2019 Sovereign Challenge Program Annual Conference

Technological Change and the Future of Irregular Warfare

Summary of Proceedings

U.S. Special Operations Command

SOVEREIGN CHALLENGE

A Global Network for a Global Command

30 April - 3 May 2019, Pittsburgh, PA

2019 Sovereign Challenge Conference Participant Countries
April 30-May 3, 2019 Pittsburgh, Pennsylvania

- Armenia+
- Australia*
- Belgium+
- Cambodia+
- Cameroon
- Canada+
- Chad+
- Colombia
- Congo
- Cote d'Ivoire+
- Croatia+
- Denmark
- Dominican Republic
- Estonia+
- France*
- Georgia+
- Greece+
- Guatemala+
- Haiti
- Honduras
- Iraq
- Israel
- Kazakhstan
- Korea
- Laos
- Latvia+
- Mali+
- Mexico
- Mongolia+
- Myanmar
- Netherlands
- N ew Zealand+
- Nigeria*
- North Macedonia
- Oman+
- Philippines
- Poland
- Romania+
- Saudi Arabia
- Senegal+
- Serbia+
- Singapore+
- Sri Lanka+
- Sudan+
- Sweden+
- Tanzania+
- Thailand+
- Trinidad & Tobago
- Ukraine
- United Kingdom
- Uzbekistan
- Zambia

Note:
+ indicates country representatives attended two consecutive years
*indicates unofficial representative

TABLE OF CONTENTS

Conference Overview

United States Special Operations Command (USSOCOM) hosted the 2019 Sovereign Challenge annual conference entitled, "Technological Change and the Future of Irregular Warfare," from April 30th - May 3rd in Pittsburgh, Pennsylvania. Speaking directly to the seventy-one defense attachés and other national security diplomats from forty-nine countries in attendance, the USSOCOM Commander, General Richard Clarke stated, "I believe that you are the best and the finest professionals that your nation sends abroad; it is a distinct honor for us to host you both in this country and at this forum." This conference, he further stated, offers a unique opportunity to discuss a contemporary global security environment that is more complex, volatile, and competitive than seen in a generation. General Clarke relayed the chief factor shaping this reality is the re-emergence of great power competition and the continued fight against violent extremist organizations around the world. In this environment, sharing responsibility and cooperatively using scarce resources is the best way to achieve a favorable balance of power. For this reason, he stressed, the U.S. military to include Special Forces, continue to invest substantial resources and expertise in building the military capability and capacity of our partners to strengthen their own self defense as well as their ability to contribute effectively to our collective efforts.

Welcoming conference participants to Pittsburgh, Mayor William "Bill" Peduto related the history of his city's growth from a frontier outpost that triggered what many historians refer to as the first world war (the "Seven Years'" or "French and Indian" War, 1754-1763) through the "Steel City" era, when Pittsburgh was the industrial powerhouse of the United States, to the city's ongoing re-emergence from recession into a leading center for technological innovation. The people of Pittsburgh, who came from around the world, were central to these transitions, he said. Going forward, Mayor Peduto recommended that policymakers should not just look at the disruptive effects of technology on the economy; rather they should consider technology's overall impact on the community and its people. It is vital, he underscored, that we ensure that our citizens' lives not only change, but also improve.

In her keynote remarks, Secretary of the Air Force, Dr. Heather Wilson, challenged the audience by asking, "How do we apply moral and ethical considerations in an era where technology enables an increasingly independent prosecution of warfare objectives?" With clarity, Secretary Wilson argued that, "We must execute a just fight, not necessarily a fair fight." Humans must continue to bound the "why" and "when" and let technology provide the "how." Echoing Mayor Peduto, Secretary Wilson stressed that people still matter and we must enable them with technology.

Introducing Carnegie Mellon University (CMU) to conference attendees, CMU President Dr. Farnam Jahanian described CMU as an interdisciplinary research institute with an inclusive mindset that is multi-national and multi-cultural and seeks to solve relevant, real-world problems. After his comments, five leading CMU scientists offered a range of exciting and thought-provoking presentations on their latest developments in Artificial Intelligence (AI). Topics included defensible AI, voice recognition and forensics, cyber security and AI, biometrics and real-time AI, and robotics and AI for defense.

During the four-day conference, over one hundred and fifty attendees examined the question of how technological change is altering the future of sovereignty, power, competition, and warfare. From the onset of cyberwar to the development of violent non-state actors (VNSAs) with conventional military capabilities and an interest in harnessing emerging technologies, the future of warfare will be qualitatively different from previous eras. The speed and disruptive nature of emerging technologies is vast, and the growing competition between great powers to develop the most cutting-edge technologies is unsettling. Meanwhile, governments and individuals ponder the legal and ethical ramifications of emerging technologies even as they rapidly transform not only their military forces, but also nations and societies.

Data is the new ammunition of warfare and computers incorporated into rapidly evolving, highly sophisticated weapons systems are decreasing the time available for leaders to make decisions, requiring decision-makers to trust their technology to an ever greater degree. Furthermore, the technological expansion of human capabilities and realities increases the potential for miscalculation, as emerging technologies disrupt the metrics and paradigms of military power, render conflict itself more abstract, and make the evaluation of relative balances of power more complicated. As these trends continue, the future national security environment will inevitably be shaped by the dichotomy between states and populations trusting technology too much or not enough.

VNSAs – terrorist organizations, gangs, or cartels – and hegemonic states are vigorously seeking to adapt existing technologies or innovate new technologies to facilitate their asymmetric activities to achieve their strategic objectives. While we continue to build a green high-tech Maginot Line, our adversaries have been investing in technologies they can use effectively and they're winning, said author Max Brooks. Reconnecting our militaries to our respective populations is essential; in the gray zone, where most of today's warfare is conducted, citizenry with the right tools and talents can engage successfully, he said. Fiction is a great way to connect with and understand people, author August Cole noted. We can encode a story with the DNA of many of these trends that are difficult to synthesize, because they are so complex and are happening with a high degree of simultaneity, he suggested.

The ethics and morality of deploying new weapons for the battlefield emerged in every major conversation at the conference. With the increased teaming of machines and humans in our future, trusting both technology and our fellow humans will be a necessity. More broadly, building ethical decision making, responsibility, and accountability into technical capabilities and incorporating it into doctrine, training, and operations should take place. Ultimately, however, moral responsibility must lie with the fully-informed, well-trained military commander who orders deployment of a weapons system, whether autonomous or not.

USSOCOM and its Sovereign Challenge program would like to thank Carnegie Mellon University, the Office of the Honorable William "Bill" Peduto, Mayor of Pittsburgh, and the Senator John Heinz History Center for their contributions to the content and execution of this conference. It would not have been a success without them.

By: Larry Cook, Sovereign Challenge Program Manager
Greg Hicks, Sovereign Challenge Program Coordinator

Technology and Irregular Warfare Converge in Pittsburgh, PA-
Lieutenant General Jim Slife

USSOCOM Vice Commander, Lt Gen Jim Slife, officially welcomed participants to the 2019 Sovereign Challenge program annual conference and expressed how honored he was to see so many attendees who participated in the 2018 fall seminar at the United States Institute of Peace in Washington, DC. USSOCOM, he said, was fortunate to hold this year's event in a location that aligned perfectly with the topic of the conference, Technological Change and the Future of Irregular Warfare. Pittsburgh, Lt Gen Slife continued, has become a leader of technological innovation in high-tech fields such as business, medicine, and academia. Moreover, it is a city that after suffering a major economic collapse, reinvented itself, proving the theory that technology and change must be fully embraced, or one risks being left behind.

Emerging technologies that companies in Pittsburgh are developing today will likely touch many facets of our lives, including national security, Lt Gen Slife emphasized. Automation, unmanned vehicles, and machine learning are enabling cost saving and even life preserving capabilities in some fields, while also creating opportunities for adversaries. There are many more disruptive technologies than these, and with the hyper-connectivity of today's world, they will affect both civilian and defense sectors in every country, Lt Gen Slife asserted. To contend with malicious use of these technologies, he added, we must first master them and make them work for us. Yet in doing so, he stressed, we must take care not to abandon our principles, which are what separate us from most of our adversaries.

These "… challenges and opportunities born of all this innovation come at a precarious time," Lt Gen Slife noted. The advent of irregular warfare over the past two decades, he continued, has thrust new missions like military information support operations, cyberspace operations, counter-threat financing, and counter weapons of mass destruction activities into the portfolio of USSOCOM. Only with a network of allies and partners can we truly understand the nature of the security challenges we face, and USSOCOM's Sovereign Challenge program provides an invaluable "… forum for increasing our collective understanding, not only of the problems in front of us, but the tools with which we'll solve them," he stressed. Together with our allies and partners, USSOCOM has a responsibility not only to deny our state and non-state adversaries an advantage in the irregular warfare arena, but to overmatch them as well, he concluded.

By: John Bergmann, USSOCOM J-59 Future Concepts Division

The Spirit of Pittsburgh
Mayor William "Bill" Peduto

Pittsburgh's Mayor, William "Bill" Peduto, stated that his city has always believed in its people, and it has succeeded because it has invested in them. "We Pittsburghers are proud of our blue collar roots," he continued, "and that our people came from all over the world and the southern United States to work in the mines, factories, and mills that built America."

The city's story, Mayor Peduto said, began when young Major George Washington of the Virginia militia challenged France's claim to this location where the Allegheny and Monongahela Rivers meet to form the Ohio River, igniting the French and Indian War in America, and the Seven Years' War in Europe. Eventually, England prevailed and named the fort erected at the confluence of those three rivers after the country's Prime Minister, William Pitt.

Initially, timber and coal, followed by glass and iron, attracted people from the farms to work in the factories of the first industrial revolution, related the mayor. On this foundation, Westinghouse and Carnegie electrified the factories that mass produced the steel and aluminum that built every city in the United States. "Every bridge and skyscraper contained Pittsburgh steel," said Mayor Peduto.

Unfortunately, the mayor pointed out, there was a price for all of this progress, and in Pittsburgh, that was polluted air and water and income disparity. So, Pittsburgh went back to work and created the first clean air act in America, as well as clean water standards, well before such steps were taken at the federal level. Workers also participated in the revitalization effort by creating unions and building a middle class, he emphasized.

All seemed well until 1979, when the mines, factories, and mills began to close and people moved away. At the time, said the mayor, Pittsburgh had become the third leading corporate center in the United States, behind only New York City and Chicago. For those who stayed, he recounted, unemployment exceeded levels during the Great Depression. The city that had built the country, instead built a larger deficit than New York City's when it declared bankruptcy, and many wrote Pittsburgh off.

However, Mayor Peduto noted, 1979 also saw the seeds of a new future sown. At Carnegie Mellon, they instituted a degree in robotics, followed a few years later by a Ph.D. in the field. Artificial intelligence became the core of another program, and the hospital at the University of Pittsburgh became the fourth largest recipient for federal grants as a research medical facility in the United States. The city of Pittsburgh became the first in the world to sign a Memorandum of Understanding with a university, allowing for unfettered cooperation in areas of mutual concern. This type of agreement, he explained, required taking on some risk, the same way Pittsburgh accepted risk in allowing the development of driverless cars. Today five different companies are developing autonomous vehicles here. Pittsburgh has learned from its past that it is not sufficient to be reactive—we must be proactive in the future to avoid the mistakes of the past.

