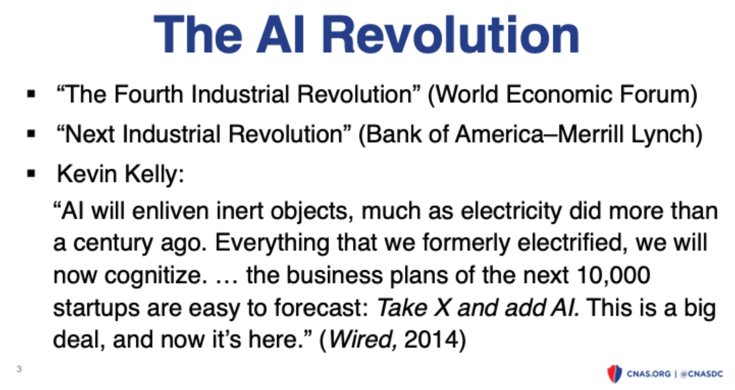


Artificial Intelligence Revolution

- The past few years have seen explosive growth in artificial intelligence (AI) and machine learning.
- Machines can now perform many tasks as good or better than humans.
  - Examples: object recognition, stock trading, driving, medical diagnoses, poker, Go, categorizing song genres, accounting, recognizing human faces & emotions
- Machines still fall far short of humans in general-purpose intelligence, however. Today's AI is "narrow."

2

CNAS.ORG | @CNASDC



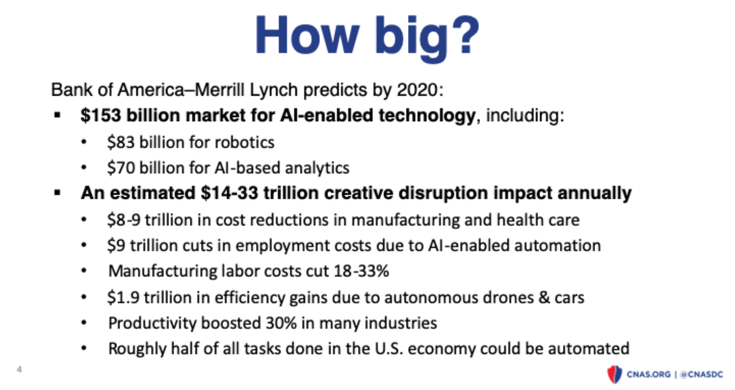
The AI Revolution

- "The Fourth Industrial Revolution" (World Economic Forum)
- "Next Industrial Revolution" (Bank of America–Merrill Lynch)
- Kevin Kelly:

  "AI will enliven inert objects, much as electricity did more than a century ago. Everything that we formerly electrified, we will now cognitize. … the business plans of the next 10,000 startups are easy to forecast: *Take X and add AI.* This is a big deal, and now it's here." (*Wired,* 2014)

3

CNAS.ORG | @CNASDC



How big?

Bank of America–Merrill Lynch predicts by 2020:

- **$153 billion market for AI-enabled technology**, including:
  - $83 billion for robotics
  - $70 billion for AI-based analytics
- **An estimated $14-33 trillion creative disruption impact annually**
  - $8-9 trillion in cost reductions in manufacturing and health care
  - $9 trillion cuts in employment costs due to AI-enabled automation
  - Manufacturing labor costs cut 18-33%
  - $1.9 trillion in efficiency gains due to autonomous drones & cars
  - Productivity boosted 30% in many industries
  - Roughly half of all tasks done in the U.S. economy could be automated

4

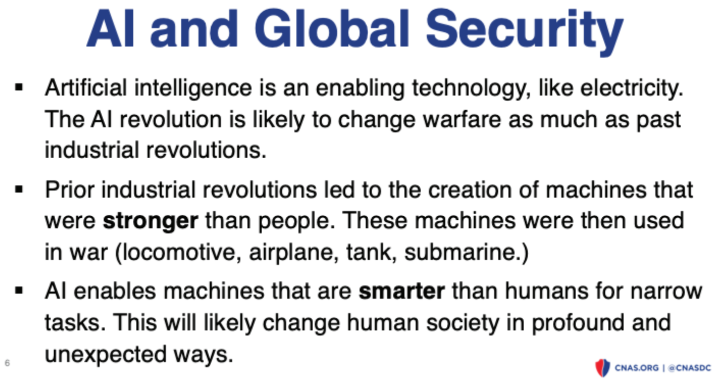
CNAS.ORG | @CNASDC

Betting Big on AI

5

5

CNAS.ORG | @CNASDC

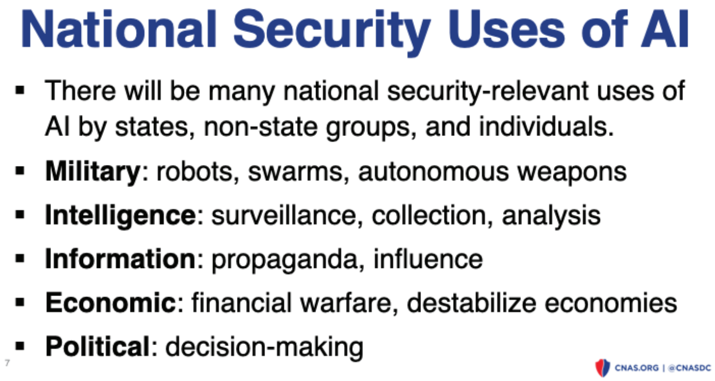


AI and Global Security

- Artificial intelligence is an enabling technology, like electricity. The AI revolution is likely to change warfare as much as past industrial revolutions.
- Prior industrial revolutions led to the creation of machines that were **stronger** than people. These machines were then used in war (locomotive, airplane, tank, submarine.)
- AI enables machines that are **smarter** than humans for narrow tasks. This will likely change human society in profound and unexpected ways.

6

CNAS.ORG | @CNASDC

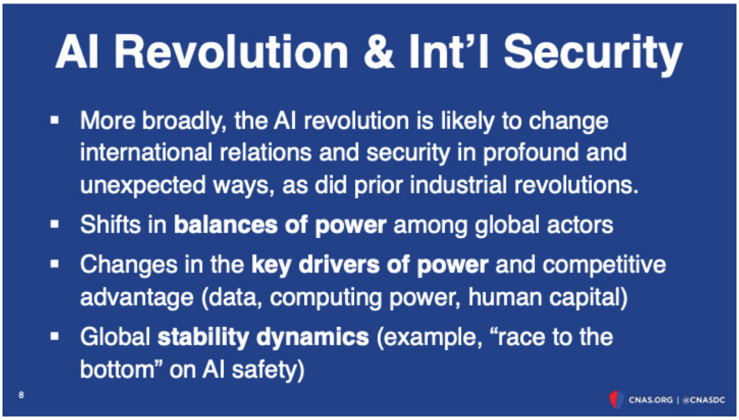


National Security Uses of AI

- There will be many national security-relevant uses of AI by states, non-state groups, and individuals.
- **Military**: robots, swarms, autonomous weapons
- **Intelligence**: surveillance, collection, analysis
- **Information**: propaganda, influence
- **Economic**: financial warfare, destabilize economies
- **Political**: decision-making

7

CNAS.ORG | @CNASDC

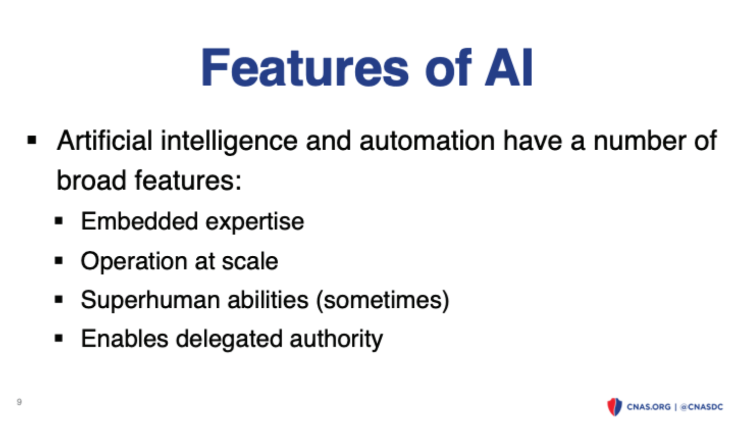


AI Revolution & Int'l Security

- More broadly, the AI revolution is likely to change international relations and security in profound and unexpected ways, as did prior industrial revolutions.
- Shifts in **balances of power** among global actors
- Changes in the **key drivers of power** and competitive advantage (data, computing power, human capital)
- Global **stability dynamics** (example, "race to the bottom" on AI safety)

8

CNAS.ORG | @CNASDC

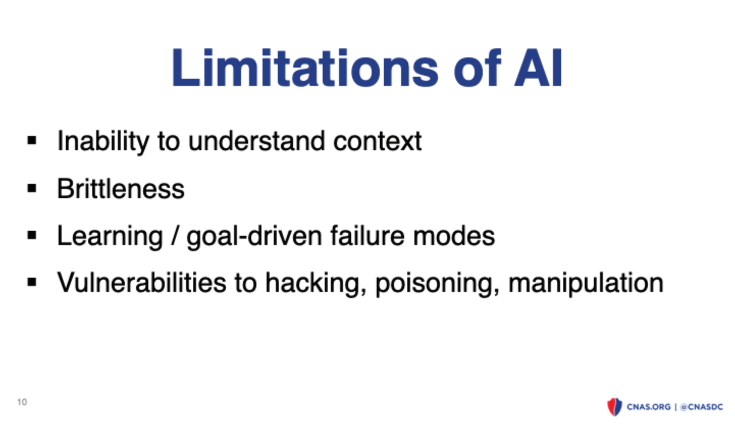


Features of AI

- Artificial intelligence and automation have a number of broad features:
  - Embedded expertise
  - Operation at scale
  - Superhuman abilities (sometimes)
  - Enables delegated authority

9

CNAS.ORG | @CNASDC

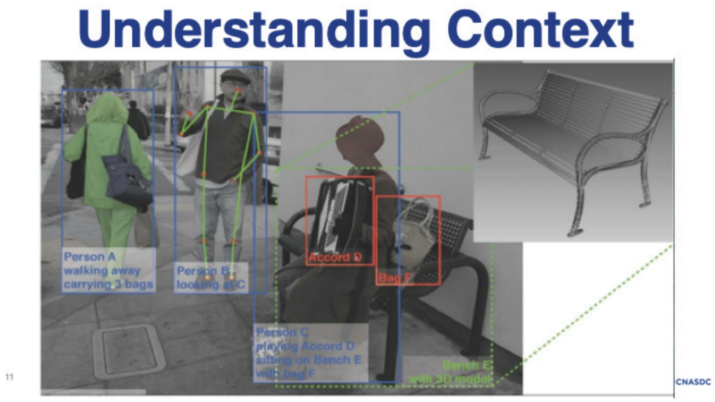


Limitations of AI

- Inability to understand context
- Brittleness
- Learning / goal-driven failure modes
- Vulnerabilities to hacking, poisoning, manipulation

10

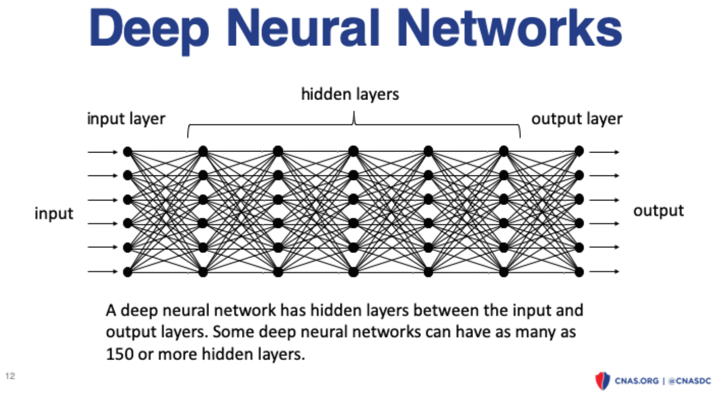
CNAS.ORG | @CNASDC



Understanding Context

11

CNASDC

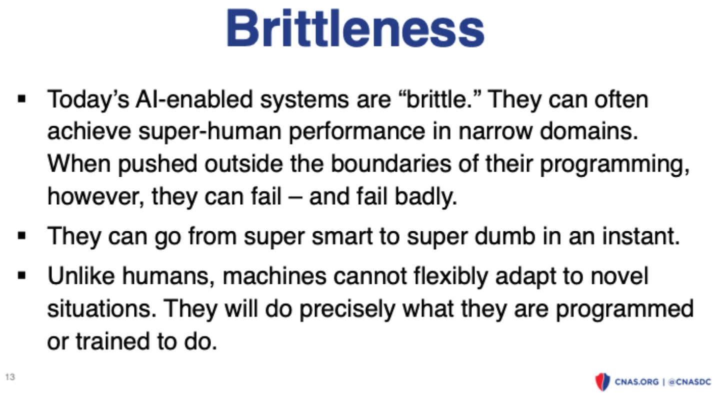


Deep Neural Networks

A deep neural network has hidden layers between the input and output layers. Some deep neural networks can have as many as 150 or more hidden layers.

12

CNAS.ORG | @CNASDC



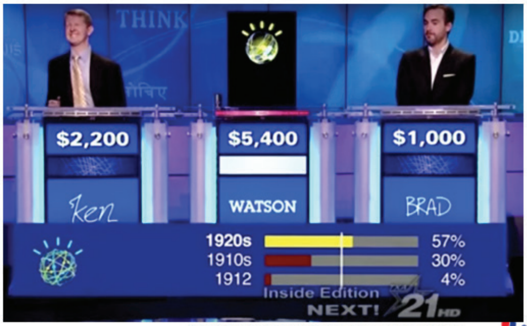
Brittleness

- Today's AI-enabled systems are "brittle." They can often achieve super-human performance in narrow domains. When pushed outside the boundaries of their programming, however, they can fail – and fail badly.
- They can go from super smart to super dumb in an instant.
- Unlike humans, machines cannot flexibly adapt to novel situations. They will do precisely what they are programmed or trained to do.

13

CNAS.ORG | @CNASDC

Watson on Jeopardy



14

http://ytcropper.com/cropped/LR589c0d765065c

CNAS.ORG | @CNASDC

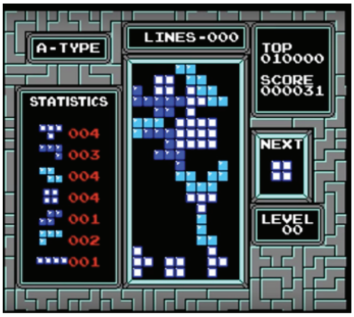
New Failure Modes

- New failure modes in machine learning or goal-driven systems:
  - Improperly specified objective function
  - Reward hacking
  - Bias – distributional shift in data
- Lack of transparency a problem for some applications (Amazon resume sifting AI)

15

CNAS.ORG | @CNASDC

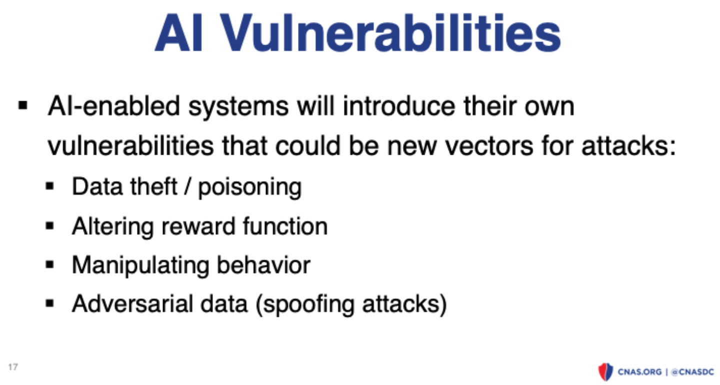
Learning the Wrong Thing



16

http://ytcropper.com/cropped/xO59bf593b9c715

CNAS.ORG | @CNASDC

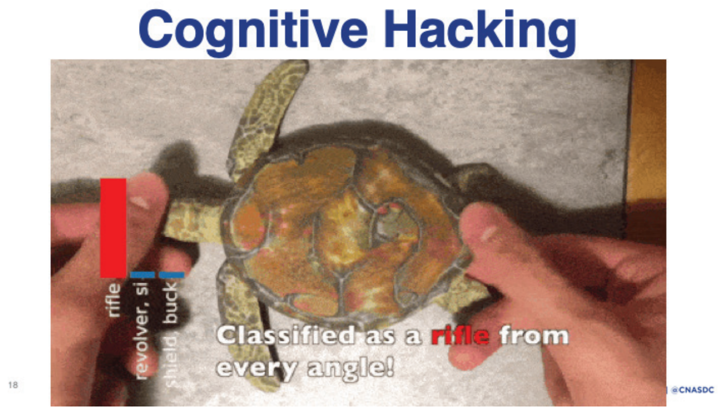


AI Vulnerabilities

- AI-enabled systems will introduce their own vulnerabilities that could be new vectors for attacks:
  - Data theft / poisoning
  - Altering reward function
  - Manipulating behavior
  - Adversarial data (spoofing attacks)

17

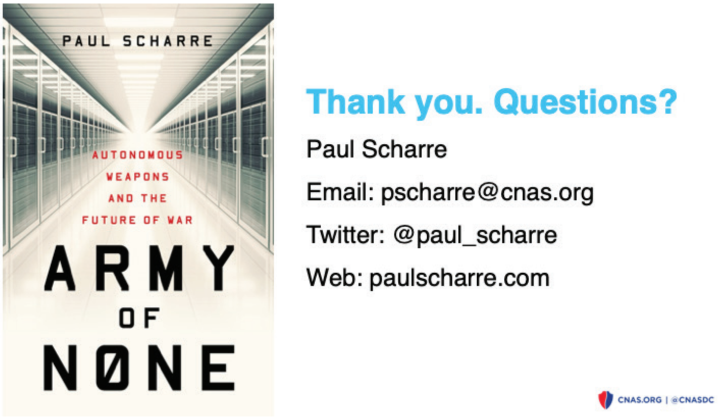
CNAS.ORG | @CNASDC



Cognitive Hacking

18

@CNASDC



PAUL SCHARRE
AUTONOMOUS WEAPONS AND THE FUTURE OF WAR
ARMY OF NØNE

Thank you. Questions?

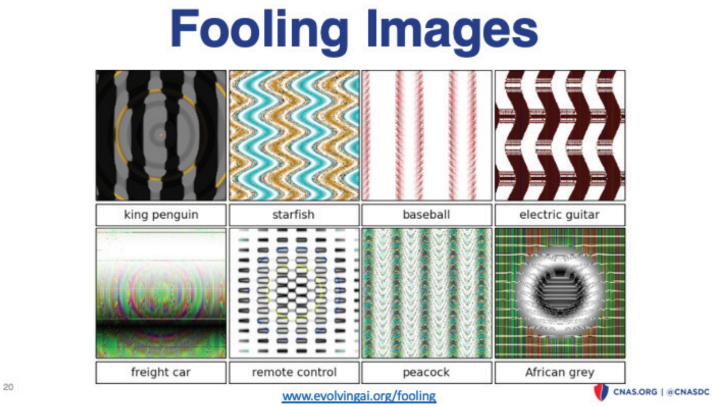
Paul Scharre

Email: pscharre@cnas.org

Twitter: @paul_scharre

Web: paulscharre.com

CNAS.ORG | @CNASDC

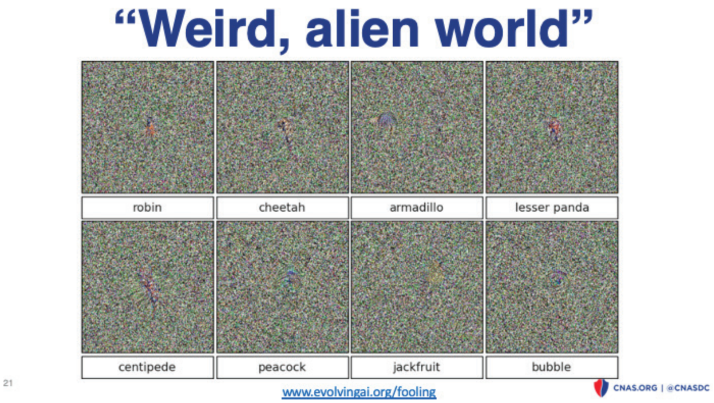


Fooling Images

www.evolvingai.org/fooling

20

CNAS.ORG | @CNASDC

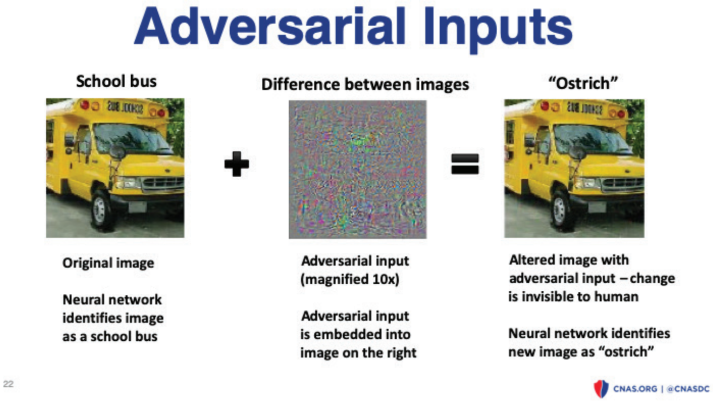


“Weird, alien world”

www.evolvingai.org/fooling

21

CNAS.ORG | @CNASDC



Adversarial Inputs

Original image

Neural network identifies image as a school bus

Adversarial input (magnified 10x)

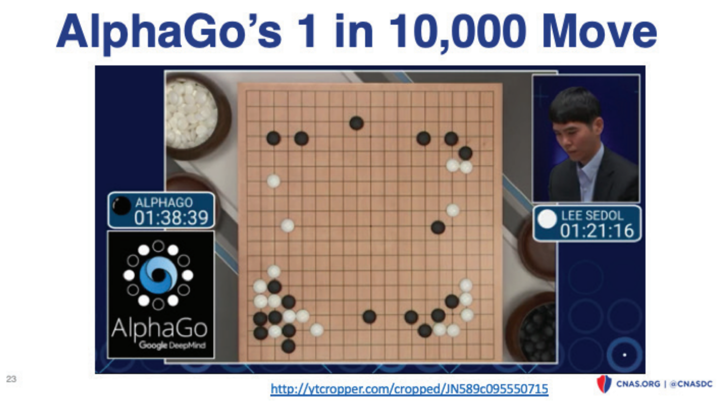
Adversarial input is embedded into image on the right

Altered image with adversarial input – change is invisible to human

Neural network identifies new image as “ostrich”

22

CNAS.ORG | @CNASDC

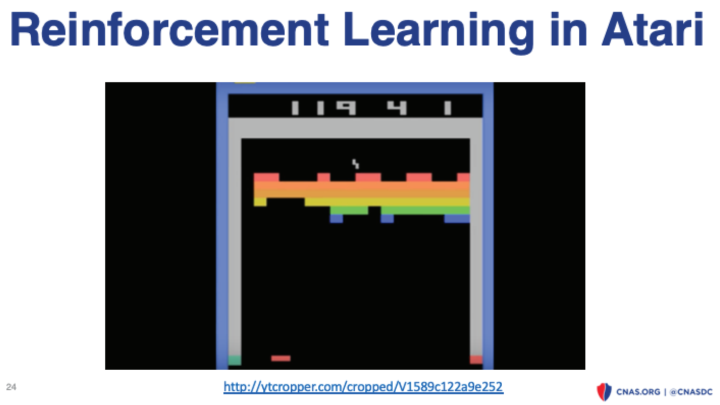


AlphaGo’s 1 in 10,000 Move

23

http://ytcropper.com/cropped/JN589c095550715

CNAS.ORG | @CNASDC

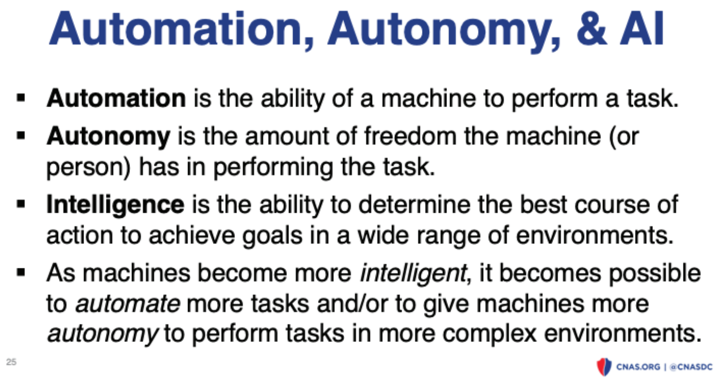


Reinforcement Learning in Atari

24

http://ytcropper.com/cropped/V1589c122a9e252

CNAS.ORG | @CNASDC



Automation, Autonomy, & AI

- **Automation** is the ability of a machine to perform a task.
- **Autonomy** is the amount of freedom the machine (or person) has in performing the task.
- **Intelligence** is the ability to determine the best course of action to achieve goals in a wide range of environments.
- As machines become more *intelligent*, it becomes possible to *automate* more tasks and/or to give machines more *autonomy* to perform tasks in more complex environments.

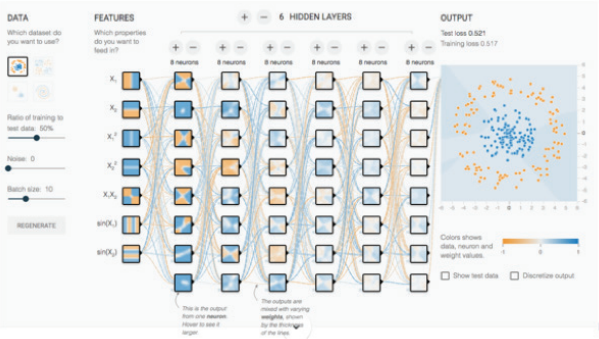
25

CNAS.ORG | @CNASDC

Machine Learning

- Learning systems do not need to follow rigid rules
- However, machine learning with giant datasets and huge, inscrutable black box deep neural networks can lead to some surprises

playground.tensorflow.org



Ratio of training to test data: 50%

Noise: 0

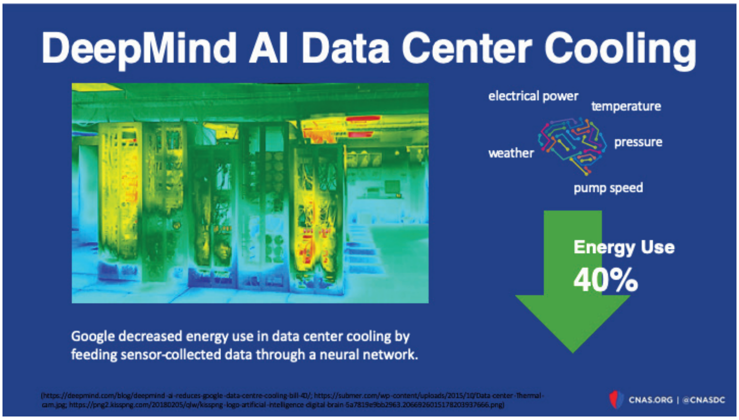
Batch size: 10

Test loss 0.521

Training loss 0.517

This is the output from one **neuron**. Hover to see it larger.

The outputs are mixed with varying **weights**, shown by the thickness of the lines.



DeepMind AI Data Center Cooling

electrical power

temperature

weather

pressure

pump speed

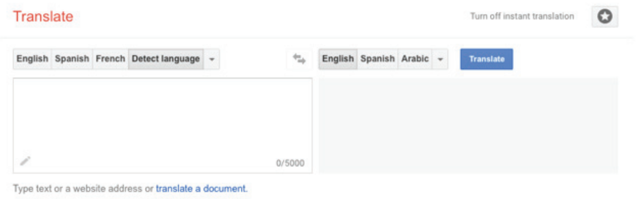
Energy Use

40%

Google decreased energy use in data center cooling by feeding sensor-collected data through a neural network.

(https://deepmind.com/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-40/; https://submer.com/wp-content/uploads/2015/10/Data-center-Thermal-cam.jpg; https://png2.kisspng.com/20180205/qlw/kisspng-logo-artificial-intelligence-digital-brain-5a7819e9bb2963.2066926015178203937666.png)

Google Translate



Translate

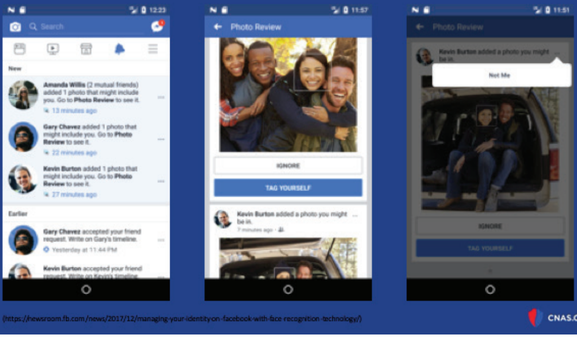
Turn off instant translation

Type text or a website address or translate a document.

29

CNAS.ORG | @CNASDC

Facebook Facial Recognition



Amanda Willis (2 mutual friends) added 1 photo that might include you. Go to Photo Review to see it.
13 minutes ago

Gary Chavez added 1 photo that might include you. Go to Photo Review to see it.
22 minutes ago

Kevin Burton added 1 photo that might include you. Go to Photo Review to see it.
27 minutes ago

Gary Chavez accepted your friend request. Write on Gary's timeline.
Yesterday at 11:44 PM

Kevin Burton accepted your friend request. Write on Kevin's timeline.

Kevin Burton added a photo you might be in.
7 minutes ago

(https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/)

CNAS.ORG | @CNASDC

Home Entry Facial Recognition

31

(https://www.wisenetlife.com/en-us/product/SmartCam/SNH-V6435DN/feature/)

CNAS.ORG | @CNASDC

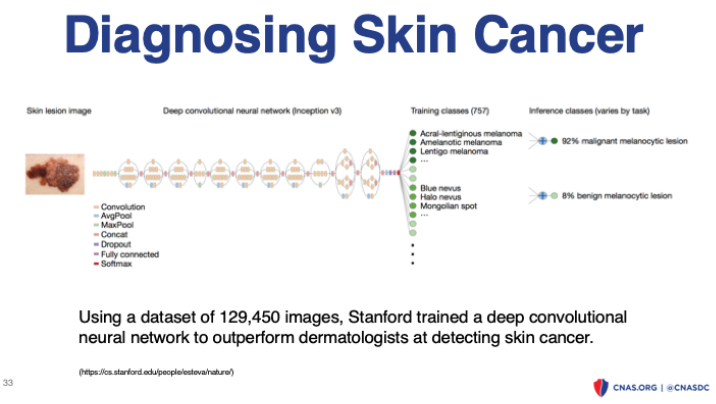
Lyrebird Synthetic Audio

Lyrebird creates digital vocal avatars using one minute of natural voice recording.

(Getty Images; https://lyrebird.ai/)

32

CNAS.ORG | @CNASDC



Diagnosing Skin Cancer

Using a dataset of 129,450 images, Stanford trained a deep convolutional neural network to outperform dermatologists at detecting skin cancer.

(https://cs.stanford.edu/people/esteva/nature/)

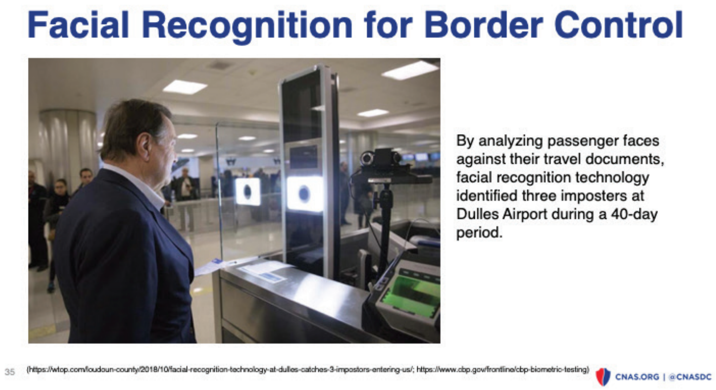
33

CNAS.ORG | @CNASDC

Anduril's Border Detection

(https://www.wired.com/story/palmer-luckey-anduril-border-wall/)

CNAS.ORG | @CNASDC

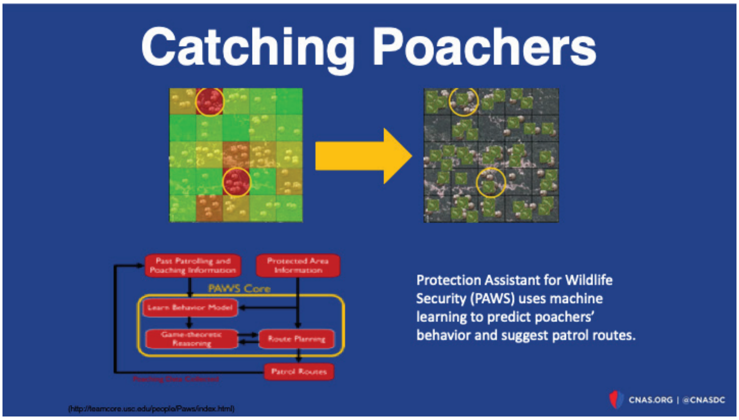


Facial Recognition for Border Control

By analyzing passenger faces against their travel documents, facial recognition technology identified three imposters at Dulles Airport during a 40-day period.

35 (https://wtop.com/loudoun-county/2018/10/facial-recognition-technology-at-dulles-catches-3-impostors-entering-us/; https://www.cbp.gov/frontline/cbp-biometric-testing)

CNAS.ORG | @CNASDC



Catching Poachers

Past Patrolling and Poaching Information

Protected Area Information

PAWS Core

Learn Behavior Model

Game-theoretic Reasoning

Route Planning

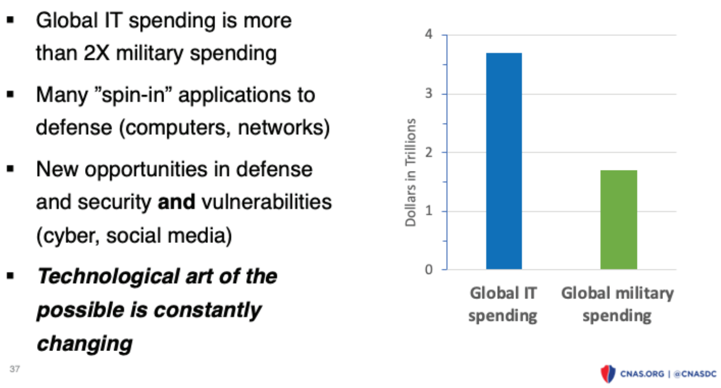
Patrol Routes

Poaching Data Collected

Protection Assistant for Wildlife Security (PAWS) uses machine learning to predict poachers' behavior and suggest patrol routes.

(http://teamcore.usc.edu/people/Paws/index.html)

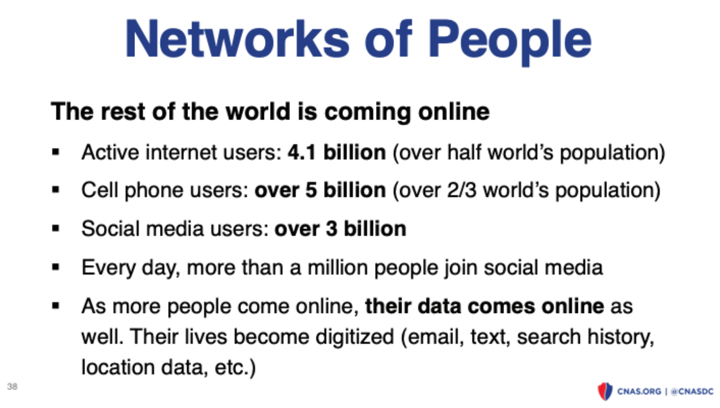
CNAS.ORG | @CNASDC



- Global IT spending is more than 2X military spending
- Many "spin-in" applications to defense (computers, networks)
- New opportunities in defense and security **and** vulnerabilities (cyber, social media)
- ***Technological art of the possible is constantly changing***

37

CNAS.ORG | @CNASDC



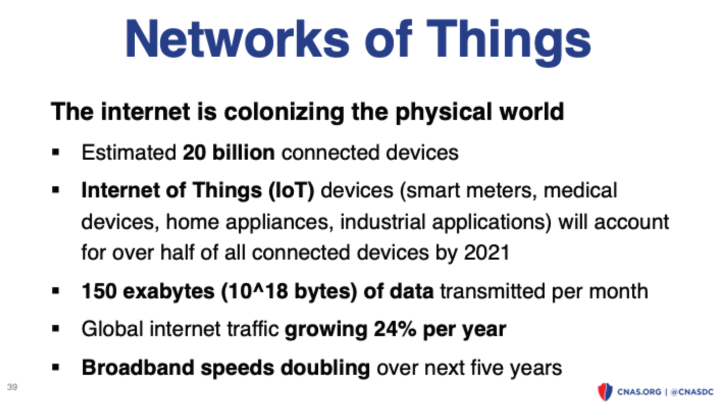
Networks of People

The rest of the world is coming online

- Active internet users: **4.1 billion** (over half world's population)
- Cell phone users: **over 5 billion** (over 2/3 world's population)
- Social media users: **over 3 billion**
- Every day, more than a million people join social media
- As more people come online, **their data comes online** as well. Their lives become digitized (email, text, search history, location data, etc.)

38

CNAS.ORG | @CNASDC



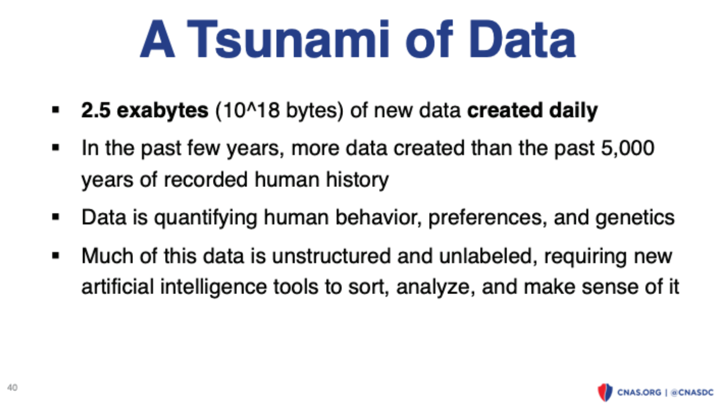
Networks of Things

The internet is colonizing the physical world

- Estimated **20 billion** connected devices
- **Internet of Things (IoT)** devices (smart meters, medical devices, home appliances, industrial applications) will account for over half of all connected devices by 2021
- **150 exabytes (10^18 bytes) of data** transmitted per month
- Global internet traffic **growing 24% per year**
- **Broadband speeds doubling** over next five years

39

CNAS.ORG | @CNASDC

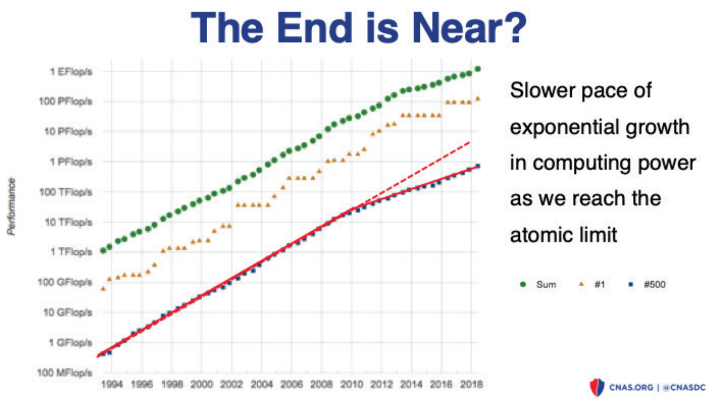


A Tsunami of Data

- **2.5 exabytes** (10^18 bytes) of new data **created daily**
- In the past few years, more data created than the past 5,000 years of recorded human history
- Data is quantifying human behavior, preferences, and genetics
- Much of this data is unstructured and unlabeled, requiring new artificial intelligence tools to sort, analyze, and make sense of it

40

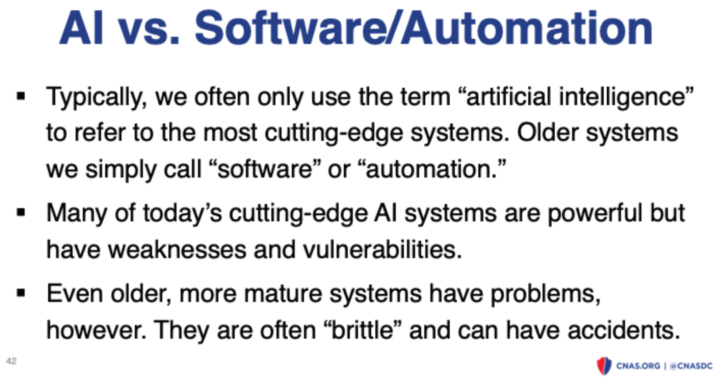
CNAS.ORG | @CNASDC



The End is Near?