New technologies and disrupters arrive all the time, said the mayor, so the city has instituted four criteria to determine if Pittsburgh will invest public money. He labeled them the four Ps, people, planet, place, and performance. For example, driverless cars will replace some workers in the market – is there a plan to retrain these individuals, and insure that they remain productive contributors to the economy? Will introduction of these vehicles lessen pollution and congestion, helping the planet and the place?

> *"We had to become reactive to clean our air, reactive to clean our water, reactive to create a society where all workers were valued and where disparity was minimized. We are not going to make that same mistake twice. Now, we use a metric that we call P4 to judge where and how we should invest public money: People, Planet, Place, Performance."*
> *– The Honorable William J. Peduto, Mayor of Pittsburgh*

Does this lead to a better world or just a different one?

Pittsburgh, he stressed, "… is a resilient city, a city that burned down, a city that was flooded, a city that had its economic heart ripped out of it, and we've been able to come back … because we have invested in our people." As a city that relied on natural resources for its initial development, Pittsburgh now has more jobs in renewable energy than coal, oil, and gas combined. The city leads the state in green jobs, and wants to continue to be an industry leader in the needs of the future. However, we still have to develop the infrastructure, rebuild the grid, and rebuild the neighborhoods.

In closing, Mayor Peduto recalled that his grandparents came to this city with little to no education, and thrived here. One of his grandfathers was fired for participating in a union organized meeting and the other died at one of the local steel mills. When he visits other cities, he said, he reminds them of the importance of putting people first and that there are values we need to have that outweigh profits. "That spirit is all around Pittsburgh," he said, "because we understand we can't do it alone, that we need partnerships." Finally, the mayor stressed, "… it's not just the technology that has brought us success; it's the spirit of the people of Pittsburgh, and that is what you need to take back with you."

By: John Bergmann, USSOCOM J-59 Future Concepts Division

The AlphaGo Zero Challenge

Dr. Heather Wilson

Just three years ago, related Secretary of the Air Force, Dr. Heather Wilson, a London company named DeepMind developed a computer program called "AlphaGo," to play the Chinese game "Go." The developers, she continued, wrote the program's algorithms based on their knowledge of thirty million possible moves, all of which had been previously played by human experts. Afterwards, AlphaGo defeated a human world champion "Go" player. A year later, DeepMind introduced an upgrade labeled "AlphaGo Zero," which learned to play "Go" without human input, self-generating scenarios and playing millions of games against itself. Moreover, "AlphaGo Zero" taught itself to play chess and defeated the best computers that had been programmed to play chess, she stressed.

"It's not hard to imagine how machine learning like this might change our lives dramatically," she stated, and it leads naturally to a discussion about the advantages and disadvantages of artificial intelligence, machine learning, and other new technologies to our societies. In the arena of national defense, Secretary Wilson stressed, the application of technology to the use of force falls within the scope of the law of war, which itself is divided into two parts: the legitimacy of the use of force and rules governing the conduct of hostilities.

From the 16th century onward, sovereigns gradually asserted a right to use violence both within their borders and against other sovereigns, and by the end of the 19th century, everyone understood that sovereign states had the exclusive right to wage war, she noted. In parallel to this process, Secretary Wilson asserted, a consensus also emerged about limitations on the methods and means of warfare. Over the last century, states codified these limitations into a series of treaties known as the Geneva Conventions. As a result, she said, we have learned to balance the desire to win with the tendency to use all means to secure victory, and that war should be the means to achieve a better peace, not the destruction of civilization. Moreover, this pattern has strongly manifested during the seventeen years fighting the war against terrorism, in which we have repeatedly shown that we can refine technology to defend our nation, while minimizing destruction and risk to innocent life.

However, new technologies, like artificial intelligence and machine learning will enable new modes of warfare, warned Secretary Wilson. As AlphaGo Zero demonstrated, they may already have the ability to teach themselves to win conflicts "… irrespective of any moral code undermining the limitations on the use of force that our societies have built over centuries," she underscored. As people of conscience, she emphasized, we must ensure that humans decide the reasons and timing of military actions, even as technologies increasingly implement them.

These concepts are particularly important as we ponder the application of new technologies in the irregular warfare context, Secretary Wilson proposed; for our experience over the last seventeen years tells us that we cannot merely bring advanced technology and operational doctrines to an irregular warfare adversary and expect to win. Irregular warfare, she continued, is traditionally a low-tech fight for hearts and minds. Yet, even that is changing with the proliferation of cheap technologies allowing adversaries to leverage the internet in ways inconceivable twenty years ago. For instance, through digital money laundering and cryptocurrency markets, non-state actors have accumulated billions of dollars in shell companies and offshore tax havens.

"In future warfare, here lies the reason for owning speed first. You can't call a 15 minute break in warfare."
– The Honorable Heather Wilson, Secretary of the Air Force

We countered with people on the ground, like our Special Forces, using technology to enhance their decision making by providing faster and better options, she emphasized. New technologies that are currently under development will further enhance our irregular warfare capabilities, she insisted, including understanding local networks, history, culture and languages. Full motion video and crowd behavior predictions from sensors might provide warnings and egress routes, she highlighted. All of this, she said, can be shared with our

"The technological pursuits of our time include data analytics and artificial intelligence and autonomy and robotics and directed energy and hypersonics and biotechnology. All of this is changing the nature of warfare. But developed nations cannot simply bring their advanced technologies and operational doctrines to an irregular adversary and hope to win."

partners, with these connections making the difference in the future of irregular warfare. However, as our adversaries develop similar capabilities, Secretary Wilson warned, we will need to command these technologies' expertise and speed, so we can present warfighting options to decision-makers faster than our opponents.

Here in Pittsburgh at the Carnegie Institute of Technology, Secretary Wilson related, the first artificial intelligence (AI) program, Logic Theorist, was produced in 1955. A study of 3,000 companies in 2017 showed that between 2013 and 2016, investment in AI tripled. From 2016-2017, these outlays doubled again, because the private sector expected a substantial return on investment. AI overlaid on the physical landscape becomes augmented reality, Secretary Wilson explained, which can be used for everything from the first down marker of a televised football game to a projected 3-D model utilized by a neurosurgeon during a delicate surgery. While industry develops these capabilities, the military must stay tightly connected to the developers, she emphasized.

Secretary Wilson stated that the recently released Air Force Science and Technology Strategy identifies five strategic capabilities to help us master time, speed and complexity. These include (1) surveillance, (2) information sharing, (3) rapid, effective decision making, (4) complexity, unpredictability and mass, and (5) speed and reach of disruption and lethality. All of these will be enhanced by advanced technology, in which the Air Force continues to make substantial investments. To be clear, she stressed, "... we are not looking for a fair fight, but will ensure a just fight, upholding our moral underpinnings despite the use of greater automation of weapons and forces."

Returning to her opening vignette, Secretary Wilson said that when AlphaGo Zero was challenged by the reigning human Go champion, the program had about 10 to the 360th power possible moves available. In the first game, the program made a move no human competitor would ever make. The champion requested a fifteen minute break to compose himself. Upon his return, he was summarily defeated. In future warfare, we have to own speed first, because we don't have the luxury of calling a fifteen minute break, she concluded.

By: John Bergmann, USSOCOM J-59 Future ConceptDivision

Getting Ahead of the Violent Non-State Actor Technology Adoption Curve

Daveed Gartenstein-Ross

Challenging conference participants, Valens Global Chief Executive Officer, Daveed Gartenstein-Ross, asserted that "… by any chosen metric, Al-Qaeda is today much more powerful than it was in 2001, despite the massive amount of resources the United States and its coalition partners have devoted over the past 18 years to its destruction." Like successful start-up companies in the commercial sector, Al-Qaeda has grown stronger because its organizational design has incentivized and facilitated the ability to innovate over time, said Gartenstein-Ross. Al-Qaeda's flat and open organizational architecture has fostered experimentation with both drones and social media, generating increasing success while experiencing some failures that have not had serious repercussions for the organization. Al-Qaeda, like many successful start-up companies, have learned to "fail fast and pivot," explained Gartenstein-Ross.

Scholar Assaf Moghadem has described Al-Qaeda, Daesh, and other VNSAs as "terrorist entrepreneurs," Gartenstein-Ross noted. Elaborating, he explained that VNSAs – terrorist organizations, gangs, or cartels – are in very real ways the start-up firms of the political organizing space. They are small, de-bureaucratized, and their organizational design is wedded to the technology they intend to deploy. Moreover, VNSA structures enable them rapidly and easily to adopt new technologies, he said.

Gartenstein-Ross proposed that a VNSA technology adoption curve provides a useful metric for analyzing the process by which they adopt new technologies, learn, and modify them for their particular uses. There are four phases in the model: early adoption, iteration, breakthrough, and competition.

For VNSAs, the early adoption phase sometimes yields success, sometimes failure, but it is always characterized by limitations, explained Gartenstein-Ross. U.S. personnel monitoring early Al-Qaeda in Iraq experiments with drones laughed at video clips that had been intercepted. On the other hand, Anwar al-Awlaki's early efforts to use social media did succeed in inspiring "lone wolf" attacks, but they achieved no lasting results, because al-Awlaki's social media campaign was never linked to a broader strategy.

In the iteration phase, continued Gartenstein-Ross, VNSAs are learning through success and failure how to adapt technologies to their broader purposes. Daesh successfully used drones, first for ISR, and then to deliver small explosives, like grenades, with substantial impact during the battle for Mosul and afterwards. On the other hand, he noted, Hayat Tahrir al-Sham's experiments with drone swarm attacks on Russian and Syrian installations have largely failed against superior air power and anti-aircraft artillery systems. In social media, Daesh recruiter Janada Hussein used Twitter to radicalize people directly and assist them with weapons acquisition and attack planning. However, his operational security shortcomings enabled security services to arrest many of his operatives before they attacked.

VNSA operatives become more effective in the breakthrough phase, continued Gartenstein-Ross. For instance, Daesh's Rachid Kassim carried social media recruitment and attack planning to a new level by adopting improved operational security. In many cases, Gartenstein-Ross said, intelligence services never comprehended his activities until after an attack had been executed. Likewise, he elaborated, Al-Qaeda has been running a successful information operation for nearly a decade that had many leading analysts believing that the organization had largely disappeared from the world stage. Furthermore, if VNSAs can achieve significant results like these on their shoestring budgets, we should not be surprised that states committing substantially larger resources to their asymmetric activities are also achieving strategic successes.

"… by any chosen metric, Al-Qaeda is today much more powerful than it was in 2001, despite the massive amount of resources the United States and its coalition partners have devoted over the past 18 years to its destruction."
– Daveed Gartenstein-Ross

The competition phase, explained Gartenstein-Ross, features state responses to VNSA use of technologies, such as counter-UAS technologies, despite the risks to commercial aircraft, and requiring social media platforms to remove from their systems VNSA-related accounts. Meanwhile, the counter social media strategy, he said, has enlisted social media companies to remove from their platforms offensive VNSA material, but these activities and processes put at risk freedom of expression principles that are the foundation of democratic government. However, once competition begins, outcomes become much more variable, he cautioned.

As argued in the recent Small Wars Journal article, "Harnessing David and Goliath," the United States and its partners need to combine strength and agility to develop strategies that get out in front of the VNSA technology adoption curve and the revisionist state actors who are following similar paths. However, there are inherent obstacles that must be overcome for states to become more innovative and daring. If VNSAs act like start-up companies, Gartenstein-Ross noted, states behave more like legacy companies that successful start-ups replace in the marketplace (e.g. Amazon and Borders Books). "… [L]ike Frankenstein's monster," he continued, state bureaucracies often lumber "… around with different parts of different agencies at different times reflecting policy, lurching from one policy to another, sometimes based on elections and new governments …," such that it is often impossible to discern a strategy or who may be driving strategic thought. Quite often, he added, "… tactics end up driving strategy."

To get ahead of the curve, he stressed, "… we need to re-examine the bureaucratic structures we have in place." If analysts and strategists are important, we should have incentives for them to bet against the crowd and get things right. As Jim Dator, an academic said, "Any useful statement about the future should at first seem ridiculous." Right now, those incentives are not in place, blinding us to what is coming and limiting our ability to innovate strategically in a highly competitive environment.

Gartenstein-Ross closed optimistically; while VNSAs may have organizational designs that enable greater creativity and innovation, they do not have the resources states can bring to bear. In a technological competition with VNSAs, states are more likely to prevail, although "… VNSAs are likely to cause a great deal of damage given the pace of technological change."

By: Greg Hicks, Sovereign Challenge Program Coordinator

Today's Technologies That Are Already Changing Warfare

Panel Discussion: Keith Dear, Natasha Bajema, Michael Horowitz, Christopher Paul

Current and emerging technologies are revolutionizing the character of conflict, especially irregular warfare, while also redefining our understanding of the human experience, offering security and ethical dilemmas to governments and societies, and challenging the boundaries of state regulation. In the past, these conversations were about the extent to which military technologies could be adapted for commercial use, but today, the discussion is about the military adaptation of commercial technologies that are "value neutral" and readily available to all. At the heart of these conversations is a second dichotomy between the ever-shortening amount of time available to make decisions in increasingly complex environments, and trusting the technology that is required to analyze the data in sufficient time to have the opportunity to make a relevant decision.

At the center of this revolution is artificial intelligence (AI) and machine learning, said Professor Michael Horowitz from the University of Pennsylvania, which in many ways is becoming a general purpose technology, not unlike the internal combustion engine or electricity, rather than some exotic weapon system. AI, Horowitz continued, has become a focal point of international competition, especially after Russian President Vladimir Putin said that "… whoever rules AI will rule the world." However, competitors may see AI's advantages differently. For instance, democracies like the United States and Israel may see AI as a means to take soldiers off the battlefield and improve processing power for better battlefield management. On the other hand, autocracies like China and Russia see the same advantages, but because they enhance dictatorial controls over their societies. Meanwhile, VNSAs may see AI as a tool to track targets in dense environments or to better masque planned attacks.

The more any specific AI algorithm approaches a military-only use that can be monopolized, the easier it will be to generate first-mover advantage, Horowitz suggested. Nevertheless, he continued, it seems likely that most military applications of AI will either be developed from commercial applications or have commercial analogues, making AI very difficult to control. Many countries and non-state actors will have access to these technologies, compounding the problem, he said.

RAND's Dr. Christopher Paul reminded everyone that people have a tendency to look for technological solutions to human problems. He also stressed that human cognition is still very, very primitive and is biased towards personal interaction, facial expression, and trust, among others, that in a modern digital environment are somewhat disadvantageous. These characteristics make humans vulnerable to deception, manipulation, and influence-operations that precision marketing and neuropolitics, enabled by artificial intelligence, can scale in ways that were previously unimaginable. This is particularly important when people are forming their initial views on a particular situation, he stressed, because the first ideas that people accept are always more durable. In influence and information operations, the first move advantage is real.

Wing Commander Keith Dear introduced the conference to three innovative directions that artificial intelligence and machine learning is opening for the military. Cognitive maneuver, he said, could use big data to predict an adversary's intentions before they have committed to them, enabling us to deter those intended actions before they are ever implemented. Trusting artificial intelligences' ability to generate "otherworldly moves," in other words, to analyze situations and recommend courses of action that a human being would never contemplate, let alone consider, could create opportunities to succeed strategically at lower cost in lives and treasure. Moreover, applying these processes to develop more rigorous human decision-making by testing forecasting accuracy and decision confidence probabilities in synthetic environments. Part of that process is for human decision-makers to make their implicit assumptions and premises explicit as they employ virtual reality simulations to better define choices. In some circumstances, courts and insurance companies will inevitably take humans out of the decision loop, simply because there will come a time when machines will be able to do certain tasks so much better than humans, both Dear and Horowitz explained.

However, both agreed that we will always frame responsibility in such a way that the human commander is making the choices and the machine is implementing them.

"Human resilience is not as impressive as we think. Worse, most of us suffer from bad blind spot bias. In moments of fatigue or inattention, everyone can be deceived."
– Christopher Paul

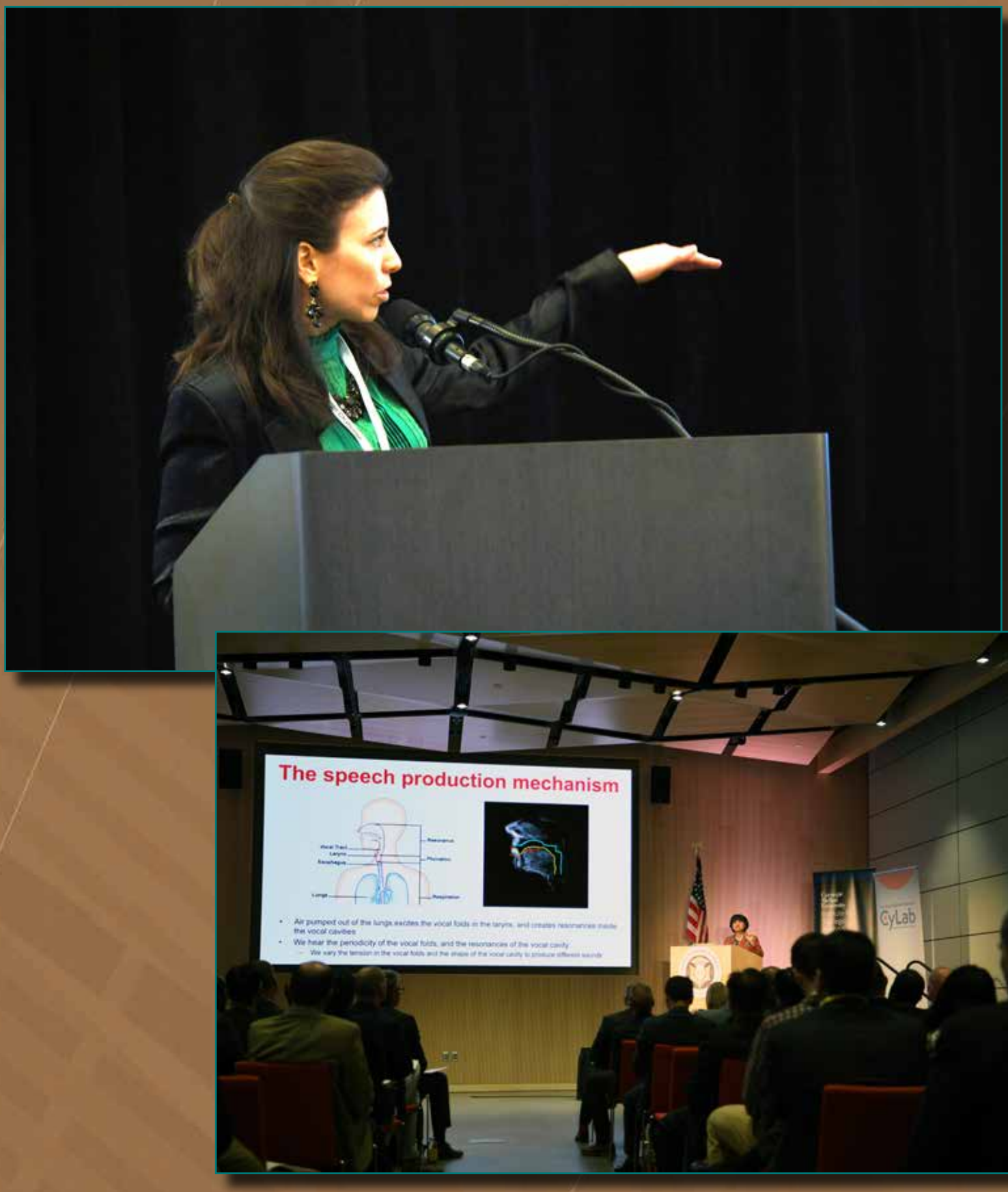
As National Defense University's Dr. Natasha Bajema related, trends in the proliferation and democratization of advanced technology like additive manufacturing, advanced robotics, and synthetic biology present a growing and dangerous national security risk with respect to weapons of mass destruction. These technologies, she continued, lower the barriers to development and use of WMD for a range of nefarious actors. In the past, governments could control the nuclear and other toxic materials that constitute WMD, but off the shelf drones, 3-D printers, machine learning tools, and gene editing kits enable do-it-yourself innovation with WMD implications. Nowhere is this more relevant than the convergence of physical to digital conversion technologies with gene sequencing technology. Using these techniques, she said, could allow the transmission of a genome by email and its reverse transformation into an active bioweapon. Mitigating the rising WMD risks associated with commercially developed technology will require new and innovative approaches because the non-proliferation tools of the past were created for a world in which access to WMD was a government monopoly, she noted. Morality and ethics, panelists agreed, would be at the heart of any proactive risk management effort that achieves positive results without compromising civil and human rights that are the cornerstone of democratic societies.

In Paul Scharre's book, Army of None, Scharre recounts the story of Lt Col Stanislav Petrov, a Soviet officer who was monitoring the U.S.S.R.'s new computerized strategic alert system in 1983, when it sounded a warning of an incoming American first strike. Petrov's first reaction was to distrust the new system and knowing he had only about twenty minutes to prove to the Soviet Union's leaders that the computers had erred, he contacted officers at other Soviet early warning systems and learned that the computers had indeed identified a phantom attack. Thirty-six years later, computers are faster, more powerful, and increasingly independent. They and rapidly evolving, highly sophisticated weapons systems are decreasing the time available to leaders to make decisions, requiring decision-makers to trust their technology to an ever greater degree. As these trends continue, the future national security environment will inevitably be shaped by the dichotomy between states and populations trusting technology too much, or not enough.

By: Greg Hicks, Sovereign Challenge Program Coordinator


Even Identical Twins Have
Different Irises
CyLab


Strategic
Analysis


The speech production mechanism
Vocal Tract
Larynx
Esophagus
Lungs
Resonance
Phonation
Respiration
Air pumped out of the lungs excites the vocal folds in the larynx, and creates resonances inside the vocal cavities
We hear the periodicity of the vocal folds, and the resonances of the vocal cavity
We vary the tension in the vocal folds and the shape of the vocal cavity to produce different sounds
CyLab

Carnegie Mellon University Presents: Artificial Intelligence for National Defense and Sovereignty

At Carnegie Mellon University's (CMU) state of the art Tepper School of Business, five leading CMU scientists offered a range of exciting and thought-provoking presentations on their latest research in Artificial Intelligence (AI). Topics included Defensible AI, Voice Recognition and Forensics, Cyber Security and AI, Biometrics and Real-Time AI, and Robotics and AI for Defense. Introducing the program, CMU President Dr. Farnam Jahanian highlighted CMU as an interdisciplinary research institute with an inclusive mindset that is multi-national, multi-cultural, and seeks to solve relevant, real-world problems. Dr. Jahanian emphasized that AI spans many disciplines and is the most important intellectual development of our time, but leaves us susceptible to a wide range of threats. Overcoming these vulnerabilities is a major challenge and opportunity.