Slower pace of exponential growth in computing power as we reach the atomic limit

CNAS.ORG | @CNASDC

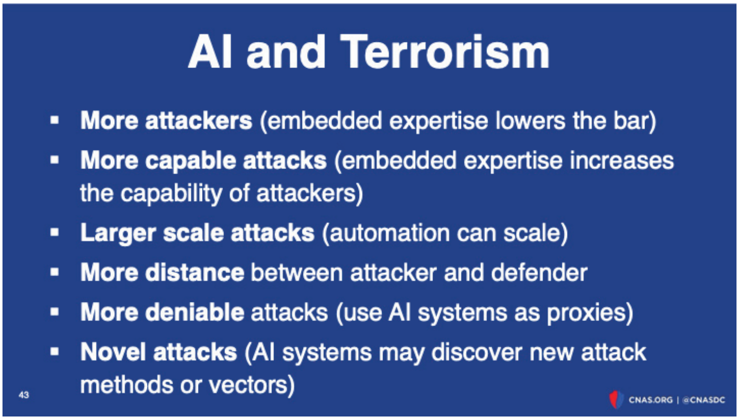


AI vs. Software/Automation

- Typically, we often only use the term “artificial intelligence” to refer to the most cutting-edge systems. Older systems we simply call “software” or “automation.”
- Many of today’s cutting-edge AI systems are powerful but have weaknesses and vulnerabilities.
- Even older, more mature systems have problems, however. They are often “brittle” and can have accidents.

42

CNAS.ORG | @CNASDC

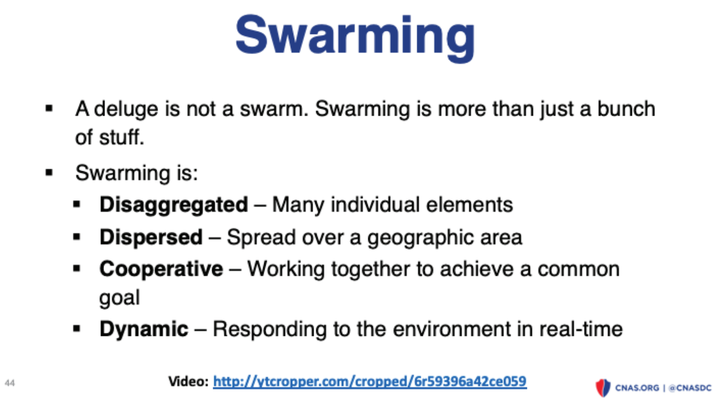


AI and Terrorism

- **More attackers** (embedded expertise lowers the bar)
- **More capable attacks** (embedded expertise increases the capability of attackers)
- **Larger scale attacks** (automation can scale)
- **More distance** between attacker and defender
- **More deniable** attacks (use AI systems as proxies)
- **Novel attacks** (AI systems may discover new attack methods or vectors)

43

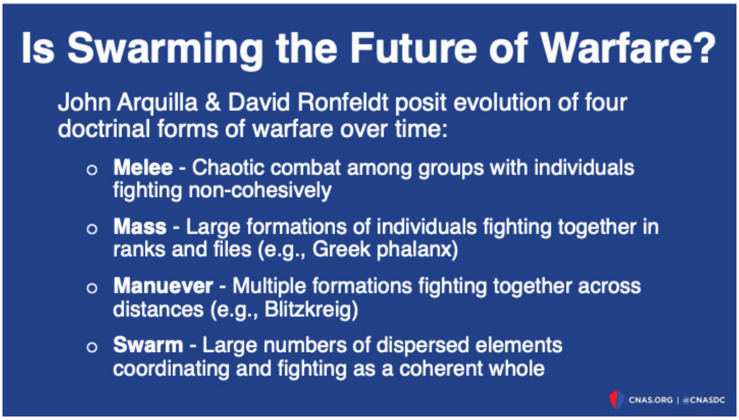
CNAS.ORG | @CNASDC



Swarming

- A deluge is not a swarm. Swarming is more than just a bunch of stuff.
- Swarming is:
  - **Disaggregated** – Many individual elements
  - **Dispersed** – Spread over a geographic area
  - **Cooperative** – Working together to achieve a common goal
  - **Dynamic** – Responding to the environment in real-time

44 Video: http://ytcropper.com/cropped/6r59396a42ce059 CNAS.ORG | @CNASDC

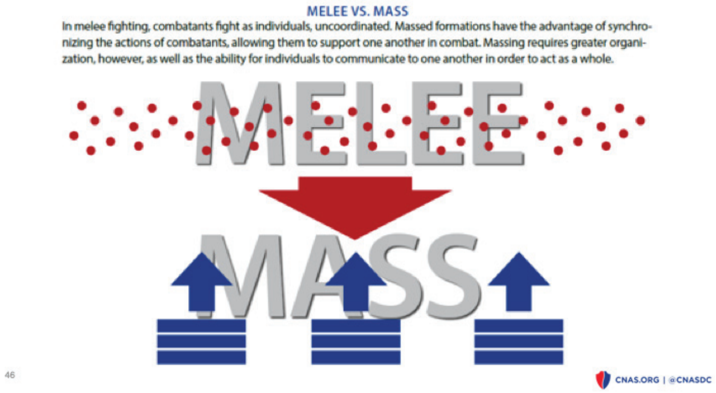


Is Swarming the Future of Warfare?

John Arquilla & David Ronfeldt posit evolution of four doctrinal forms of warfare over time:

- **Melee** - Chaotic combat among groups with individuals fighting non-cohesively
- **Mass** - Large formations of individuals fighting together in ranks and files (e.g., Greek phalanx)
- **Manuever** - Multiple formations fighting together across distances (e.g., Blitzkrieg)
- **Swarm** - Large numbers of dispersed elements coordinating and fighting as a coherent whole

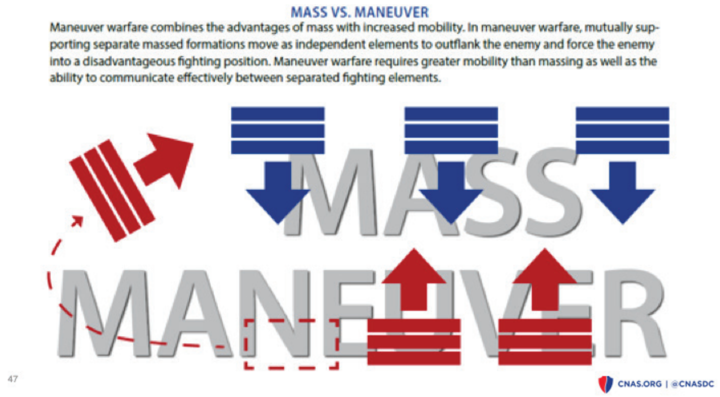
CNAS.ORG | @CNASDC



MELEE VS. MASS

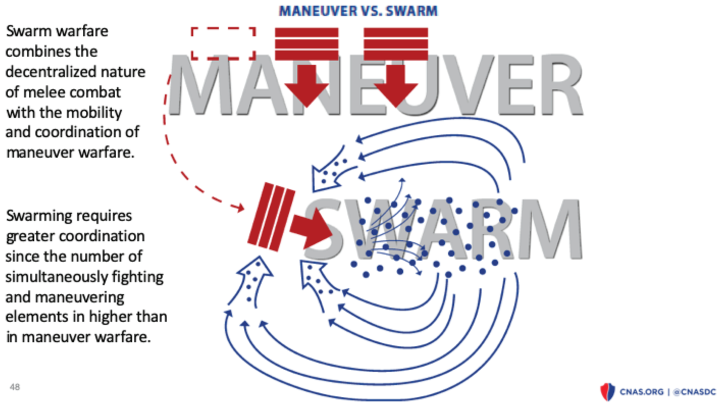
In melee fighting, combatants fight as individuals, uncoordinated. Massed formations have the advantage of synchronizing the actions of combatants, allowing them to support one another in combat. Massing requires greater organization, however, as well as the ability for individuals to communicate to one another in order to act as a whole.

46 CNAS.ORG | @CNASDC



MASS VS. MANEUVER

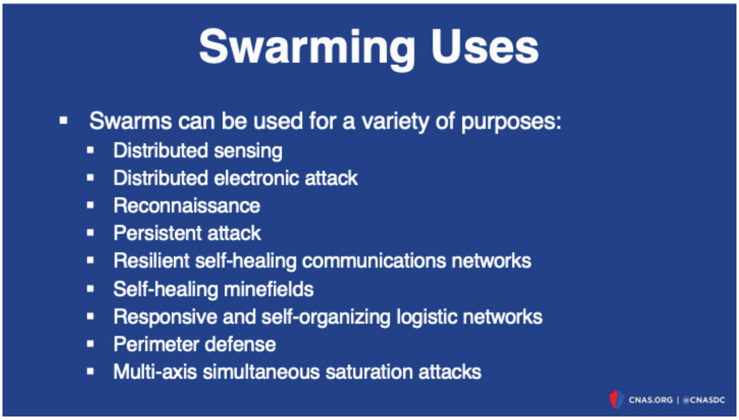
Maneuver warfare combines the advantages of mass with increased mobility. In maneuver warfare, mutually supporting separate massed formations move as independent elements to outflank the enemy and force the enemy into a disadvantageous fighting position. Maneuver warfare requires greater mobility than massing as well as the ability to communicate effectively between separated fighting elements.



MANEUVER VS. SWARM

Swarm warfare combines the decentralized nature of melee combat with the mobility and coordination of maneuver warfare.

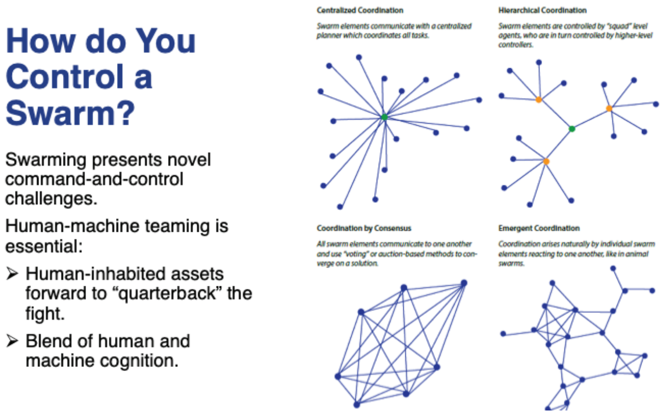
Swarming requires greater coordination since the number of simultaneously fighting and maneuvering elements in higher than in maneuver warfare.



Swarming Uses

- Swarms can be used for a variety of purposes:
  - Distributed sensing
  - Distributed electronic attack
  - Reconnaissance
  - Persistent attack
  - Resilient self-healing communications networks
  - Self-healing minefields
  - Responsive and self-organizing logistic networks
  - Perimeter defense
  - Multi-axis simultaneous saturation attacks

CNAS.ORG | @CNASDC



How do You Control a Swarm?

Swarming presents novel command-and-control challenges.

Human-machine teaming is essential:

- Human-inhabited assets forward to “quarterback” the fight.
- Blend of human and machine cognition.

Centralized Coordination

Swarm elements communicate with a centralized planner which coordinates all tasks.

Hierarchical Coordination

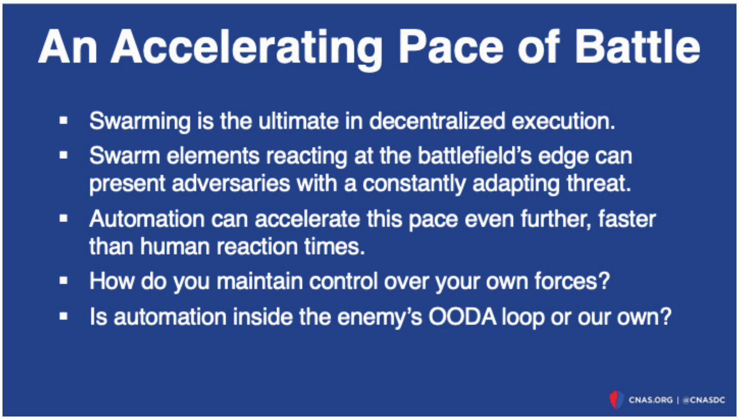
Swarm elements are controlled by “squad” level agents, who are in turn controlled by higher-level controllers.

Coordination by Consensus

All swarm elements communicate to one another and use “voting” or auction-based methods to converge on a solution.

Emergent Coordination

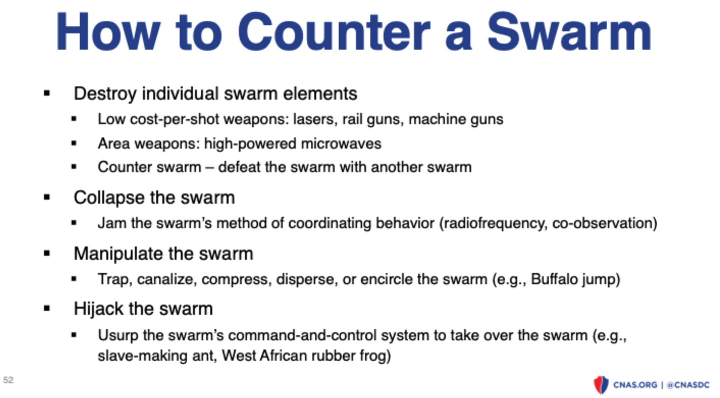
Coordination arises naturally by individual swarm elements reacting to one another, like in animal swarms.



An Accelerating Pace of Battle

- Swarming is the ultimate in decentralized execution.
- Swarm elements reacting at the battlefield’s edge can present adversaries with a constantly adapting threat.
- Automation can accelerate this pace even further, faster than human reaction times.
- How do you maintain control over your own forces?
- Is automation inside the enemy’s OODA loop or our own?

CNAS.ORG | @CNASDC

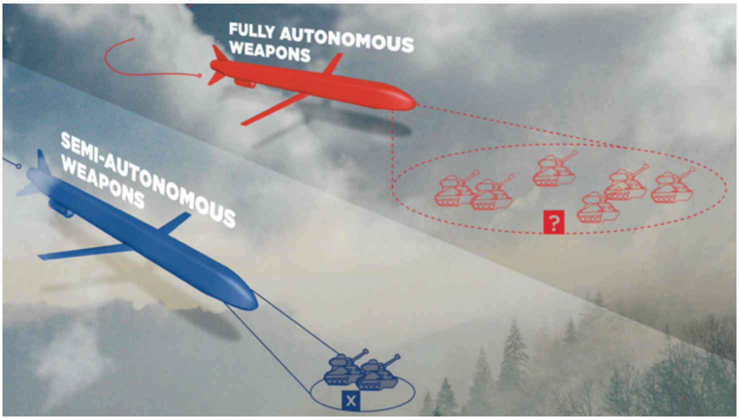


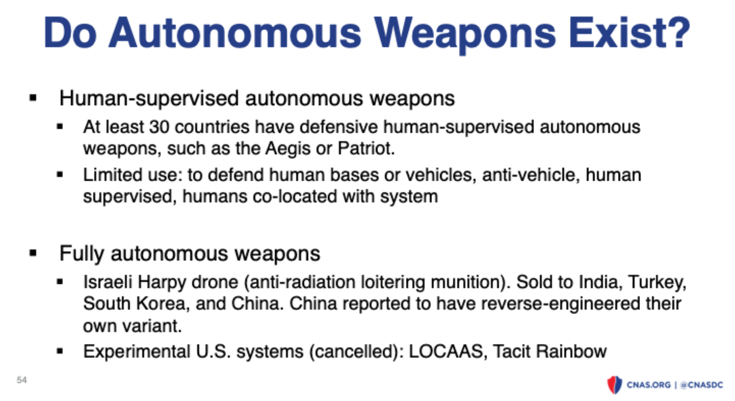
How to Counter a Swarm

- Destroy individual swarm elements
  - Low cost-per-shot weapons: lasers, rail guns, machine guns
  - Area weapons: high-powered microwaves
  - Counter swarm – defeat the swarm with another swarm
- Collapse the swarm
  - Jam the swarm’s method of coordinating behavior (radiofrequency, co-observation)
- Manipulate the swarm
  - Trap, canalize, compress, disperse, or encircle the swarm (e.g., Buffalo jump)
- Hijack the swarm
  - Usurp the swarm’s command-and-control system to take over the swarm (e.g., slave-making ant, West African rubber frog)

52

CNAS.ORG | @CNASDC



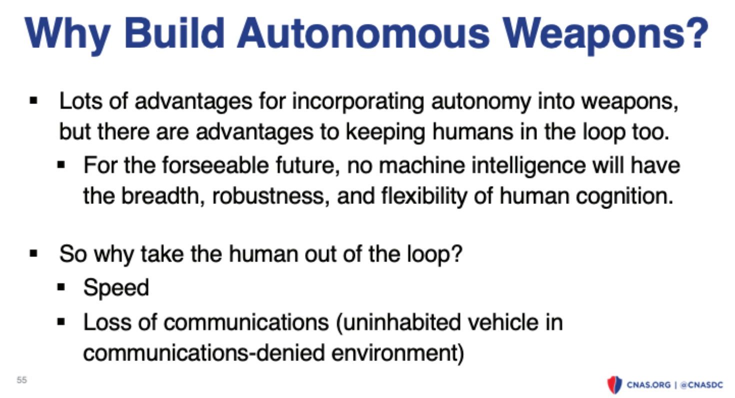


Do Autonomous Weapons Exist?

- Human-supervised autonomous weapons
  - At least 30 countries have defensive human-supervised autonomous weapons, such as the Aegis or Patriot.
  - Limited use: to defend human bases or vehicles, anti-vehicle, human supervised, humans co-located with system
- Fully autonomous weapons
  - Israeli Harpy drone (anti-radiation loitering munition). Sold to India, Turkey, South Korea, and China. China reported to have reverse-engineered their own variant.
  - Experimental U.S. systems (cancelled): LOCAAS, Tacit Rainbow

54

CNAS.ORG | @CNASDC

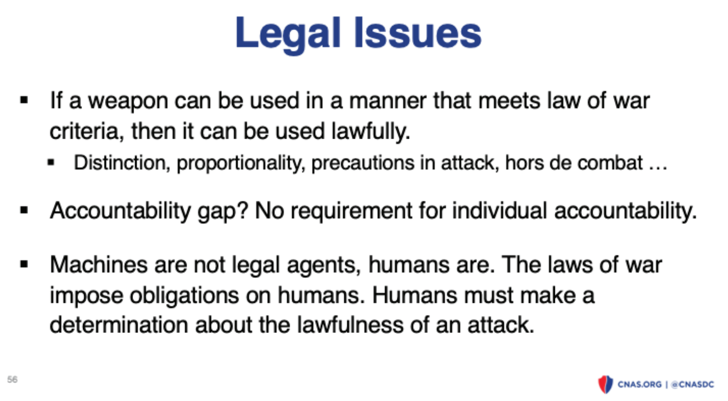


Why Build Autonomous Weapons?

- Lots of advantages for incorporating autonomy into weapons, but there are advantages to keeping humans in the loop too.
  - For the forseeable future, no machine intelligence will have the breadth, robustness, and flexibility of human cognition.
- So why take the human out of the loop?
  - Speed
  - Loss of communications (uninhabited vehicle in communications-denied environment)

55

CNAS.ORG | @CNASDC

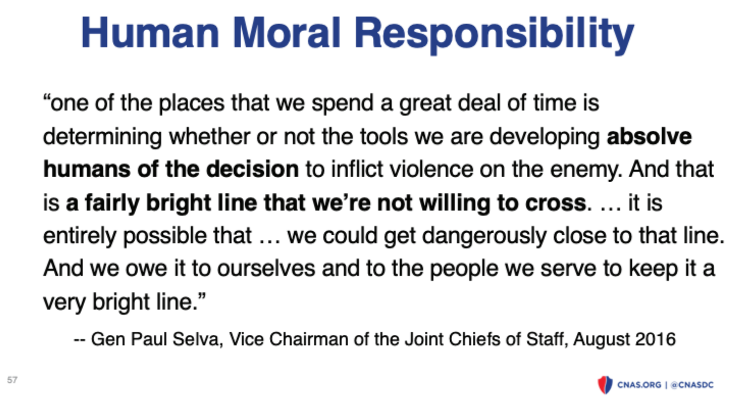


Legal Issues

- If a weapon can be used in a manner that meets law of war criteria, then it can be used lawfully.
  - Distinction, proportionality, precautions in attack, hors de combat …
- Accountability gap? No requirement for individual accountability.
- Machines are not legal agents, humans are. The laws of war impose obligations on humans. Humans must make a determination about the lawfulness of an attack.

56

CNAS.ORG | @CNASDC



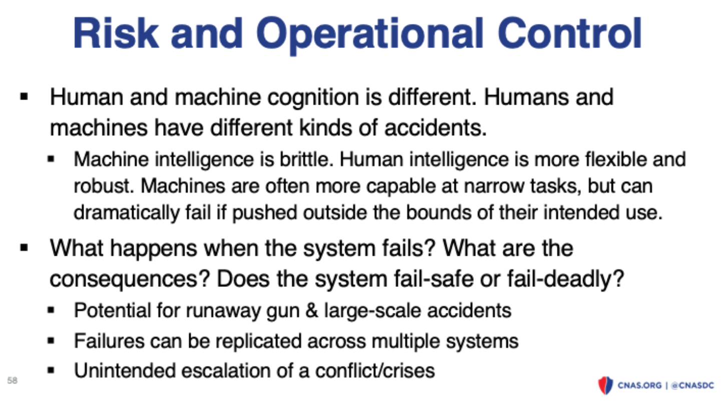
Human Moral Responsibility

"one of the places that we spend a great deal of time is determining whether or not the tools we are developing **absolve humans of the decision** to inflict violence on the enemy. And that is **a fairly bright line that we're not willing to cross**. … it is entirely possible that … we could get dangerously close to that line. And we owe it to ourselves and to the people we serve to keep it a very bright line."

-- Gen Paul Selva, Vice Chairman of the Joint Chiefs of Staff, August 2016

57

CNAS.ORG | @CNASDC

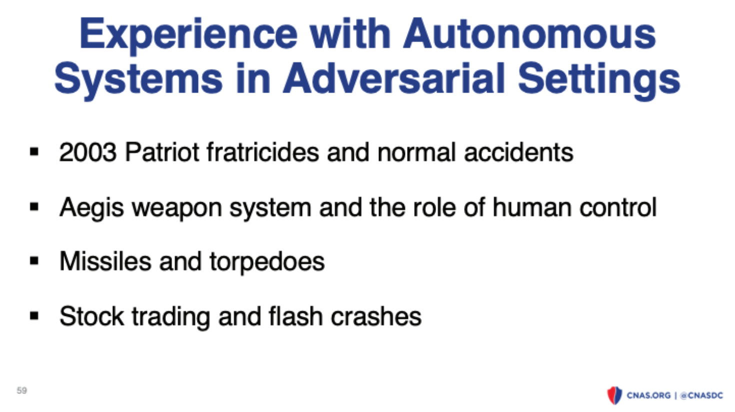


Risk and Operational Control

- Human and machine cognition is different. Humans and machines have different kinds of accidents.
  - Machine intelligence is brittle. Human intelligence is more flexible and robust. Machines are often more capable at narrow tasks, but can dramatically fail if pushed outside the bounds of their intended use.
- What happens when the system fails? What are the consequences? Does the system fail-safe or fail-deadly?
  - Potential for runaway gun & large-scale accidents
  - Failures can be replicated across multiple systems
  - Unintended escalation of a conflict/crises

58

CNAS.ORG | @CNASDC

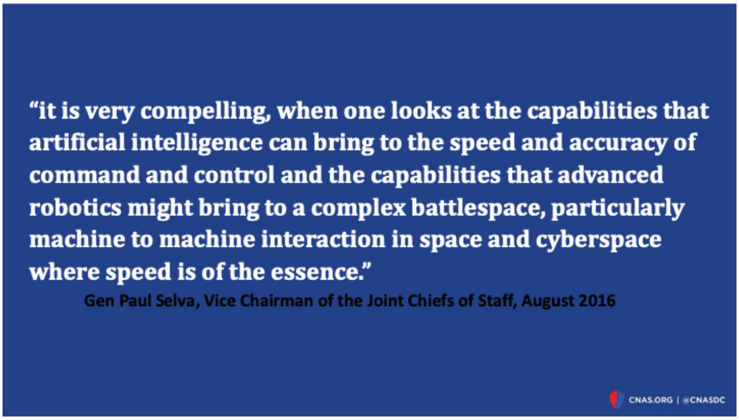


Experience with Autonomous Systems in Adversarial Settings

- 2003 Patriot fratricides and normal accidents
- Aegis weapon system and the role of human control
- Missiles and torpedoes
- Stock trading and flash crashes

59

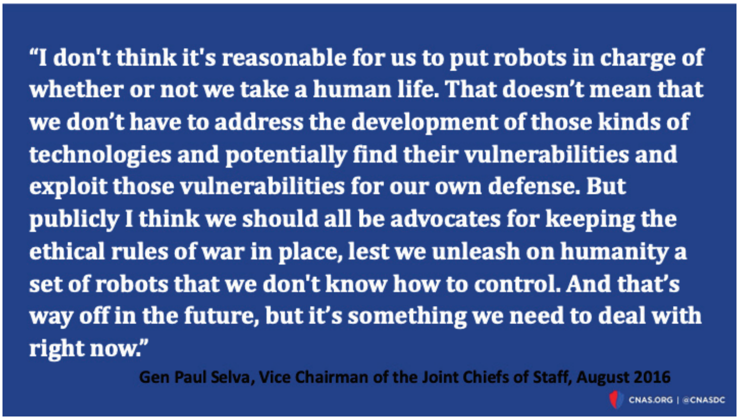
CNAS.ORG | @CNASDC



"it is very compelling, when one looks at the capabilities that artificial intelligence can bring to the speed and accuracy of command and control and the capabilities that advanced robotics might bring to a complex battlespace, particularly machine to machine interaction in space and cyberspace where speed is of the essence."

Gen Paul Selva, Vice Chairman of the Joint Chiefs of Staff, August 2016

CNAS.ORG | @CNASDC



"I don't think it's reasonable for us to put robots in charge of whether or not we take a human life. That doesn't mean that we don't have to address the development of those kinds of technologies and potentially find their vulnerabilities and exploit those vulnerabilities for our own defense. But publicly I think we should all be advocates for keeping the ethical rules of war in place, lest we unleash on humanity a set of robots that we don't know how to control. And that's way off in the future, but it's something we need to deal with right now."

Gen Paul Selva, Vice Chairman of the Joint Chiefs of Staff, August 2016

CNAS.ORG | @CNASDC

Leading Humans in the Age of AI: Why We Need Integrator Leaders

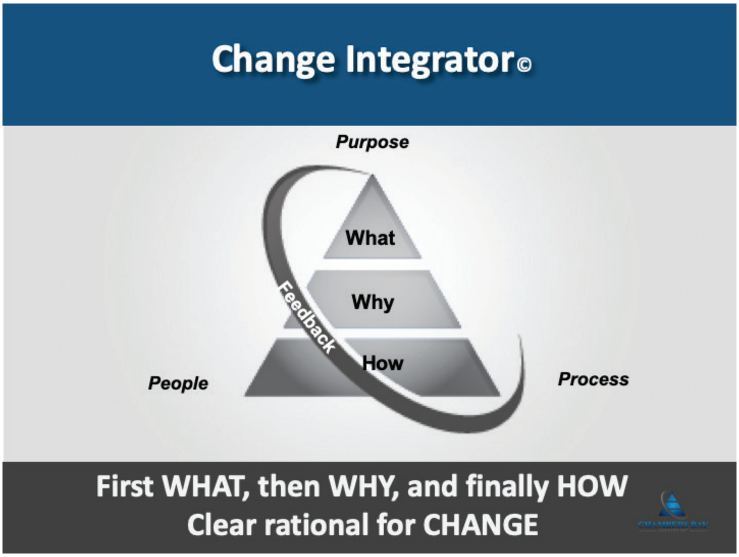
Bruce LaRue, Ph.D. and Jim Solomon

CHAMBERS BAY
INSTITUTE
Leading Humans in the Age of AI
Why We Need Integrator Leaders

LEADING IN THE AGE OF AI REQUIRES THAT YOU LEARN TO SEE POSSIBILITIES WHERE OTHERS SEE OBSTACLES, INSPIRING OTHERS WITH FRESH VISIONS OF THE FUTURE.

Change How You See the World

Escape the Prison of the Known



Change Integrator©

Purpose

What

Why

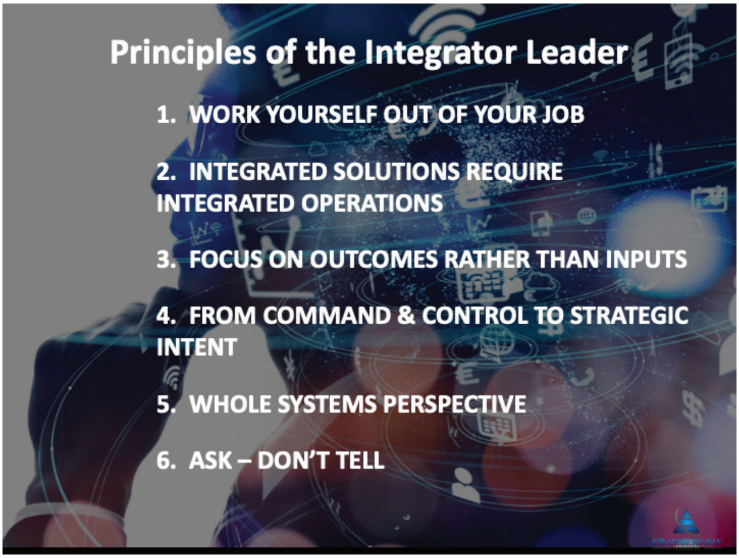
How

Feedback

People

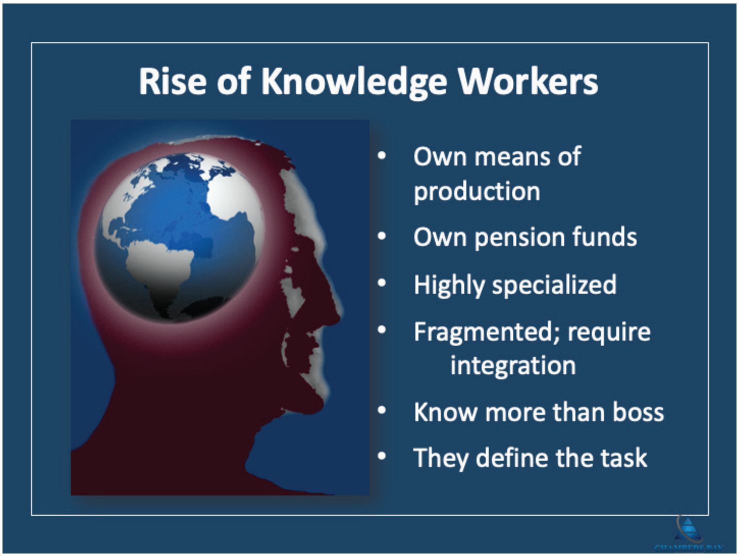
Process

First WHAT, then WHY, and finally HOW
Clear rational for CHANGE



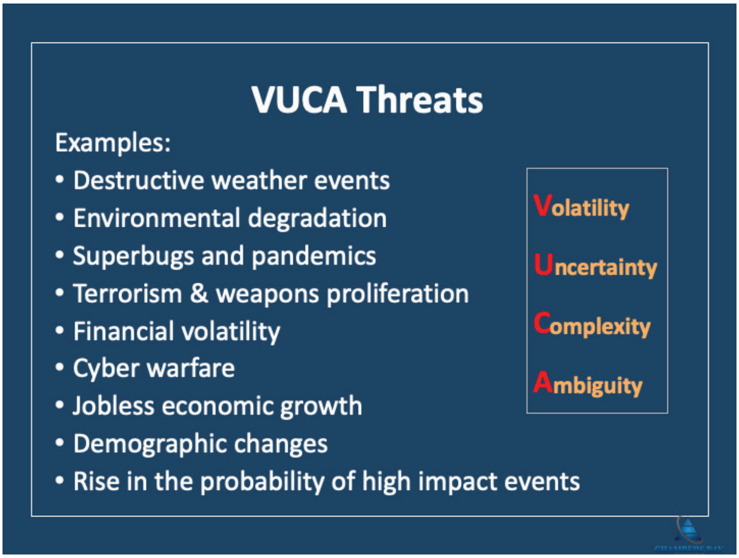
Principles of the Integrator Leader

1. WORK YOURSELF OUT OF YOUR JOB
2. INTEGRATED SOLUTIONS REQUIRE INTEGRATED OPERATIONS
3. FOCUS ON OUTCOMES RATHER THAN INPUTS
4. FROM COMMAND & CONTROL TO STRATEGIC INTENT
5. WHOLE SYSTEMS PERSPECTIVE
6. ASK – DON'T TELL



Rise of Knowledge Workers

- Own means of production
- Own pension funds
- Highly specialized
- Fragmented; require integration
- Know more than boss
- They define the task



VUCA Threats

Examples:

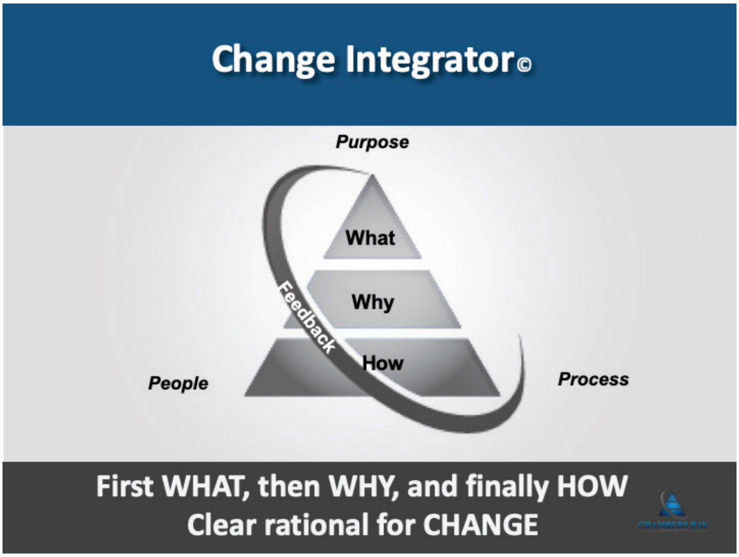
- Destructive weather events
- Environmental degradation
- Superbugs and pandemics
- Terrorism & weapons proliferation
- Financial volatility
- Cyber warfare
- Jobless economic growth
- Demographic changes
- Rise in the probability of high impact events

Volatility

Uncertainty

Complexity

Ambiguity



Change Integrator©

Purpose

What

Why

How

Feedback

People

Process

First WHAT, then WHY, and finally HOW
Clear rational for CHANGE

CHAMBERS BAY
INSTITUTE
Leading Humans in the Age of AI
Why We Need Integrator Leaders

www.chambersbayinstitute.com

Weaponization of Technology and Leading Future Warfighting

Colonel Candice E. Frost

AMERICA'S ARMY:
GLOBALLY RESPONSIVE
REGIONALLY ENGAGED

UNCLASSIFIED

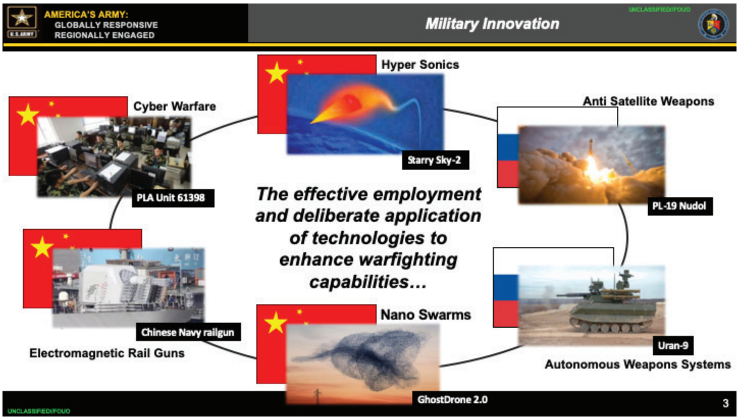
The Evolving Threat

Presented to:
ILSS Symposium
COL Candice E. Frost
HQDA, G-2
13 November 2019

OVERALL CLASSIFICATION: UNCLASSIFIED//FOUO

UNCLASSIFIED

One Vision, One Vector, One Voice



AMERICA'S ARMY:
GLOBALLY RESPONSIVE
REGIONALLY ENGAGED

Military Innovation

UNCLASSIFIED//FOUO

Cyber Warfare

PLA Unit 61398

Hyper Sonics

Starry Sky-2

Anti Satellite Weapons

PL-19 Nudol

The effective employment and deliberate application of technologies to enhance warfighting capabilities…

Chinese Navy railgun

Electromagnetic Rail Guns

Nano Swarms

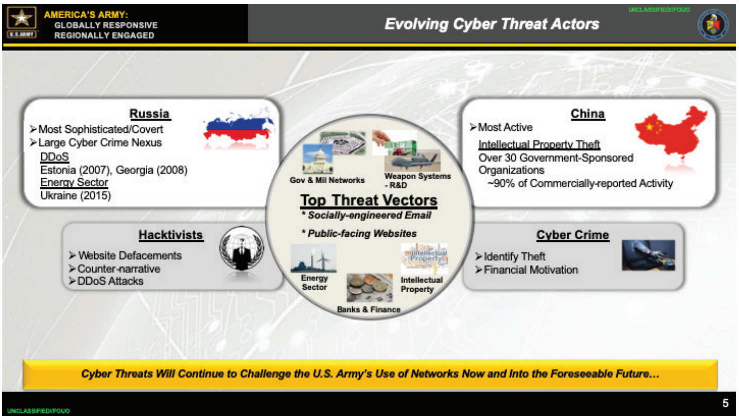
GhostDrone 2.0

Uran-9

Autonomous Weapons Systems

UNCLASSIFIED//FOUO

3



UNCLASSIFIED//FOUO

AMERICA'S ARMY:
GLOBALLY RESPONSIVE
REGIONALLY ENGAGED

Evolving Cyber Threat Actors

Russia

- Most Sophisticated/Covert
- Large Cyber Crime Nexus

DDoS
Estonia (2007), Georgia (2008)
Energy Sector
Ukraine (2015)

China

- Most Active

Intellectual Property Theft
Over 30 Government-Sponsored Organizations
~90% of Commercially-reported Activity

Top Threat Vectors

** Socially-engineered Email*

** Public-facing Websites*

Hacktivists

- Website Defacements
- Counter-narrative
- DDoS Attacks

Cyber Crime

- Identify Theft
- Financial Motivation

Cyber Threats Will Continue to Challenge the U.S. Army's Use of Networks Now and Into the Foreseeable Future…

UNCLASSIFIED//FOUO

5

Law, Ethics, and Autonomy: The Challenge for Military Leaders

Major General Charles (Charlie) Dunlap, Jr.