Elaborating on Dr. Jahanian's remarks, Dr. J. Michael McQuade, CMU Vice President for Research, highlighted the importance of applying CMU capabilities toward real-world challenges and the involvement of CMU's 14,500 students and 1,400 faculty members both in fundamental research and in key national conversations about those problems.

With respect to AI, CMU's focus areas include the algorithms of AI, the ethics of autonomy and AI, human teaming with AI, the process of engineering AI systems, data cleansing and data bias, AI education for the workforce, and trust and sensing. This work, Dr. McQuade emphasized, will have ramifications across many disciplines, from the basic sciences, to engineering, to social sciences and the arts.

Dr. Greg Shannon, Chief Scientist for the CERT® Division at the Carnegie Mellon Software Engineering Institute, suggested that in the context of cybersecurity, the term defensible AI is more appropriate than the term secure. The term "secure," he asserted, can be a misnomer, indicating a certainty or assuredness that there is no possibility something bad will occur. In cybersecurity, this is not possible, he underscored. To manage the risk associated with AI, he suggested that we must make attacks expensive, inconvenient and consequential for attackers. Dr. Shannon also emphasized the importance of AI design to prevent system compromise, as well as the notion of a Computer Security Incident Response Team (CSIRT) for AI.

Associate Research Professor at the CMU Language Technologies Institute Dr. Rita Singh delivered a captivating presentation on "Profiling Humans from Their Voice." Deploying audio and visual examples from her study, which examines the information available from the micro-level data from a person's voice, Dr. Singh explained that data from the voice is language agnostic and includes markers for physical stature, weight, height, age, health, psychological parameters, mental health, physical health, disease, personality, sociological background, and even facial features. Through the application of artificial intelligence, she said, we can identify these markers and predict the identity of a human being, as we successfully demonstrated last year in China. In response to a question about deepfakes, Dr. Singh said that at this time, cloned voices have too much consistency at a very fine level, compared to real human voices which are never consistent at any level.

Key CyLab cybersecurity projects are at the intersection of AI, Machine Learning (ML) and cybersecurity, related Dr. Lujo Bauer, Director of CyLab Cyber Autonomy Research Center and Associate Professor of Electrical and Computer Engineering and Computer Science at CMU. The landscape of cybersecurity threats and capabilities is rapidly changing, he added, with attackers becoming increasingly sophisticated and determined, while the systems we are defending are much more complex. CyLab is utilizing two main research themes – leveraging AI and ML to enable new defenses, and understand the risks posed by increased use of machine learning. The two themes,

he said, underscore four main research thrusts which include utilizing AI and ML to automate software vulnerability detection and prevention, network level defenses, predictive analytics, and counter-autonomy/hardened autonomy.

Dr. Marios Savvides, founder and Director of the CyLab Biometrics Center and Professor of Artificial Intelligence at CMU, delivered a fascinating presentation on Facial Recognition 2.0 in which he described a system developed at CyLab that is capable of capturing personal identification information from a person's iris up to 12-meters away. The system is capable of capturing this data at extreme angles, reflected in rear-view mirrors, or when a person is wearing a mask. The iris is considered unique for each person, and also thought to be stable over a person's lifetime.

"…[C]omputing is at the center of a global transformation that's underpinning economic prosperity and accelerating the pace of discovery across almost all fields of inquiry," and "…unprecedented access to data is transforming every sector of our economy. Software enabled systems are now critical to our operations across government, industry, and global defense; and Artificial Intelligence, perhaps the most important intellectual development of our time, is quickly becoming the next frontier."
– Farhan Jahanian

Dr. Howie Choset, Professor of Robotics and Co-Director of the Bio-Robotics Lab at CMU, discussed initiatives regarding robots and AI across two efforts - search and rescue technologies for first responders, and manufacturing. Dr. Choset emphasized the importance of working with first responders on fielded systems in order to stress test ideas and ensure the right problems are being solved. He also highlighted an on-going initiative to stand up a center which can bring together universities, large companies and small companies to create a cohesive techno-centric response, hand-in-hand with rescue workers. On manufacturing, Dr. Choset discussed objectives of the Advanced Robotics for Manufacturing Institute, which include empowering the American worker to be able to be cost competitive with laborers in other countries, as well as lowering the cost and education barriers for small companies to integrate automation.

By: Maj Christine Rhyne, USSOCOM J43/5

Connecting the Military, Technology, and the Public
Max Brooks

Author, scholar, and teacher Max Brooks delivered an insightful look at policy changes the U.S. military should adopt to maintain its dominance and to counter emerging threats now and in the future. He argued that the "separation" of the U.S. military from the rest of the general population is becoming a critical security issue, noting that societal and technological advancements require a different approach to build a whole of nation approach to comprehensive defense.

Brooks asserted that the worst war the United States ever fought was Operation Desert Storm in 1991. In overpowering Iraq with overwhelming conventional force, the United States taught its adversaries not to meet the U.S. military on the battlefield, but to use asymmetric techniques to reduce influence and attrition capabilities. "While we continue to build a green high-tech Maginot Line …," our adversaries have been investing in technologies they can use effectively, "… and they're winning …," he said.

Answering his own rhetorical questions about Hollywood being out-messaged by terrorists and Silicon Valley being out-hacked by Russia, Brooks stated that Hollywood is not in the fight and for the most part, Silicon Valley is not in the fight either. While the United States is facing Russia, China, and Iran, "… they are not facing the United States, they're only facing the U.S. military and its associated defense industry, not the entire country."

Hollywood could be more involved though, he said, because at any given time, 90 percent of the screenwriters, actors, and producers, are not working. "… [A]ll this talent that influences the entire world is just sitting there." Instead, like in World War II, they could be better explaining our concepts and ideas. One of our allies, the United Kingdom, has reactivated an information warfare unit, the 77th Brigade, to counteract foreign influence operations. Meanwhile, one of our adversaries, China, understands this, he noted, so they are buying movie companies, and at Chinese direction, inserting Chinese actors and themes into their shows.

The United States "… used to have a strategy of 'all give some, some give all," but that mantra has evolved to "… you give all, and I go to the mall," said Brooks. This divorce between the U.S. military and the American people began around the 1950s, Brooks argued, and society has come to view the U.S. military as a "warrior class" of distant heroes. "Thank you for your service" is code, he said, for "better you than me." The end of the draft after the Vietnam War marked an important milestone in this disassociation between people and the military. This sentiment was further amplified in the post-9/11 efforts to bring America together by the Commander in Chief's attitude of "we've got this!" and instructions for the population to turn their attention to the economy rather than worry about war.

Brooks offered three main paths for the American people to become re-engaged in national security. First, he recommended reversing course on allowing transgender individuals to serve in the U.S. military. While the ban only applies to a small portion of the population, younger generations are growing up in a time of heightened identity politics, and the military, Brooks believes, is perceived to be out of step with the societal norms of their generation. He said that the transgender ban "… is alienating an entire generation of young people from any kind of government service, military or otherwise."

Second, he recommended a practice of recruiting the recruiters to find new types of talent from Silicon Valley and the tech center. Success depends on gaining trust in these new technology "tribes," he argued. The direct commissioning program, he suggested, might be a useful tool.

Third, he urged that the U.S. military embrace identity politics as a reason to defend the country. Our adversaries do not respect individuality, so we should, while informing the American population of America's unique character relative to the oppression of gays in Russia, the gender fluid in Iran, women under ISIS or the Taliban, or anyone wishing to speak their own mind in China. In those countries, he continued, people still end up in re-education camps and have their cultural identity erased, "… sometimes simply for worshipping the wrong God."

Getting this right is important not only for the United States, but also for its allies and partners, he said, because since the United States stepped onto the world stage in 1917, the American brand has been that "… we fight for a better world," not for empire or natural resources. "Morality is not a luxury for the United States …," he reminded the audience, especially with alternative models reappearing on the world stage. For instance, he continued, China's model is to buy client states through lending governments money to build roads and naval bases. Russia's approach is to do whatever necessary to regain its empire.

In the gray zone, where most of today's warfare is conducted, citizenry with the right tools and talents can engage successfully, Brooks emphasized. The public needs to be involved, to be reconnected to the military, he stressed so that when Russia, China, and Iran are facing the United States, they know that they are facing not only the U.S. military, but a united country. This requires us to remember our principles, to embrace change, and some of that may require some bottom-up re-engineering of the connection between societies and their warriors.

By: Julie Hillson, USSOCOM J-35 Future Operations Division

"Desert Storm … was the [w]orst war ever because it taught us the exact wrong lesson. We thought that we were showing the world 'Don't mess with us, because if you meet us on the battlefield, we will annihilate you.' And the rest of the world said, 'Okay, we will mess with you by going around your battlefield.'"
– Max Brooks

New Technologies, New Strategic Realities, and New Battlefields

Panel Discussion: John Watts, Lydia Kostopoulos, Nicolas Christin, Elsa Kania

Emerging technologies such as Artificial Intelligence, Machine Learning, Additive Manufacturing (3-D printing), the internet of things, and Virtual/Augmented Reality are currently altering the conduct of warfare now, and this expanding reality will continue to widen the scope of warfare into the future. As the Atlantic Council's John Watts related, Syria, Iraq, Libya, and Ukraine, among others, have become active Irregular Warfare laboratories in which Non-State Actors are converting Rocket Propelled Grenades into mortars and operating autonomous rocket launcher bearing All-Terrain Vehicles with modified X-Box controllers. Meanwhile, Russia is experimenting, without much success so far, with autonomous weapons systems in Ukraine.

Looking forward, we can expect autonomous systems to saturate all aspects of the military profession both in analysis and prediction of events as well as integration of autonomous decision making in the systems delivering effects on the battlefield. CMU's Mayhem algorithm, which automatically identifies code vulnerabilities and follows up by developing code to exploit them, offers a glimpse of things to come in cyber warfare, noted CMU's Dr. Nicolas Christin. Adversarial machine learning, he continued, will inevitably become an essential element of future conflict and competition. For instance, CMU researchers have shown that autonomous vehicle systems can be fooled into navigation or other driving errors by applying scotch tape to a stop sign, and facial recognition software has been deceived by simply wearing oddly shaped or decorated glasses.

> *"…[T]hose who can tell a compelling narrative will be the ones who win the information war. [I]t doesn't matter if that's a narrative that we agree with or disagree with; it's the one that is told the best. …[N]ow we have more tools to tell that story in an immersive way, and if we ignore virtual reality or augmented reality, the next generation will be told a story by other people in a compelling way that we are going to miss." – Lydia Kostopoulos*

However, Dr. Christin related we should not jump to the conclusion that machines will be "fighting" machines without human involvement. Full autonomy is a long way away, and we may never reach it, he underscored. Humans currently have an improving set of tools for both offense and defense, but will always have to examine and interpret the analytical results machines provide, he asserted.