UNG UNIVERSITY *of* NORTH GEORGIA™
THE MILITARY COLLEGE OF GEORGIA®

Law, Ethics, and Autonomy:
The Challenge for Military Leaders

SOLDIER-LEADERS IN THE AGE OF AI

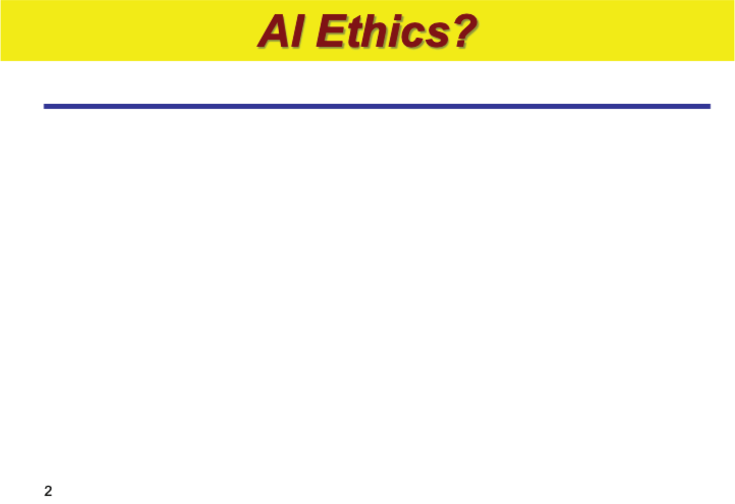
THE FUTURE OF PRE-COMMISSIONING EDUCATION

November 13 - 14, 2019

Center on Law, Ethics and National Security

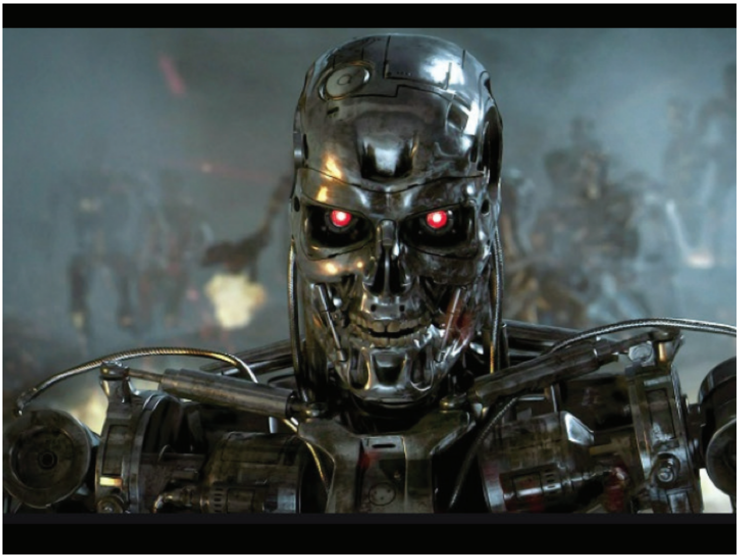
Presented by
Maj Gen Charlie Dunlap, USAF (Ret.)
Copyright © 2019

DUKE LAW

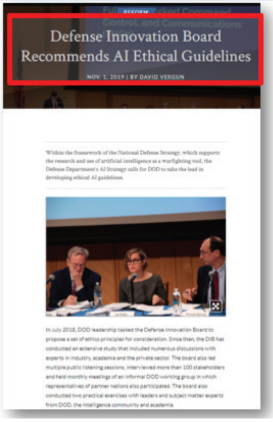


AI Ethics?

2



AI Ethics?



REFORM

Defense Innovation Board Recommends AI Ethical Guidelines

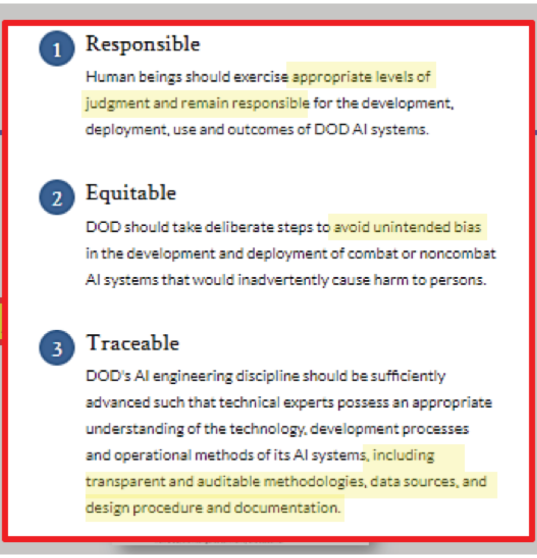
NOV. 1, 2019 | BY DAVID VERGUN

Within the framework of the National Defense Strategy, which supports the research and use of artificial intelligence as a warfighting tool, the Defense Department's AI Strategy calls for DOD to take the lead in developing ethical AI guidelines.

In July 2018, DOD leadership tasked the Defense Innovation Board to propose a set of ethics principles for consideration. Since then, the DIB has conducted an extensive study that included numerous discussions with experts in industry, academia and the private sector. The board also led multiple public listening sessions, interviewed more than 100 stakeholders and held monthly meetings of an informal DOD working group in which representatives of partner nations also participated. The board also conducted two practical exercises with leaders and subject matter experts from DOD, the intelligence community and academia.

1 Nov 2019

4



1 **Responsible**

Human beings should exercise appropriate levels of judgment and remain responsible for the development, deployment, use and outcomes of DOD AI systems.

2 **Equitable**

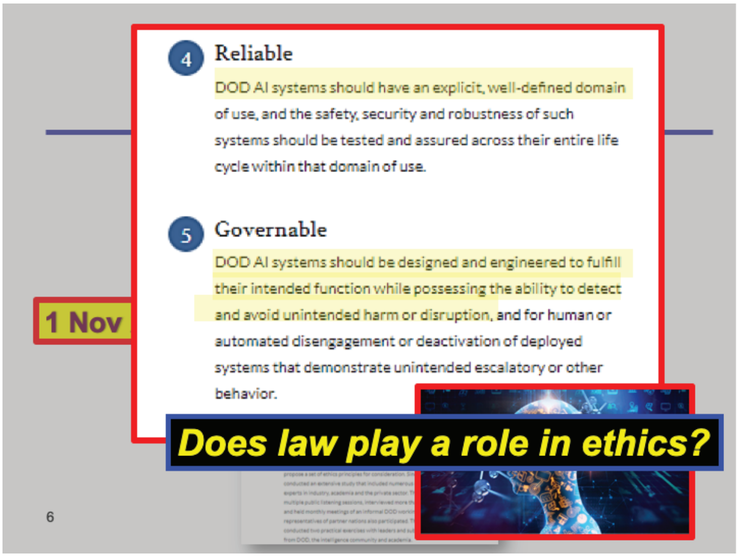
DOD should take deliberate steps to avoid unintended bias in the development and deployment of combat or noncombat AI systems that would inadvertently cause harm to persons.

3 **Traceable**

DOD's AI engineering discipline should be sufficiently advanced such that technical experts possess an appropriate understanding of the technology, development processes and operational methods of its AI systems, including transparent and auditable methodologies, data sources, and design procedure and documentation.

1 Nov

5



1 Nov

4 Reliable

DOD AI systems should have an explicit, well-defined domain of use, and the safety, security and robustness of such systems should be tested and assured across their entire life cycle within that domain of use.

5 Governable

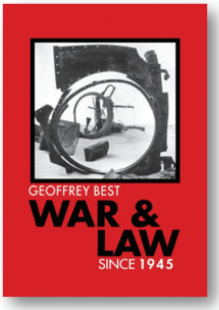
DOD AI systems should be designed and engineered to fulfill their intended function while possessing the ability to detect and avoid unintended harm or disruption, and for human or automated disengagement or deactivation of deployed systems that demonstrate unintended escalatory or other behavior.

Does law play a role in ethics?

propose a set of ethics principles for consideration. Sin
conducted an extensive study that included numerous
experts in industry, academia and the private sector. Th
multiple public listening sessions, interviewed more th
and held monthly meetings of an informal DOD workin
representatives of partner nations also participated. Th
conducted two practical exercises with leaders and su
from DOD, the intelligence community and academia.

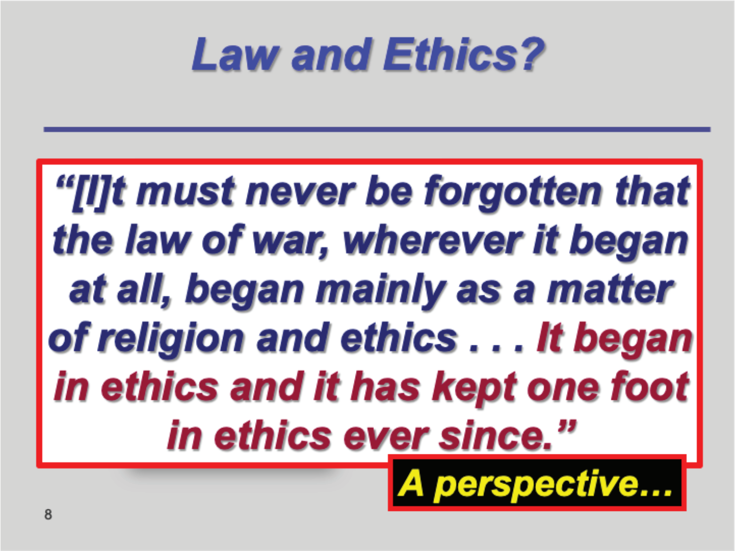
6

Law and Ethics?



Prof Geoffrey Best

7

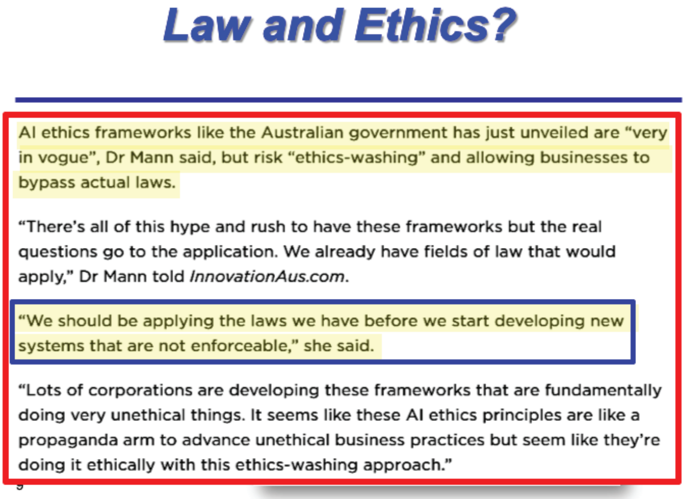


Law and Ethics?

"[I]t must never be forgotten that the law of war, wherever it began at all, began mainly as a matter of religion and ethics . . . It began in ethics and it has kept one foot in ethics ever since."

A perspective…

8



Law and Ethics?

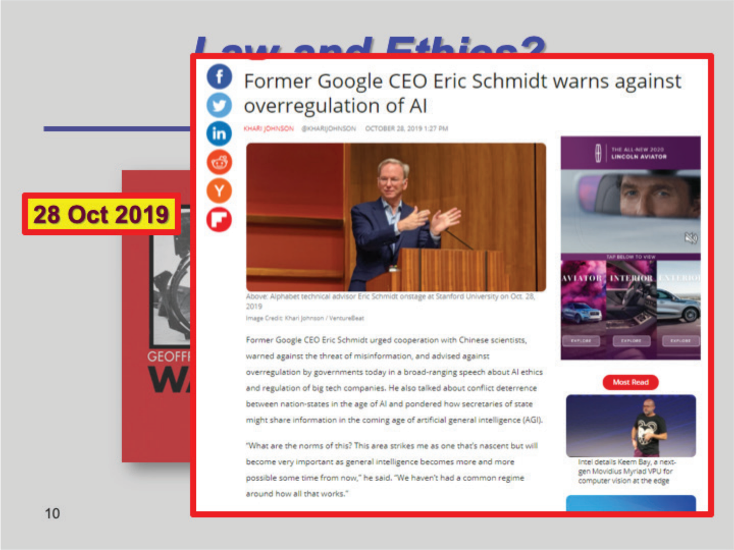
AI ethics frameworks like the Australian government has just unveiled are "very in vogue", Dr Mann said, but risk "ethics-washing" and allowing businesses to bypass actual laws.

"There's all of this hype and rush to have these frameworks but the real questions go to the application. We already have fields of law that would apply," Dr Mann told *InnovationAus.com*.

"We should be applying the laws we have before we start developing new systems that are not enforceable," she said.

"Lots of corporations are developing these frameworks that are fundamentally doing very unethical things. It seems like these AI ethics principles are like a propaganda arm to advance unethical business practices but seem like they're doing it ethically with this ethics-washing approach."

9



Law and Ethics?

28 Oct 2019

Former Google CEO Eric Schmidt warns against overregulation of AI

KHARI JOHNSON @KHARIJOHNSON OCTOBER 28, 2019 1:27 PM

Above: Alphabet technical advisor Eric Schmidt onstage at Stanford University on Oct. 28, 2019

Image Credit: Khari Johnson / VentureBeat

Former Google CEO Eric Schmidt urged cooperation with Chinese scientists, warned against the threat of misinformation, and advised against overregulation by governments today in a broad-ranging speech about AI ethics and regulation of big tech companies. He also talked about conflict deterrence between nation-states in the age of AI and pondered how secretaries of state might share information in the coming age of artificial general intelligence (AGI).

"What are the norms of this? This area strikes me as one that's nascent but will become very important as general intelligence becomes more and more possible some time from now," he said. "We haven't had a common regime around how all that works."

Most Read

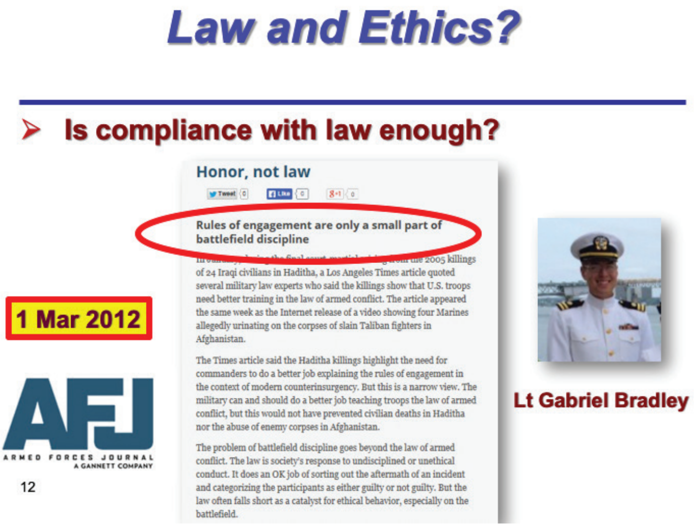
Intel details Keem Bay, a next-gen Movidius Myriad VPU for computer vision at the edge

10

Law and Ethics?

- ➢ Is compliance with law enough?

11



Law and Ethics?

➢ Is compliance with law enough?

1 Mar 2012

AFJ ARMED FORCES JOURNAL A GANNETT COMPANY

Honor, not law

Tweet 0 Like 0 +1 0

Rules of engagement are only a small part of battlefield discipline

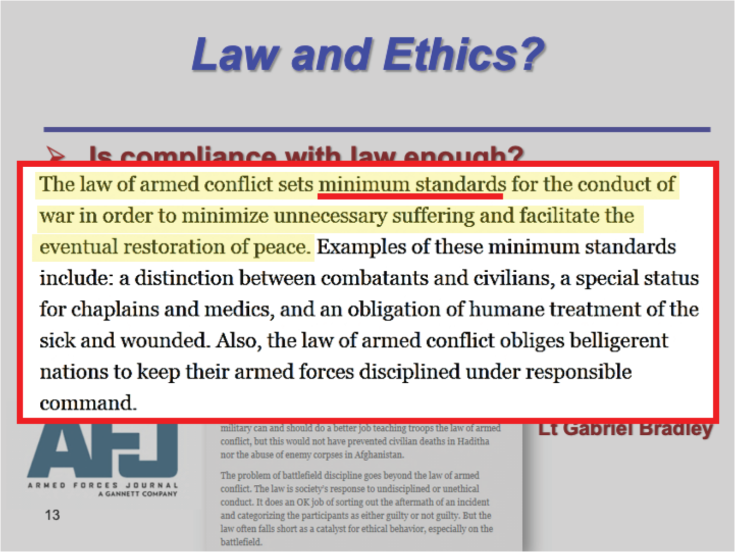
In January, during the final court-martial arising from the 2005 killings of 24 Iraqi civilians in Haditha, a Los Angeles Times article quoted several military law experts who said the killings show that U.S. troops need better training in the law of armed conflict. The article appeared the same week as the Internet release of a video showing four Marines allegedly urinating on the corpses of slain Taliban fighters in Afghanistan.

The Times article said the Haditha killings highlight the need for commanders to do a better job explaining the rules of engagement in the context of modern counterinsurgency. But this is a narrow view. The military can and should do a better job teaching troops the law of armed conflict, but this would not have prevented civilian deaths in Haditha nor the abuse of enemy corpses in Afghanistan.

The problem of battlefield discipline goes beyond the law of armed conflict. The law is society's response to undisciplined or unethical conduct. It does an OK job of sorting out the aftermath of an incident and categorizing the participants as either guilty or not guilty. But the law often falls short as a catalyst for ethical behavior, especially on the battlefield.

Lt Gabriel Bradley

12



Law and Ethics?

➢ Is compliance with law enough?

The law of armed conflict sets minimum standards for the conduct of war in order to minimize unnecessary suffering and facilitate the eventual restoration of peace. Examples of these minimum standards include: a distinction between combatants and civilians, a special status for chaplains and medics, and an obligation of humane treatment of the sick and wounded. Also, the law of armed conflict obliges belligerent nations to keep their armed forces disciplined under responsible command.

military can and should do a better job teaching troops the law of armed conflict, but this would not have prevented civilian deaths in Haditha nor the abuse of enemy corpses in Afghanistan.

The problem of battlefield discipline goes beyond the law of armed conflict. The law is society's response to undisciplined or unethical conduct. It does an OK job of sorting out the aftermath of an incident and categorizing the participants as either guilty or not guilty. But the law often falls short as a catalyst for ethical behavior, especially on the battlefield.

Lt Gabriel Bradley

AFJ ARMED FORCES JOURNAL A GANNETT COMPANY

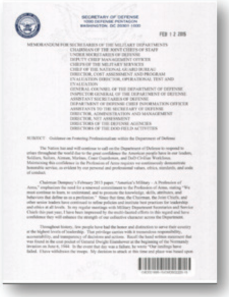
13

Do ethics 'matter'?

A former soldier's perspective…

Do ethics 'matter'?

12 Feb 2015



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

FEB 12 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION DIRECTOR, OPERATIONAL TEST AND
EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Guidance on Fostering Professionalism within the Department of Defense

The Nation has and will continue to call on the Department of Defense to respond to crises throughout the world due to the great confidence the American people have in our leaders, Soldiers, Sailors, Airmen, Marines, Coast Guardsmen, and DoD Civilian Workforce. Maintaining this confidence in the Profession of Arms requires we continuously demonstrate honorable service, as evident by our personal and professional values, ethics, standards, and code of conduct.

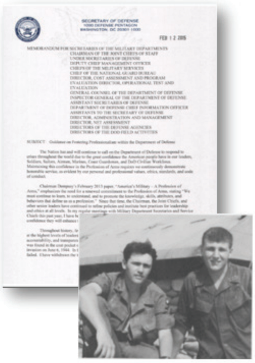
Chairman Dempsey's February 2013 paper, "America's Military – A Profession of Arms," emphasizes the need for a renewed commitment to the Profession of Arms, stating "We must continue to learn, to understand, and to promote the knowledge, skills, attributes, and behaviors that define us as a profession." Since that time, the Chairman, the Joint Chiefs, and other senior leaders have continued to refine policies and institute best practices for leadership and ethics at all levels. In my regular meetings with Military Department Secretaries and Service Chiefs this past year, I have been impressed by the multi-faceted efforts in this regard and have confidence they will enhance the strength of our collective character across the Department.

Throughout history, few people have had the honor and distinction to serve their country at the highest levels of leadership. That privilege carries with it tremendous responsibility, accountability, and transparency of decisions and actions. Recall the hand written statement that was found in the coat pocket of General Dwight Eisenhower at the beginning of the Normandy invasion on June 6, 1944. In the event that day was a failure, he wrote "Our landings have failed. I have withdrawn the troops. My decision to attack at this time and place was based upon

Former U.S.
Secretary of Defense
Chuck Hagel

Do ethics 'matter'?

12 Feb 2015



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

FEB 1 2 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

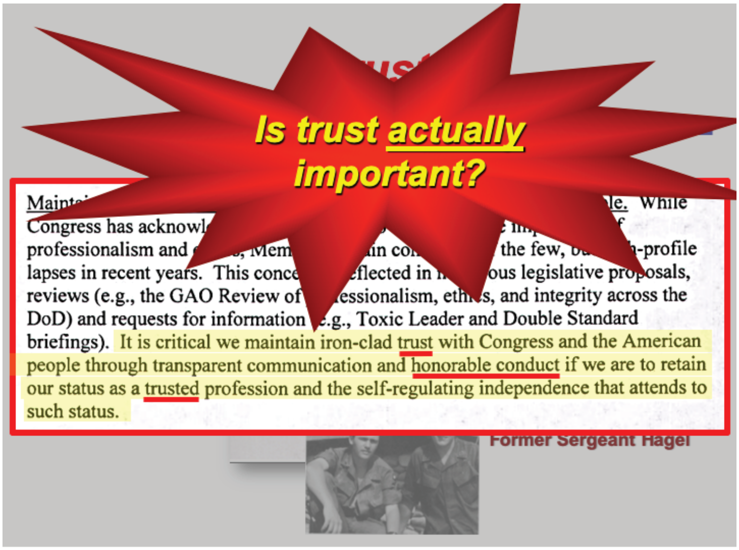
SUBJECT: Guidance on Fostering Professionalism within the Department of Defense

The Nation has and will continue to call on the Department of Defense to respond to crises throughout the world due to the great confidence the American people have in our leaders, Soldiers, Sailors, Airmen, Marines, Coast Guardsmen, and DoD Civilian Workforce. Maintaining this confidence in the Profession of Arms requires we continuously demonstrate honorable service, as evident by our personal and professional values, ethics, standards, and code of conduct.

Chairman Dempsey's February 2012 paper, "America's Military – A Profession of Arms," emphasizes the need for a renewed commitment to the Profession of Arms, stating "We must continue to learn, to understand, and to promote the knowledge, skills, attributes, and behaviors that define us as a profession." Since that time, the Chairman, the Joint Chiefs, and other senior leaders have continued to refine policies and institute best practices for leadership and ethics at all levels. In my regular meetings with Military Department Secretaries and Service Chiefs this past year, I have b
confidence they will enhance

Throughout history, Ar
at the highest levels of leader
accountability, and transparen
was found in the coat pocket o
invasion on June 6, 1944. In t
failed. I have withdrawn the

Former Sergeant Hagel

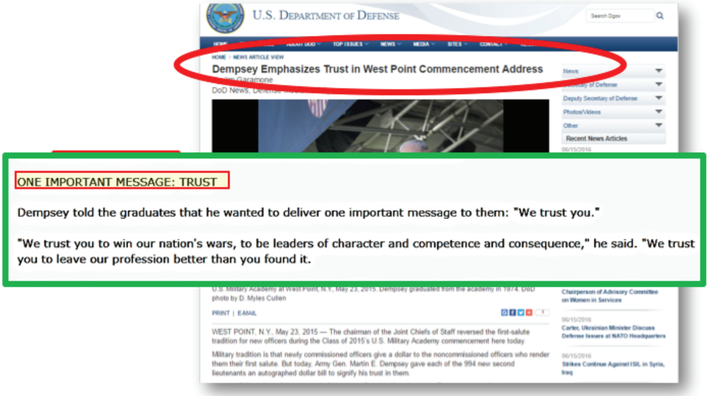


Is trust actually important?

Maint le. While Congress has acknowl professionalism and , Mem in co the few, b -profile lapses in recent years. This conce flected in ous legislative proposals, reviews (e.g., the GAO Review of essionalism, eth s, and integrity across the DoD) and requests for information e.g., Toxic Leader and Double Standard briefings). It is critical we maintain iron-clad trust with Congress and the American people through transparent communication and honorable conduct if we are to retain our status as a trusted profession and the self-regulating independence that attends to such status.

Former Sergeant Hagel

Trust



Dempsey Emphasizes Trust in West Point Commencement Address

Jim Garamone

DoD News, Defense

ONE IMPORTANT MESSAGE: TRUST

Dempsey told the graduates that he wanted to deliver one important message to them: "We trust you."

"We trust you to win our nation's wars, to be leaders of character and competence and consequence," he said. "We trust you to leave our profession better than you found it.

U.S. Military Academy at West Point, N.Y., May 23, 2015. Dempsey graduated from the academy in 1974. DoD photo by D. Myles Cullen

WEST POINT, N.Y., May 23, 2015 — The chairman of the Joint Chiefs of Staff reversed the first-salute tradition for new officers during the Class of 2015's U.S. Military Academy commencement here today.

Military tradition is that newly commissioned officers give a dollar to the noncommissioned officers who render them their first salute. But today, Army Gen. Martin E. Dempsey gave each of the 994 new second lieutenants an autographed dollar bill to signify his trust in them.

06/15/2016

Chairperson of Advisory Committee on Women in Services

06/15/2016

Carter, Ukrainian Minister Discuss Defense Issues at NATO Headquarters

06/15/2016

Strikes Continue Against ISIL in Syria, Iraq

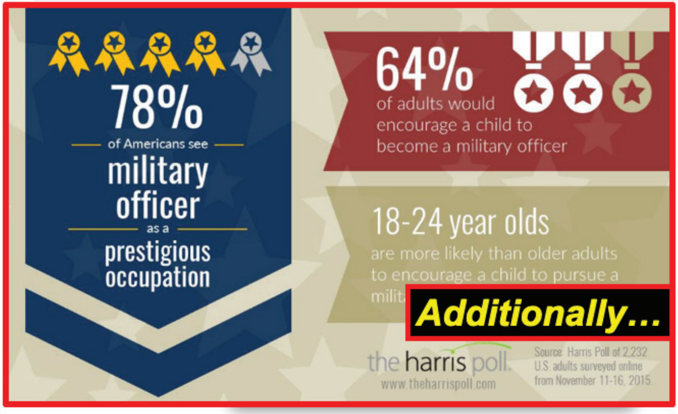
Do ethics 'matter'?

To sustaining the all-volunteer military?

Currently in the U.S.....

19

Do ethics ‘matter’?



78% of Americans see military officer as a prestigious occupation

64% of adults would encourage a child to become a military officer

18-24 year olds are more likely than older adults to encourage a child to pursue a milit

Additionally…

the harris poll
www.theharrispoll.com

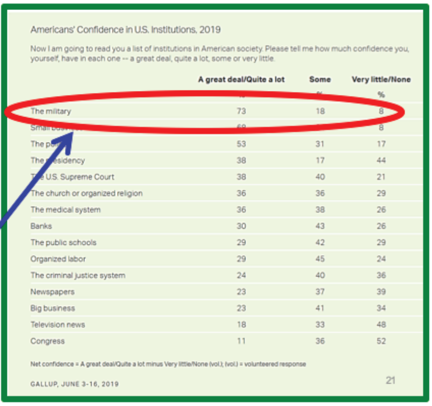
Source: Harris Poll of 2,232 U.S. adults surveyed online from November 11-16, 2015.

Do ethics ‘matter’?

GALLUP POLL

Confidence in Institutions
June 2019

Military



Americans' Confidence in U.S. Institutions, 2019

Now I am going to read you a list of institutions in American society. Please tell me how much confidence you, yourself, have in each one -- a great deal, quite a lot, some or very little.

	A great deal/Quite a lot	Some	Very little/None
	%	%	%
The military	73	18	8
Small business	69	[illegible]	8
The p[illegible]	53	31	17
The presidency	38	17	44
The U.S. Supreme Court	38	40	21
The church or organized religion	36	36	29
The medical system	36	38	26
Banks	30	43	26
The public schools	29	42	29
Organized labor	29	45	24
The criminal justice system	24	40	36
Newspapers	23	37	39
Big business	23	41	34
Television news	18	33	48
Congress	11	36	52

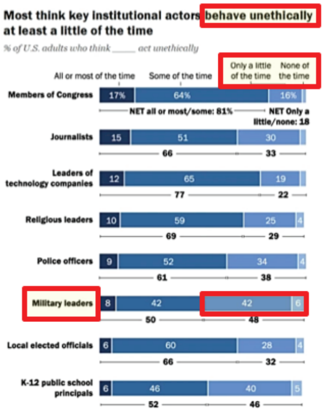
Net confidence = A great deal/Quite a lot minus Very little/None (vol.); (vol.) = volunteered response

GALLUP, JUNE 3-16, 2019

21

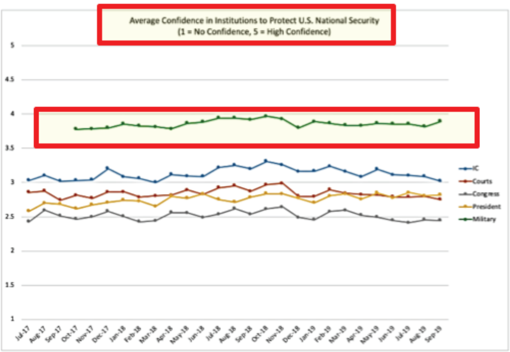
Do ethics 'matter'?

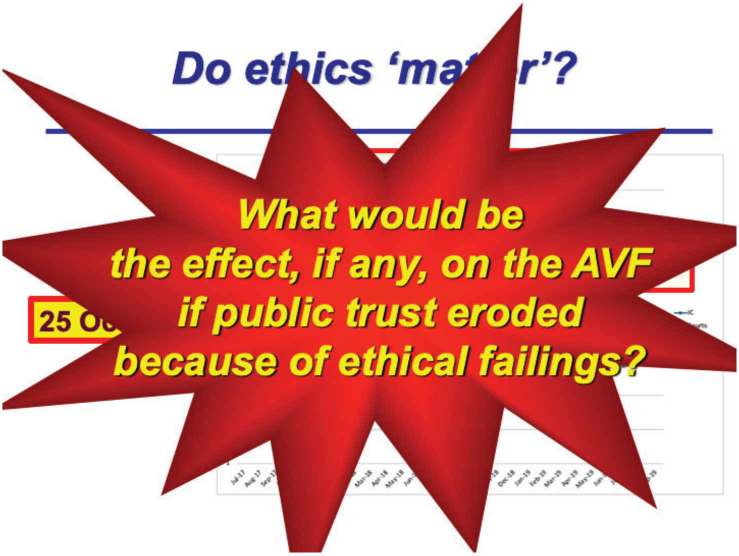
19 Sept 2019



Do ethics 'matter'?

25 Oct 2019



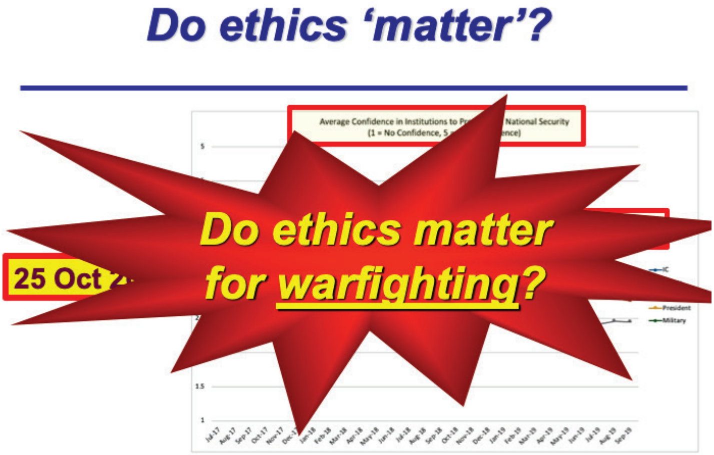


Do eth ics 'ma r'?

What would be
the effect, if any, on the AVF
if public trust eroded
because of ethical failings?

25 Oc

Jul-17
Aug-17
Sep-17
Mar-18
Apr-18
May-18
Jun-
Dec-18
Jan-19
Feb-19
Mar-19
Apr-19
May-19
Jun-
IC
urts



Do ethics 'matter'?

Do ethics matter
for warfighting?

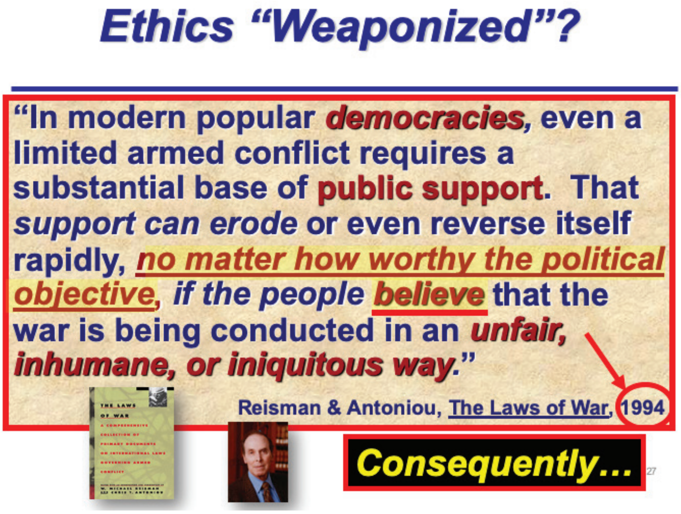
25 Oct 2

Average Confidence in Institutions to Pr National Security
(1 = No Confidence, 5 = ence)
5
1.5
1
Jul-17
Aug-17
Sep-17
Oct-17
Nov-17
Dec-17
Jan-18
Feb-18
Mar-18
Apr-18
May-18
Jun-18
Jul-18
Aug-18
Sep-18
Oct-18
Nov-18
Dec-18
Jan-19
Feb-19
Mar-19
Apr-19
May-19
Jun-19
Jul-19
Aug-19
Sep-19
IC
President
Military

Do ethics 'matter'?

- Moral and ethical behavior *can* impact warfighting capability

Have today's adversaries 'weaponized' ethics?



Ethics "Weaponized"?

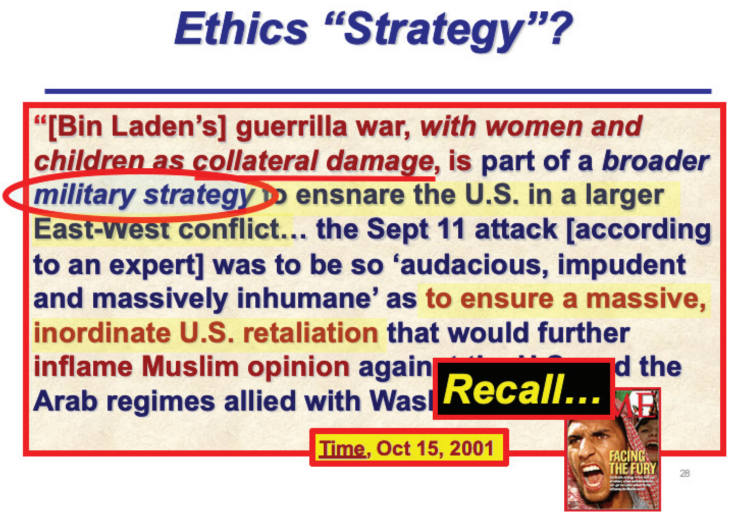
"In modern popular *democracies*, even a limited armed conflict requires a substantial base of public support. That *support can erode* or even reverse itself rapidly, *no matter how worthy the political objective*, *if the people* believe that the war is being conducted in an *unfair, inhumane, or iniquitous way*."

Reisman & Antoniou, The Laws of War, 1994

THE LAWS OF WAR

Consequently…

27



Ethics "Strategy"?

"[Bin Laden's] guerrilla war, *with women and children as collateral damage*, is part of a *broader military strategy* to ensnare the U.S. in a larger East-West conflict… the Sept 11 attack [according to an expert] was to be so 'audacious, impudent and massively inhumane' as to ensure a massive, inordinate U.S. retaliation that would further inflame Muslim opinion again d the Arab regimes allied with Wash

Recall…

Time, Oct 15, 2001

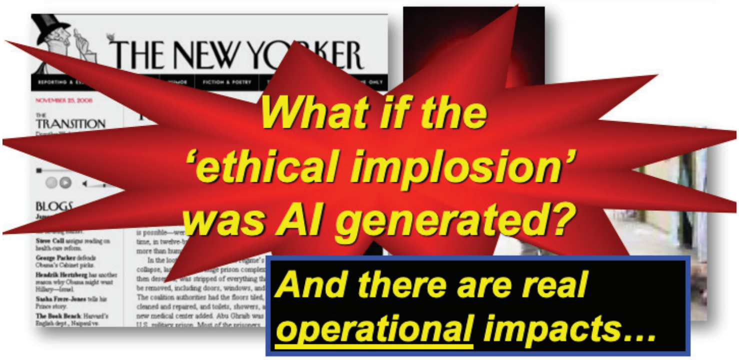
28

America's Worst Defeat Since 9/11

An ethical 'implosion'

29

America's Worst Defeat Since 9/11


THE NEW YORKER
REPORTING & ES
HUMOR
FICTION & POETRY
NOVEMBER 25, 2008
THE TRANSITION
BLOGS
Steve Coll assigns reading on health-care reform.
George Packer defends Obama's Cabinet picks.
Hendrik Hertzberg has another reason why Obama might want Hillary—Israel.
Sasha Frere-Jones tells his Prince story.
The Book Bench: Harvard's English dept., Naipaul vs.
is possible—wer
time, in twelve-b
more than hum
In the loo
regime's
collapse, la
ge prison complex
then dese
was stripped of everything th
be removed, including doors, windows, and
The coalition authorities had the floors tiled,
cleaned and repaired, and toilets, showers,
new medical center added. Abu Ghraib was
U.S. military prison. Most of the prisoners

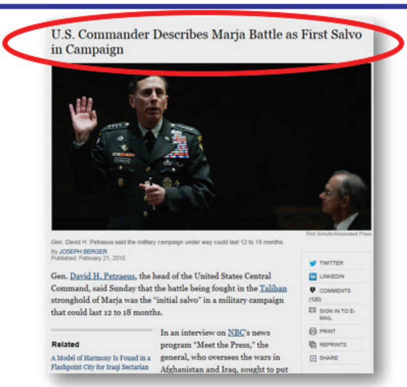
What if the 'ethical implosion' was AI generated?

And there are real <u>operational</u> impacts…

30

Strategic Consequences

21 Feb 2010



U.S. Commander Describes Marja Battle as First Salvo in Campaign

Rich Schultz/Associated Press

Gen. David H. Petraeus said the military campaign under way could last 12 to 18 months.