Rather than fearing a world of machines fighting each other, Dr. Christin said, we are more likely to lean toward a future of cyborgs, humans with capabilities enhanced via machine interfaces. As Dr. Lydia Kostopoulos elaborated, Elon Musk's company Neuralink is exploring the means to connect machine and human brain together so that we can be faster, and so that we may be able to communicate with each other without using voice. This may realize the potential for humans and machines together to be both more efficient and more ethical, because machine systems do not think about problems the same way humans do. Nevertheless, computers, no matter how sophisticated, are still subject to the Garbage In-Garbage Out (GIGO) rule, Dr. Christin reminded the audience.

Dr. Kostopoulos fascinated the audience with the potential for super-empowered individuals as access to virtual reality and augmented reality becomes increasingly democratized. On the other hand, individuals' and societies' perceptions of reality will be exposed to influence, she stressed, because more avenues are opening to relate stories in more immersive and persuasive ways. Those who can tell and retell the most compelling narratives designed to affect specific generations will prevail in the growing information competition between states and non-state actors, she stressed. Inevitably, she underscored, virtual and augmented reality will become battlefields, and so we must not only improve our own storytelling, but also strengthen the resiliency of our own populations to resist hostile information operations.

"If we talk about influence, that's where the warfare is going to eventually migrate. … [W]ithin the context of future warriors, if the people are going to be in online virtual reality, then warfare will inevitably go there." – John Watts

As a case study for upgrading military capability through adaptation of cutting edge technologies, CNAS's Elsa Kania illuminated China's military modernization. Since the 1990's, that country's leaders and scholars have been intensively studying the Western way of war, both as the model to copy and as the model to defeat, she said. Based on their analysis, China is looking to "informationize" warfare by closing the technological gap between the U.S. and China and looking for ways to win without fighting through incrementally mitigating Chinese weaknesses and improving Chinese advantages. One application, she noted, is using new technologies to compensate for the Chinese military's lack of actual combat experience, especially at senior levels. Thus, Chinese leaders are experimenting with modern technology, such as augmented reality, to improve planning and decision making skills at the most senior levels.

To win without fighting, Kania continued, China's leaders are examining propaganda and public opinion management applications of emerging technologies for both domestic and international deployment. Conceptually, China's leaders frame this effort as harnessing "discourse power," by seizing control of the narrative to shape major international conversations, especially about technology standards. Thus, the global competition over 5G/6G technology leadership may be very important for military strategists to track. China, she said, is actively exploring the use of 5G's high speed, low latency connectivity in controlling autonomous systems and command and control. As we monitor China's military transformation, policymakers need to ponder our willingness to accept potential disruption through companies like Huawei acting as a commercial host of our networks. It is possible, she warned, that a company like Huawei could affect our power projection over distance if the network is disrupted.

Panelists warned that as the adoption of new technologies expands human capabilities and realities, the potential for miscalculation looms large, especially as warfare becomes increasingly abstract. With emerging technologies rapidly disrupting both the metrics and paradigms of military power, evaluating relative balances of power in any particular military area of operations is becoming ever more complicated. This increasing risk is compounded as politicians slide decision-making responsibilities about conflict to military leaders. As important, one participant stressed that decision-makers must avoid false assumptions about the capabilities of allies and partners because they have different decision-making processes and operate under different legal authorities. However, at the end of the day, competition and cooperation are not mutually exclusive, as the commercial development of most new technologies through international collaboration on basic research and global supply chain relationships amply illustrates.

By: LTC Kenneth Starskov, Denmark
USSOCOM J-3 International Division

Data is the New Ammunition
August Cole

"Ghost Fleet" co-author August Cole explored crucial issues arising from the intersection of ethics and technological change as it relates to future conflicts and irregular warfare. Just as data has become the new oil from an economic perspective, he said, data has become the new ammunition in the field of military power. With that in mind, he continued, military leaders should begin considering the application of the same imperatives to digital warfare that we currently use in kinetic warfare. One aspect that will complicate matters in this area will be resolving the question of who owns the new ammunition, especially as so much of it resides in the virtual "cloud."

We are already seeing glimpses today of the machine speed effect of warfare that we will experience in the next decade, Cole said. Civilians are experiencing the machine speed effect through fundamental behavioral changes that are manifesting in our social practices, for instance, in how we find lovers or new jobs. As the machine speed effect gradually works its way into our lives, Cole continued, it is rewriting human experience.

Among national security professionals, the machine speed effect is already testing the Law of Armed Conflict and international humanitarian law in new ways that will require a different kind of conversation among nation-states, Cole said. The existing political framework which currently underpins wartime alliances with international partners, not to mention our own domestic situations, is out of phase with the technological transformation we are currently experiencing.

The companies leading this transformation – Google, Facebook, Twitter, etc. – are very much in their adolescence, Cole contended, and they continue to innovate and develop at scale new technologies faster than governments can make rules related to them. He added that, as we look at this big mess of aspirational technology companies within our current political and legal contexts, there exists a large gap waiting to be filled. Within this space, he warned, there is substantial opportunity for conflict to erupt.

The defense and national security community, and potentially even the special operations community, Cole mentioned, have an interesting opportunity to come up with durable legal, ethical, and operational frameworks to address these emerging trends. Rules are important, he reminded the audience, because "…[w]e want to make sure we're doing as little harm as possible as we try to make the world a better place." Cole suggested that the private sector, which is rushing forward to develop these technologies as quickly as possible (investment in just the industrial internet of things is estimated at $60 trillion over the next decade), is more likely to approach these legal and ethical problems remedially, after a fine has been levied, a controversy emerged, or a scandal has broken.

Such an approach, Cole explained, is inconsistent with the Western military tradition of proactively interpreting the Law of Armed Conflict. Thus, national security communities can stand firmly on a firm traditional foundation as they begin this very necessary legal and ethical conversation about technologies that are very difficult to understand. Moreover, this raises the question of whether the national security community could actually lead a larger public conversation around the world about how technology will shape environments for better or for worse, he offered.

Cole asserted that a conversation about ethics and technology will be essential for future operational military success. "The sensorization of everything," he said, will create pools of data that will affect every aspect of military operations, not only the discrete task of finding and identifying a specific individual, but also information about the welfare of your personnel, predicting the potential success of recruits, or assessing the wear and tear status of equipment. In the context of John Boyd's Observe, Orient, Decide, and Act loop, Cole suggested that humans will cede observation and action to machines, leaving themselves the roles of aiming the machine and deciding what it will do.

"…[D]ata is going to be so foundational to every aspect of military operations, not only in the discrete sense of finding an individual but understanding the welfare of your force … As we enter into the era of complete datafication and AI modeling fusion, the deviation and divergence from predictable behaviors, from predictable organizations, is going to confer operational advantage in ways that few other advances can."
– August Cole

Fundamentally, he said, the rapidly changing environment requires us to rethink the roles we assign to humans and machines to achieve military objectives. However, we must recognize that this matter goes well beyond sending a robot through the door, rather we should be considering the types of effects and influences we can create without using physical capability at all. For the special operations and irregular warfare perspective, the importance of enablers is critical too. If enablers aren't moving at machine speed, you'll be at an incredible operational disadvantage. For humans to keep up with machine speed cyber and kinetic action, bio-modification, including both physical and neurological enhancement, is inevitable, Cole commented.

For the military, examining these questions of technology, law, and ethics from the opposite perspective – the willingness to break any particular norms and rules, perhaps generally or only in specific circumstances – may prove vital, he commented. Such a process is out of step with much of the conventional thinking about big organizations, which are rule bound for good reason. As we enter into the era of complete "datafication" and AI modeling fusion, he stressed, deviation and divergence from predictable behaviors and predictable organizations is going to confer operational advantage in ways that few other advances can.

The most important aspect of this process is understanding the human dimension, Cole contended. Fiction is a great way to connect with and understand people, he noted. We can encode a story with the DNA of many of these trends that are difficult to synthesize, because they are so complex and are happening with a high degree of simultaneity. Often, he continued, one of the challenges in writing narratives is comprehending the cultural truths of a given community and forecasting the changes that might or might not occur. For those in the military, he stressed, your thoughts on the evolution or not of certain truths will be vital to creating the most accurate and compelling picture of your profession's future.

To be ready for the future world, Cole contended, we should acknowledge the simple strangeness of the world in 2019 and imagining what 2029 and 2039 and on are going to portend, we will be better prepared to make necessary changes now. If we can establish the kind of leadership on ethical and legal considerations within communities that are respected and operationally experienced, such as the USSOCOM community and partner SOF communities, we can get ahead of some of these problems that should be predictable, he suggested, if we can just find the proper perspective.

""The human is going to have to change, too. We're going to see biomodification. We're going to see neurological enhancement .... The idea that our cognitive capabilities can keep up with 5G, 6G era, I think, is wrong. If your enablers aren't moving at machine speed, if they aren't on pace with the same enhancements, either biological or technological, you'll be at an incredible operational disadvantage."
– August Cole

By: Maj Christine Rhyne, USSOCOM J43/5

Ethical Considerations in Deploying Autonomous Weapons and Other New Technologies

Panel Discussion: David Danks, Jacinta Carroll, Osonde Osoba, Lt Col Ilse Verdiesen

Hypothetically, suppose a Command and Control (C2) decision support algorithm written in the Netherlands, employed on a drone built in the United States, operated by the Australians, shooting at a target in Mali, produces a contrary outcome. "Who is responsible?" asked one conference participant.

"Ethics tells us what we should do – how values, interests, and desires should be translated into action," explained CMU Philosophy professor David Danks. RAND's Osonde Osoba elaborated that science allows us to think more clearly about the consequences of the ethical decisions that we make. However, Osoba suggested that in a world characterized by value pluralism, in other words, a world in which people live under different ethical, cultural, and regulatory norms, we should not expect all people, everywhere, to adopt a single, common norm to follow.

To illustrate the difficulties of reaching consensus, Osoba described four examples related to the application of ethical standards to the use of autonomous weapons and new technologies in military conflict. The U.S. doctrine, he said, is no use of autonomous weapons without meaningful human oversight. China, on the other hand, appears more likely to deploy autonomous weapons because its leaders may trust technology to make decisions more than China's military officers, he related. Meanwhile, Osoba explained that VNSAs may not have a vested interest in peace, while private sector innovation remains leaps and bounds ahead of governments.

Adjudicating between plural rationalities becomes the challenge for reconciling disagreements, keeping the peace, if you will, between stakeholders, noted Osoba. He suggested that convening stakeholders to exchange views on the values, implications, and consequences of deploying a particular technology might at least establish normative clarity, a first step on a path to consensus. Venues like Sovereign Challenge program events can contribute to such a process.

Questions about the ethical use of autonomous weapons come down to issues related to governance, regulation, control, and accountability, according to Lt Col Ilse Verdiesen of the Royal Netherlands Armed Forces. Governments, ministries of defense, and military commanders provide governance for implementing military technologies, explained Lt Col Verdiesen. Regulation, such as through additions to the Laws of War, is an avenue for defining ethical use of new technologies on the battlefield, and for establishing consensus norms for governance, she added. In the military, control of autonomous weapons occurs either before use, through rules of engagement or other directives, or during use, when a human determines the target and initiates action, she explained. After a weapon is used, oversight, potentially at multiple levels (political, administrative, professional, and social), assigns accountability for weapons usage. Establishing both causal and moral responsibility, commented Osoba, can help determine human accountability for the use or misuse of a weapons system, because ultimately, a human will make the decision to deploy the system.