By JOSEPH BERGER
Published: February 21, 2010

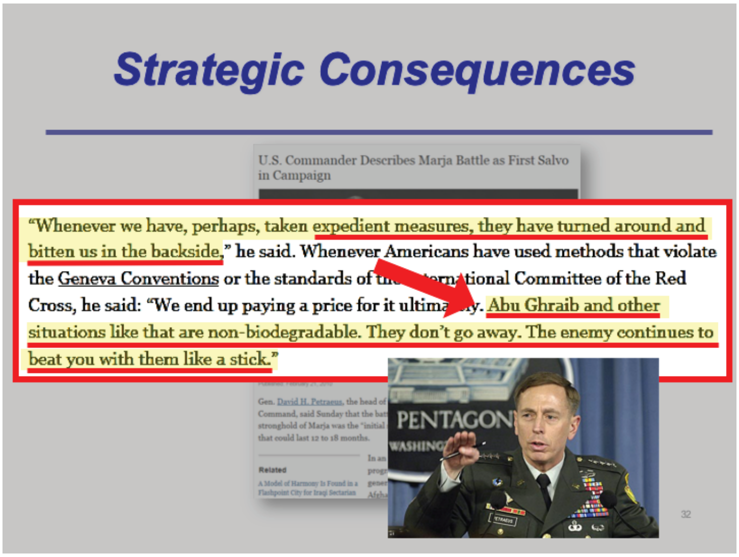
Gen. David H. Petraeus, the head of the United States Central Command, said Sunday that the battle being fought in the Taliban stronghold of Marja was the "initial salvo" in a military campaign that could last 12 to 18 months.

In an interview on NBC's news program "Meet the Press," the general, who oversees the wars in Afghanistan and Iraq, sought to put

Related

A Model of Harmony Is Found in a Flashpoint City for Iraqi Sectarian

31



Strategic Consequences

U.S. Commander Describes Marja Battle as First Salvo in Campaign

"Whenever we have, perhaps, taken expedient measures, they have turned around and bitten us in the backside," he said. Whenever Americans have used methods that violate the Geneva Conventions or the standards of the International Committee of the Red Cross, he said: "We end up paying a price for it ultimately. Abu Ghraib and other situations like that are non-biodegradable. They don't go away. The enemy continues to beat you with them like a stick."

Published: February 21, 2010

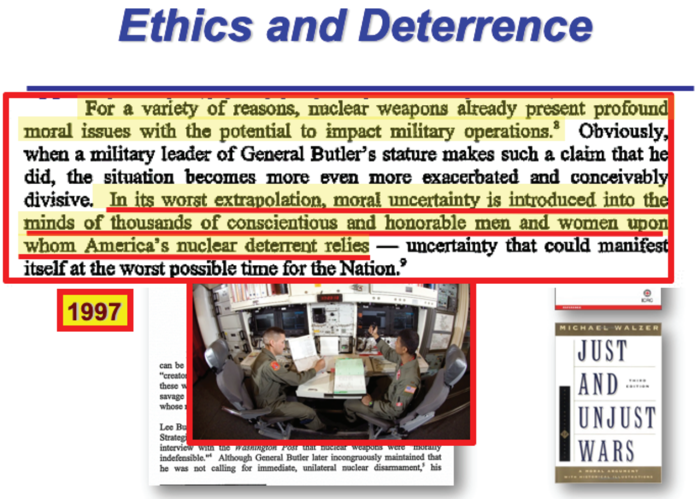
Gen. David H. Petraeus, the head of
Command, said Sunday that the bat
stronghold of Marja was the "initial
that could last 12 to 18 months.

In an
progr
gener
Afgha

Related

A Model of Harmony Is Found in a Flashpoint City for Iraqi Sectarian

32



Ethics and Deterrence

For a variety of reasons, nuclear weapons already present profound moral issues with the potential to impact military operations.[8] Obviously, when a military leader of General Butler's stature makes such a claim that he did, the situation becomes more even more exacerbated and conceivably divisive. In its worst extrapolation, moral uncertainty is introduced into the minds of thousands of conscientious and honorable men and women upon whom America's nuclear deterrent relies — uncertainty that could manifest itself at the worst possible time for the Nation.[9]

1997

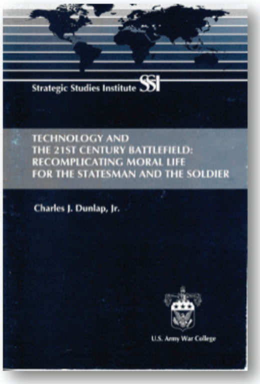
can be
"creato
these w
savage
whose

Lee Bu
Strategi
interview with the *Washington Post* that nuclear weapons were "morally indefensible."[4] Although General Butler later incongruously maintained that he was not calling for immediate, unilateral nuclear disarmament,[5] his

Leadership and Technology

Leadership and Technology

1999



Strategic Studies Institute SSI

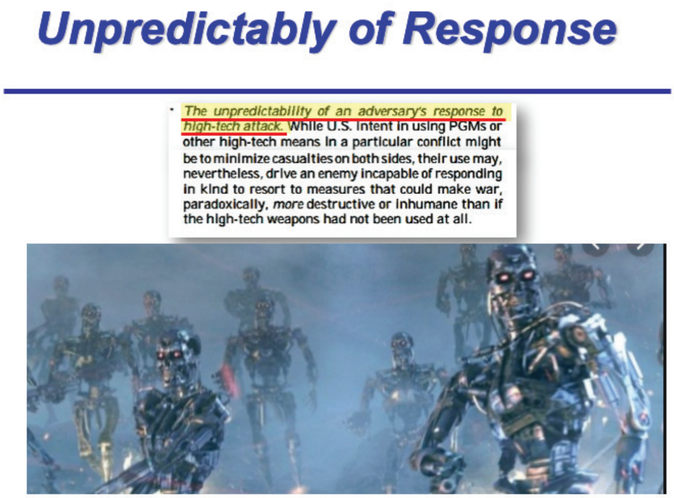
TECHNOLOGY AND
THE 21ST CENTURY BATTLEFIELD:
RECOMPLICATING MORAL LIFE
FOR THE STATESMAN AND THE SOLDIER

Charles J. Dunlap, Jr.

U.S. Army War College

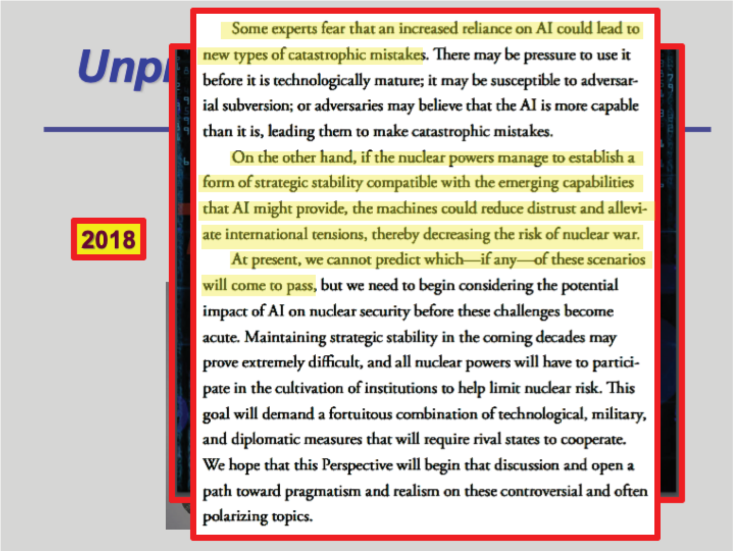
Application to AI

Unpredictably of Response



Unpredictably of Response

- *The unpredictability of an adversary's response to high-tech attack.* While U.S. intent in using PGMs or other high-tech means in a particular conflict might be to minimize casualties on both sides, their use may, nevertheless, drive an enemy incapable of responding in kind to resort to measures that could make war, paradoxically, *more* destructive or inhumane than if the high-tech weapons had not been used at all.

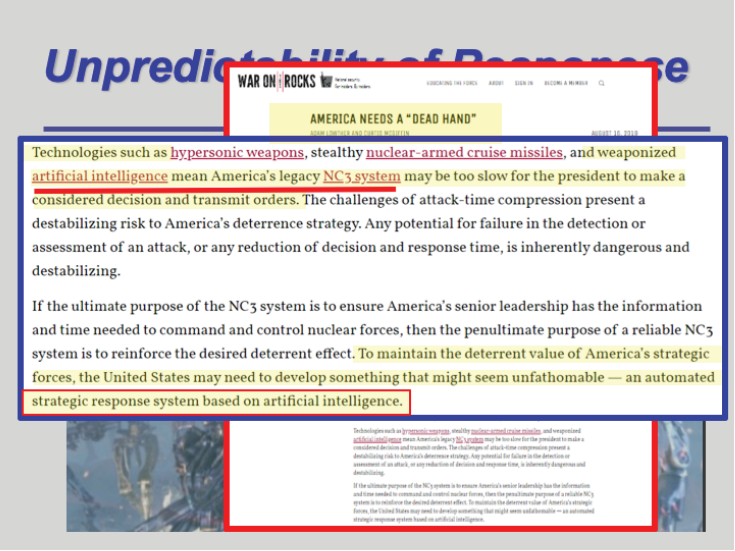


2018

Some experts fear that an increased reliance on AI could lead to new types of catastrophic mistakes. There may be pressure to use it before it is technologically mature; it may be susceptible to adversarial subversion; or adversaries may believe that the AI is more capable than it is, leading them to make catastrophic mistakes.

On the other hand, if the nuclear powers manage to establish a form of strategic stability compatible with the emerging capabilities that AI might provide, the machines could reduce distrust and alleviate international tensions, thereby decreasing the risk of nuclear war.

At present, we cannot predict which—if any—of these scenarios will come to pass, but we need to begin considering the potential impact of AI on nuclear security before these challenges become acute. Maintaining strategic stability in the coming decades may prove extremely difficult, and all nuclear powers will have to participate in the cultivation of institutions to help limit nuclear risk. This goal will demand a fortuitous combination of technological, military, and diplomatic measures that will require rival states to cooperate. We hope that this Perspective will begin that discussion and open a path toward pragmatism and realism on these controversial and often polarizing topics.



Unpredictability of Response

AMERICA NEEDS A "DEAD HAND"

ADAM LOWTHER AND CURTIS MCGIFFIN

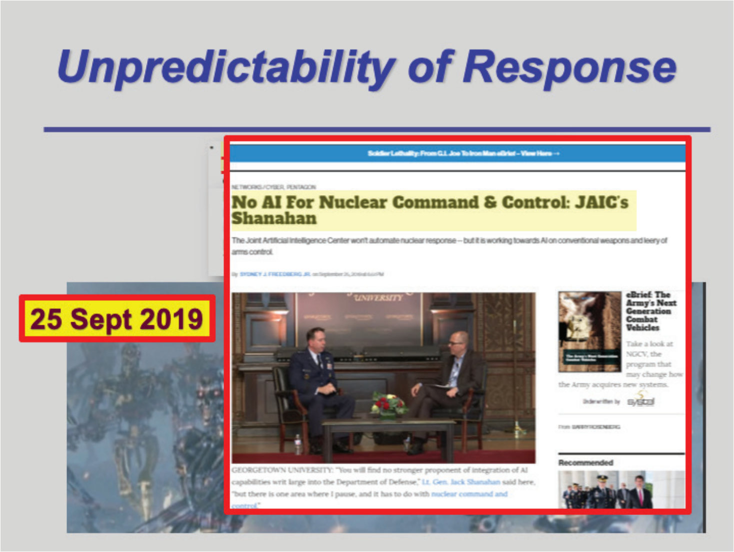
AUGUST 16, 2019

Technologies such as hypersonic weapons, stealthy nuclear-armed cruise missiles, and weaponized artificial intelligence mean America's legacy NC3 system may be too slow for the president to make a considered decision and transmit orders. The challenges of attack-time compression present a destabilizing risk to America's deterrence strategy. Any potential for failure in the detection or assessment of an attack, or any reduction of decision and response time, is inherently dangerous and destabilizing.

If the ultimate purpose of the NC3 system is to ensure America's senior leadership has the information and time needed to command and control nuclear forces, then the penultimate purpose of a reliable NC3 system is to reinforce the desired deterrent effect. To maintain the deterrent value of America's strategic forces, the United States may need to develop something that might seem unfathomable — an automated strategic response system based on artificial intelligence.

Technologies such as hypersonic weapons, stealthy nuclear-armed cruise missiles, and weaponized artificial intelligence mean America's legacy NC3 system may be too slow for the president to make a considered decision and transmit orders. The challenges of attack-time compression present a destabilizing risk to America's deterrence strategy. Any potential for failure in the detection or assessment of an attack, or any reduction of decision and response time, is inherently dangerous and destabilizing.

If the ultimate purpose of the NC3 system is to ensure America's senior leadership has the information and time needed to command and control nuclear forces, then the penultimate purpose of a reliable NC3 system is to reinforce the desired deterrent effect. To maintain the deterrent value of America's strategic forces, the United States may need to develop something that might seem unfathomable — an automated strategic response system based on artificial intelligence.



Unpredictability of Response

25 Sept 2019

Soldier Lethality: From G.I. Joe To Iron Man eBrief – View Here →

NETWORKS/CYBER, PENTAGON

No AI For Nuclear Command & Control: JAIC's Shanahan

The Joint Artificial Intelligence Center won't automate nuclear response -- but it is working towards AI on conventional weapons and leery of arms control.

By SYDNEY J. FREEDBERG JR. on September 26, 2019 at [illegible]

GEORGETOWN UNIVERSITY: "You will find no stronger proponent of integration of AI capabilities writ large into the Department of Defense," Lt. Gen. Jack Shanahan said here, "but there is one area where I pause, and it has to do with nuclear command and control."

eBrief: The Army's Next Generation Combat Vehicles

Take a look at NGCV, the program that may change how the Army acquires new systems.

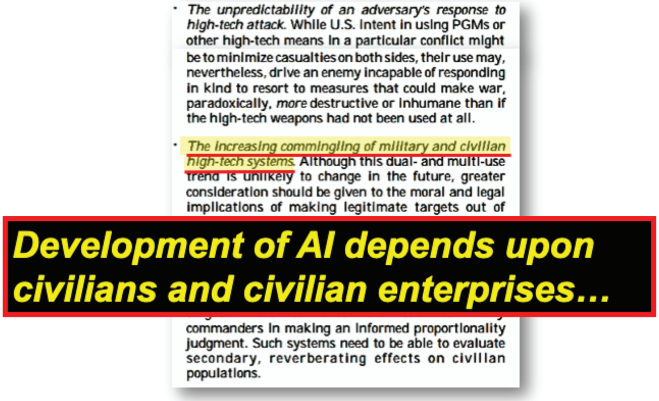
Underwritten by systal

From BARRY ROSENBERG

Recommended

Comingling of Systems

Comingling of Systems

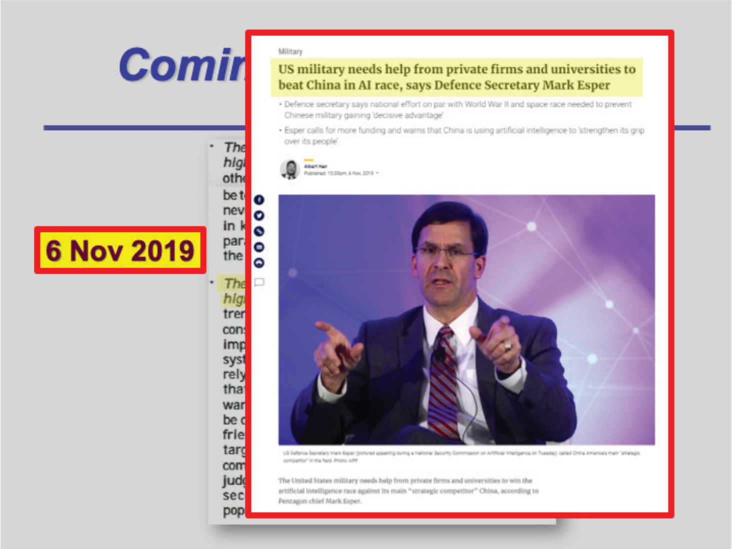


- *The unpredictability of an adversary's response to high-tech attack.* While U.S. intent in using PGMs or other high-tech means in a particular conflict might be to minimize casualties on both sides, their use may, nevertheless, drive an enemy incapable of responding in kind to resort to measures that could make war, paradoxically, *more* destructive or inhumane than if the high-tech weapons had not been used at all.

- *The increasing commingling of military and civilian high-tech systems.* Although this dual- and multi-use trend is unlikely to change in the future, greater consideration should be given to the moral and legal implications of making legitimate targets out of

Development of AI depends upon civilians and civilian enterprises…

commanders in making an informed proportionality judgment. Such systems need to be able to evaluate secondary, reverberating effects on civilian populations.



Comin

6 Nov 2019

- The higl othe be t nev in k par the
- The higl tren con imp syst rely tha war be c frie targ com judg sec pop

Military

US military needs help from private firms and universities to beat China in AI race, says Defence Secretary Mark Esper

- Defence secretary says national effort on par with World War II and space race needed to prevent Chinese military gaining 'decisive advantage'
- Esper calls for more funding and warns that China is using artificial intelligence to 'strengthen its grip over its people'

Albert Han
Published: 10:30pm, 6 Nov, 2019

US Defence Secretary Mark Esper (pictured speaking during a National Security Commission on Artificial Intelligence on Tuesday) called China America's main "strategic competitor" in the field. Photo: AFP

The United States military needs help from private firms and universities to win the artificial intelligence race against its main "strategic competitor" China, according to Pentagon chief Mark Esper.

Comin

6 Nov 2019

- The higl othe be t nev in k par the
- The higl tren con imp syst rely tha war be c frie targ com judg sec pop

Military

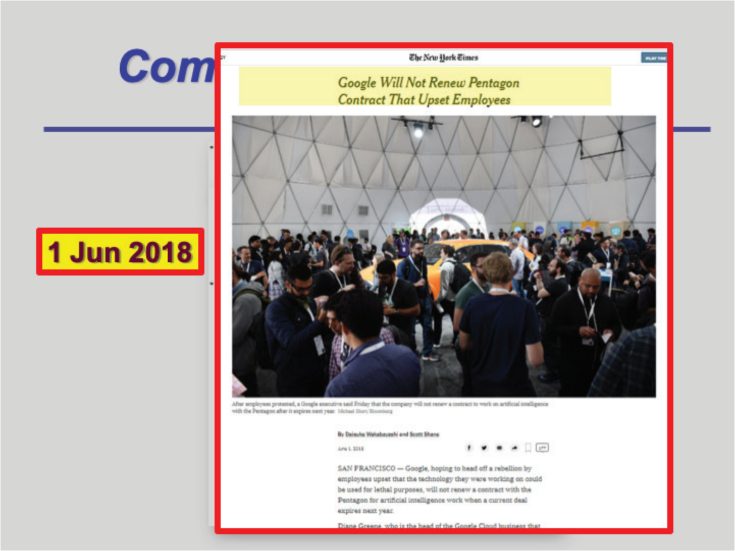
US military needs help from private firms and universities to beat China in AI race, says Defence Secretary Mark Esper

- Defence secretary says national effort on par with World War II and space race needed to prevent Chinese military gaining 'decisive advantage'
- Esper calls for more funding and warns that China is using artificial intelligence to 'strengthen its grip over its people'

Albert Han
Published: 10:30pm, 6 Nov, 2019

US Defence Secretary Mark Esper (pictured speaking during a National Security Commission on Artificial Intelligence on Tuesday) called China America's main "strategic competitor" in the field. Photo: AFP

The United States military needs help from private firms and universities to win the artificial intelligence race against its main "strategic competitor" China, according to Pentagon chief Mark Esper.



1 Jun 2018

The New York Times

Google Will Not Renew Pentagon Contract That Upset Employees

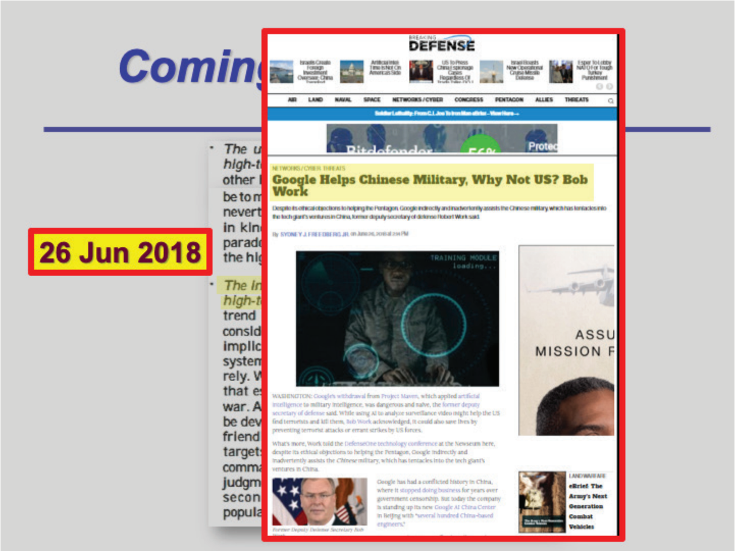
After employees protested, a Google executive said Friday that the company will not renew a contract to work on artificial intelligence with the Pentagon after it expires next year. Michael Short/Bloomberg

By Daisuke Wakabayashi and Scott Shane

June 1, 2018

SAN FRANCISCO — Google, hoping to head off a rebellion by employees upset that the technology they were working on could be used for lethal purposes, will not renew a contract with the Pentagon for artificial intelligence work when a current deal expires next year.

Diane Greene, who is the head of the Google Cloud business that



26 Jun 2018

NETWORKS / CYBER THREATS

Google Helps Chinese Military, Why Not US? Bob Work

Despite its ethical objections to helping the Pentagon, Google indirectly and inadvertently assists the Chinese military, which has tentacles into the tech giant's ventures in China, former deputy secretary of defense Robert Work said.

By SYDNEY J. FREEDBERG JR. on June 26, 2018 at 2:04 PM

WASHINGTON: Google's withdrawal from Project Maven, which applied artificial intelligence to military intelligence, was dangerous and naïve, the former deputy secretary of defense said. While using AI to analyze surveillance video might help the US find terrorists and kill them, Bob Work acknowledged, it could also save lives by preventing terrorist attacks or errant strikes by US forces.

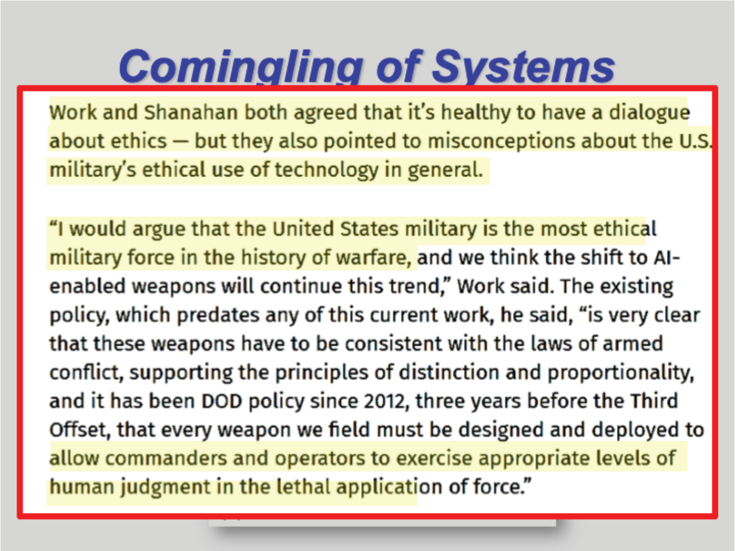
What's more, Work told the DefenseOne technology conference at the Newseum here, despite its ethical objections to helping the Pentagon, Google indirectly and inadvertently assists the Chinese military, which has tentacles into the tech giant's ventures in China.

Former Deputy Defense Secretary Bob Work

Google has had a conflicted history in China, where it stopped doing business for years over government censorship. But today the company is standing up its new Google AI China Center in Beijing with "several hundred China-based engineers."

LANDWARFARE

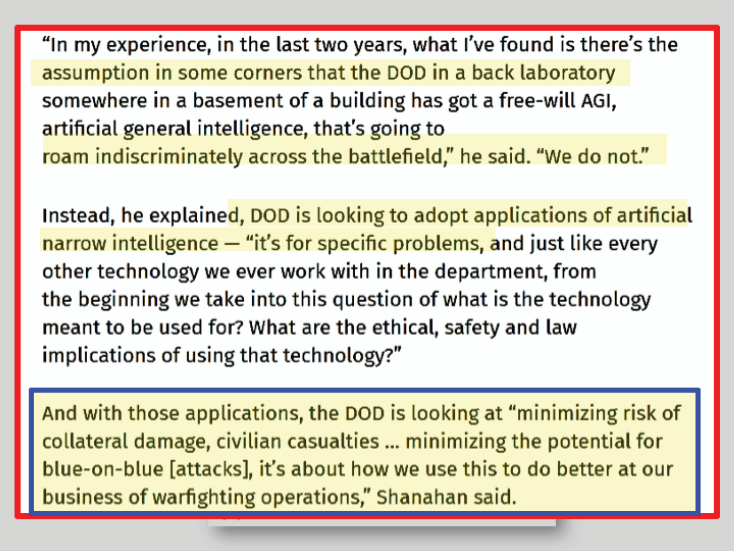
eBrief The Army's Next Generation Combat Vehicles



Comingling of Systems

Work and Shanahan both agreed that it's healthy to have a dialogue about ethics — but they also pointed to misconceptions about the U.S. military's ethical use of technology in general.

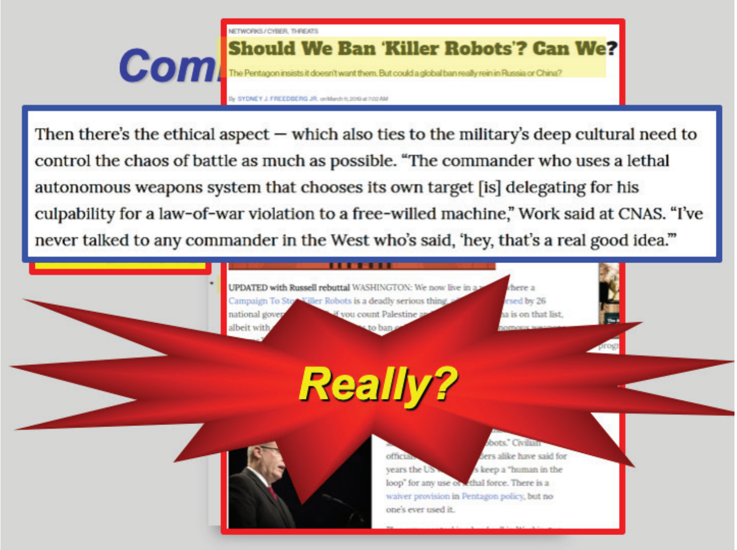
"I would argue that the United States military is the most ethical military force in the history of warfare, and we think the shift to AI-enabled weapons will continue this trend," Work said. The existing policy, which predates any of this current work, he said, "is very clear that these weapons have to be consistent with the laws of armed conflict, supporting the principles of distinction and proportionality, and it has been DOD policy since 2012, three years before the Third Offset, that every weapon we field must be designed and deployed to allow commanders and operators to exercise appropriate levels of human judgment in the lethal application of force."



"In my experience, in the last two years, what I've found is there's the assumption in some corners that the DOD in a back laboratory somewhere in a basement of a building has got a free-will AGI, artificial general intelligence, that's going to roam indiscriminately across the battlefield," he said. "We do not."

Instead, he explained, DOD is looking to adopt applications of artificial narrow intelligence — "it's for specific problems, and just like every other technology we ever work with in the department, from the beginning we take into this question of what is the technology meant to be used for? What are the ethical, safety and law implications of using that technology?"

And with those applications, the DOD is looking at "minimizing risk of collateral damage, civilian casualties ... minimizing the potential for blue-on-blue [attacks], it's about how we use this to do better at our business of warfighting operations," Shanahan said.



Com

NETWORKS / CYBER, THREATS

Should We Ban 'Killer Robots'? Can We?

The Pentagon insists it doesn't want them. But could a global ban really rein in Russia or China?

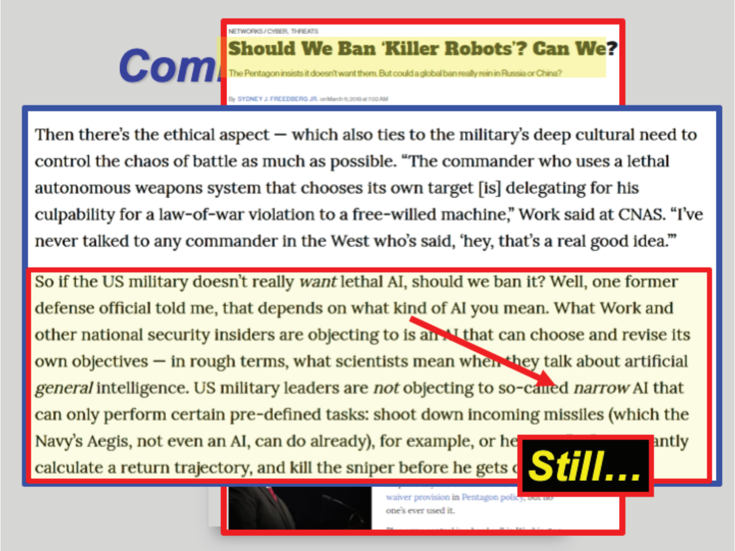
By SYDNEY J. FREEDBERG JR. on March 11, 2019 at 7:02 AM

Then there's the ethical aspect — which also ties to the military's deep cultural need to control the chaos of battle as much as possible. "The commander who uses a lethal autonomous weapons system that chooses its own target [is] delegating for his culpability for a law-of-war violation to a free-willed machine," Work said at CNAS. "I've never talked to any commander in the West who's said, 'hey, that's a real good idea.'"

UPDATED with Russell rebuttal WASHINGTON: We now live in a … where a Campaign To Sto… Killer Robots is a deadly serious thing, … rsed by 26 national gover… if you count Palestine a… na is on that list, albeit with … to ban … nomous …

… progr…

… bots." Civilian officia… ders alike have said for years the US … s keep a "human in the loop" for any use o… ethal force. There is a waiver provision in Pentagon policy, but no one's ever used it.



Com

NETWORKS / CYBER, THREATS

Should We Ban 'Killer Robots'? Can We?

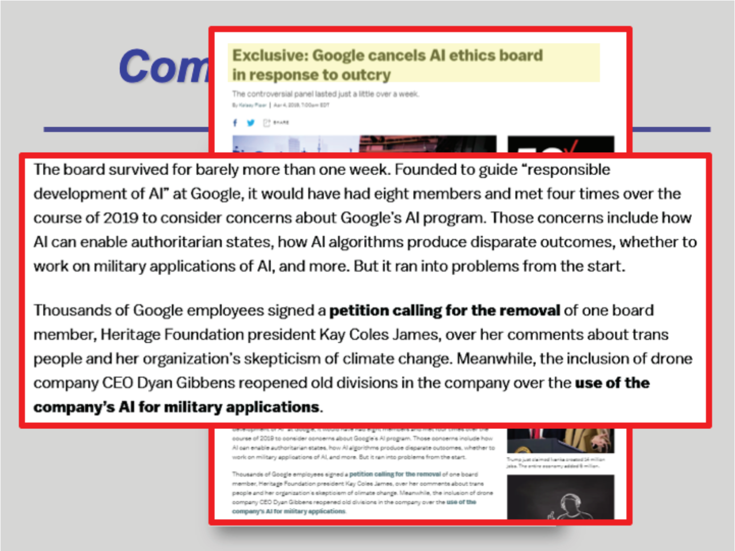
The Pentagon insists it doesn't want them. But could a global ban really rein in Russia or China?

By SYDNEY J. FREEDBERG JR. on March 11, 2019 at 7:02 AM

Then there's the ethical aspect — which also ties to the military's deep cultural need to control the chaos of battle as much as possible. "The commander who uses a lethal autonomous weapons system that chooses its own target [is] delegating for his culpability for a law-of-war violation to a free-willed machine," Work said at CNAS. "I've never talked to any commander in the West who's said, 'hey, that's a real good idea.'"

So if the US military doesn't really *want* lethal AI, should we ban it? Well, one former defense official told me, that depends on what kind of AI you mean. What Work and other national security insiders are objecting to is an AI that can choose and revise its own objectives — in rough terms, what scientists mean when they talk about artificial *general* intelligence. US military leaders are *not* objecting to so-called *narrow* AI that can only perform certain pre-defined tasks: shoot down incoming missiles (which the Navy's Aegis, not even an AI, can do already), for example, or he… antly calculate a return trajectory, and kill the sniper before he gets c…

waiver provision in Pentagon polic… one's ever used it.



Com

Exclusive: Google cancels AI ethics board in response to outcry

The controversial panel lasted just a little over a week.

By Kelsey Piper | Apr 4, 2019, 7:00am EDT

The board survived for barely more than one week. Founded to guide “responsible development of AI” at Google, it would have had eight members and met four times over the course of 2019 to consider concerns about Google’s AI program. Those concerns include how AI can enable authoritarian states, how AI algorithms produce disparate outcomes, whether to work on military applications of AI, and more. But it ran into problems from the start.

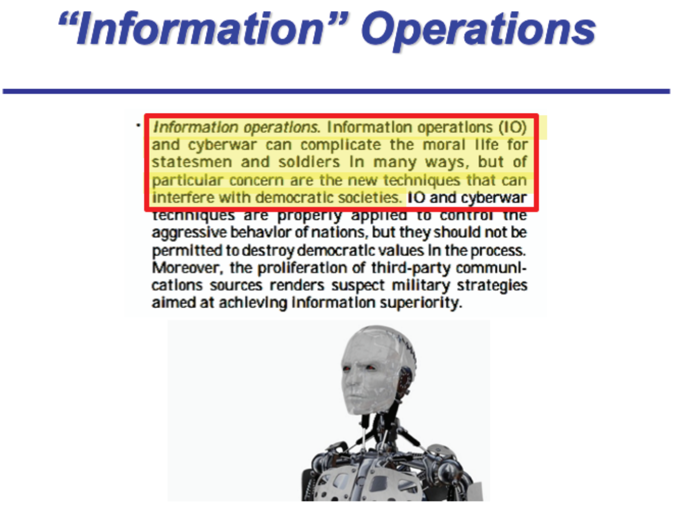
Thousands of Google employees signed a **petition calling for the removal** of one board member, Heritage Foundation president Kay Coles James, over her comments about trans people and her organization’s skepticism of climate change. Meanwhile, the inclusion of drone company CEO Dyan Gibbens reopened old divisions in the company over the **use of the company’s AI for military applications**.

course of 2019 to consider concerns about Google’s AI program. Those concerns include how AI can enable authoritarian states, how AI algorithms produce disparate outcomes, whether to work on military applications of AI, and more. But it ran into problems from the start.

Thousands of Google employees signed a **petition calling for the removal** of one board member, Heritage Foundation president Kay Coles James, over her comments about trans people and her organization’s skepticism of climate change. Meanwhile, the inclusion of drone company CEO Dyan Gibbens reopened old divisions in the company over the **use of the company’s AI for military applications**.

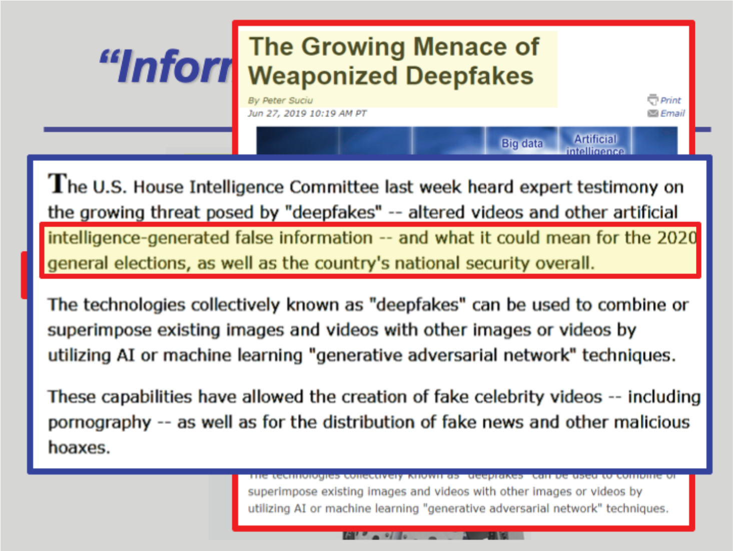
Trump just claimed Ivanka created 14 million jobs. The entire economy added 6 million.

“Information” Operations



“Information” Operations

- *Information operations.* Information operations (IO) and cyberwar can complicate the moral life for statesmen and soldiers in many ways, but of particular concern are the new techniques that can interfere with democratic societies. IO and cyberwar techniques are properly applied to control the aggressive behavior of nations, but they should not be permitted to destroy democratic values in the process. Moreover, the proliferation of third-party communications sources renders suspect military strategies aimed at achieving information superiority.



“Infor

The Growing Menace of Weaponized Deepfakes

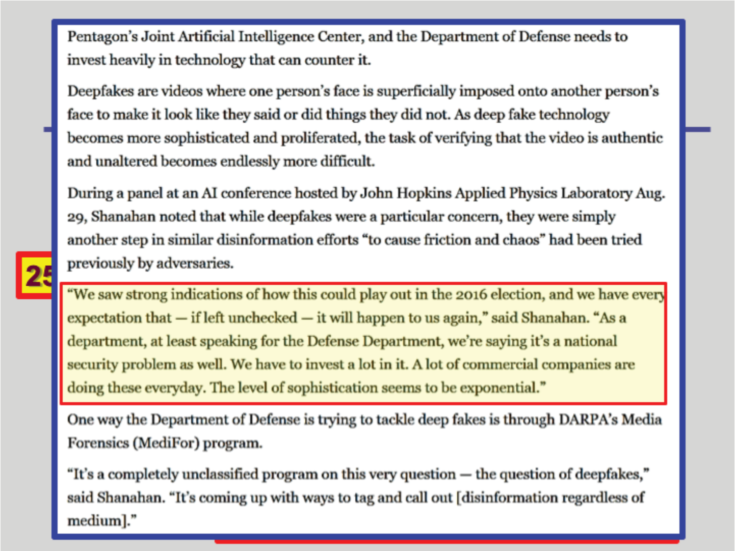
By Peter Suciu
Jun 27, 2019 10:19 AM PT

The U.S. House Intelligence Committee last week heard expert testimony on the growing threat posed by "deepfakes" -- altered videos and other artificial intelligence-generated false information -- and what it could mean for the 2020 general elections, as well as the country's national security overall.

The technologies collectively known as "deepfakes" can be used to combine or superimpose existing images and videos with other images or videos by utilizing AI or machine learning "generative adversarial network" techniques.

These capabilities have allowed the creation of fake celebrity videos -- including pornography -- as well as for the distribution of fake news and other malicious hoaxes.

The technologies collectively known as "deepfakes" can be used to combine or superimpose existing images and videos with other images or videos by utilizing AI or machine learning "generative adversarial network" techniques.



25

Pentagon's Joint Artificial Intelligence Center, and the Department of Defense needs to invest heavily in technology that can counter it.

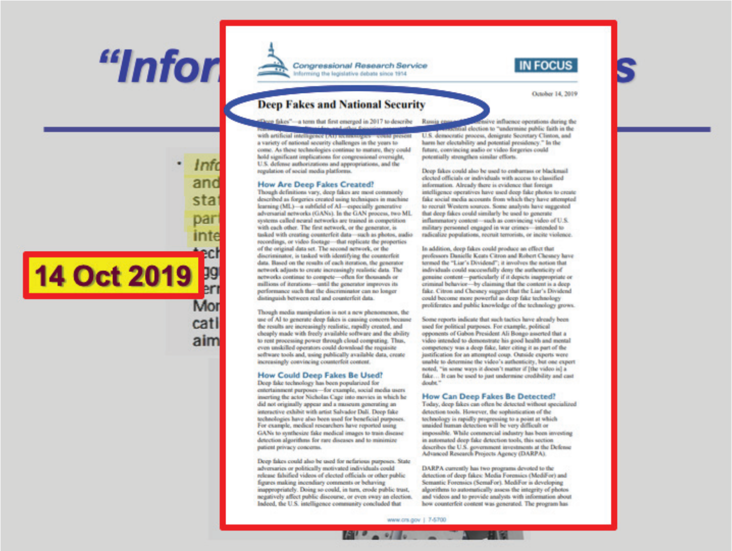
Deepfakes are videos where one person's face is superficially imposed onto another person's face to make it look like they said or did things they did not. As deep fake technology becomes more sophisticated and proliferated, the task of verifying that the video is authentic and unaltered becomes endlessly more difficult.

During a panel at an AI conference hosted by John Hopkins Applied Physics Laboratory Aug. 29, Shanahan noted that while deepfakes were a particular concern, they were simply another step in similar disinformation efforts "to cause friction and chaos" had been tried previously by adversaries.

"We saw strong indications of how this could play out in the 2016 election, and we have every expectation that — if left unchecked — it will happen to us again," said Shanahan. "As a department, at least speaking for the Defense Department, we're saying it's a national security problem as well. We have to invest a lot in it. A lot of commercial companies are doing these everyday. The level of sophistication seems to be exponential."

One way the Department of Defense is trying to tackle deep fakes is through DARPA's Media Forensics (MediFor) program.

"It's a completely unclassified program on this very question — the question of deepfakes," said Shanahan. "It's coming up with ways to tag and call out [disinformation regardless of medium]."


"Infor
s
Info
and
stat
par
inte
tech
gg
err
Mor
catl
aim

14 Oct 2019

Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

October 14, 2019

Deep Fakes and National Security

"Deep fakes"—a term that first emerged in 2017 to describe [illegible] with artificial intelligence (AI) technologies—could present a variety of national security challenges in the years to come. As these technologies continue to mature, they could hold significant implications for congressional oversight, U.S. defense authorizations and appropriations, and the regulation of social media platforms.

How Are Deep Fakes Created?

Though definitions vary, deep fakes are most commonly described as forgeries created using techniques in machine learning (ML)—a subfield of AI—especially generative adversarial networks (GANs). In the GAN process, two ML systems called neural networks are trained in competition with each other. The first network, or the generator, is tasked with creating counterfeit data—such as photos, audio recordings, or video footage—that replicate the properties of the original data set. The second network, or the discriminator, is tasked with identifying the counterfeit data. Based on the results of each iteration, the generator network adjusts to create increasingly realistic data. The networks continue to compete—often for thousands or millions of iterations—until the generator improves its performance such that the discriminator can no longer distinguish between real and counterfeit data.

Though media manipulation is not a new phenomenon, the use of AI to generate deep fakes is causing concern because the results are increasingly realistic, rapidly created, and cheaply made with freely available software and the ability to rent processing power through cloud computing. Thus, even unskilled operators could download the requisite software tools and, using publically available data, create increasingly convincing counterfeit content.

How Could Deep Fakes Be Used?

Deep fake technology has been popularized for entertainment purposes—for example, social media users inserting the actor Nicholas Cage into movies in which he did not originally appear and a museum generating an interactive exhibit with artist Salvador Dali. Deep fake technologies have also been used for beneficial purposes. For example, medical researchers have reported using GANs to synthesize fake medical images to train disease detection algorithms for rare diseases and to minimize patient privacy concerns.

Deep fakes could also be used for nefarious purposes. State adversaries or politically motivated individuals could release falsified videos of elected officials or other public figures making incendiary comments or behaving inappropriately. Doing so could, in turn, erode public trust, negatively affect public discourse, or even sway an election. Indeed, the U.S. intelligence community concluded that Russia [illegible] extensive influence operations during the [illegible] presidential election to "undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency." In the future, convincing audio or video forgeries could potentially strengthen similar efforts.

Deep fakes could also be used to embarrass or blackmail elected officials or individuals with access to classified information. Already there is evidence that foreign intelligence operatives have used deep fake photos to create fake social media accounts from which they have attempted to recruit Western sources. Some analysts have suggested that deep fakes could similarly be used to generate inflammatory content—such as convincing video of U.S. military personnel engaged in war crimes—intended to radicalize populations, recruit terrorists, or incite violence.

In addition, deep fakes could produce an effect that professors Danielle Keats Citron and Robert Chesney have termed the "Liar's Dividend"; it involves the notion that individuals could successfully deny the authenticity of genuine content—particularly if it depicts inappropriate or criminal behavior—by claiming that the content is a deep fake. Citron and Chesney suggest that the Liar's Dividend could become more powerful as deep fake technology proliferates and public knowledge of the technology grows.

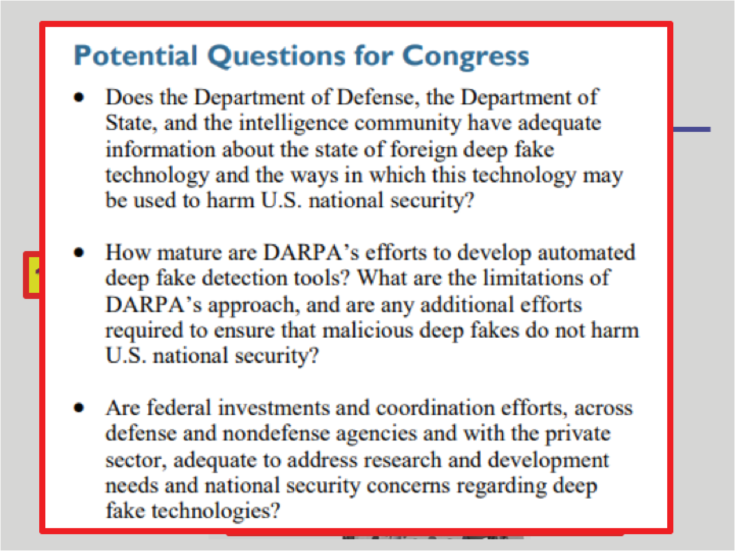
Some reports indicate that such tactics have already been used for political purposes. For example, political opponents of Gabon President Ali Bongo asserted that a video intended to demonstrate his good health and mental competency was a deep fake, later citing it as part of the justification for an attempted coup. Outside experts were unable to determine the video's authenticity, but one expert noted, "in some ways it doesn't matter if [the video is] a fake… It can be used to just undermine credibility and cast doubt."

How Can Deep Fakes Be Detected?

Today, deep fakes can often be detected without specialized detection tools. However, the sophistication of the technology is rapidly progressing to a point at which unaided human detection will be very difficult or impossible. While commercial industry has been investing in automated deep fake detection tools, this section describes the U.S. government investments at the Defense Advanced Research Projects Agency (DARPA).

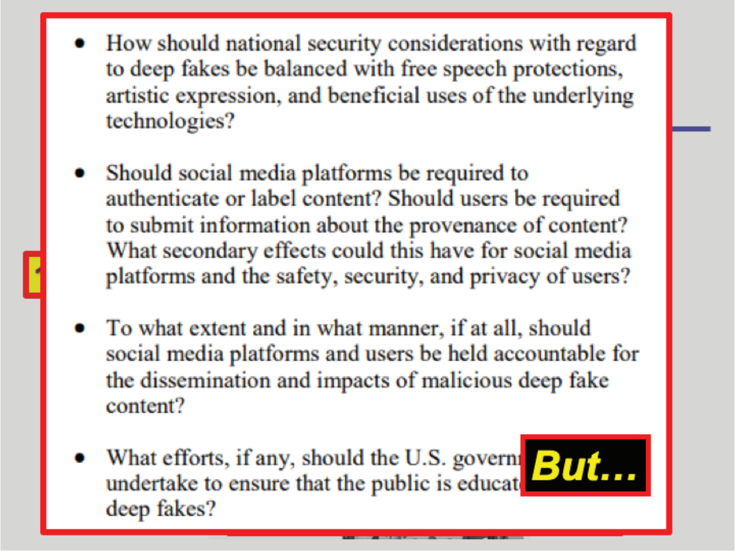
DARPA currently has two programs devoted to the detection of deep fakes: Media Forensics (MediFor) and Semantic Forensics (SemaFor). MediFor is developing algorithms to automatically assess the integrity of photos and videos and to provide analysts with information about how counterfeit content was generated. The program has

www.crs.gov | 7-5700

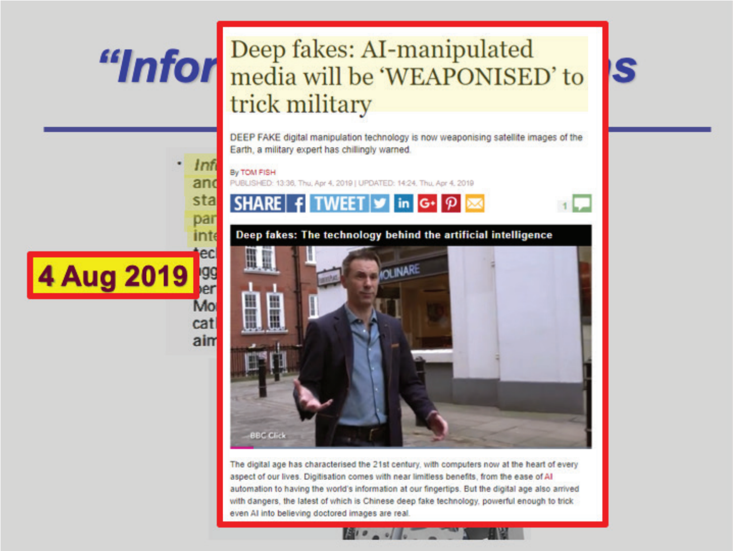


Potential Questions for Congress

- Does the Department of Defense, the Department of State, and the intelligence community have adequate information about the state of foreign deep fake technology and the ways in which this technology may be used to harm U.S. national security?
- How mature are DARPA's efforts to develop automated deep fake detection tools? What are the limitations of DARPA's approach, and are any additional efforts required to ensure that malicious deep fakes do not harm U.S. national security?
- Are federal investments and coordination efforts, across defense and nondefense agencies and with the private sector, adequate to address research and development needs and national security concerns regarding deep fake technologies?



- How should national security considerations with regard to deep fakes be balanced with free speech protections, artistic expression, and beneficial uses of the underlying technologies?
- Should social media platforms be required to authenticate or label content? Should users be required to submit information about the provenance of content? What secondary effects could this have for social media platforms and the safety, security, and privacy of users?
- To what extent and in what manner, if at all, should social media platforms and users be held accountable for the dissemination and impacts of malicious deep fake content?
- What efforts, if any, should the U.S. governm undertake to ensure that the public is educat deep fakes?



“Infor ... s

- *Inf*
and
sta
par
inte
tec
agg
per
Mo
cat
aim

4 Aug 2019

Deep fakes: AI-manipulated media will be ‘WEAPONISED’ to trick military

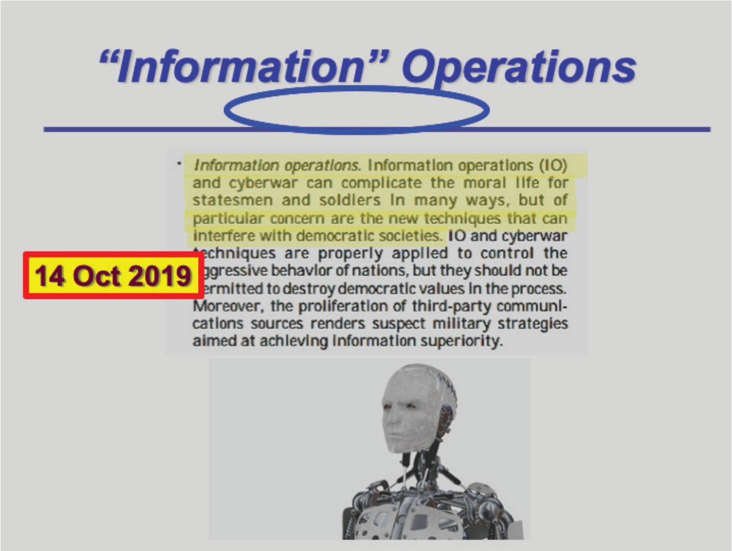
DEEP FAKE digital manipulation technology is now weaponising satellite images of the Earth, a military expert has chillingly warned.

By TOM FISH

PUBLISHED: 13:36, Thu, Apr 4, 2019 | UPDATED: 14:24, Thu, Apr 4, 2019

SHARE
f
TWEET
in
G+
1
Deep fakes: The technology behind the artificial intelligence
MOLINARE
BBC Click

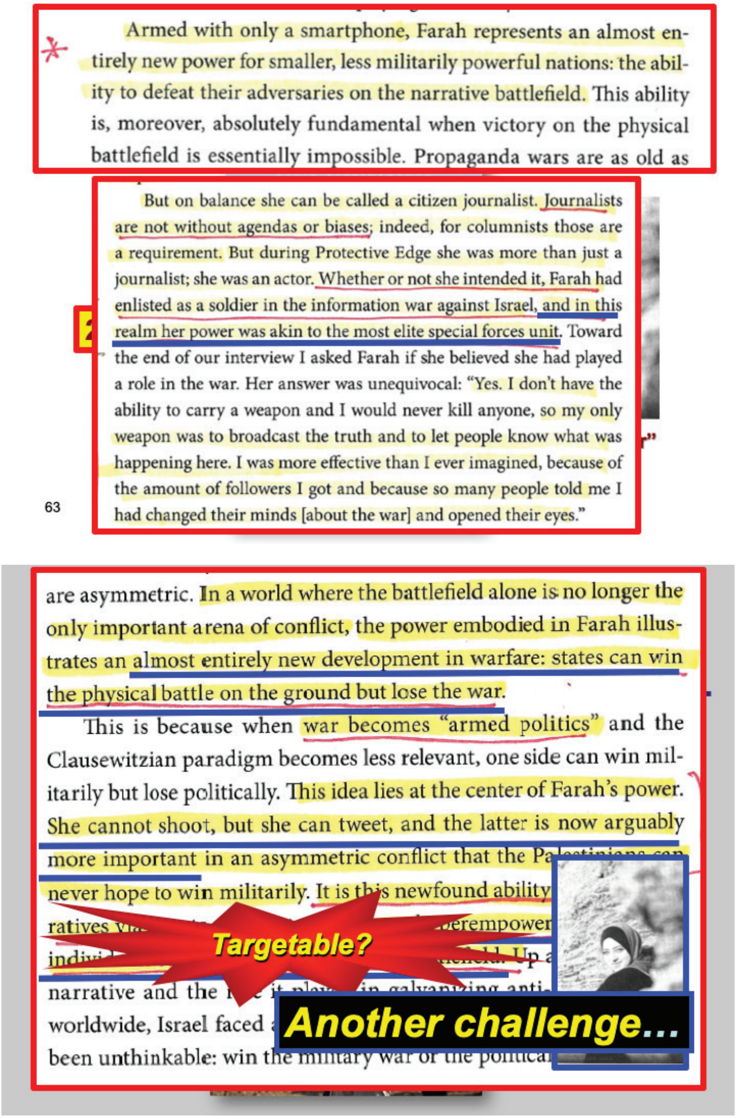
The digital age has characterised the 21st century, with computers now at the heart of every aspect of our lives. Digitisation comes with near limitless benefits, from the ease of AI automation to having the world's information at our fingertips. But the digital age also arrived with dangers, the latest of which is Chinese deep fake technology, powerful enough to trick even AI into believing doctored images are real.



“Information” Operations

- *Information operations.* Information operations (IO) and cyberwar can complicate the moral life for statesmen and soldiers in many ways, but of particular concern are the new techniques that can interfere with democratic societies. IO and cyberwar echniques are properly applied to control the ggressive behavior of nations, but they should not be ermitted to destroy democratic values in the process. Moreover, the proliferation of third-party communications sources renders suspect military strategies aimed at achieving information superiority.

14 Oct 2019



*Armed with only a smartphone, Farah represents an almost entirely new power for smaller, less militarily powerful nations: the ability to defeat their adversaries on the narrative battlefield. This ability is, moreover, absolutely fundamental when victory on the physical battlefield is essentially impossible. Propaganda wars are as old as

But on balance she can be called a citizen journalist. Journalists are not without agendas or biases; indeed, for columnists those are a requirement. But during Protective Edge she was more than just a journalist; she was an actor. Whether or not she intended it, Farah had enlisted as a soldier in the information war against Israel, and in this realm her power was akin to the most elite special forces unit. Toward the end of our interview I asked Farah if she believed she had played a role in the war. Her answer was unequivocal: "Yes. I don't have the ability to carry a weapon and I would never kill anyone, so my only weapon was to broadcast the truth and to let people know what was happening here. I was more effective than I ever imagined, because of the amount of followers I got and because so many people told me I had changed their minds [about the war] and opened their eyes."

63

are asymmetric. In a world where the battlefield alone is no longer the only important arena of conflict, the power embodied in Farah illustrates an almost entirely new development in warfare: states can win the physical battle on the ground but lose the war.

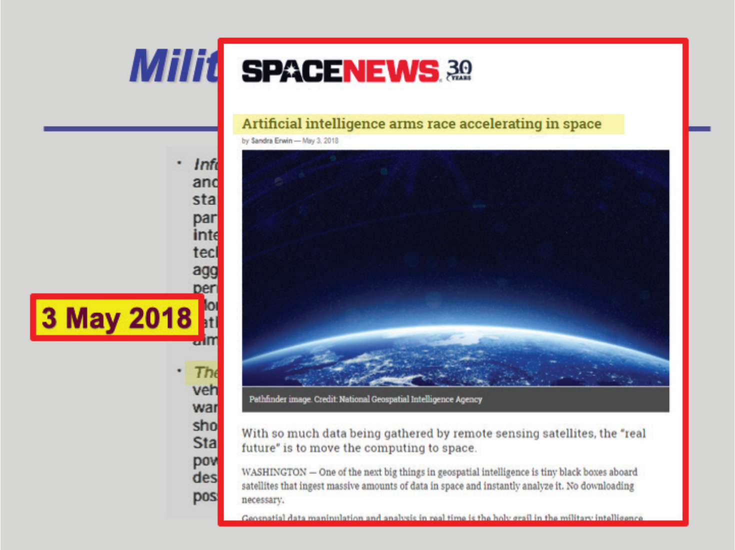
This is because when war becomes "armed politics" and the Clausewitzian paradigm becomes less relevant, one side can win militarily but lose politically. This idea lies at the center of Farah's power. She cannot shoot, but she can tweet, and the latter is now arguably more important in an asymmetric conflict that the Palestinians can never hope to win militarily. It is this newfound ability ratives via ... peremplower indivi ... field. Up a narrative and the r... it play... in galvanizing anti- worldwide, Israel faced a been unthinkable: win the military war or the political

Militarization of Space

Militarization of Space

-

- *The militarization of space* Satellites and space vehicles are irrevocably integrated into modern warfare. However, this does not mean that space should become another battlefield. Rather, the United States should use its prestige as the preeminent space power to forge an international consensus that designates space a neutral area and, therefore, possibly avoid a space weapons race.



3 May 2018

Artificial intelligence arms race accelerating in space

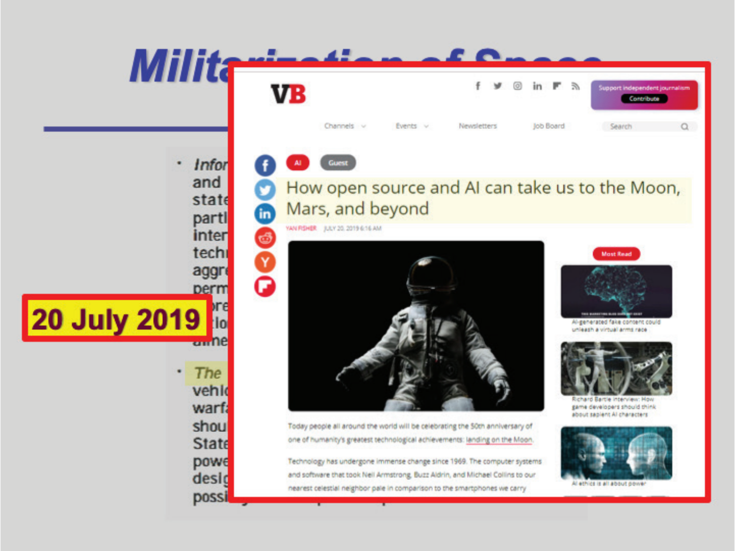
by Sandra Erwin — May 3, 2018

Pathfinder image. Credit: National Geospatial Intelligence Agency

With so much data being gathered by remote sensing satellites, the "real future" is to move the computing to space.

WASHINGTON — One of the next big things in geospatial intelligence is tiny black boxes aboard satellites that ingest massive amounts of data in space and instantly analyze it. No downloading necessary.

Geospatial data manipulation and analysis in real time is the holy grail in the military intelligence



20 July 2019

How open source and AI can take us to the Moon, Mars, and beyond

YAN FISHER JULY 20, 2019 6:16 AM

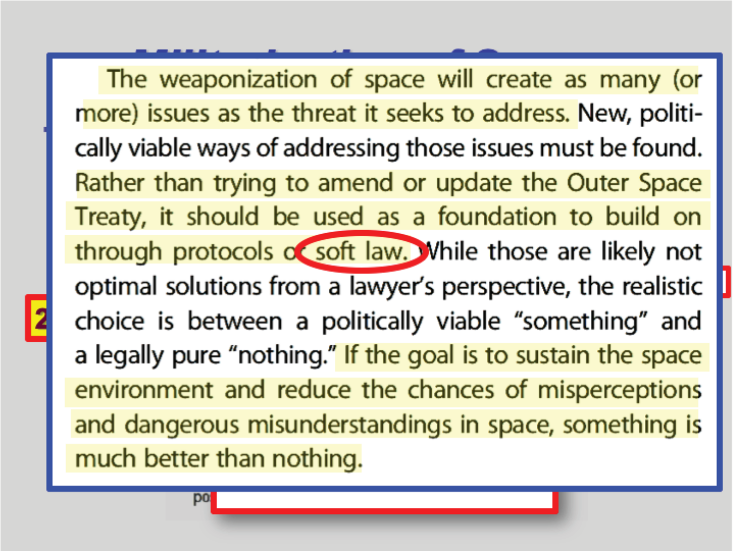
Today people all around the world will be celebrating the 50th anniversary of one of humanity's greatest technological achievements: landing on the Moon.

Technology has undergone immense change since 1969. The computer systems and software that took Neil Armstrong, Buzz Aldrin, and Michael Collins to our nearest celestial neighbor pale in comparison to the smartphones we carry

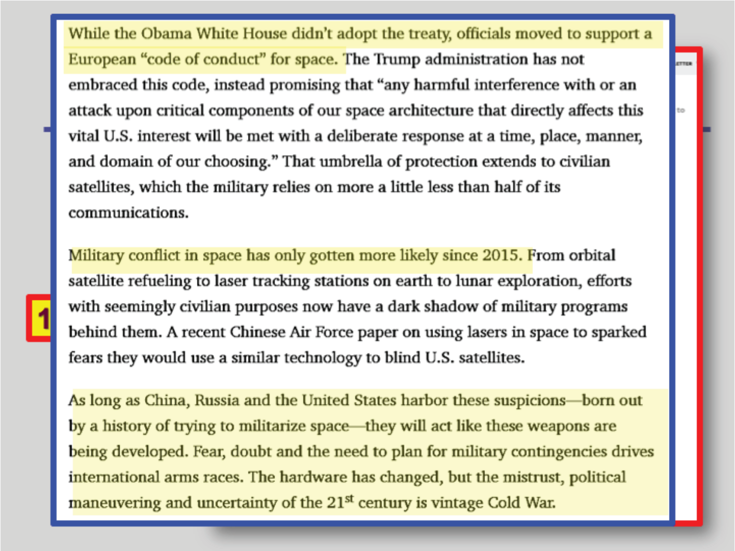
AI-generated fake content could unleash a virtual arms race

Richard Bartle interview: How game developers should think about sapient AI characters

AI ethics is all about power



The weaponization of space will create as many (or more) issues as the threat it seeks to address. New, politically viable ways of addressing those issues must be found. Rather than trying to amend or update the Outer Space Treaty, it should be used as a foundation to build on through protocols or soft law. While those are likely not optimal solutions from a lawyer's perspective, the realistic choice is between a politically viable "something" and a legally pure "nothing." If the goal is to sustain the space environment and reduce the chances of misperceptions and dangerous misunderstandings in space, something is much better than nothing.



While the Obama White House didn't adopt the treaty, officials moved to support a European "code of conduct" for space. The Trump administration has not embraced this code, instead promising that "any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing." That umbrella of protection extends to civilian satellites, which the military relies on more a little less than half of its communications.

Military conflict in space has only gotten more likely since 2015. From orbital satellite refueling to laser tracking stations on earth to lunar exploration, efforts with seemingly civilian purposes now have a dark shadow of military programs behind them. A recent Chinese Air Force paper on using lasers in space to sparked fears they would use a similar technology to blind U.S. satellites.

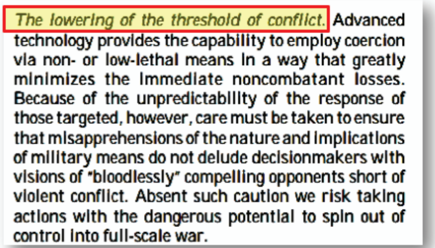
As long as China, Russia and the United States harbor these suspicions—born out by a history of trying to militarize space—they will act like these weapons are being developed. Fear, doubt and the need to plan for military contingencies drives international arms races. The hardware has changed, but the mistrust, political maneuvering and uncertainty of the 21st century is vintage Cold War.

Militarization of Space

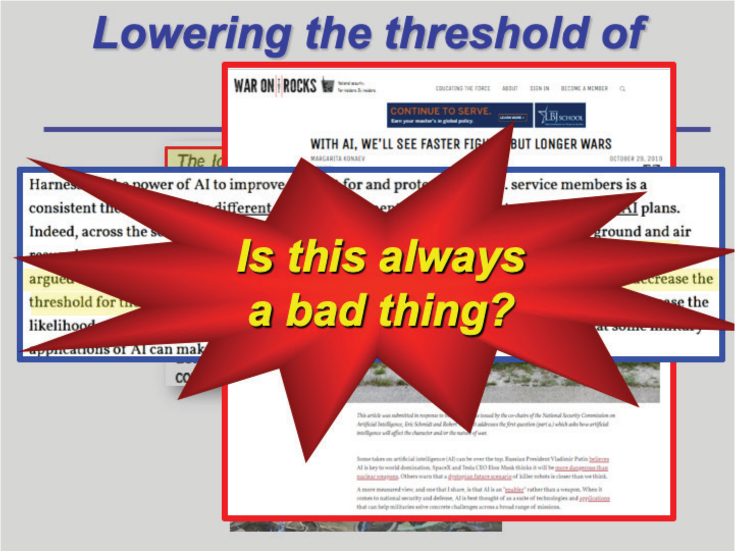
- *The militarization of space.* Satellites and space vehicles are irrevocably integrated into modern warfare. However, this does not mean that space should become another battlefield. Rather, the United States should use its prestige as the preeminent space power to forge an international consensus that designates space a neutral area and, therefore, possibly avoid a space weapons race.

Lowering the threshold of conflict?

Lowering the threshold of conflict?



The lowering of the threshold of conflict. Advanced technology provides the capability to employ coercion via non- or low-lethal means in a way that greatly minimizes the immediate noncombatant losses. Because of the unpredictability of the response of those targeted, however, care must be taken to ensure that misapprehensions of the nature and implications of military means do not delude decisionmakers with visions of "bloodlessly" compelling opponents short of violent conflict. Absent such caution we risk taking actions with the dangerous potential to spin out of control into full-scale war.



Lowering the threshold of

WAR ON ROCKS

EDUCATING THE FORCE ABOUT SIGN IN BECOME A MEMBER

CONTINUE TO SERVE. Earn your master's in global policy. LBJ SCHOOL

WITH AI, WE'LL SEE FASTER FIG BUT LONGER WARS

MARGARITA KONAEV

OCTOBER 29, 2019

The lo

Harnes power of AI to improve for and prote . service members is a consistent th different AI plans. Indeed, across the s ground and air

argued crease the threshold for th se the likelihood at some military applications of AI can mak

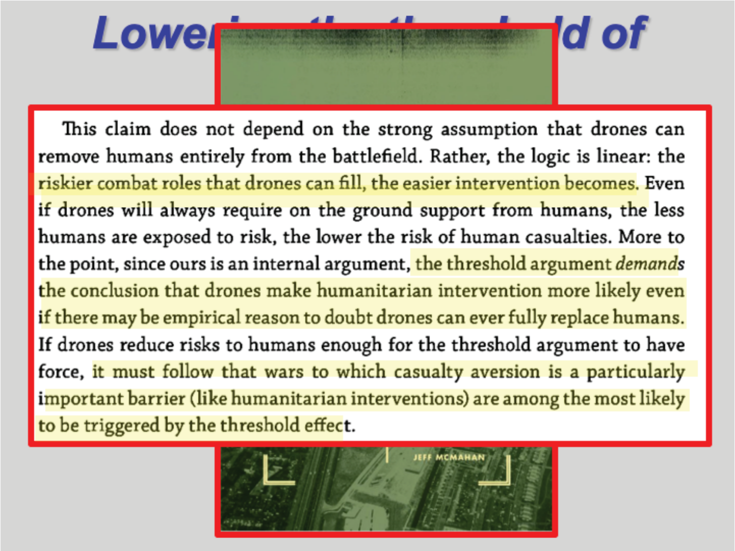
co

Is this always a bad thing?

This article was submitted in response to issued by the co-chairs of the National Security Commission on Artificial Intelligence, Eric Schmidt and Robert addresses the first question (part a.) which asks how artificial intelligence will affect the character and/or the natu of war.

Some takes on artificial intelligence (AI) can be over the top. Russian President Vladimir Putin believes AI is key to world domination. SpaceX and Tesla CEO Elon Musk thinks it will be more dangerous than nuclear weapons. Others warn that a dystopian future scenario of killer robots is closer than we think.

A more measured view, and one that I share, is that AI is an "enabler" rather than a weapon. When it comes to national security and defense, AI is best thought of as a suite of technologies and applications that can help militaries solve concrete challenges across a broad range of missions.

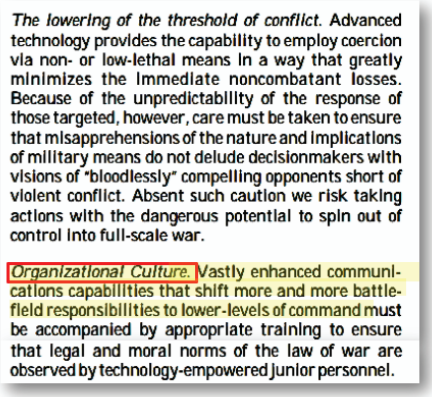


Lowe d of

This claim does not depend on the strong assumption that drones can remove humans entirely from the battlefield. Rather, the logic is linear: the riskier combat roles that drones can fill, the easier intervention becomes. Even if drones will always require on the ground support from humans, the less humans are exposed to risk, the lower the risk of human casualties. More to the point, since ours is an internal argument, the threshold argument *demands* the conclusion that drones make humanitarian intervention more likely even if there may be empirical reason to doubt drones can ever fully replace humans. If drones reduce risks to humans enough for the threshold argument to have force, it must follow that wars to which casualty aversion is a particularly important barrier (like humanitarian interventions) are among the most likely to be triggered by the threshold effect.

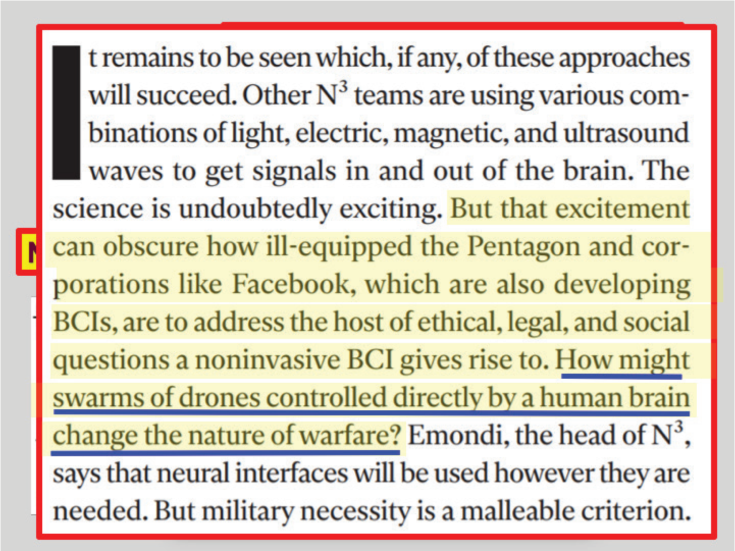
Organizational Culture

Organizational Culture

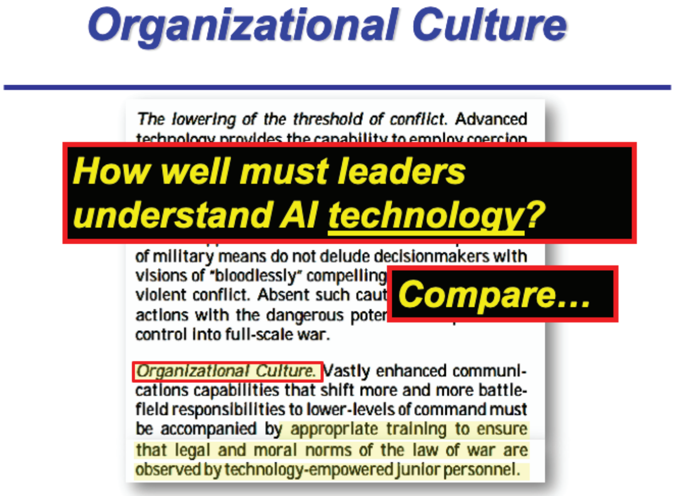


The lowering of the threshold of conflict. Advanced technology provides the capability to employ coercion via non- or low-lethal means in a way that greatly minimizes the immediate noncombatant losses. Because of the unpredictability of the response of those targeted, however, care must be taken to ensure that misapprehensions of the nature and implications of military means do not delude decisionmakers with visions of "bloodlessly" compelling opponents short of violent conflict. Absent such caution we risk taking actions with the dangerous potential to spin out of control into full-scale war.

Organizational Culture. Vastly enhanced communications capabilities that shift more and more battlefield responsibilities to lower-levels of command must be accompanied by appropriate training to ensure that legal and moral norms of the law of war are observed by technology-empowered junior personnel.



It remains to be seen which, if any, of these approaches will succeed. Other N^3 teams are using various combinations of light, electric, magnetic, and ultrasound waves to get signals in and out of the brain. The science is undoubtedly exciting. But that excitement can obscure how ill-equipped the Pentagon and corporations like Facebook, which are also developing BCIs, are to address the host of ethical, legal, and social questions a noninvasive BCI gives rise to. How might swarms of drones controlled directly by a human brain change the nature of warfare? Emondi, the head of N^3, says that neural interfaces will be used however they are needed. But military necessity is a malleable criterion.



Organizational Culture

The lowering of the threshold of conflict. Advanced technology provides the capability to employ coercion

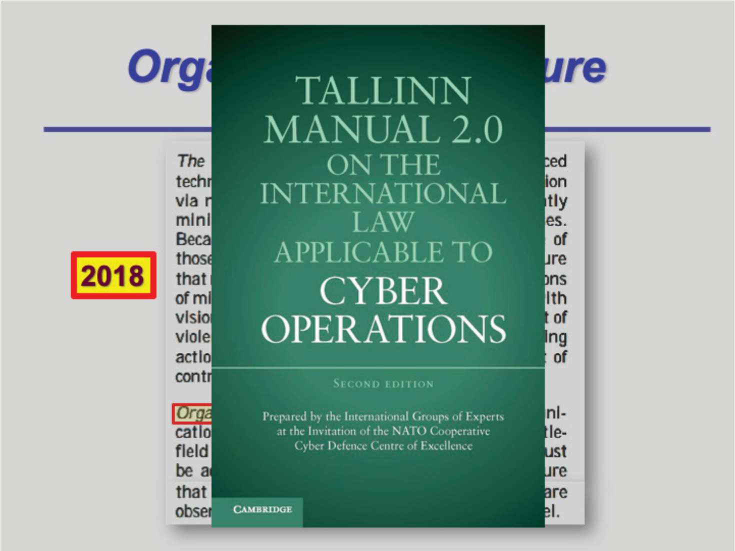
How well must leaders understand AI technology?

of military means do not delude decisionmakers with visions of "bloodlessly" compelling

Compare…

violent conflict. Absent such caut actions with the dangerous poter control into full-scale war.

Organizational Culture. Vastly enhanced communications capabilities that shift more and more battlefield responsibilities to lower-levels of command must be accompanied by appropriate training to ensure that legal and moral norms of the law of war are observed by technology-empowered junior personnel.



Org ure

The ced
techn ion
via r tly
mini es.
Beca of
those ure
that ons
of mi ith
visio t of
viole ing
actio of
contr

Orga ni-
catio tle-
field ust
be a ure
that are
obser el.

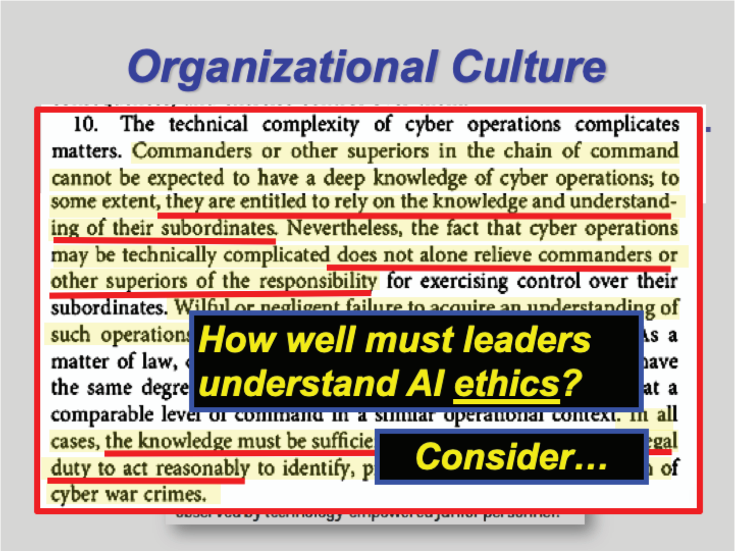
2018

TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

Second edition

Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence

Cambridge



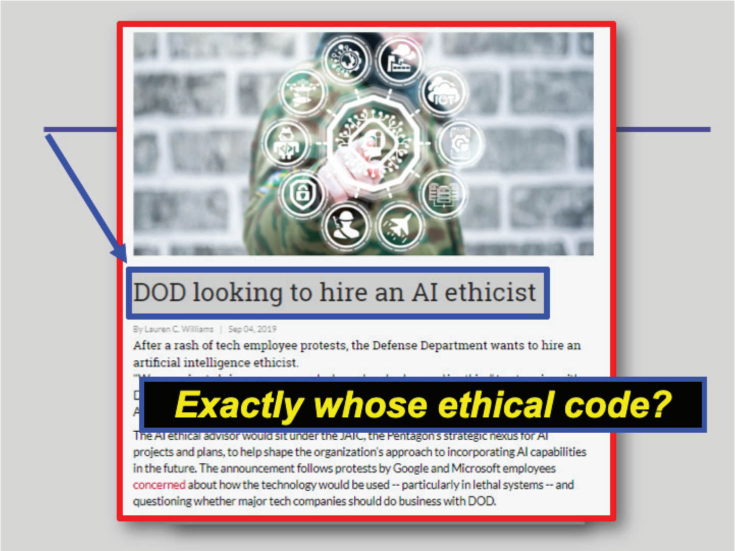
Organizational Culture

10. The technical complexity of cyber operations complicates matters. Commanders or other superiors in the chain of command cannot be expected to have a deep knowledge of cyber operations; to some extent, they are entitled to rely on the knowledge and understanding of their subordinates. Nevertheless, the fact that cyber operations may be technically complicated does not alone relieve commanders or other superiors of the responsibility for exercising control over their subordinates. Wilful or negligent failure to acquire an understanding of
such operation
matter of law,
the same degre
comparable level of command in a similar operational context. In all
cases, the knowledge must be sufficie
duty to act reasonably to identify, p
cyber war crimes.