Danks reminded everyone that every major modern military is using AI to process intelligence, surveillance, and reconnaissance before any human being ever sees it. "We have an amazing opportunity ahead of us …," he said, to take systems that perform repetitive functions, mechanical processing, and sustained vigilance that humans do not perform well, and pair them with humans who can contribute context recognition, creativity and creating novel actions to necessary tasks. Increased teaming of machines and humans is very much in our future, Danks asserted.

This growing intertwining of humans and machines, Danks continued, will

> *"Ethics is not about telling you what you cannot do; it's telling you what you ought to do. It's asking questions about the ways in which your values, your interests, your desires ought to be translated into action, how you ought to realize those values through the ways that you interact with the rest of the world, whether on the battlefield or in the office or in your home."*
> *– David Danks*

require us to trust both technology and team, despite the human instinct not to trust technology the way we would trust a human. Danks explained that trust of any autonomous system, one that can do something without explicit direction (like humans), depends on our understanding of how the system operates. If we want to deploy a system that is even semi-autonomous in an ethical manner as part of a human-machine team, he stressed, it is critical for the people making the deployment decisions to have an understanding of how the system functions in such a way that they can know, in particular, when it might fail, especially in an adversarial setting. Hence, rethinking the systems by which we train and teach military personnel, and transmit information not only to leaders and commanders, but also to the general population, is becoming an imperative, argued Danks.

"Technology and innovation have always excited humans," recalled Australian National University professor Jacinta Carroll. We're fascinated by our own creativity, the ability to find a clever, easier, quicker, more efficient, more powerful, and more lethal way to do something. We always believe that the tool, the machine, the communications system, or the sensor system worked for us to make things better, she said, just like the dual use, multimodal technology that is enabling and facilitating such mundane tasks as banking, shopping, and researching, etc.

However, because some of these technologies, like encrypted cell phone communications, among others, have become enablers of a number of direct security terrorist threats to Australia and other countries, national security professionals, business leaders, and the general public should engage in a thorough conversation about standards, asserted Carroll. While developing consensus on standards may be a difficult task, she said, undertaking it can contribute to establishing new behavioral norms. Carroll recommended building ethical decision making, responsibility, and accountability into technical capabilities and incorporating it into doctrine, training, and operations. Nevertheless, such efforts alone will not retain the moral authority that is ultimately the center of gravity in ongoing conflicts with VNSAs and competitions with emerging hegemonic powers, she cautioned. "It's our responsibility not only to demonstrate that our cause is just, but also to continue to demonstrate that it's executed in a just manner," she stressed.

While generally agreeing with the thrust of Carroll's comments, Osoba cautioned that encoding moral laws as crisply as possible into autonomous military systems could prove to be counterproductive at the margins. One of the values of human ethical decision making is that people often recognize when the context of a situation requires the breaking of a rule. Osoba suggested that because machines have heretofore not shown a capability to discern context, it is probably very difficult and may possibly be impossible to program autonomous moral machines, especially when norms are contested. Ultimately, the panelists agreed, moral responsibility must lie with the fully-informed, well-trained military commander who orders deployment of a weapons system, whether autonomous or not.

By: Julie Hillson, USSOCOM J-35 Future Operations Division

"Right now, … technological systems … are incredibly good … at repetition. They're very good at mechanical processing of large amounts of information. They're very good at sustained vigilance, and they're very bad at context recognition. They're very bad at analogical reasoning; they're very bad at creativity; and they're very bad at recognizing what they don't know." – David Danks

Allies and Partners Go Far Together

General Richard D. Clarke

A little more than month after taking command of United States Special Operations Command, General Richard Clarke addressed 166 participants from 52 countries who were attending the 2019 Sovereign Challenge program annual conference. Speaking directly to the 71 Defense Attachés and other national security diplomats from 49 countries, General Clarke said, "I believe that you are the best and the finest professionals that your nation sends abroad; it is a distinct honor for us to host you both in this country and at this forum."

Recalling an old African proverb: "[I]f you want to go fast, you go alone. If you want to go far, go together," General Clarke stressed that alliances and partnerships formed by sovereign states committed to the principles of democracy and national sovereignty are time tested ways of preserving freedom and confronting aggression. Consistent with the U.S. National Defense Strategy's second line of effort, strengthening alliances and attracting new partners is an indispensable part of the United States strategy to meet 21st century challenges. Elaborating on the point, General Clarke associated the Sovereign Challenge program with the fourth SOF Truth: "Competent Special Operations Forces cannot be created after emergencies occur – neither can relationships between like-minded nations deeply rooted in common values, objectives, and trust." For this reason, he stressed, the U.S. military and U.S. Special Forces continue to invest substantial resources and expertise in building the military capability and capacity of our partners to strengthen their own self defense as well as their ability to contribute effectively to our collective efforts.

Reflecting on the current national security challenges for the United States, its allies and partners, and U.S. Special Operations Command, General Clarke stated that "[t]he contemporary global security environment is more complex, it's more volatile, and it's more competitive than we've seen …" in at least a generation. The chief factor shaping today's operational environment, he explained, is the reemergence of great power competition – while we still need to be laser-focused on violent non-state actors such as ISIS and Al-Qaeda. U.S. Special Operations Command's first priority continues to be fighting global terrorist networks and their enablers while balancing and supporting the Global Combatant Command's regional campaign plans, he amplified. The terrorist attack in Sri Lanka and the re-surfacing of Abu Bakr al-Baghdadi underline the need to keep the pressure on the terrorist networks even though the so-called 'physical caliphate' is eradicated, General Clarke stressed.

> *"Applied data science and artificial intelligence can help us in information sharing by allowing us to see trends, correlate events, and connect data that seem disparate and unassociated. We are actively seeking ways to harness artificial intelligence and machine learning to more rapidly spot trends, counter false or misleading information, especially as those narratives cross boundaries ..."*
> *– General Richard Clarke*

In this increasingly competitive world, General Clarke continued, we must accept that our adversaries and competitors are pressing us in the technological space by stealing our technology and developing new and creative ways to employ it. Additionally, not all state and non-state actors have the same moral and ethical limitations in deploying new technological capabilities, he stressed. "Resisting technological change will leave us behind on the battlefield," General Clarke acknowledged. Applied data science and artificial intelligence, he noted, can help us in information sharing by allowing us to see trends, correlate events, and connect data that seem disparate and unassociated. Moreover, he continued, cloud technologies will allow us to make this data rapidly accessible and also discoverable.

General Clarke emphasized that the sharing of information is equally important to the adoption of new technology. International Defense Attachés and other national security diplomats, along with the international liaison officers assigned at U.S. Special Operations Command, are integral to our collaborative efforts in this area, he stressed. "The faster we can share information, the faster we can create common understanding and narratives … that promote

dignity and freedom," he said. Citing Operation Gallant Phoenix, through which the 27 countries of the ISIS Coalition identify and share foreign fighter information to interdict their movements and disrupt potential terrorist activities, General Clarke suggested that it could be considered a model for future information collaboration in an increasingly competitive world.

Meanwhile, he explained, USSOCOM is taking the lead for the U.S. military in crafting narratives and counter-messaging to compete with violent non-state actors and coercive states, and we are actively looking at harnessing artificial intelligence and machine learning to spot trends rapidly and counter false and misleading information. To get ahead of our competitors' narratives, to be faster than our adversaries, we are examining closely at which point humans are making decisions, while we convert our special operations professionals from digital and data enthusiasts to conversant AI practitioners, he commented.

In closing, General Clarke reminded participants that the level of effort and investment that rogue powers and coercive and hegemonic states expend to sow domestic and international division and promote conflict among the international community is indicative of their fear of the collective efforts of sovereign states pursuing their shared interests. "… [A]s we work as partners to face the challenges of embracing technology in support of all of our interests and values, we will find that we … have improved ability … to defend … freedom and opportunity for our nations and preserve an international order that allows all of our countries to thrive."

By: LTC Kenneth Starskov, Denmark
USSOCOM J3-International

"If we want to achieve a free and open international order and prevail against the forces of aggression and coercion, strong relationships …among like-minded nations are a must. I am confident that as we work as partners to face the challenges of embracing technology in support of all of our interests and values, we will find that we too have improved ability in our mission to defend …freedom and opportunity for our nation and preserve an international order that allows all of our countries to thrive."

– General Richard Clarke

Participant Perspectives

During the final plenary, break out group spokespersons shared highlights of their discussions about the major themes presented during the previous three days. During the conference, participants organized into eight separate discussion groups, six of which were regionally-oriented, and two reflected global representation.

"Defense attachés are one or at the most two degrees of separation from our chiefs of defense and ministers of national defense. By including defense attachés in this conference, USSOCOM has a direct line back to those nations ... from their involvement in Sovereign Challenge"

Drawing on a vignette from Sesame Street (set in New York City) in the city of Mr. Rogers' Neighborhood, a European participant constructed his presentation around words containing the letter "C". Their group, he said, observed that the current technological boom is "commercially-led," but asked whether governments should continue to allow businesses to lead? In that sense, group members viewed the situation as cloudy in two senses. Meteorologically, we can't clearly see the way ahead, and technologically, so much data is held in the cloud, but the ownership of that data is unclear.

Group members worried that AI and other technologies appear to have the potential to collapse traditional organizational structures and change them before we can adapt AI and new technologies into more familiar frameworks. Additionally, the group worried that the range of complicated interdependencies associated with international competition and technological innovation will inevitably lead to conflict, maybe not full scale war, but possibly cyber conflict, or something in between. In facing these challenges, we should maintain or develop coherent coalitions and be creative in [our] choices, he said.

Many people, observed a Latin American participant, erroneously think of technology as a solver of complex problems. Instead, he argued that it is better suited to solving simple problems. We need to remember, he suggested, that "humans are fallible, and humans created technology; therefore technology is fallible." Their group, he said, advocated that complex decisions involving meaning and value are better made by humans.

A participant from Asia noted that people in their region of the world find that the speed of technological change is both awe-inspiring and frightening. This group stressed that governments and societies must deal directly with ethical considerations arising from the application of new technologies and be prepared to apply new regulations to stymie the harmful use of technology. Echoing this theme, a presenter from a separate group commented that ideas drive technological change, which then propagates new ideas. "As policy makers, he said, we have to determine how far that technology will be allowed to go."

The presenter from a group comprised of participants from across the Eurasian continent elaborated that emerging technologies are raising questions about core values in their societies, but flagged that tampering with societies' existing ethical foundations is not the right path to follow. Nevertheless, because technology is an integral part of life, the new generation of leaders' trusts technology more than their elders, he said. As the new generation assumes responsibility, the integration of technology into lives will increase and questions about trusting it will fade, he predicted.

"We must never forget to invest in our people," the Eurasian group representative stressed. They enable adaptation to change and are the purpose for technological innovation. This will be especially important in the context of relating our military forces to our populations, he stated. His country among others, he shared, is considering "cyber conscription" to meet the demands for talent to integrate rapidly evolving technologies into their military forces. More broadly, some in their group argued for allowing individuals with disabilities that would normally disqualify them from military service to join the armed forces if their technological skills were needed. However, a participant from a different group cautioned that the next generation "… recognize hate, they recognize diversity, and they recognize discrimination," so we have to be mindful as we move forward.

Trade and investment restrictions along with a lack of scientific infrastructure across Africa are inhibiting the growth and use and development of emerging technologies, said one participant. Moreover, retaining skilled and talented Africans in the face of competing opportunities elsewhere in the world is another factor impeding technological adoption and innovation on their continent. Nevertheless, many African nations desire to build their own companies that create new technologies that directly address African issues, said the participant. Finally, he appealed to more advanced countries to regulate technologies more forcefully so that African VNSAs are less able to obtain and use them. Technology, another participant added, must remain in the hands of responsible and ethical users.