As a
have
at a
egal
of

How well must leaders understand AI *ethics*?

Consider…



DOD looking to hire an AI ethicist

By Lauren C. Williams | Sep 04, 2019

After a rash of tech employee protests, the Defense Department wants to hire an artificial intelligence ethicist.

The AI ethical advisor would sit under the JAIC, the Pentagon's strategic nexus for AI projects and plans, to help shape the organization's approach to incorporating AI capabilities in the future. The announcement follows protests by Google and Microsoft employees concerned about how the technology would be used -- particularly in lethal systems -- and questioning whether major tech companies should do business with DOD.

Exactly whose ethical code?

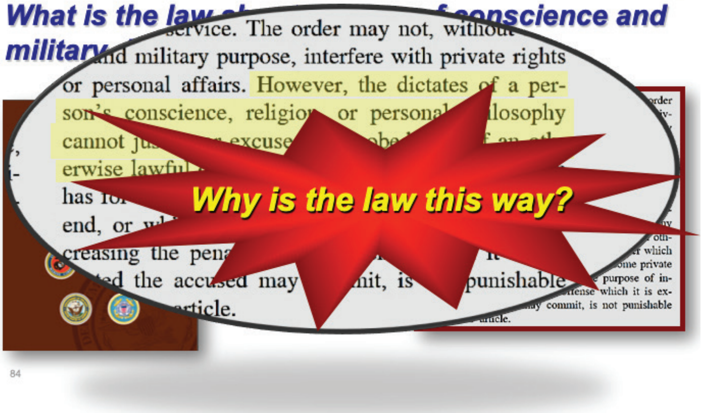
Ethics Codes

What is the law about matters of conscience and military duties?

83

Ethics Codes

What is the law a… …conscience and military…



service. The order may not, without
…nd military purpose, interfere with private rights
or personal affairs. However, the dictates of a per-
son's conscience, religio… or personal …ilosophy
cannot ju… …excuse… …obe… …f an oth-
erwise lawful…
has fo…
end, or w…
creasing the pena…
…ted the accused may …mit, is … punishable
…article.

84

Ethics Codes

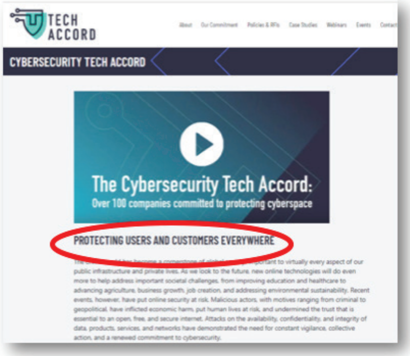
➢ **Do we live in a world of ethical asymmetries?**

85

Ethics Codes

➢ **Do we live in a world of ethical asymmetries?**

14 Apr 2018



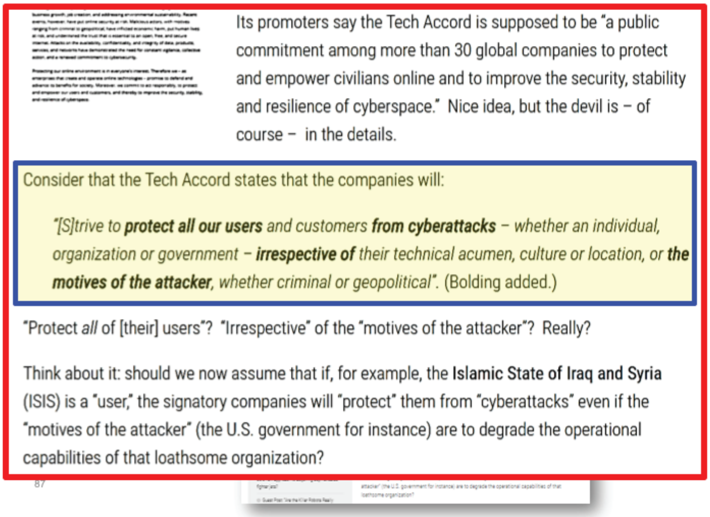
CYBERSECURITY TECH ACCORD

The Cybersecurity Tech Accord:
Over 100 companies committed to protecting cyberspace

PROTECTING USERS AND CUSTOMERS EVERYWHERE

The online world has become a cornerstone of global society, important to virtually every aspect of our public infrastructure and private lives. As we look to the future, new online technologies will do even more to help address important societal challenges, from improving education and healthcare to advancing agriculture, business growth, job creation, and addressing environmental sustainability. Recent events, however, have put online security at risk. Malicious actors, with motives ranging from criminal to geopolitical, have inflicted economic harm, put human lives at risk, and undermined the trust that is essential to an open, free, and secure internet. Attacks on the availability, confidentiality, and integrity of data, products, services, and networks have demonstrated the need for constant vigilance, collective action, and a renewed commitment to cybersecurity.

86



Its promoters say the Tech Accord is supposed to be "a public commitment among more than 30 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace." Nice idea, but the devil is – of course – in the details.

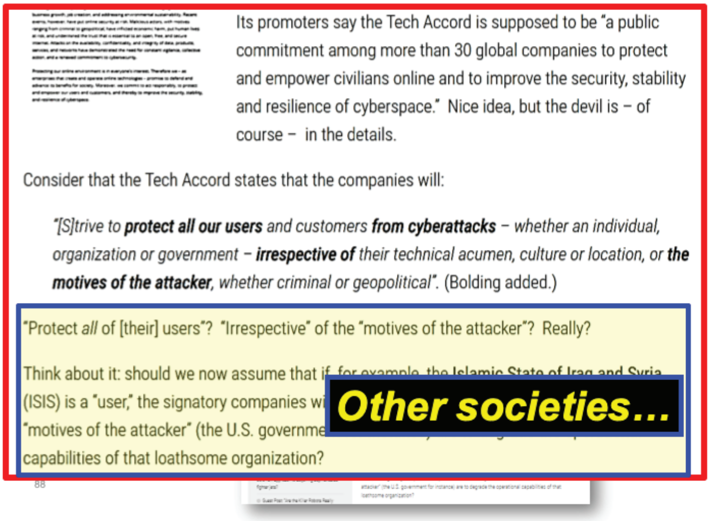
Consider that the Tech Accord states that the companies will:

> "[S]trive to **protect all our users** and customers **from cyberattacks** – whether an individual, organization or government – **irrespective of** their technical acumen, culture or location, or **the motives of the attacker**, whether criminal or geopolitical". (Bolding added.)

"Protect *all* of [their] users"? "Irrespective" of the "motives of the attacker"? Really?

Think about it: should we now assume that if, for example, the **Islamic State of Iraq and Syria** (ISIS) is a "user," the signatory companies will "protect" them from "cyberattacks" even if the "motives of the attacker" (the U.S. government for instance) are to degrade the operational capabilities of that loathsome organization?

87



Its promoters say the Tech Accord is supposed to be "a public commitment among more than 30 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace." Nice idea, but the devil is – of course – in the details.

Consider that the Tech Accord states that the companies will:

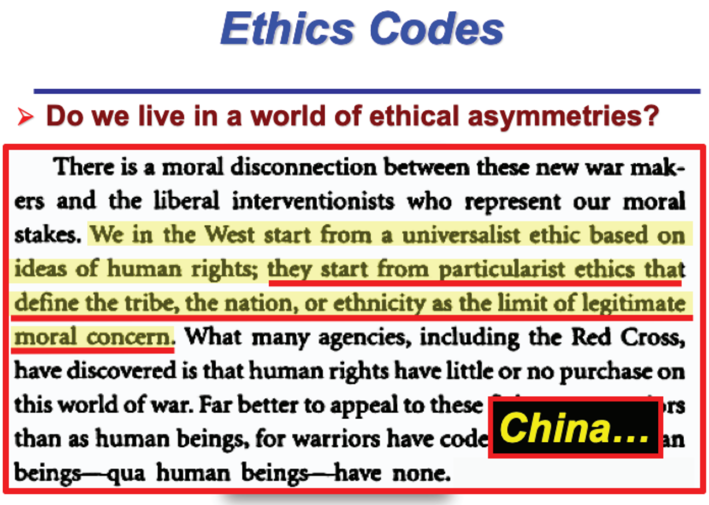
> "[S]trive to **protect all our users** and customers **from cyberattacks** – whether an individual, organization or government – **irrespective of** their technical acumen, culture or location, or **the motives of the attacker**, whether criminal or geopolitical". (Bolding added.)

"Protect *all* of [their] users"? "Irrespective" of the "motives of the attacker"? Really?

Think about it: should we now assume that if, for example, the Islamic State of Iraq and Syria (ISIS) is a "user," the signatory companies wi "motives of the attacker" (the U.S. governme capabilities of that loathsome organization?

Other societies…

88

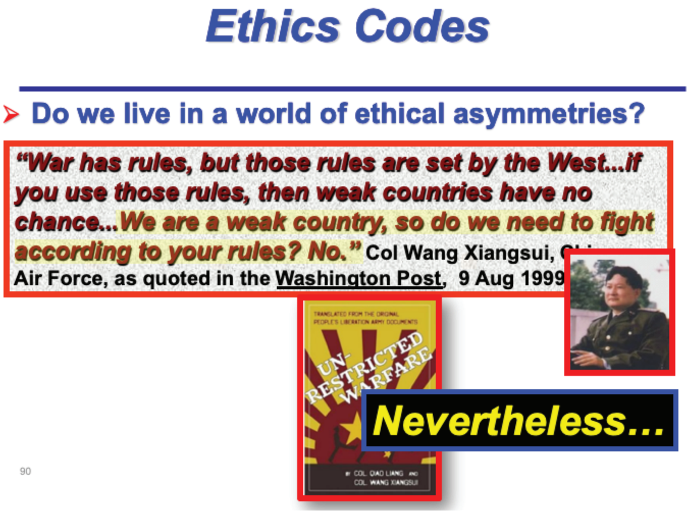


Ethics Codes

- Do we live in a world of ethical asymmetries?

There is a moral disconnection between these new war makers and the liberal interventionists who represent our moral stakes. We in the West start from a universalist ethic based on ideas of human rights; they start from particularist ethics that define the tribe, the nation, or ethnicity as the limit of legitimate moral concern. What many agencies, including the Red Cross, have discovered is that human rights have little or no purchase on this world of war. Far better to appeal to these f rs than as human beings, for warriors have code an beings—qua human beings—have none.

China…



Ethics Codes

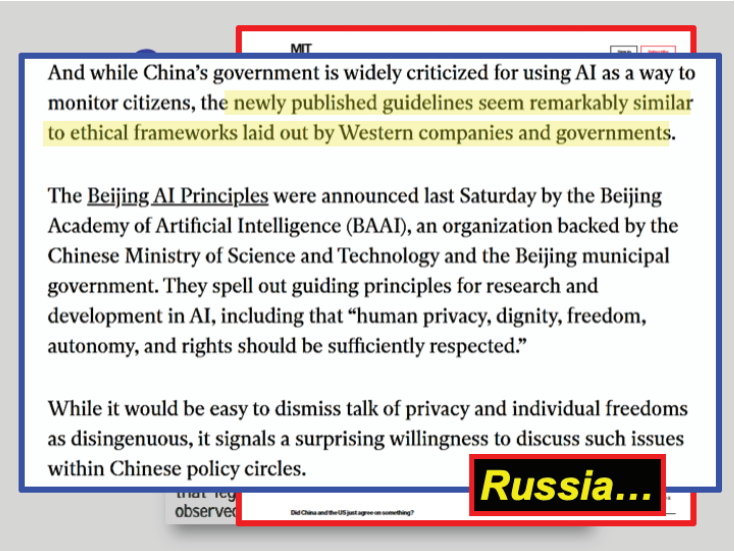
- Do we live in a world of ethical asymmetries?

"War has rules, but those rules are set by the West...if you use those rules, then weak countries have no chance...We are a weak country, so do we need to fight according to your rules? No." Col Wang Xiangsui, Chi Air Force, as quoted in the Washington Post, 9 Aug 1999

TRANSLATED FROM THE ORIGINAL PEOPLE'S LIBERATION ARMY DOCUMENTS
UN-RESTRICTED WARFARE
BY COL. QIAO LIANG AND COL. WANG XIANGSUI

Nevertheless…

90



And while China's government is widely criticized for using AI as a way to monitor citizens, the newly published guidelines seem remarkably similar to ethical frameworks laid out by Western companies and governments.

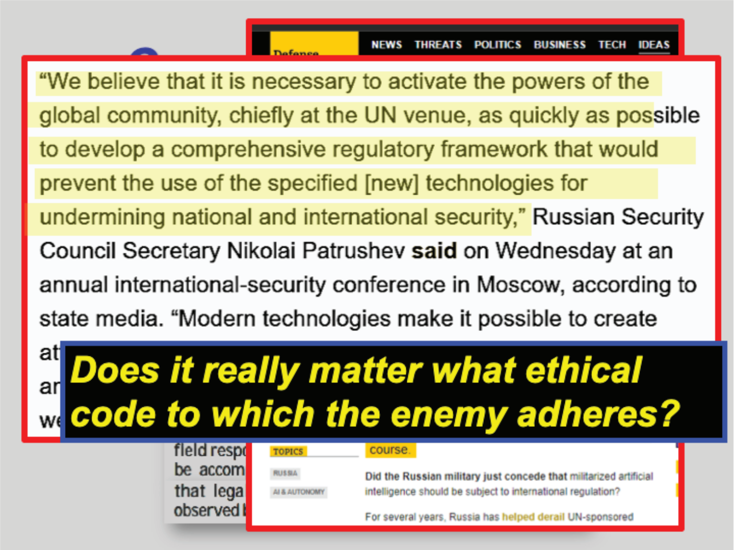
The Beijing AI Principles were announced last Saturday by the Beijing Academy of Artificial Intelligence (BAAI), an organization backed by the Chinese Ministry of Science and Technology and the Beijing municipal government. They spell out guiding principles for research and development in AI, including that "human privacy, dignity, freedom, autonomy, and rights should be sufficiently respected."

While it would be easy to dismiss talk of privacy and individual freedoms as disingenuous, it signals a surprising willingness to discuss such issues within Chinese policy circles.

Russia…

observed

Did China and the US just agree on something?



"We believe that it is necessary to activate the powers of the global community, chiefly at the UN venue, as quickly as possible to develop a comprehensive regulatory framework that would prevent the use of the specified [new] technologies for undermining national and international security," Russian Security Council Secretary Nikolai Patrushev **said** on Wednesday at an annual international-security conference in Moscow, according to state media. "Modern technologies make it possible to create

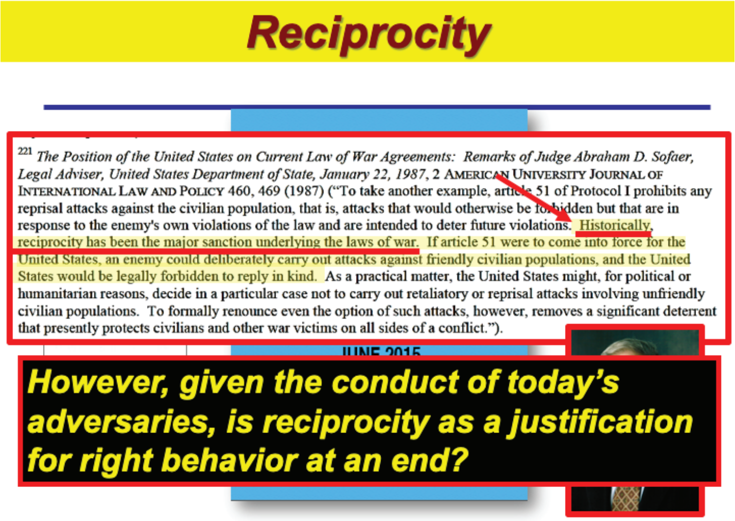
Does it really matter what ethical code to which the enemy adheres?

field respo
be accom
that lega
observed

course.

Did the Russian military just concede that militarized artificial intelligence should be subject to international regulation?

For several years, Russia has helped derail UN-sponsored

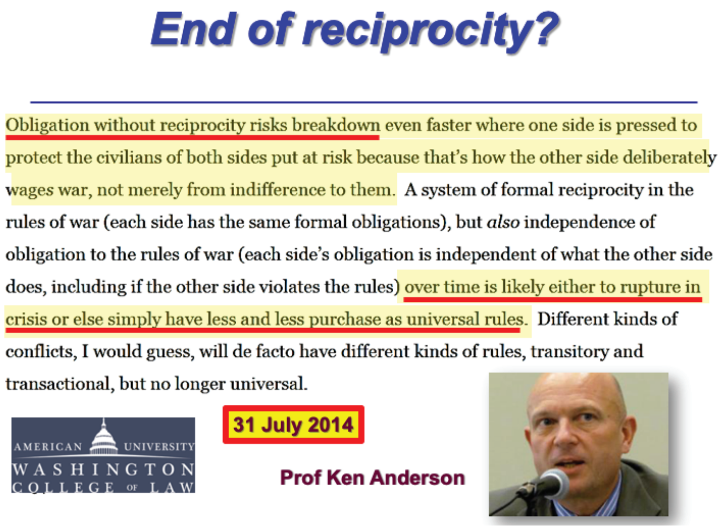


Reciprocity

[221] *The Position of the United States on Current Law of War Agreements: Remarks of Judge Abraham D. Sofaer, Legal Adviser, United States Department of State, January 22, 1987*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 460, 469 (1987) ("To take another example, article 51 of Protocol I prohibits any reprisal attacks against the civilian population, that is, attacks that would otherwise be forbidden but that are in response to the enemy's own violations of the law and are intended to deter future violations. Historically, reciprocity has been the major sanction underlying the laws of war. If article 51 were to come into force for the United States, an enemy could deliberately carry out attacks against friendly civilian populations, and the United States would be legally forbidden to reply in kind. As a practical matter, the United States might, for political or humanitarian reasons, decide in a particular case not to carry out retaliatory or reprisal attacks involving unfriendly civilian populations. To formally renounce even the option of such attacks, however, removes a significant deterrent that presently protects civilians and other war victims on all sides of a conflict.").

JUNE 2015

However, given the conduct of today's adversaries, is reciprocity as a justification for right behavior at an end?



End of reciprocity?

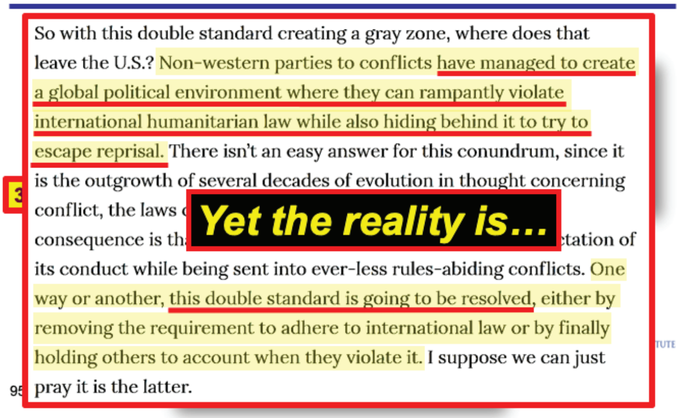
Obligation without reciprocity risks breakdown even faster where one side is pressed to protect the civilians of both sides put at risk because that's how the other side deliberately wages war, not merely from indifference to them. A system of formal reciprocity in the rules of war (each side has the same formal obligations), but *also* independence of obligation to the rules of war (each side's obligation is independent of what the other side does, including if the other side violates the rules) over time is likely either to rupture in crisis or else simply have less and less purchase as universal rules. Different kinds of conflicts, I would guess, will de facto have different kinds of rules, transitory and transactional, but no longer universal.

AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW

31 July 2014

Prof Ken Anderson

End of reciprocity?



So with this double standard creating a gray zone, where does that leave the U.S.? Non-western parties to conflicts have managed to create a global political environment where they can rampantly violate international humanitarian law while also hiding behind it to try to escape reprisal. There isn't an easy answer for this conundrum, since it is the outgrowth of several decades of evolution in thought concerning conflict, the laws

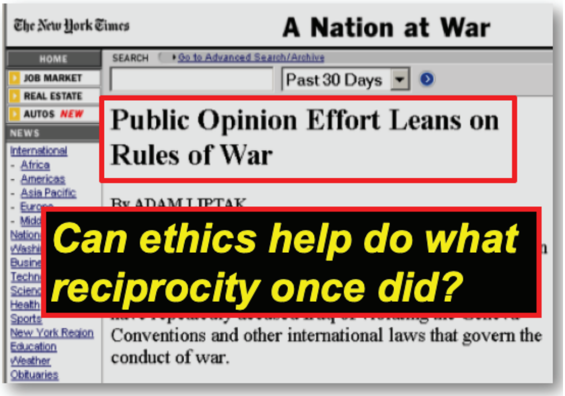
consequence is th

tation of its conduct while being sent into ever-less rules-abiding conflicts. One way or another, this double standard is going to be resolved, either by removing the requirement to adhere to international law or by finally holding others to account when they violate it. I suppose we can just pray it is the latter.

Yet the reality is…

Reality of 21st Century Conflicts

26 Mar 2003

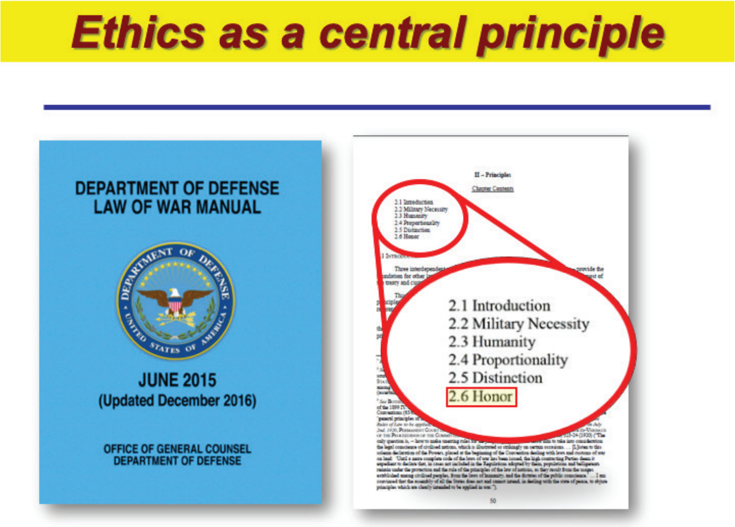


Public Opinion Effort Leans on Rules of War

By ADAM LIPTAK

Conventions and other international laws that govern the conduct of war.

Can ethics help do what reciprocity once did?



Ethics as a central principle

DEPARTMENT OF DEFENSE
LAW OF WAR MANUAL

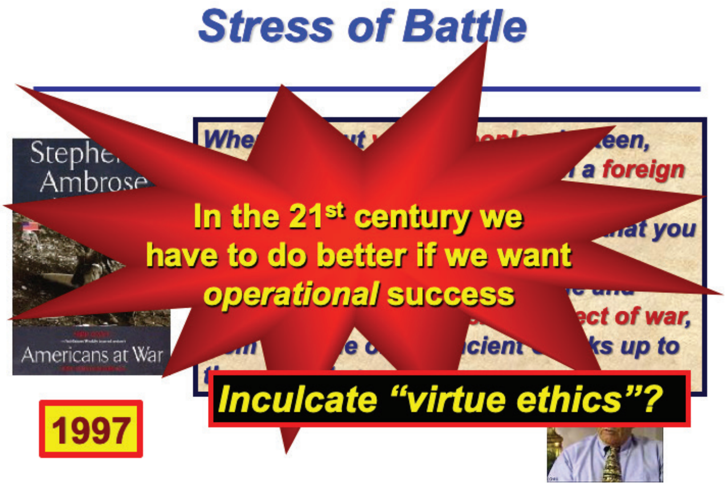
JUNE 2015
(Updated December 2016)

OFFICE OF GENERAL COUNSEL
DEPARTMENT OF DEFENSE

II – Principles

Chapter Contents

2.1 Introduction
2.2 Military Necessity
2.3 Humanity
2.4 Proportionality
2.5 Distinction
2.6 Honor

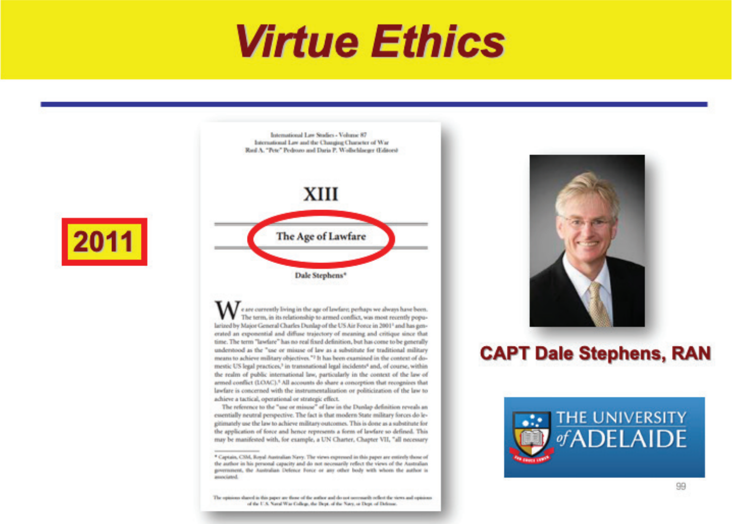


Stress of Battle

1997

In the 21st century we have to do better if we want *operational* success

Inculcate “virtue ethics”?



Virtue Ethics

2011

International Law Studies - Volume 87
International Law and the Changing Character of War
Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger (Editors)

XIII

The Age of Lawfare

Dale Stephens*

We are currently living in the age of lawfare; perhaps we always have been. The term, in its relationship to armed conflict, was most recently popularized by Major General Charles Dunlap of the US Air Force in 2001[1] and has generated an exponential and diffuse trajectory of meaning and critique since that time. The term "lawfare" has no real fixed definition, but has come to be generally understood as the "use or misuse of law as a substitute for traditional military means to achieve military objectives."[2] It has been examined in the context of domestic US legal practices,[3] in transnational legal incidents[4] and, of course, within the realm of public international law, particularly in the context of the law of armed conflict (LOAC).[5] All accounts do share a conception that recognizes that lawfare is concerned with the instrumentalization or politicization of the law to achieve a tactical, operational or strategic effect.

The reference to the "use or misuse" of law in the Dunlap definition reveals an essentially neutral perspective. The fact is that modern State military forces do legitimately use the law to achieve military outcomes. This is done as a substitute for the application of force and hence represents a form of lawfare so defined. This may be manifested with, for example, a UN Charter, Chapter VII, "all necessary

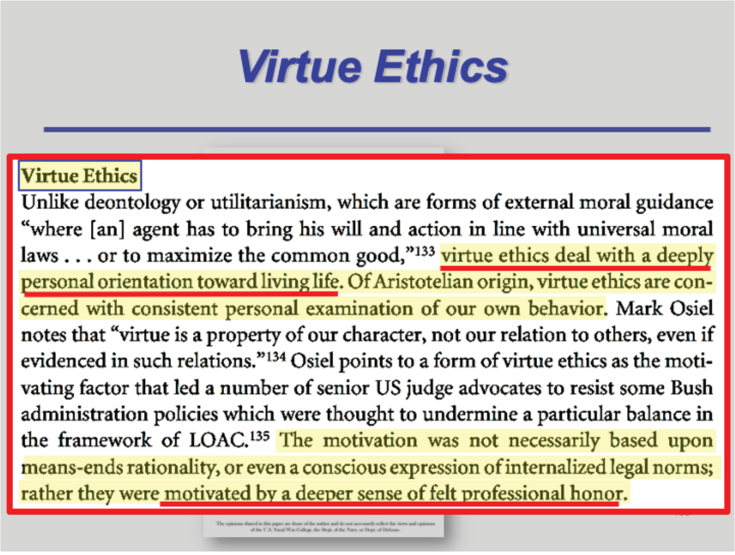
* Captain, CSM, Royal Australian Navy. The views expressed in this paper are entirely those of the author in his personal capacity and do not necessarily reflect the views of the Australian government, the Australian Defence Force or any other body with whom the author is associated.

The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy, or Dept. of Defense.

CAPT Dale Stephens, RAN

THE UNIVERSITY of ADELAIDE

99

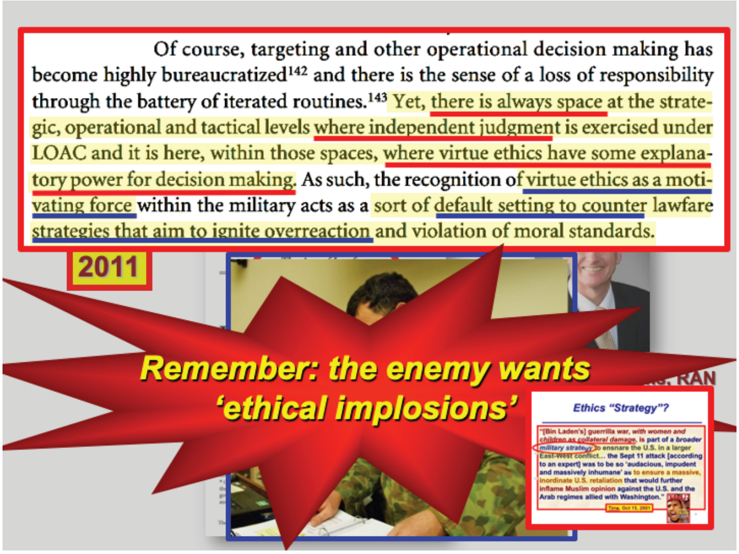


Virtue Ethics

Virtue Ethics

Unlike deontology or utilitarianism, which are forms of external moral guidance "where [an] agent has to bring his will and action in line with universal moral laws . . . or to maximize the common good,"[133] virtue ethics deal with a deeply personal orientation toward living life. Of Aristotelian origin, virtue ethics are concerned with consistent personal examination of our own behavior. Mark Osiel notes that "virtue is a property of our character, not our relation to others, even if evidenced in such relations."[134] Osiel points to a form of virtue ethics as the motivating factor that led a number of senior US judge advocates to resist some Bush administration policies which were thought to undermine a particular balance in the framework of LOAC.[135] The motivation was not necessarily based upon means-ends rationality, or even a conscious expression of internalized legal norms; rather they were motivated by a deeper sense of felt professional honor.

The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy, or Dept. of Defense.



Of course, targeting and other operational decision making has become highly bureaucratized[142] and there is the sense of a loss of responsibility through the battery of iterated routines.[143] Yet, there is always space at the strategic, operational and tactical levels where independent judgment is exercised under LOAC and it is here, within those spaces, where virtue ethics have some explanatory power for decision making. As such, the recognition of virtue ethics as a motivating force within the military acts as a sort of default setting to counter lawfare strategies that aim to ignite overreaction and violation of moral standards.

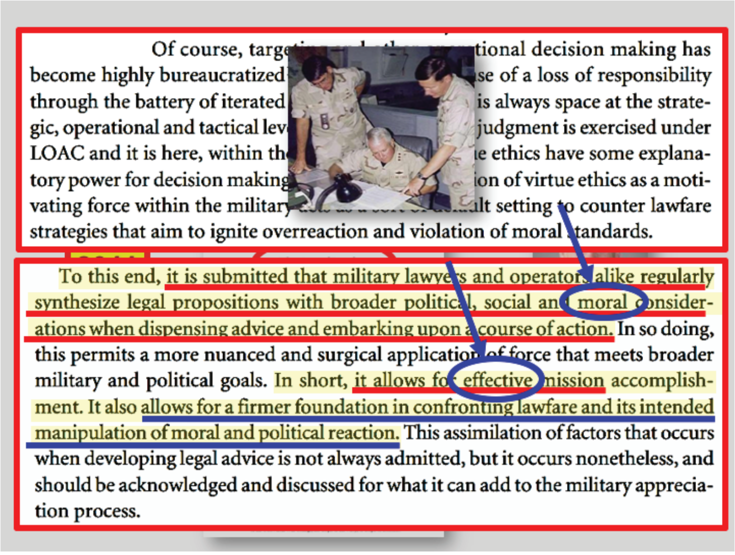
2011

Remember: the enemy wants 'ethical implosions'

Ethics "Strategy"?

"[Bin Laden's] guerrilla war, *with women and children as collateral damage*, is part of a *broader military strategy* to ensnare the U.S. in a larger East-West conflict... the Sept 11 attack [according to an expert] was to be so 'audacious, impudent and massively inhumane' as to ensure a massive, inordinate U.S. retaliation that would further inflame Muslim opinion against the U.S. and the Arab regimes allied with Washington."

Time, Oct 15, 2001



Of course, targe … tional decision making has
become highly bureaucratized … se of a loss of responsibility
through the battery of iterated … is always space at the strate-
gic, operational and tactical lev … judgment is exercised under
LOAC and it is here, within th … e ethics have some explana-
tory power for decision making … ion of virtue ethics as a moti-
vating force within the militar … lt setting to counter lawfare
strategies that aim to ignite overreaction and violation of moral standards.

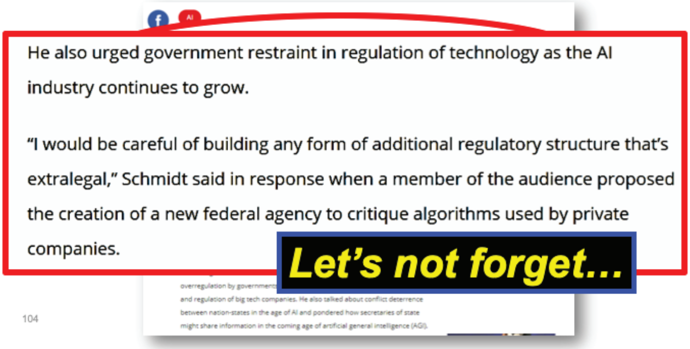
To this end, it is submitted that military lawyers and operators alike regularly synthesize legal propositions with broader political, social and moral considerations when dispensing advice and embarking upon a course of action. In so doing, this permits a more nuanced and surgical application of force that meets broader military and political goals. In short, it allows for effective mission accomplishment. It also allows for a firmer foundation in confronting lawfare and its intended manipulation of moral and political reaction. This assimilation of factors that occurs when developing legal advice is not always admitted, but it occurs nonetheless, and should be acknowledged and discussed for what it can add to the military appreciation process.

Final Thoughts

103

Final Thoughts

- The risks of over-regulation



He also urged government restraint in regulation of technology as the AI industry continues to grow.

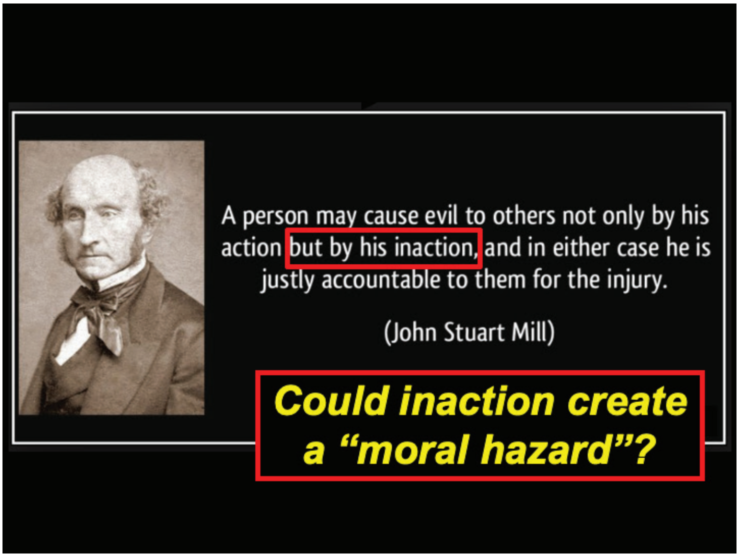
“I would be careful of building any form of additional regulatory structure that’s extralegal,” Schmidt said in response when a member of the audience proposed the creation of a new federal agency to critique algorithms used by private companies.

overregulation by governments

and regulation of big tech companies. He also talked about conflict deterrence between nation-states in the age of AI and pondered how secretaries of state might share information in the coming age of artificial general intelligence (AGI).

Let’s not forget…

104



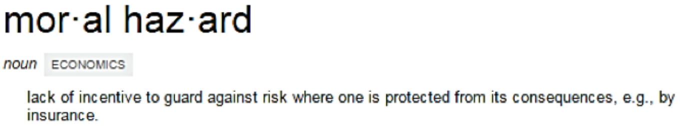
A person may cause evil to others not only by his action but by his inaction, and in either case he is justly accountable to them for the injury.

(John Stuart Mill)

Could inaction create a “moral hazard”?

Moral hazard?

➤ **Traditional definition:**



mor·al haz·ard

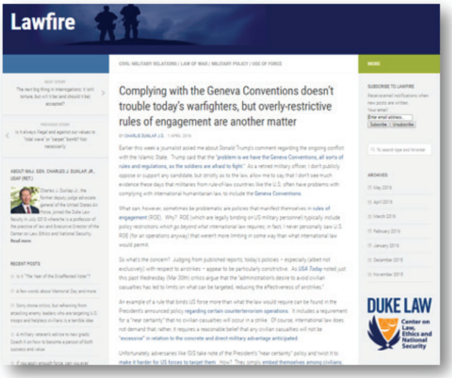
noun ECONOMICS

lack of incentive to guard against risk where one is protected from its consequences, e.g., by insurance.

A new one?

Moral hazard?

1 April 2016



Lawfire

CIVIL-MILITARY RELATIONS / LAW OF WAR / MILITARY POLICY / USE OF FORCE

Complying with the Geneva Conventions doesn't trouble today's warfighters, but overly-restrictive rules of engagement are another matter

BY CHARLIE DUNLAP J.D. · 1 APRIL 2016

Earlier this week a journalist asked me about Donald Trump's comment regarding the ongoing conflict with the Islamic State. Trump said that the "problem is we have the Geneva Conventions, all sorts of rules and regulations, so the soldiers are afraid to fight." As a retired military officer, I don't publicly oppose or support any candidate, but strictly as to the law, allow me to say that I don't see much evidence these days that militaries from rule-of-law countries like the U.S. often have problems with complying with international humanitarian law, to include the Geneva Conventions.

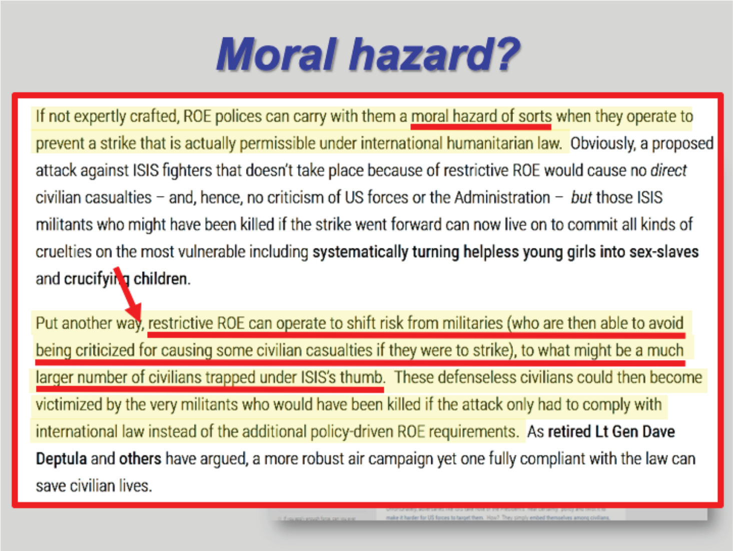
What can, however, sometimes be problematic are policies that manifest themselves in rules of engagement (ROE). Why? ROE (which are legally binding on US military personnel) typically include policy restrictions which go beyond what international law requires; in fact, I never personally saw U.S. ROE (for air operations anyway) that weren't more limiting in some way than what international law would permit.

So what's the concern? Judging from published reports, today's policies – especially (albeit not exclusively) with respect to airstrikes – appear to be particularly constrictive. As USA Today noted just this past Wednesday (Mar 30th) critics argue that the "administration's desire to avoid civilian casualties has led to limits on what can be targeted, reducing the effectiveness of airstrikes."

An example of a rule that binds US force more than what the law would require can be found in the President's announced policy regarding certain counterterrorism operations. It includes a requirement for a "near certainty" that no civilian casualties will occur in a strike. Of course, international law does not demand that; rather, it requires a reasonable belief that any civilian casualties will not be "excessive" in relation to the concrete and direct military advantage anticipated.

Unfortunately, adversaries like ISIS take note of the President's "near certainty" policy and twist it to make it harder for US forces to target them. How? They simply embed themselves among civilians.

NEXT STORY
The next big thing in interrogations: it isn't torture, but will it be (and should it be) accepted?
PREVIOUS STORY
Is it always illegal and against our values to "tidal wave" or "carpet" bomb? Not necessarily
ABOUT MAJ. GEN. CHARLES J. DUNLAP, JR., USAF (RET.)
Charles J. Dunlap Jr., the former deputy judge advocate general of the United States Air Force, joined the Duke Law faculty in July 2010 where he is a professor of the practice of law and Executive Director of the Center on Law, Ethics and National Security.
Read more
RECENT POSTS
Is it "The Year of the Disaffected Voter"?
A few words about Memorial Day and more
Sorry drone critics, but refraining from attacking enemy leaders who are targeting U.S. troops and helpless civilians is a terrible idea
A military veteran's advice to new grads: Coach K on how to become a person of both success and value
If you apply enough force, can you ever
MORE
SUBSCRIBE TO LAWFIRE
Receive email notifications when new posts are written.
Your email:
Enter email address...
Subscribe
Unsubscribe
To search type and hit enter
ARCHIVES
May 2016
April 2016
March 2016
February 2016
January 2016
December 2015
November 2015
DUKE LAW
Center on Law, Ethics and National Security



Moral hazard?

If not expertly crafted, ROE polices can carry with them a moral hazard of sorts when they operate to prevent a strike that is actually permissible under international humanitarian law. Obviously, a proposed attack against ISIS fighters that doesn't take place because of restrictive ROE would cause no *direct* civilian casualties – and, hence, no criticism of US forces or the Administration – *but* those ISIS militants who might have been killed if the strike went forward can now live on to commit all kinds of cruelties on the most vulnerable including **systematically turning helpless young girls into sex-slaves** and **crucifying children**.

Put another way, restrictive ROE can operate to shift risk from militaries (who are then able to avoid being criticized for causing some civilian casualties if they were to strike), to what might be a much larger number of civilians trapped under ISIS's thumb. These defenseless civilians could then become victimized by the very militants who would have been killed if the attack only had to comply with international law instead of the additional policy-driven ROE requirements. As **retired Lt Gen Dave Deptula** and **others** have argued, a more robust air campaign yet one fully compliant with the law can save civilian lives.

Final Thoughts

- ➢ The indispensable factor: courage

There are two types of courage…

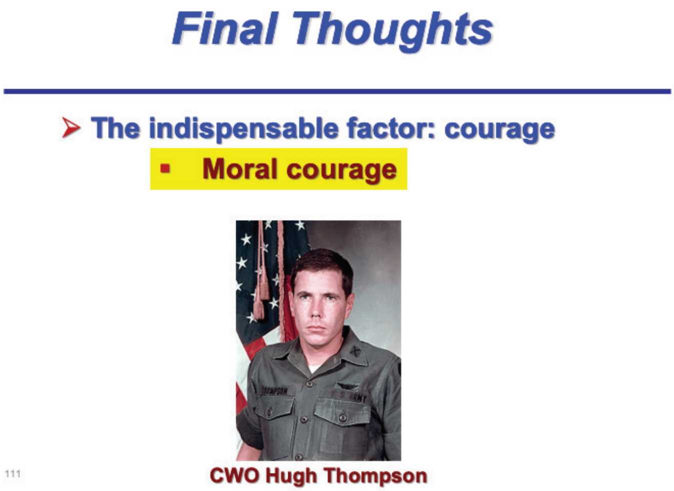
109

Final Thought

- ➢ The indispensable factor: courage
  - ▪ Physical courage

What happens if AI eliminates the need for physical courage…

110

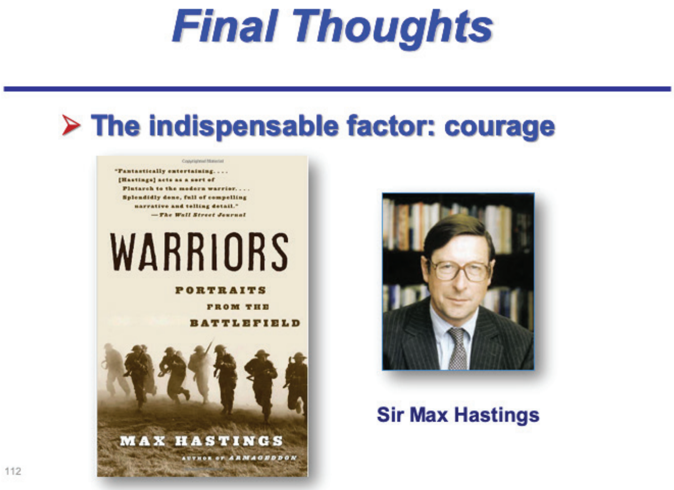


Final Thoughts

- The indispensable factor: courage
  - Moral courage

CWO Hugh Thompson

111



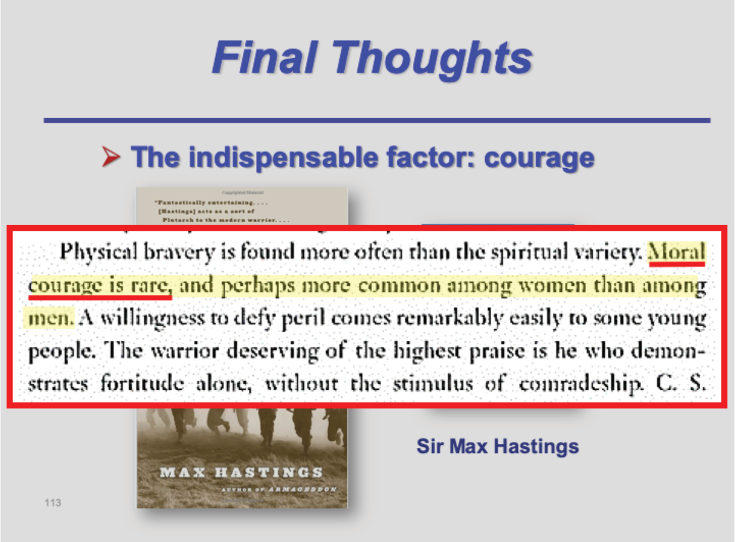
Final Thoughts

- The indispensable factor: courage

"Fantastically entertaining. . . .
[Hastings] acts as a sort of
Plutarch to the modern warrior. . . .
Splendidly done, full of compelling
narrative and telling detail."
—The Wall Street Journal
WARRIORS
PORTRAITS
FROM THE
BATTLEFIELD
MAX HASTINGS
AUTHOR OF ARMAGEDDON

Sir Max Hastings

112



Final Thoughts

- The indispensable factor: courage

Copyrighted Material

"Fantastically entertaining. . . . [Hastings] acts as a sort of Plutarch to the modern warrior. . . .

Physical bravery is found more often than the spiritual variety. Moral courage is rare, and perhaps more common among women than among men. A willingness to defy peril comes remarkably easily to some young people. The warrior deserving of the highest praise is he who demonstrates fortitude alone, without the stimulus of comradeship. C. S.

MAX HASTINGS

AUTHOR OF ARMAGEDDON

Sir Max Hastings

113

UNG UNIVERSITY of NORTH GEORGIA™

THE MILITARY COLLEGE OF GEORGIA®

Law, Ethics, an[d]

The Challe[nge] ...[le]aders

Your questions & comments please!

...DIER-LEADERS IN THE AGE OF AI

THE FUTURE OF PRE-COMMISSIONING EDUCATION

November 13 - 14, 2019

Center on Law, Ethics and National Security

Presented by

Maj Gen Charlie Dunlap, USAF (Ret.)

Copyright © 2019

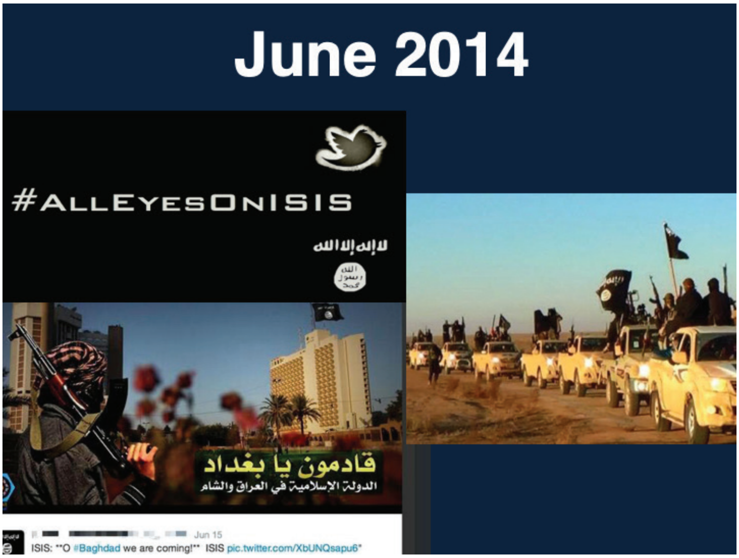
DUKE LAW

Social Media has Transformed the Wars of Today. It will Revolutionize the Wars of Tomorrow.

Emerson T. Brooking

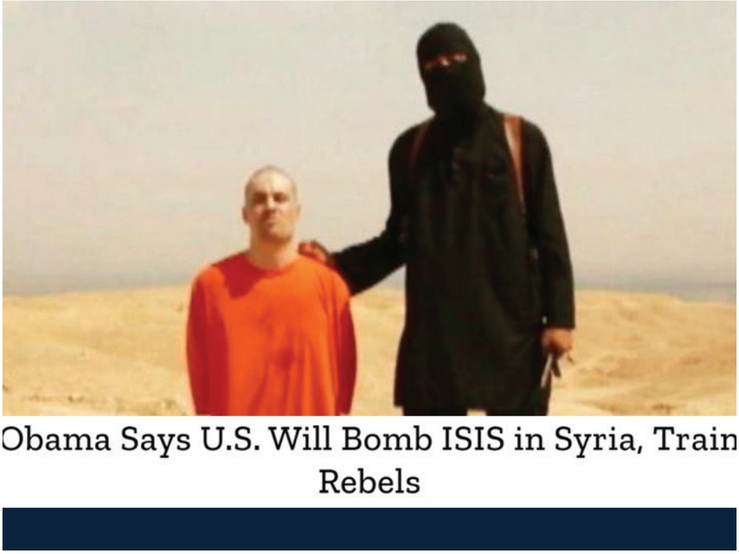
"Extremely timely and fascinating." —New York Times
"Seriously. If you use social media in any capacity, you should read this." —The Verge
LIKEWAR
THE WEAPONIZATION OF SOCIAL MEDIA
P. W. SINGER AND EMERSON T. BROOKING

Emerson T. Brooking
@etbrooking
Resident Fellow, DFRLab
Atlantic Council

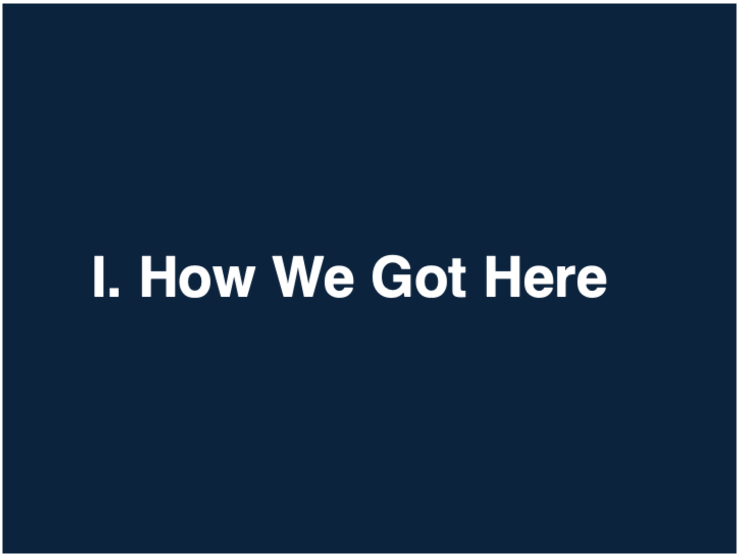

June 2014

[redacted] Jun 15
ISIS: "O #Baghdad we are coming!" ISIS pic.twitter.com/XbUNQsapu6"

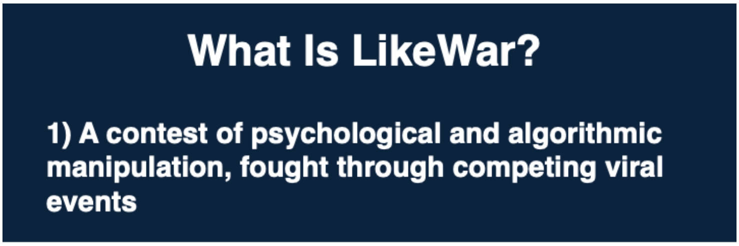
Obama Allows Limited Airstrikes on ISIS



Obama Says U.S. Will Bomb ISIS in Syria, Train Rebels

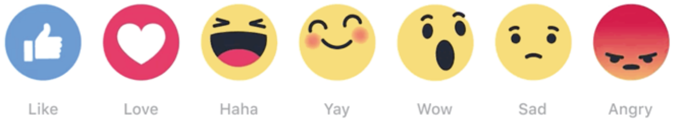


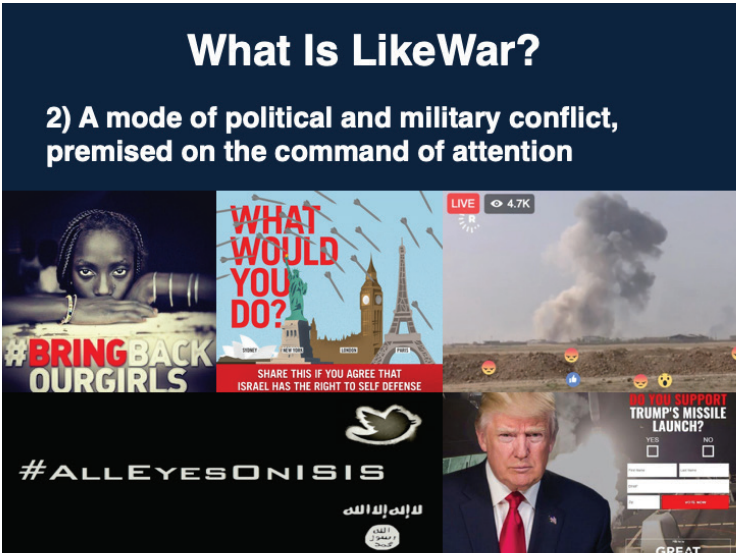
I. How We Got Here



What Is LikeWar?

1) A contest of psychological and algorithmic manipulation, fought through competing viral events

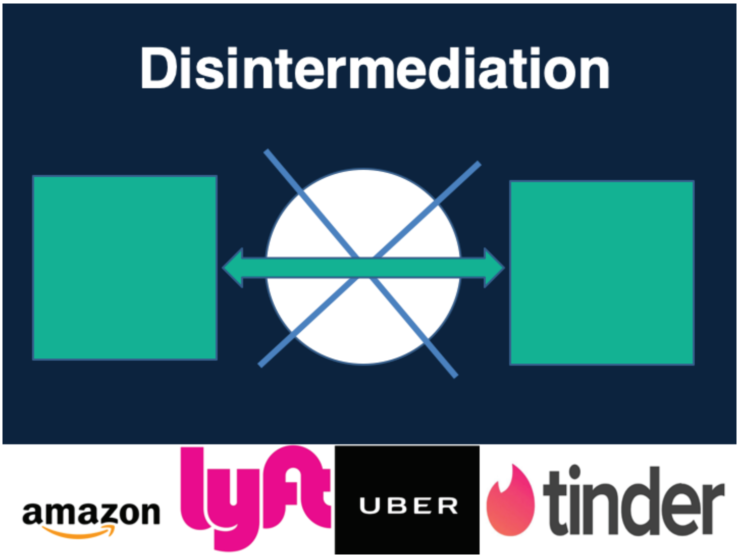




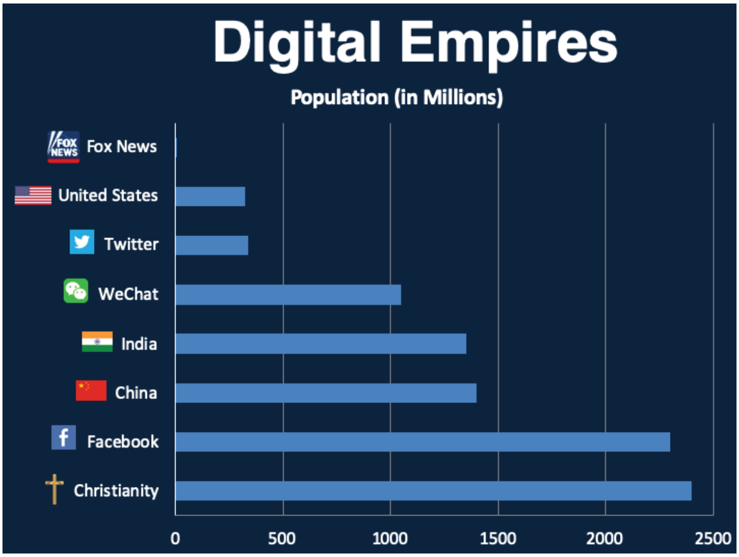
What Is LikeWar?

2) A mode of political and military conflict, premised on the command of attention

#BRINGBACK
OURGIRLS
WHAT WOULD YOU DO?
SYDNEY
NEW YORK
LONDON
PARIS
SHARE THIS IF YOU AGREE THAT ISRAEL HAS THE RIGHT TO SELF DEFENSE
LIVE
4.7K
#ALLEYESONISIS
DO YOU SUPPORT TRUMP'S MISSILE LAUNCH?
YES
NO
VOTE NOW
GREAT

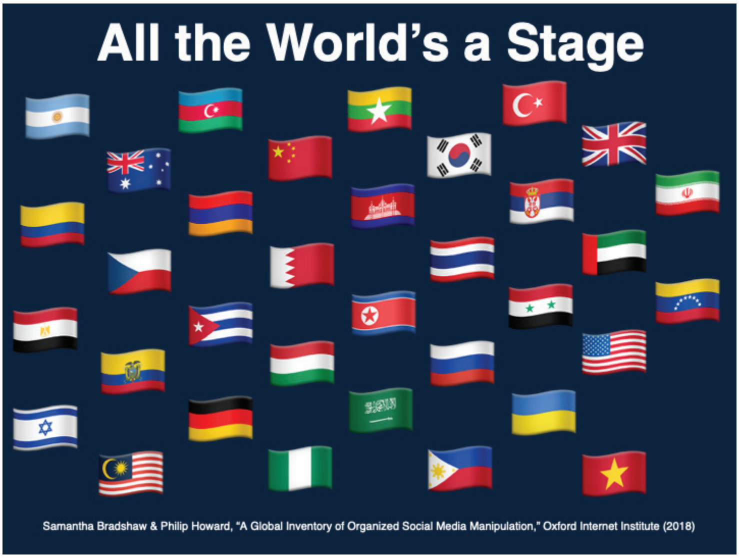


Disintermediation



Digital Empires

Population (in Millions)

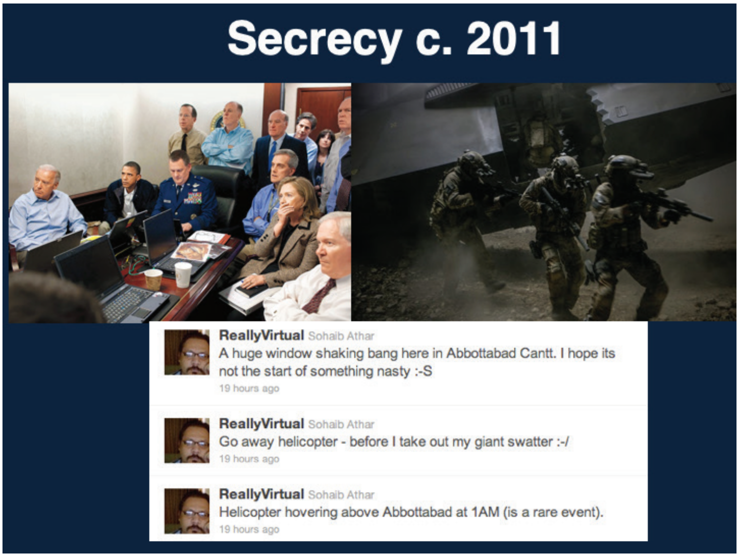


All the World's a Stage

Samantha Bradshaw & Philip Howard, "A Global Inventory of Organized Social Media Manipulation," Oxford Internet Institute (2018)

II. TMI

Secrecy c. 1944

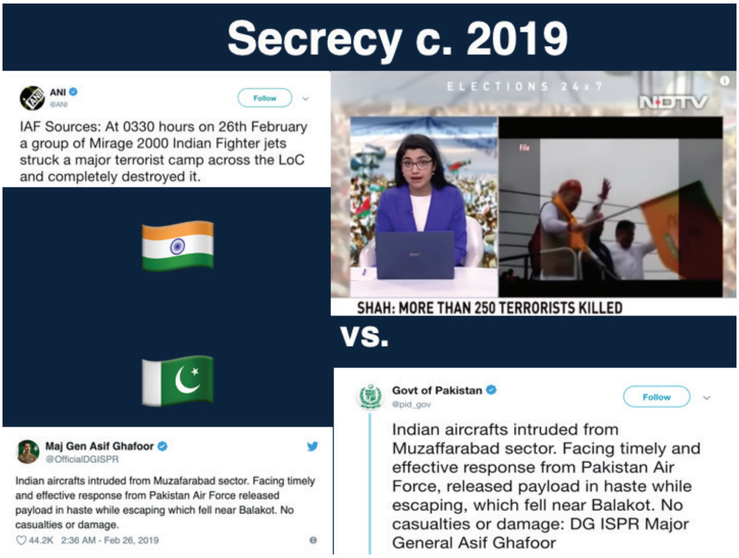


Secrecy c. 2011

ReallyVirtual Sohaib Athar
A huge window shaking bang here in Abbottabad Cantt. I hope its not the start of something nasty :-S
19 hours ago

ReallyVirtual Sohaib Athar
Go away helicopter - before I take out my giant swatter :-/
19 hours ago

ReallyVirtual Sohaib Athar
Helicopter hovering above Abbottabad at 1AM (is a rare event).
19 hours ago



Secrecy c. 2019

ANI @ANI

IAF Sources: At 0330 hours on 26th February a group of Mirage 2000 Indian Fighter jets struck a major terrorist camp across the LoC and completely destroyed it.

SHAH: MORE THAN 250 TERRORISTS KILLED

vs.

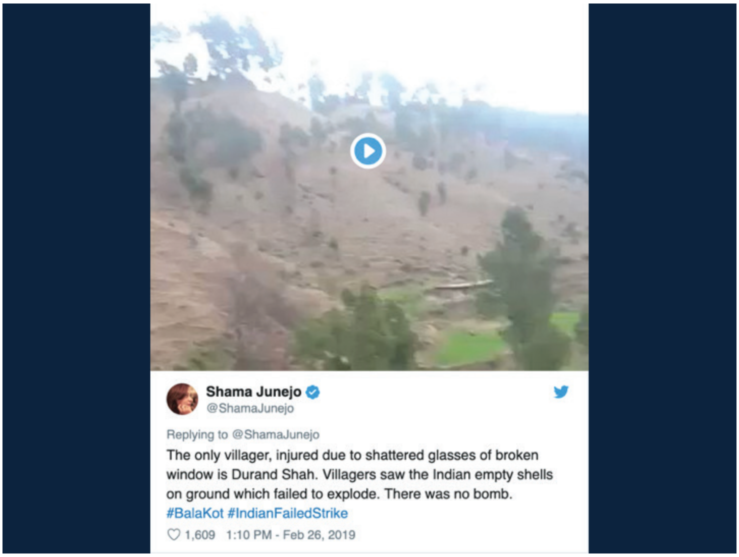
Maj Gen Asif Ghafoor @OfficialDGISPR

Indian aircrafts intruded from Muzafarabad sector. Facing timely and effective response from Pakistan Air Force released payload in haste while escaping which fell near Balakot. No casualties or damage.

♡ 44.2K 2:36 AM - Feb 26, 2019

Govt of Pakistan @pid_gov

Indian aircrafts intruded from Muzaffarabad sector. Facing timely and effective response from Pakistan Air Force, released payload in haste while escaping, which fell near Balakot. No casualties or damage: DG ISPR Major General Asif Ghafoor

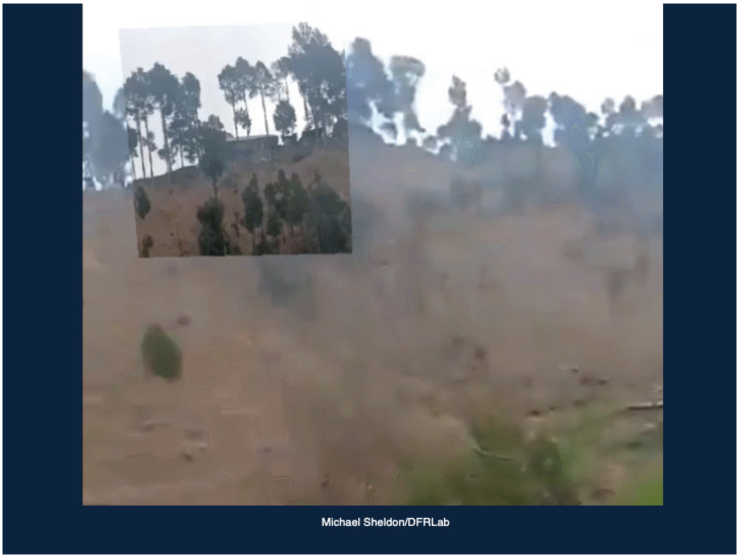


Shama Junejo
@ShamaJunejo

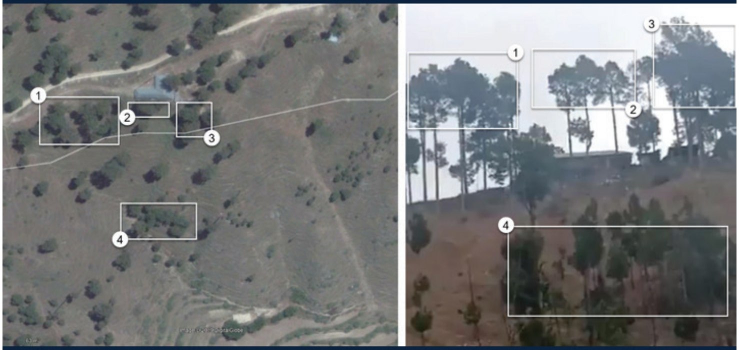
Replying to @ShamaJunejo

The only villager, injured due to shattered glasses of broken window is Durand Shah. Villagers saw the Indian empty shells on ground which failed to explode. There was no bomb. #BalaKot #IndianFailedStrike

♡ 1,609 1:10 PM - Feb 26, 2019

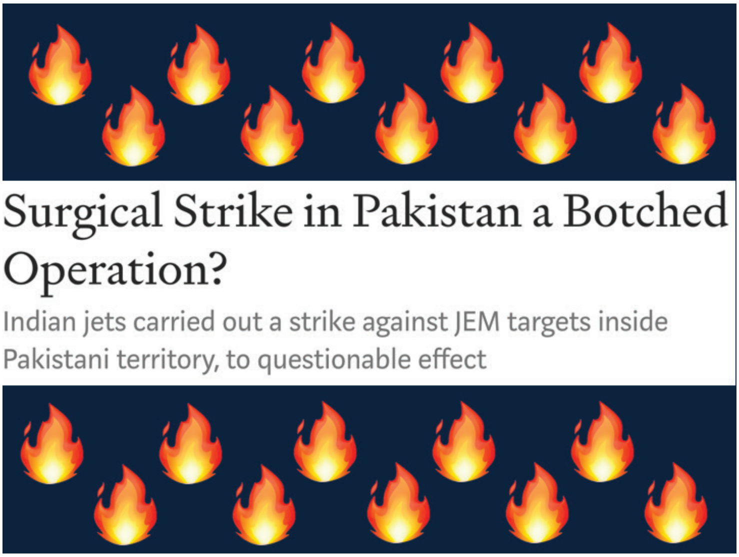


Michael Sheldon/DFRLab



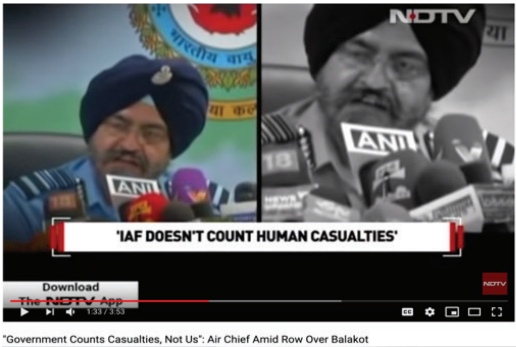
Michael Sheldon/DFRLab

Michael Sheldon/DFRLab



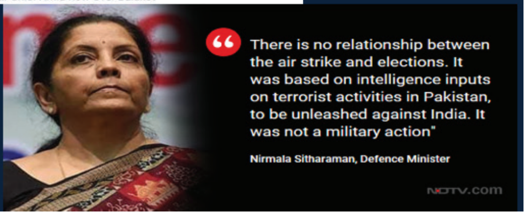
Surgical Strike in Pakistan a Botched Operation?

Indian jets carried out a strike against JEM targets inside Pakistani territory, to questionable effect



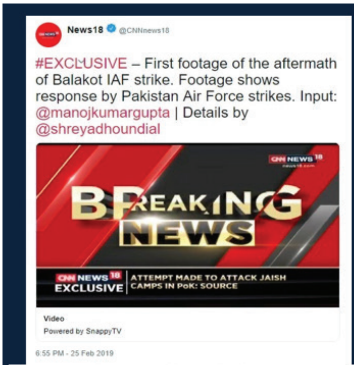
'IAF DOESN'T COUNT HUMAN CASUALTIES'

"Government Counts Casualties, Not Us": Air Chief Amid Row Over Balakot



"There is no relationship between the air strike and elections. It was based on intelligence inputs on terrorist activities in Pakistan, to be unleashed against India. It was not a military action"

Nirmala Sitharaman, Defence Minister

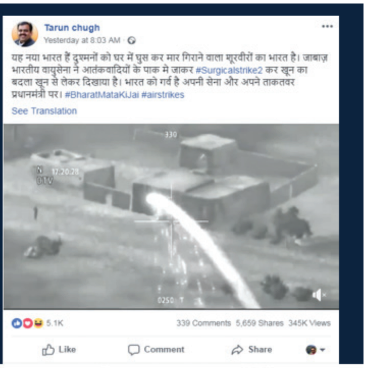


News18 @CNNnews18

#EXCLUSIVE – First footage of the aftermath of Balakot IAF strike. Footage shows response by Pakistan Air Force strikes. Input: @manojkumargupta | Details by @shreyadhoundial

Video
Powered by SnappyTV

6:55 PM - 25 Feb 2019

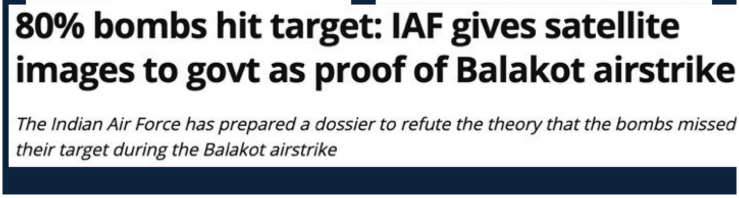


Tarun chugh
Yesterday at 8:03 AM ·

यह नया भारत हैं दुश्मनों को घर में घुस कर मार गिराने वाला शूरवीरों का भारत है। जाबाज़ भारतीय वायुसेना ने आतंकवादियों के पाक मे जाकर #Surgicalstrike2 कर खून का बदला खून से लेकर दिखाया है। भारत को गर्व है अपनी सेना और अपने ताकतवर प्रधानमंत्री पर। #BharatMataKiJai #airstrikes

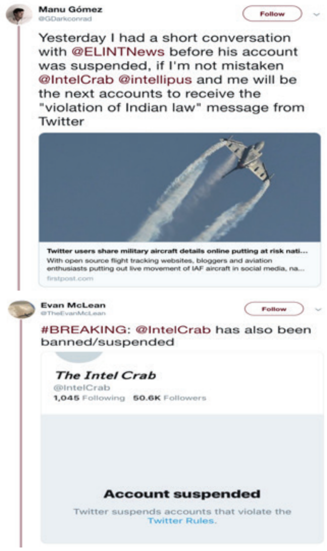
See Translation

5.1K · 339 Comments 5,659 Shares 345K Views



80% bombs hit target: IAF gives satellite images to govt as proof of Balakot airstrike

The Indian Air Force has prepared a dossier to refute the theory that the bombs missed their target during the Balakot airstrike



Manu Gómez
@GDarkconrad

Yesterday I had a short conversation with @ELINTNews before his account was suspended, if I'm not mistaken @IntelCrab @intellipus and me will be the next accounts to receive the "violation of Indian law" message from Twitter

Twitter users share military aircraft details online putting at risk nati...
With open source flight tracking websites, bloggers and aviation enthusiasts putting out live movement of IAF aircraft in social media, na...
firstpost.com

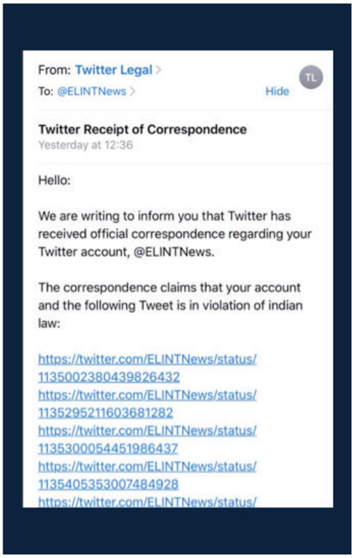
Evan McLean
@TheEvanMcLean

#BREAKING: @IntelCrab has also been banned/suspended

The Intel Crab
@IntelCrab
1,045 Following 50.6K Followers

Account suspended

Twitter suspends accounts that violate the Twitter Rules.



From: Twitter Legal
To: @ELINTNews

Twitter Receipt of Correspondence
Yesterday at 12:36

Hello:

We are writing to inform you that Twitter has received official correspondence regarding your Twitter account, @ELINTNews.

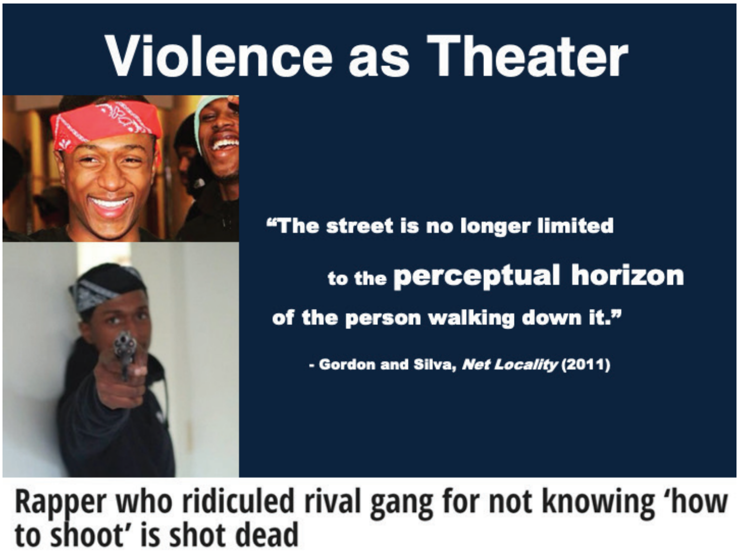
The correspondence claims that your account and the following Tweet is in violation of indian law:

https://twitter.com/ELINTNews/status/1135002380439826432
https://twitter.com/ELINTNews/status/1135295211603681282
https://twitter.com/ELINTNews/status/1135300054451986437
https://twitter.com/ELINTNews/status/1135405353007484928
https://twitter.com/ELINTNews/status/

III. War in the Open

Theater Is Everything

Everything Is Theater

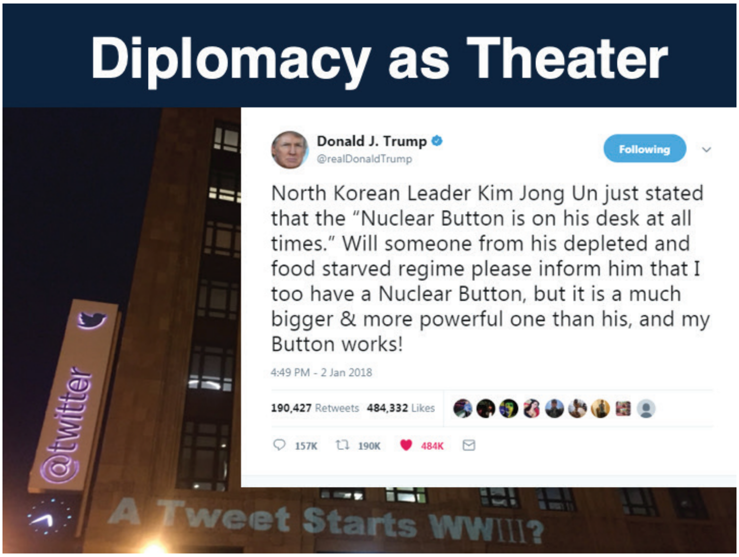


Violence as Theater

"The street is no longer limited to the perceptual horizon of the person walking down it."

- Gordon and Silva, *Net Locality* (2011)

Rapper who ridiculed rival gang for not knowing 'how to shoot' is shot dead



Diplomacy as Theater

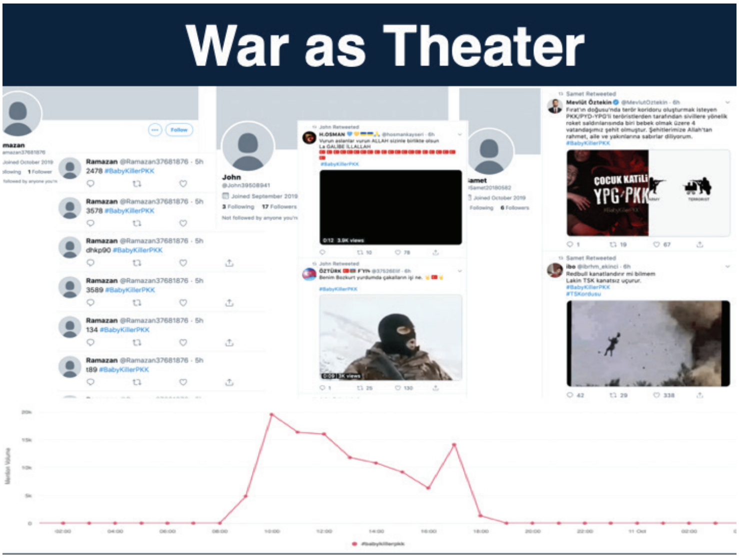
Donald J. Trump
@realDonaldTrump
Following

North Korean Leader Kim Jong Un just stated that the "Nuclear Button is on his desk at all times." Will someone from his depleted and food starved regime please inform him that I too have a Nuclear Button, but it is a much bigger & more powerful one than his, and my Button works!