The importance of working closely with allies and partners on technology issues was an important theme that emerged from multiple groups. Declaring that "there is power in unity," and urging that we must "strengthen our partnership[s] as we move forward to face challenges, opportunities and risks," one presenter underscored that multilateral organizations can strengthen resolve to resist authoritarian coercion. "While threats are transnational, so are the means to defeat them, whether it's the diversity of thought that our nations bring as nation states, the different genders that are represented therein, or the militaries that are brought up through their shared experiences …," added another participant.

However, several partners flagged the importance of addressing interoperability issues among coalition partners and allies arising from the introduction of new technologies. One participant expressed concern that U.S. "Third Offset" advances could leave many allies behind. Echoing that thought, another participant said that gaps exist, whether they are found in the strategies that are produced by our countries in regard to technology or the technology itself. Unless we are working together to bridge those gaps, we won't be able to combat our adversaries." From a related viewpoint, another partner cautioned that allies and partners must recognize that each country has different laws, rules, and policies related to technology, and these differences also affect our ability to work together.

Finally, a participant commented that Sovereign Challenge program events and other similar forums need to continue to focus on the issue of technological change, because it will always attract an audience. "Defense attachés are one or at the most two degrees of separation from our chiefs of defense and ministers of national defense. By including defense attachés in this conference, USSOCOM has a direct line back to those nations ... from their involvement in Sovereign Challenge" events, noted one participant.

By: Larry Cook, Sovereign Challenge Program Manager
Greg Hicks, Sovereign Challenge Program Coordinator

Speaker Biographies

General Richard D. Clarke, Commander, U.S. Special Operations Command

General Clarke assumed command of U.S. Special Operations Command on 29 March 2019 after successfully completing his assignment as Director for Strategic Plans and Policy, J5, Joint Staff at the Pentagon. Previously, he commanded the 82nd Airborne Division and 75th Ranger Regiment, and has also served previously as a battalion, company, and platoon commander. General Clarke has deployed on numerous tours overseas, including Operations Desert Shield and Desert Storm, Operation Enduring Freedom, Operation Iraqi Freedom, and Operation Inherent Resolve. He holds a Bachelor of Science degree from West Point, a Master of Business Administration from Benedictine College and a Master's degree in Security and Strategic Studies from the National War College.

The Honorable Heather Wilson, Secretary of the Air Force

Heather Wilson is the 24th Secretary of the Air Force and is responsible for the organizing, training and equipping and providing for the welfare of 685,000 active-duty, Guard, Reserve, and civilian personnel as well as their families. She oversees the Air Force's annual budget of more than $138 billion and directs strategy and policy development, risk management, weapons acquisition, technology investments and human resource management across a global enterprise. In her 35 years of professional life, Dr. Wilson has been a U.S. Representative, New Mexico cabinet secretary, university president, entrepreneur, and government national security expert. She served as an officer in the U.S. Air Force from 1982-89, after graduating from the U.S. Air Force Academy. She also earned her master's and doctorate degrees as a Rhodes Scholar at Oxford University.

The Honorable Bill Peduto, Mayor of Pittsburgh, Pennsylvania

Bill Peduto took office as Pittsburgh's 60th Mayor in January 2014. Prior to assuming office, he worked for 19 years on Pittsburgh's City Council – seven years as a staffer and twelve years as a Member of Council. In the latter role, he wrote the comst comprehensive package of reform legislation in Pittsburgh's history. He strengthened the Ethics Code, created the city's first Campaing Finance Limits, established Lobbyist Disclosure and Lobbyist

Registration and ended No-Bid Contracts. As Mayor, he champions the protection and enhancement of Pittsburgh's new reputation – maintaining fiscal responsibility, establishing community-based development plans, embracing innovative solutions, and becoming a leader in green initiatives. A graduate of Pennsylvania State University, Mayor Peduto holds a master's degree in public policy and management from the University of Pittsburgh.

Lt Gen James C. "Jim" Slife, Vice Commander, U.S. Special Operations Command

Lt Gen Slife is a career helicopter pilot who has commanded U.S. Air Force Special Operations units from Squadron to Wing level; he has also held general officer positions at U.S. Central Command, United Nations Command, and U.S. Forces Korea. Prior to assuming his current duties, Lt Gen Slife was Chief of Staff of the U.S. Special Operations Command at MacDill Air Force Base, Florida.

Dr. Farnam Jahanian, President, Carnegie Mellon University

Farnam Jahanian became president of CMU in March 2018, after serving the university as provost and interim president. A nationally recognized computer scientist, entrepreneur, public servant, and education leader, Dr. Jahanian joined CMU as vice president for research in 2014. Previously, he led the National Science Foundation Directorate for Computer and Information Science and Engineering (CISE) from 2011 to 2014. From 2007 to 2011, he chaired the Computer Science and Engineering Department at the University of Michigan. He holds a Ph.D. in computer science from the University of Texas at Austin.

Mr. William J. Miller, Director of Strategy, Plans, and Policy, U.S. Special Operations Command

Upon graduation from the University of Florida, he received a commission as a 2nd Lieutenant in the cavalry. During his 26-year Army career, he led and commanded U.S. and allied soldiers from the platoon through the brigade level. He has extensive operational experience, including numerous deployments to Kosovo, Bosnia, Kuwait, Iraq, and Afghanistan.

Dr. Daveed Gartenstein-Ross, Senior Fellow, Foundation for the Defense of Democracies (FDD), and CEO, Valens Global

"A rising star in the counterterrorism community," Mr. Gartenstein-Ross's career has focused on understanding how terrorist groups and other violent non-state actors are changing the world and fashioning creative solutions to this growing challenge. Before joining FDD, he served as senior advisor to the Director of the U.S. Department of Homeland Security's Office for Community Partnerships, as a fellow with Google's think tank, Jigsaw, and as an adjunct professor at Georgetown University's Security Studies Program. Known for his rigorous scholarship, he is the author or volume editor of 23 books and monographs.

Wing Commander Keith Dear, RAF, United Kingdom Joint Forces Command

A Royal Air Force intelligence officer with 16 years' experience, WC Dear recently completed his Doctorate in Experimental Psychology from Oxford University while also serving as a Research Fellow at the university's Changing Character of War Programme. He is also co-executive producer and expert consultant to the Royal United Services Institute's Artificial Intelligence & the Future Programme. He is a founding member and co-lead of the Defence Entrepreneurs' Forum and founder and CEO of Airbridge Aviation, a not-for-profit start-up dedicated to delivering humanitarian aid by cargo drone.

Dr. Natasha E. Bajema, Director of the Program for Emerging Leaders, Center for the Study of Weapons of Mass Destruction, National Defense University

Dr. Bajema is a subject matter expert in nuclear nonproliferation, cooperative threat reduction and WMD terrorism who has served in the Office of the Secretary of Defense and in the Department of Energy. Prior to joining NDU, she worked at New York University's Center on International Cooperation and at the United Nations. Dr. Bajema is the co-editor of two books on WMD and terrorism.

Dr. Michael C. Horowitz, Professor of Political Science and Associate Director, Perry World House, University of Pennsylvania

Co-author of Why Leaders Fight and author of the award-winning, The Diffusion of Military Power: Causes and Consequences for International Politics, Professor Horowitz's research interests include technology and global politics, military innovation, the role of leaders in international politics, and forecasting. Previously, he worked for the Office of the Undersecretary of Defense for Policy in the Department of Defense. He is the International Studies Association's 2017 Karl Deutsch Award winner for that year's most significant contribution to the study of international relations and peace research.

Dr. Christopher Paul, Senior Social Scientist and Professor, Pardee RAND Graduate School

Dr. Paul is a senior social scientist at the RAND Corporation and professor at the Pardee RAND Graduate School. He is also a member of the adjunct faculty in the Center for Economic Development in the Heinz College at Carnegie Mellon University. Prior to joining RAND full-time in July 2002, Paul worked as an adjunct at RAND for six years and on the statistics faculty at the University of California, Los Angeles (UCLA) in 2001–02. Paul has developed methodological competencies in comparative historical and case study approaches, evaluation research, various forms of quantitative analysis, and survey research that he has applied to asymmetric warfare, counterterrorism, information operations, and military strategy, among others. Paul received his Ph.D. in sociology from UCLA.

Dr. J. Michael McQuade, Vice President for Research, Carnegie Mellon University

Prior to assuming his current position, Dr. McQuade served as senior vice president for Science & Technology at United Technologies Corporation (UTC). He has also held senior positions with technology development and business oversight at 3M, Imation, and Eastman Kodak. He has served as a member of the President's Council of Advisors on Science and Technology, the Secretary of Energy Advisory Board, and is a member of the Defense Innovation Board. Dr. McQuade holds Ph.D., M.S., and B.S. degrees in physics from Carnegie Mellon University.

Dr. Greg Shannon, Chief Scientist for the CERT® Division, Carnegie Mellon University

As Chief Scientist for the CERT® Division of CMU's Software Engineering Institute, he is responsible for expanding cybersecurity research, advancing national and international research agendas, and promoting efficient cybersecurity. Dr. Shannon serves on the U.S. Air Force Scientific Advisory Board and has served in the Office of Science & Technology at the White House, where he led development of the 2016 Federal Cybersecurity Research and Development Strategic Plan. He earned his Ph.D. and M.S. in Computer Sciences at Purdue University.

Dr. Rita Singh, Associate Research Professor, Carnegie Mellon University

Dr. Singh is an Associate Research Professor at Carnegie Mellon University's Language Technologies Institute, and (by courtesy) at the Department of Electrical and Computer Engineering. She is an affiliate of the Institute for Strategic Analysis at CMU, and of the DHS Center of Excellence in Criminal Investigations and Network Analysis at George Mason University. At CMU she leads the Forensic Voice Analysis group. She also co-leads the Robust Speech Recognition group and the Machine Learning for Signal Processing groups at CMU. She is the co-lead designer of the CMU Sphinx-4 speech recognition system, which was one of the most popular ASR systems in the world over the past decade. Currently her research focuses on profiling humans from their voices.

Dr. Lujo Bauer, Associate Professor, Carnegie Mellon University

An Associate Professor of Electrical and Computer Engineering, and of Computer Science, Dr. Bauer is also Director of CMU's Cyber Autonomy Research Center at CyLab. Dr. Bauer's research examines many aspects of computer security and privacy, including developing high-assurance access-control systems, building systems in which usability and security co-exist, and designing practical tools for identifying software vulnerabilities. His recent work focuses on developing tools and guidance to help users stay safer online and on examining how advances in machine learning can (or might not) lead to a more secure future. He received his Ph.d. in Computer Science from Princeton University

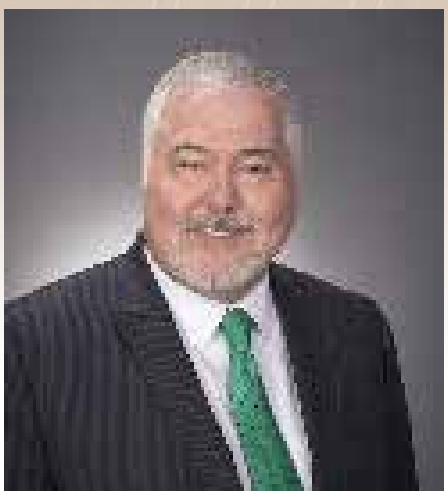
Dr. Marios Savvides, Research Professor, Carnegie Mellon University

Prof. Savvides is the Founder and Director of the Biometrics Center at Carnegie Mellon University and is a Research Professor at the Electrical & Computer Engineering Department and CMU CyLab. He is also one of the tapped researchers to form the Office of the Director of National Intelligence (ODNI) 1st Center of Academic Excellence in Science and Technology (CASIS). His research is mainly focused on developing algorithms for robust face and iris biometrics as well as pattern recognition, machine vision and computer image understanding for enhancing biometric systems performance. His achievements include leading the R&D in CMU's past participation at National Institute for Science & Technology's (NIST's) Open Face Recognition Grand Challenge 2005 (CMU ranked #1 in Academia and Industry at hardest experiment #4) and also in NIST's Iris Challenge Evaluation (CMU ranked #1 in Academia and #2 against iris vendors) - his group was the only one to attempt both challenges. He earned his Ph.D. in electrical and computer engineering at CMU.

Dr. Howie Choset, Professor of Robotics, Carnegie Mellon University

Dr. Choset is Kavcic-Moura Professor of Robotics at Carnegie Mellon University where he serves as the co-director of the Biorobotics Lab and as director of the Robotics Major. Choset's research group reduces complicated high-dimensional problems found in robotics to low-dimensional simpler ones for design, analysis, and planning. Motivated by applications in confined spaces, Choset has created a comprehensive program in modular, high DOF, and multi- robot systems, which has led to basic research in mechanism design, path planning, motion planning, and estimation. Choset's research program has made contributions to challenging and strategically significant problems in diverse areas such as surgery, manufacturing, infrastructure inspection, and search and rescue. In addition to publications, this work has led Choset, along with his students, to form several companies including Medrobotics, for surgical systems, Hebi Robotics, for modular robots, and Bito Robotics for autonomous guided vehicles. He received his Masters and Ph.D. from Caltech in 1991 and 1996.

Mr. Mark Nolan, Associate Vice President, Institutional Partnerships, Carnegie Mellon University



Mr. Nolan leads private sector engagement efforts for Carnegie Mellon University – managing the central corporate/business engagement and foundation relations teams. With 20 years of university-technology based economic development experience, Nolan also works with state and local economic development agencies and government officials to grow communities with great jobs. Prior to joining Carnegie Mellon in February 2016, Nolan was the director of IT and economic development at the University of Illinois at Urbana-Champaign (2006-2015), head of economic development and private sector engagement at the National Center for Supercomputing Applications (2001-2006), and held various program management positions within large corporations, government contractors, and university and VC-funded startups. He holds a B.A. in Speech Communications from West Virginia Wesleyan College and an M.S. LIS from the University of Illinois at Urbana-Champaign.

Mr. Michael Lisanti, CyLab Director of Partnerships, Carnegie Mellon University

Mr. Lisanti is the Director of Partnerships at CyLab, the Carnegie Mellon University Security and Privacy Institute. In this role, Michael leads the CyLab business engagement program, building relationships and developing strategies for corporate and government partners to collaborate with CMU faculty and student researchers. Prior to CMU, he led product management and business development teams at technology companies including Keylingo Translations, DynaVox Mayer-Johnson (now Tobii Dynavox), iDirect, Ericsson (formerly Marconi/FORE Systems), AT&T/NCR, EDS (now HP), and IBM. Michael earned a bachelor of science in Mechanical Engineering from Penn State University, and a master of science/MBA from Carnegie Mellon University's Tepper School of Business.

Mr. Max Brooks, Author, Scholar, and Teacher

Through his best-selling books, The Zombie Survival Guide, World War Z, and the Zombie Survival Guide, Recorded Attacks, Brooks challenges old ways of thinking and encourages mental agility and flexibility for problem solvers and leaders. Currently, a Fellow of West Point's Modern War Institute and an Atlantic Council Non-Resident Fellow, Mr. Brooks studies, writes about, and lectures on current conflicts, disaster preparedness, crisis management, and survival.

Dr. Nicolas Christin, Associate Research Professor, Schools of Computer Science and Engineering & Public Policy, Carnegie Mellon University

A leading expert in cybersecurity, Dr. Christin is also affiliated with CMU's Institute for Software Research and CyLab, the university-wide information security institute. Prior to joining CMU's faculty, Dr. Christin was a researcher at the School of Information at the University of California, Berkeley. He has numerous publications related to security analytics, online crime modeling, and the economics and human aspects of computer security.

Ms. Elsa B. Kania, Adjunct Senior Fellow, Technology and National Security Program, Center for a New American Security (CNAS)

Ms. Kania's research focuses on Chinese military innovation in emerging technologies in support of the Artificial Intelligence and Global Security Initiative at CNAS, where she also is a member of the research team for the new Task Force on Artificial Intelligence and National Security. Her analytic interests include Chinese military modernization, information warfare, and defense science and technology. She is an independent analyst, consultant, and co-founder of the China Cyber and Intelligence Studies Institute. A PhD student in Harvard University's Department of Government, her undergraduate thesis on the evolution of the PLA's strategic thinking on information warfare was awarded the James Gordon Bennett Prize.

Dr. Lydia Kostopoulos, Consultant, European School of Management and Technology, Berlin

Dr. Kostopoulos (@Lkcyber) consults on the intersection of people, strategy, technology, education, and national security. A professor teaching national security at several universities, including the U.S. National Defense University and Joint Special Operations University, her professional experience spans three continents, several countries and multi-cultural environments. She speaks and writes on disruptive technology convergence, innovation, tech ethics, and national security and has addressed United Nations member states on the military effects panel at the Group of Governmental Experts (GGE) meeting on Lethal Autonomous Weapons Systems (LAWS). To raise awareness on AI and ethics she is working on a reflectional art series [#ArtAboutAI], and a game about emerging technology and ethics called Sapien2.0.

Mr. John Watts, Nonresident Senior Fellow, Atlantic Council Scowcroft Center for Strategy and Security

Mr. Watts has spent more than a dozen years working across military, government, and industry, focused predominantly on the nature of future warfare and implications of complex emerging security risks. As part of the Scowcroft Center for Strategy and Security he is focused on Middle East and Indo-Pacific security issues. He has co-led wargames on Islamic State and researched the role Australia can play in Gulf security. Previously, as a senior consultant with Noetic Corporation, he advised international, military, federal, and local government agencies. Prior to moving to the United States, he was a Staff Officer at the Australian Department of Defence, working in a variety of strategic planning, implementation, evaluation, and management roles.

Mr. August Cole, Non-Resident Senior Fellow, Brent Scowcroft Center on International Security and Director of the Art of Future War Project, Atlantic Council

The co-author (with P.W. Singer) of the novel, Ghost Fleet, August Cole's fiction explores themes at the core of U.S. foreign and national security policy in the 21st century, including the privatization of military and intelligence operations in the Pacific. Previously, Mr. Cole was the Wall Street Journal's defense correspondent in Washington, DC and the editor and reporter for MarketWatch.com, a pioneering financial news website, where he covered defense issues.

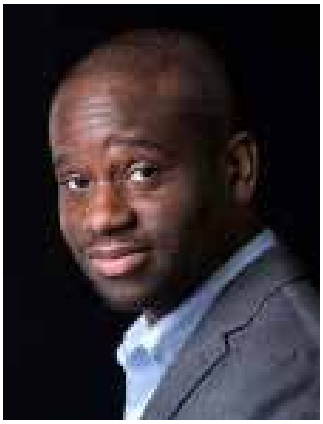
Dr. David Danks, L.L. Thurstone Professor of Philosophy and Psychology and Head of the Department of Philosophy, Carnegie Mellon University

Dr. Danks' research interests are principally at the intersection of philosophy, cognitive science, and machine learning, as he integrates ideas, methods, and frameworks from each to advance our understanding of complex, cross-disciplinary problems. Most recently, he has been examining ethical, psychological, and policy issues arising around the introduction of autonomous technologies, including in the defense, transportation, healthcare, and privacy domains.

Ms. Jacinta Carroll, Director, National Security Policy, National Security College of Australian National University

Before joining the National Security College, Dr. Carroll was the inaugural Head of the Australian Strategic Policy Institute's (ASPI) Counter Terrorism Policy Centre. Previously, she held senior executive appointments in the Australian government, including the Defence and Attorney-General's Departments. During her career, she has worked on wide variety of national security issues and has published a number of books and reports on such topics.

Dr. Osonde Osoba, Professor, Pardee RAND Graduate School



Dr. Osoba is an information scientist at the RAND Corporation and a core professor at the Pardee RAND Graduate School. He has a background in the design and optimization of machine learning algorithms. He has applied his machine learning expertise to diverse policy areas such as health, defense, and technology policy. His more recent focus has been on data privacy and fairness in artificial intelligence and algorithmic systems more generally. Prior to joining RAND, he was a researcher at the University of Southern California (USC). Dr. Osoba received his Ph.D. in electrical engineering from USC and his B.S. in electrical and computer engineering from the University of Rochester.

LtCol Ilse Verdiesen, Policy Advisor, Innovation Centre Front/Defence Staff Armed Forces, Kingdom of The Netherlands Armed Forces

LtCol Verdiesen currently provides the Dutch military with advice on the ethics associated with adapting new technologies to military applications. Her PhD research at Delft University of Technology focuses on the design of human oversight of autonomous weapons, particularly the establishment of appropriate control mechanisms that provide meaningful human control in military decision-making processes. Her previous research at the media lab of MIT examined moral values related to autonomous weapons. Previously, she served on military deployments to Bosnia and Afghanistan.

Headquarters United States Special Operations Command (USSOCOM) was activated in April 1987 to provide command, control and training for all Special Operations Forces (SOF) in the United States.

USSOCOM is located at MacDill Air Force Base, FL. Its components include the U.S. Army Special Operations Command (USASOC), Fort Bragg, NC; the Air Force Special Operations Command (AFSOC), Hurlburt Field, FL; the Naval Special Warfare Command, (NSWC), Coronado, CA, and the Joint Special Operations Command (JSOC), Fort Bragg, NC.

SOF Truths

- Humans are more important than hardware
- Quality is better than quantity
- SOF cannot be mass produced
- Competent SOF cannot be created after emergencies occur
- Most Special Operations require non-SOF support

Counterterrorism Fellowship Program

The Counterterrorism Fellowship Program (CTFP) is a United States Department of Defense program specifically designed to strengthen the capabilities of friendly countries to fight terrorism, as well as construct and strengthen the global network of experts and professionals who are dedicated to this fight.

USSOCOM appreciates the support of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict for the globally-recognized Sovereign Challenge Program.

Editors:
Larry Cook
Greg Hicks

Acknowledgements

HQ U.S. Special Operations Command and its Sovereign Challenge program gratefully acknowledge the contributions of the Office of Mayor William Peduto, Carnegie Mellon University, the Senator John Heinz History Center, and the Kimpton Hotel Monaco to this conference. Their partnership in this event was essential to its success.

Carnegie Mellon University
CyLab
Security and Privacy Institute

Carnegie Mellon University
Institute for Strategic Analysis

KIMPTON HOTEL
MONACO
PITTSBURGH

SENATOR JOHN HEINZ
HISTORY CENTER
IN ASSOCIATION WITH THE SMITHSONIAN INSTITUTION