4:49 PM - 2 Jan 2018

190,427 Retweets 484,332 Likes

157K 190K 484K



War as Theater

Ramazan
@Ramazan37681876
Joined October 2019
Following 1 Follower
Not followed by anyone you're
Follow

Ramazan @Ramazan37681876 · 5h
2478 #BabyKillerPKK

Ramazan @Ramazan37681876 · 5h
3578 #BabyKillerPKK

Ramazan @Ramazan37681876 · 5h
dhkp90 #BabyKillerPKK

Ramazan @Ramazan37681876 · 5h
3589 #BabyKillerPKK

Ramazan @Ramazan37681876 · 5h
134 #BabyKillerPKK

Ramazan @Ramazan37681876 · 5h
t89 #BabyKillerPKK

John
@John39508941
Joined September 2019
3 Following 17 Followers
Not followed by anyone you're

John Retweeted
H.OSMAN @hosmankayseri · 6h
Vurun aslanlar vurun ALLAH sizinle birlikte olsun
La GALİBE İLLALLAH
#BabyKillerPKK
0:12 3.9K views
10 78

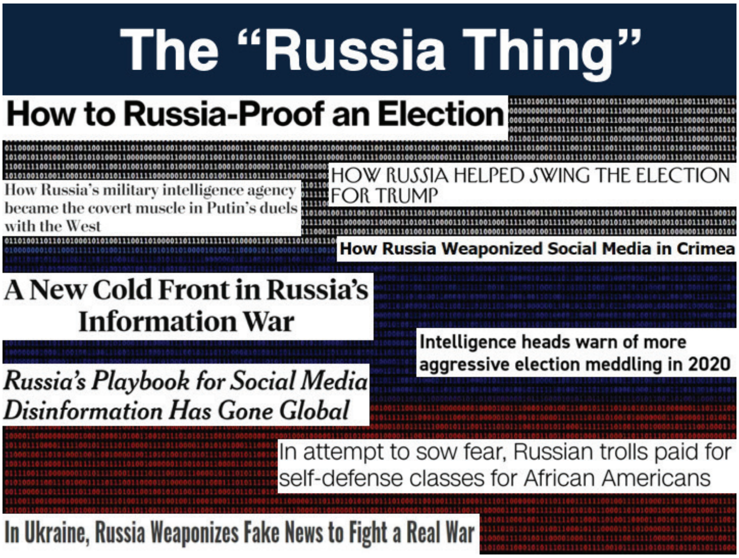
John Retweeted
ÖZTÜRK F'YIN @37526891 · 6h
Benim Bozkurt yurdumda çakalların işi ne.
#BabyKillerPKK
3K views
1 25 130

Samet
@Samet20180582
Joined October 2019
Following 6 Followers

Samet Retweeted
Mevlüt Öztekin @MevlutOztekin · 6h
Fırat'ın doğusu'nda terör koridoru oluşturmak isteyen PKK/PYD-YPG'li teröristlerden tarafından sivillere yönelik roket saldırılarısında biri bebek olmak üzere 4 vatandaşımız şehit olmuştur. Şehitlerimize Allah'tan rahmet, aile ve yakınlarına sabırlar diliyorum.
#BabyKillerPKK
1 19 67

Samet Retweeted
ibo @ibrhm_ekinci · 6h
Redbull kanatlandırır mı bilmem
Lakin TSK kanatsız uçurur.
#BabyKillerPKK
#TSKordusu
42 29 338

IV. The War You Cannot See



The "Russia Thing"

How to Russia-Proof an Election

How Russia's military intelligence agency became the covert muscle in Putin's duels with the West

HOW RUSSIA HELPED SWING THE ELECTION FOR TRUMP

How Russia Weaponized Social Media in Crimea

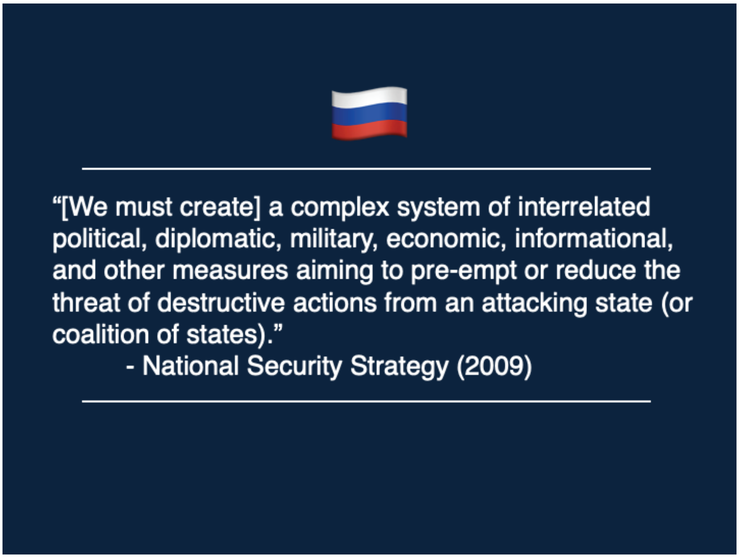
A New Cold Front in Russia's Information War

Intelligence heads warn of more aggressive election meddling in 2020

Russia's Playbook for Social Media Disinformation Has Gone Global

In attempt to sow fear, Russian trolls paid for self-defense classes for African Americans

In Ukraine, Russia Weaponizes Fake News to Fight a Real War



🇷🇺

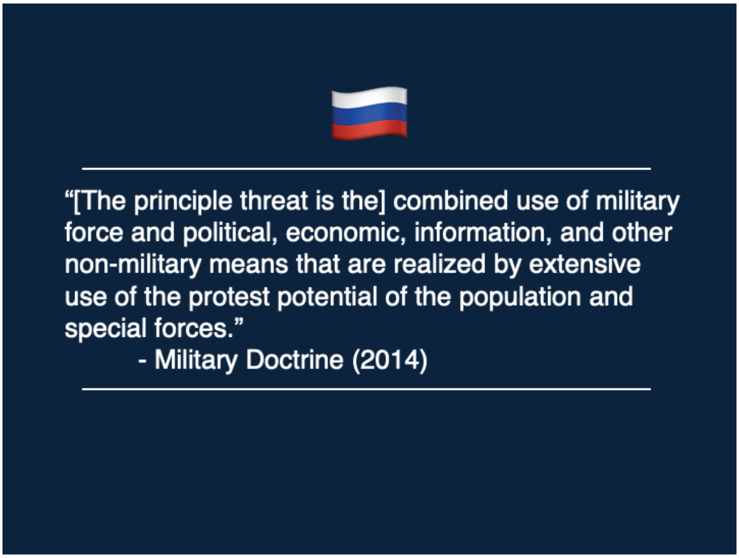
"[We must create] a complex system of interrelated political, diplomatic, military, economic, informational, and other measures aiming to pre-empt or reduce the threat of destructive actions from an attacking state (or coalition of states)."

- National Security Strategy (2009)

ТРЕБУЕМ ПЕРЕСЧЕТА ГОЛОСОВ!
НАМ НУЖНЫ ЧЕСТНЫЕ ВЫБОРЫ!
НАМ НУЖНЫ ЧЕСТНЫЕ ВЫБОРЫ!

🇷🇺

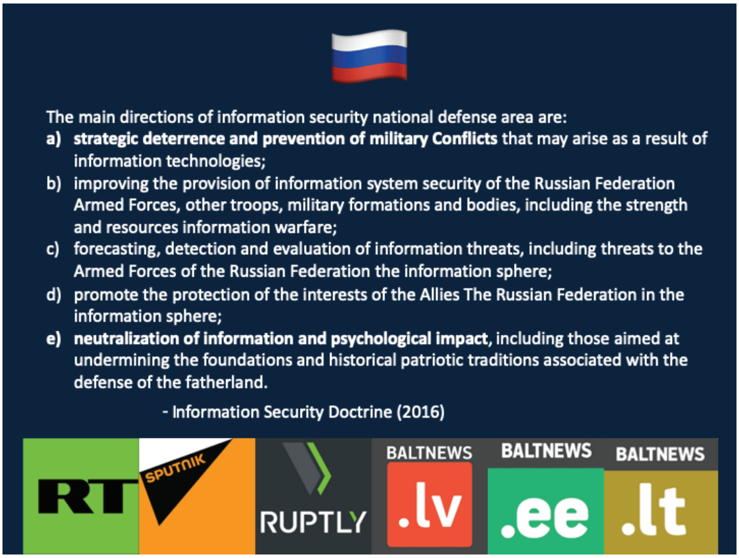
> “Extremist organizations actively employ modern technologies, including…the Internet, to spread extremist material, to attract new members into their ranks, and to coordinate illegal activity.”
>
> - 2013 Concept For Security of the Society



🇷🇺

"[The principle threat is the] combined use of military force and political, economic, information, and other non-military means that are realized by extensive use of the protest potential of the population and special forces."

- Military Doctrine (2014)



The main directions of information security national defense area are:

a) **strategic deterrence and prevention of military Conflicts** that may arise as a result of information technologies;

b) improving the provision of information system security of the Russian Federation Armed Forces, other troops, military formations and bodies, including the strength and resources information warfare;

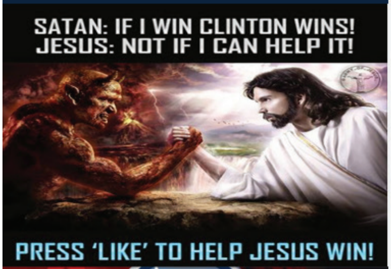
c) forecasting, detection and evaluation of information threats, including threats to the Armed Forces of the Russian Federation the information sphere;

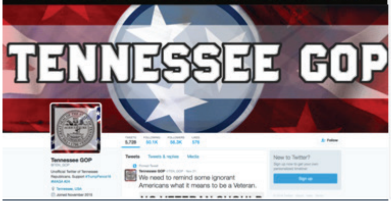
d) promote the protection of the interests of the Allies The Russian Federation in the information sphere;

e) **neutralization of information and psychological impact**, including those aimed at undermining the foundations and historical patriotic traditions associated with the defense of the fatherland.

- Information Security Doctrine (2016)

War By Other Memes


SATAN: IF I WIN CLINTON WINS!
JESUS: NOT IF I CAN HELP IT!
PRESS 'LIKE' TO HELP JESUS WIN!



Tennessee GOP

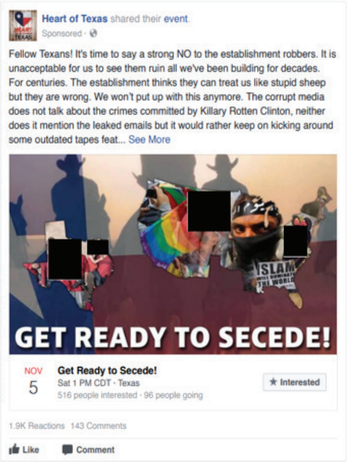
Unofficial Twitter of Tennessee Republicans. Support #TrumpPence16 #MAGA #2A

Tennessee, USA

Joined November 2015

Tennessee GOP

We need to remind some ignorant Americans what it means to be a Veteran.



Heart of Texas shared their event.

Sponsored ·

Fellow Texans! It's time to say a strong NO to the establishment robbers. It is unacceptable for us to see them ruin all we've been building for decades. For centuries. The establishment thinks they can treat us like stupid sheep but they are wrong. We won't put up with this anymore. The corrupt media does not talk about the crimes committed by Killary Rotten Clinton, neither does it mention the leaked emails but it would rather keep on kicking around some outdated tapes feat... See More

NOV 5 Get Ready to Secede!

Sat 1 PM CDT · Texas

516 people interested · 96 people going

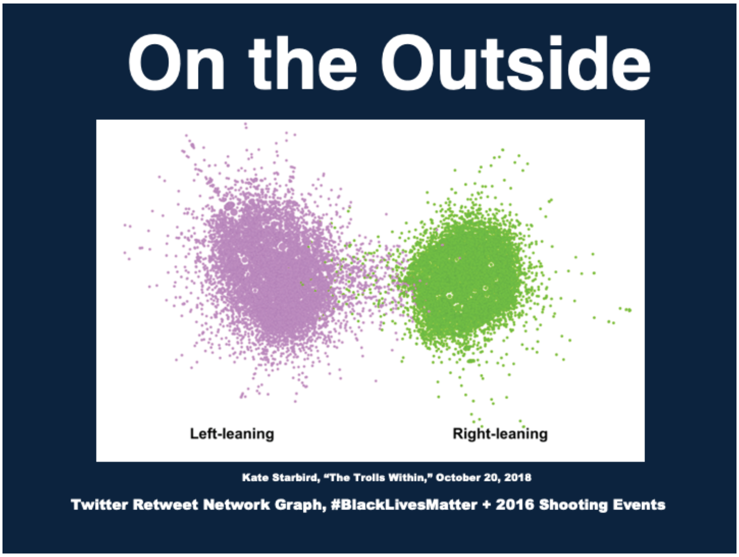
★ Interested

1.9K Reactions 143 Comments

Like Comment

"Troll Factories"

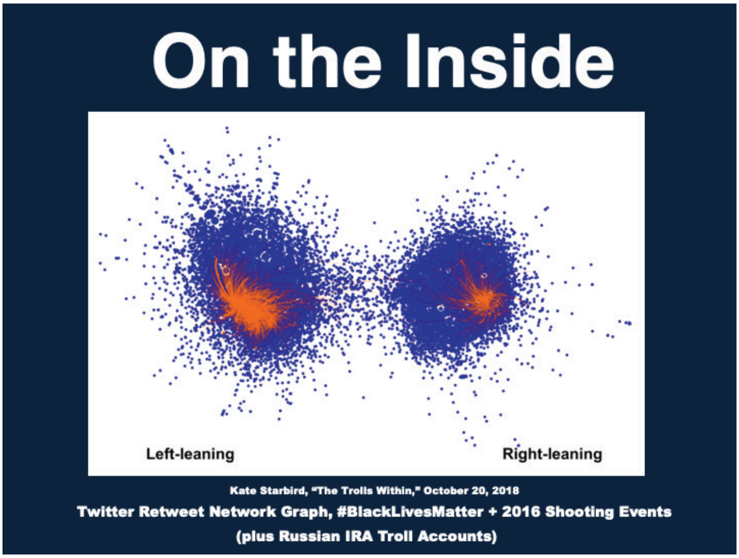
"We wrote about 200 comments and 20 news posts each day...
...I bought myself a Mazda Six."
- Anonymous Russian Troll



On the Outside

Kate Starbird, "The Trolls Within," October 20, 2018

Twitter Retweet Network Graph, #BlackLivesMatter + 2016 Shooting Events

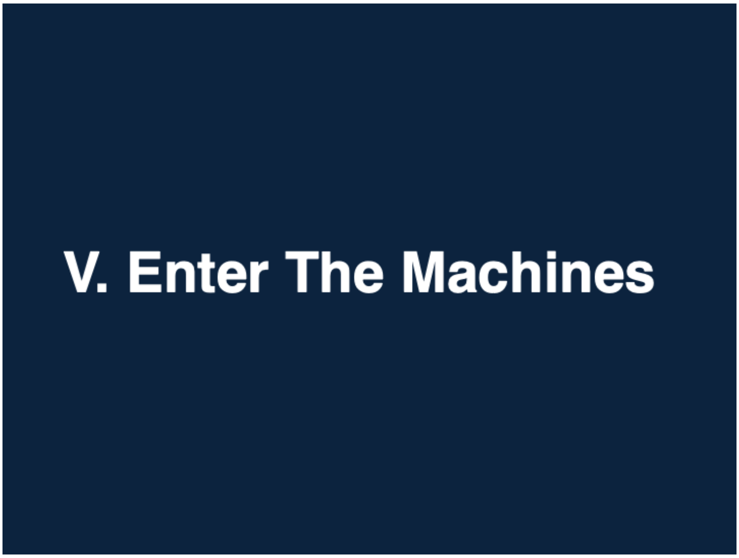


On the Inside

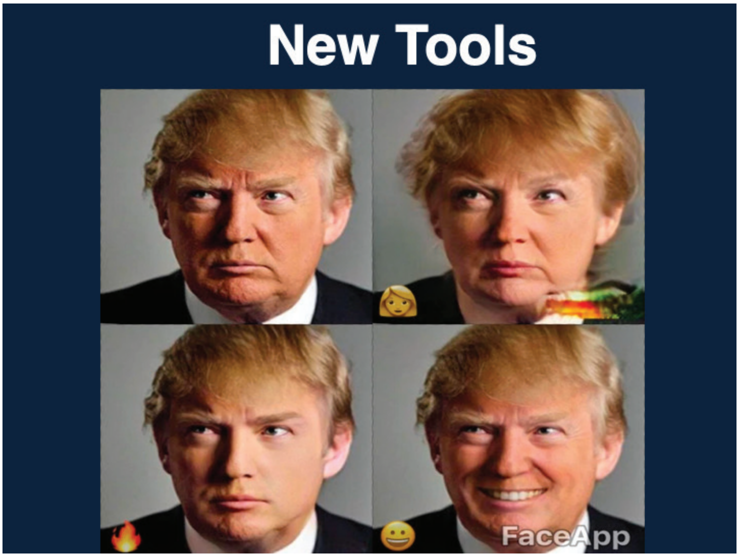
Kate Starbird, "The Trolls Within," October 20, 2018

Twitter Retweet Network Graph, #BlackLivesMatter + 2016 Shooting Events
(plus Russian IRA Troll Accounts)

The Goal

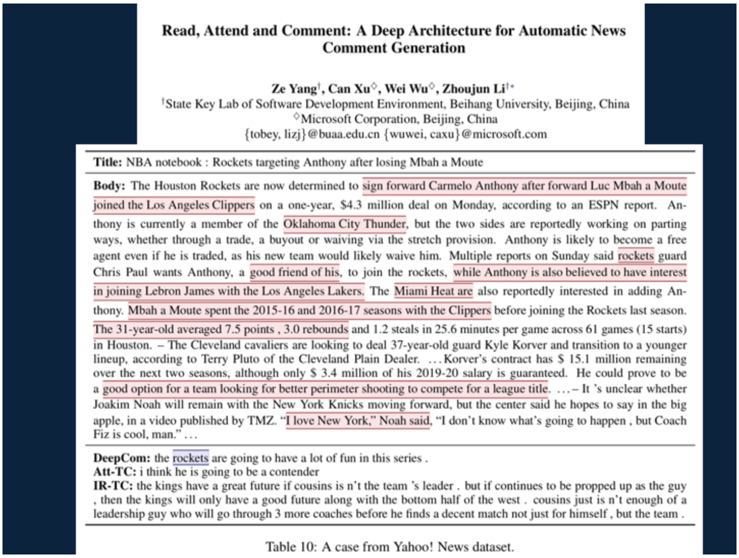


V. Enter The Machines



New Tools

A Million Faces



Read, Attend and Comment: A Deep Architecture for Automatic News Comment Generation

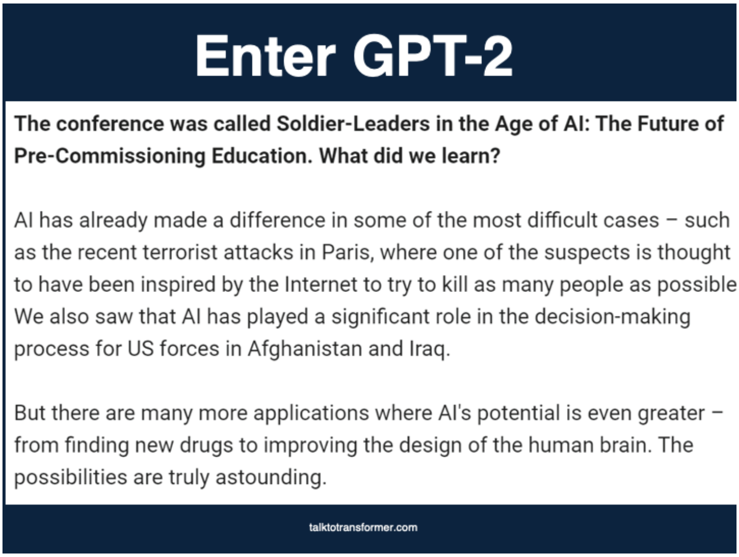
Ze Yang[†], Can Xu[◇], Wei Wu[◇], Zhoujun Li[†*]
[†]State Key Lab of Software Development Environment, Beihang University, Beijing, China
[◇]Microsoft Corporation, Beijing, China
{tobey, lizj}@buaa.edu.cn {wuwei, caxu}@microsoft.com

Title: NBA notebook : Rockets targeting Anthony after losing Mbah a Moute

Body: The Houston Rockets are now determined to sign forward Carmelo Anthony after forward Luc Mbah a Moute joined the Los Angeles Clippers on a one-year, $4.3 million deal on Monday, according to an ESPN report. Anthony is currently a member of the Oklahoma City Thunder, but the two sides are reportedly working on parting ways, whether through a trade, a buyout or waiving via the stretch provision. Anthony is likely to become a free agent even if he is traded, as his new team would likely waive him. Multiple reports on Sunday said rockets guard Chris Paul wants Anthony, a good friend of his, to join the rockets, while Anthony is also believed to have interest in joining Lebron James with the Los Angeles Lakers. The Miami Heat are also reportedly interested in adding Anthony. Mbah a Moute spent the 2015-16 and 2016-17 seasons with the Clippers before joining the Rockets last season. The 31-year-old averaged 7.5 points , 3.0 rebounds and 1.2 steals in 25.6 minutes per game across 61 games (15 starts) in Houston. – The Cleveland cavaliers are looking to deal 37-year-old guard Kyle Korver and transition to a younger lineup, according to Terry Pluto of the Cleveland Plain Dealer. …Korver's contract has $ 15.1 million remaining over the next two seasons, although only $ 3.4 million of his 2019-20 salary is guaranteed. He could prove to be a good option for a team looking for better perimeter shooting to compete for a league title. …– It 's unclear whether Joakim Noah will remain with the New York Knicks moving forward, but the center said he hopes to say in the big apple, in a video published by TMZ. "I love New York," Noah said, "I don't know what's going to happen , but Coach Fiz is cool, man." …

DeepCom: the rockets are going to have a lot of fun in this series .
Att-TC: i think he is going to be a contender
IR-TC: the kings have a great future if cousins is n't the team 's leader . but if continues to be propped up as the guy , then the kings will only have a good future along with the bottom half of the west . cousins just is n't enough of a leadership guy who will go through 3 more coaches before he finds a decent match not just for himself , but the team .

Table 10: A case from Yahoo! News dataset.



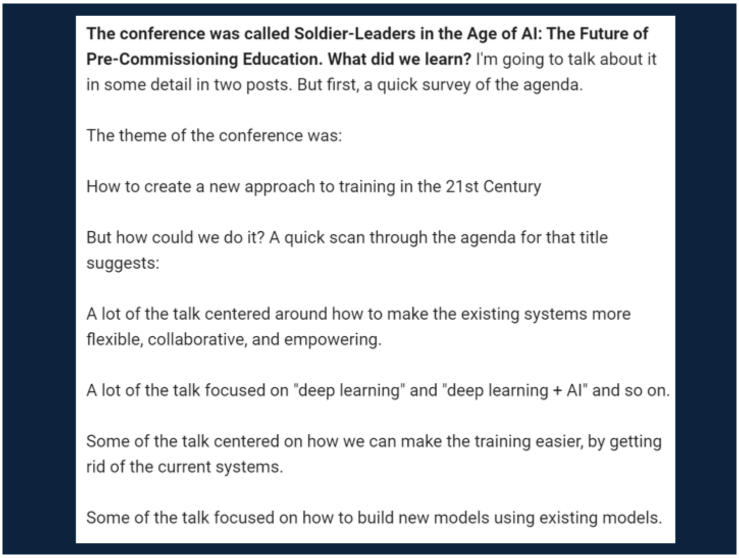
Enter GPT-2

The conference was called Soldier-Leaders in the Age of AI: The Future of Pre-Commissioning Education. What did we learn?

AI has already made a difference in some of the most difficult cases – such as the recent terrorist attacks in Paris, where one of the suspects is thought to have been inspired by the Internet to try to kill as many people as possible We also saw that AI has played a significant role in the decision-making process for US forces in Afghanistan and Iraq.

But there are many more applications where AI's potential is even greater – from finding new drugs to improving the design of the human brain. The possibilities are truly astounding.

talktotransformer.com



The conference was called Soldier-Leaders in the Age of AI: The Future of Pre-Commissioning Education. What did we learn? I'm going to talk about it in some detail in two posts. But first, a quick survey of the agenda.

The theme of the conference was:

How to create a new approach to training in the 21st Century

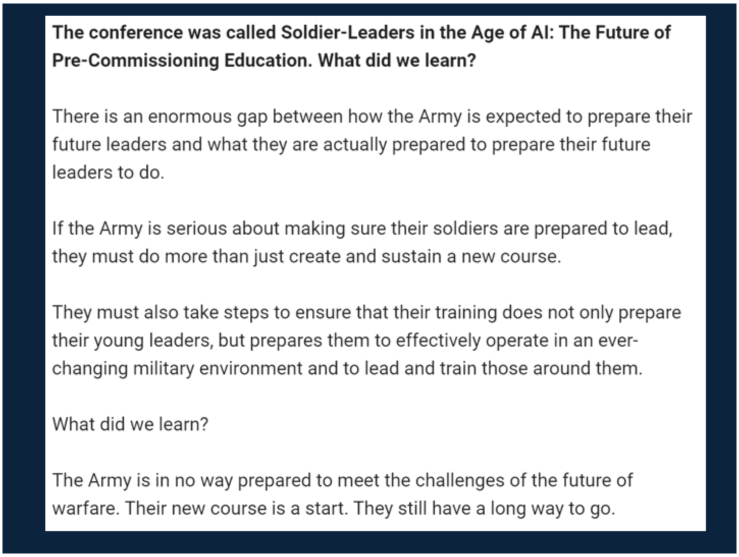
But how could we do it? A quick scan through the agenda for that title suggests:

A lot of the talk centered around how to make the existing systems more flexible, collaborative, and empowering.

A lot of the talk focused on "deep learning" and "deep learning + AI" and so on.

Some of the talk centered on how we can make the training easier, by getting rid of the current systems.

Some of the talk focused on how to build new models using existing models.



The conference was called Soldier-Leaders in the Age of AI: The Future of Pre-Commissioning Education. What did we learn?

There is an enormous gap between how the Army is expected to prepare their future leaders and what they are actually prepared to prepare their future leaders to do.

If the Army is serious about making sure their soldiers are prepared to lead, they must do more than just create and sustain a new course.

They must also take steps to ensure that their training does not only prepare their young leaders, but prepares them to effectively operate in an ever-changing military environment and to lead and train those around them.

What did we learn?

The Army is in no way prepared to meet the challenges of the future of warfare. Their new course is a start. They still have a long way to go.

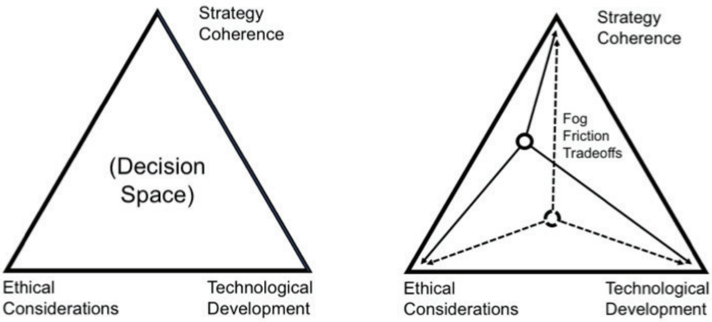
"Extremely timely and fascinating." —New York Times
"Seriously. If you use social media in any capacity, you should read this." —The Verge
LIKEWAR
THE WEAPONIZATION OF SOCIAL MEDIA
P. W. SINGER AND EMERSON T. BROOKING

Thank You!

Emerson T. Brooking
@etbrooking
Resident Fellow, DFRLab
Atlantic Council

Iron Triangle of Painful Tradeoffs” and Responsible Decision-making with Respect to Lethal Autonomous Weapons Systems (LAWS)

Chaplain (Lieutenant Colonel) Jacob Scott



The LAWS “Iron Triangle”

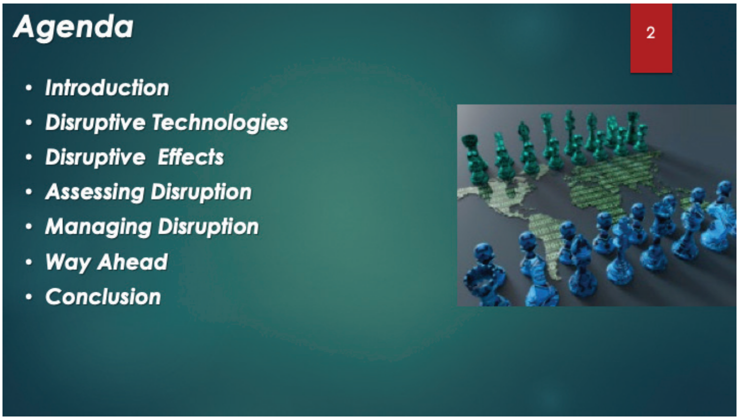
The Ethics of Acquiring Disruptive Technology

Colonel Tony Pfaff, Ph.D.

1

The Ethics of Acquiring New Technologies

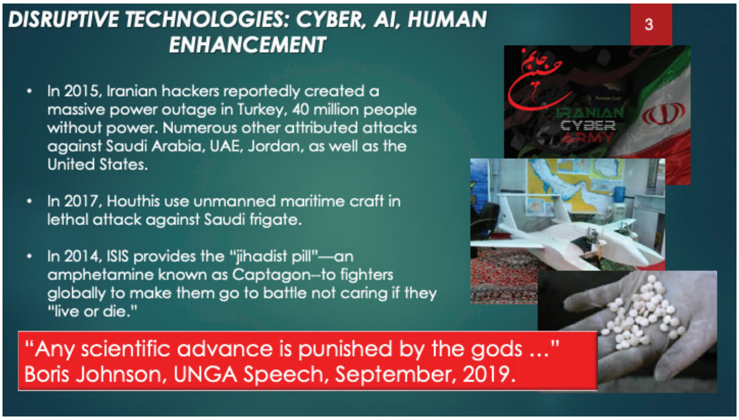
Dr. C. Anthony Pfaff



Agenda

2

- *Introduction*
- *Disruptive Technologies*
- *Disruptive Effects*
- *Assessing Disruption*
- *Managing Disruption*
- *Way Ahead*
- *Conclusion*



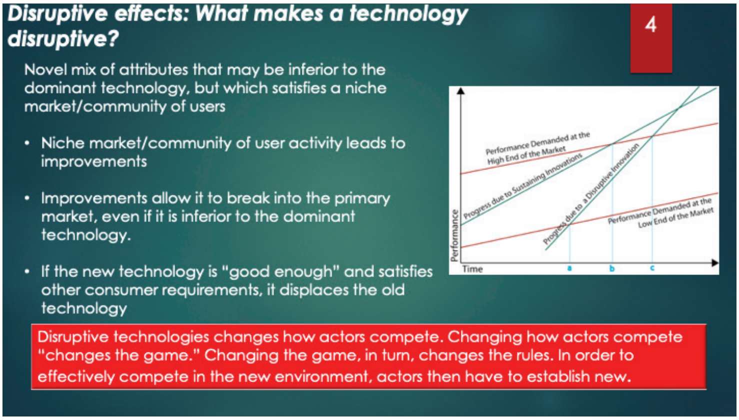
DISRUPTIVE TECHNOLOGIES: CYBER, AI, HUMAN ENHANCEMENT

3

- In 2015, Iranian hackers reportedly created a massive power outage in Turkey, 40 million people without power. Numerous other attributed attacks against Saudi Arabia, UAE, Jordan, as well as the United States.
- In 2017, Houthis use unmanned maritime craft in lethal attack against Saudi frigate.
- In 2014, ISIS provides the "jihadist pill"—an amphetamine known as Captagon--to fighters globally to make them go to battle not caring if they "live or die."

"Any scientific advance is punished by the gods …"
Boris Johnson, UNGA Speech, September, 2019.

IRANIAN
CYBER
ARMY



Disruptive effects: What makes a technology disruptive?

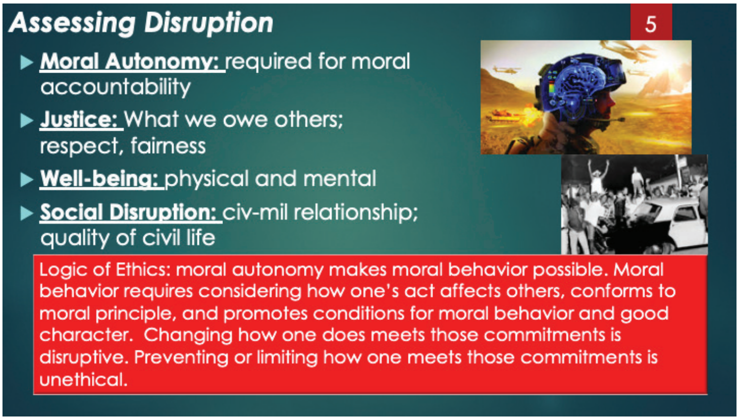
4

Novel mix of attributes that may be inferior to the dominant technology, but which satisfies a niche market/community of users

- Niche market/community of user activity leads to improvements
- Improvements allow it to break into the primary market, even if it is inferior to the dominant technology.
- If the new technology is "good enough" and satisfies other consumer requirements, it displaces the old technology

Disruptive technologies changes how actors compete. Changing how actors compete "changes the game." Changing the game, in turn, changes the rules. In order to effectively compete in the new environment, actors then have to establish new.

Performance Demanded at the High End of the Market
Progress due to Sustaining Innovations
Progress due to a Disruptive Innovation
Performance Demanded at the Low End of the Market
Performance
Time
a
b
c

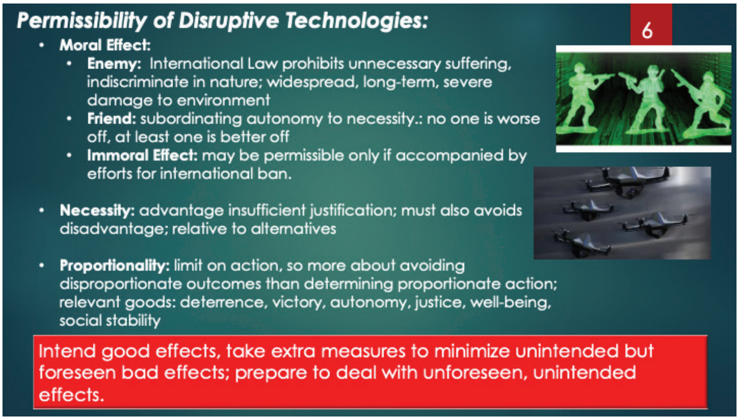


Assessing Disruption

5

- **Moral Autonomy:** required for moral accountability
- **Justice:** What we owe others; respect, fairness
- **Well-being:** physical and mental
- **Social Disruption:** civ-mil relationship; quality of civil life

Logic of Ethics: moral autonomy makes moral behavior possible. Moral behavior requires considering how one's act affects others, conforms to moral principle, and promotes conditions for moral behavior and good character. Changing how one does meets those commitments is disruptive. Preventing or limiting how one meets those commitments is unethical.

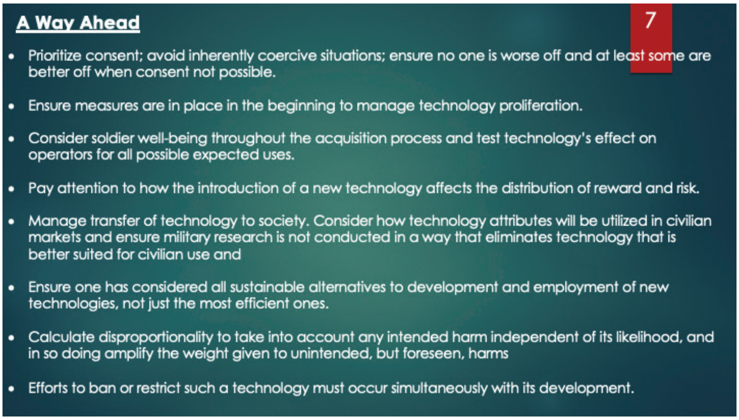


Permissibility of Disruptive Technologies:

6

- **Moral Effect:**
  - **Enemy:** International Law prohibits unnecessary suffering, indiscriminate in nature; widespread, long-term, severe damage to environment
  - **Friend:** subordinating autonomy to necessity.: no one is worse off, at least one is better off
  - **Immoral Effect:** may be permissible only if accompanied by efforts for international ban.
- **Necessity:** advantage insufficient justification; must also avoids disadvantage; relative to alternatives
- **Proportionality:** limit on action, so more about avoiding disproportionate outcomes than determining proportionate action; relevant goods: deterrence, victory, autonomy, justice, well-being, social stability

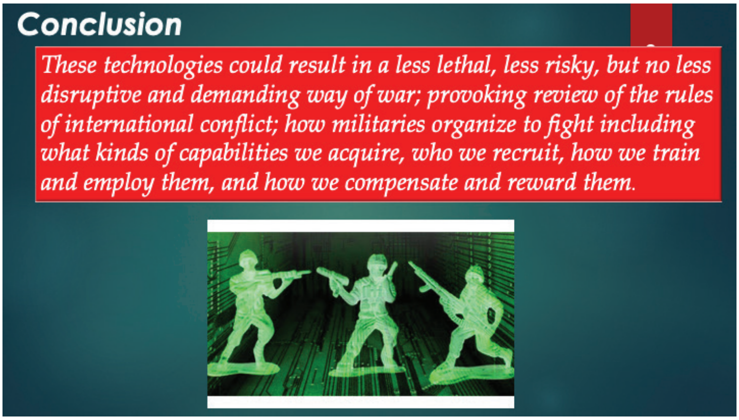
Intend good effects, take extra measures to minimize unintended but foreseen bad effects; prepare to deal with unforeseen, unintended effects.



A Way Ahead

7

- Prioritize consent; avoid inherently coercive situations; ensure no one is worse off and at least some are better off when consent not possible.
- Ensure measures are in place in the beginning to manage technology proliferation.
- Consider soldier well-being throughout the acquisition process and test technology's effect on operators for all possible expected uses.
- Pay attention to how the introduction of a new technology affects the distribution of reward and risk.
- Manage transfer of technology to society. Consider how technology attributes will be utilized in civilian markets and ensure military research is not conducted in a way that eliminates technology that is better suited for civilian use and
- Ensure one has considered all sustainable alternatives to development and employment of new technologies, not just the most efficient ones.
- Calculate disproportionality to take into account any intended harm independent of its likelihood, and in so doing amplify the weight given to unintended, but foreseen, harms
- Efforts to ban or restrict such a technology must occur simultaneously with its development.



Conclusion

These technologies could result in a less lethal, less risky, but no less disruptive and demanding way of war; provoking review of the rules of international conflict; how militaries organize to fight including what kinds of capabilities we acquire, who we recruit, how we train and employ them, and how we compensate and reward them.