2018 International Concept Development & Experimentation Conference Synopsis

Confronting the Challenge of a Disrupted Security Environment
Washington, D.C., United States
30 October to 1 November 2018

Conference Speakers and Senior Attendees (l-r): CAN BGen Derek Basinger, ROU BG Dragos Iacob, DNK BG Per Knudsen, USA MG William Hickman, ALB BG Tonin Marku, GBR VAdm Paul Bennett, USA Dr. Andrew Moore, USA RDML Andrew Loiselle, GBR MG Gerald Mitchell, DEU Dr. Ulrike Franke, AUS ACDRE Richard Lennon, USA Dr. David Kilcullen, MAR COL-MAJ Fouad Moumen, AUS AVM Alan Clements, GBR BRIG Ewen Murchison.

Contents

Introduction

The Joint Staff hosted the eighteenth annual International Concept Development & Experimentation (ICD&E) Conference from 30 October to 1 November 2018 in Washington, D.C. Headquarters Supreme Allied Command Transformation (HQ SACT), Deputy Chief of Staff Strategic Plans and Policy, and United States Joint Staff (JS), Directorate for Joint Force Development (J-7) cosponsored the event. The theme was "CD&E: Confronting the Challenge of a Disrupted Security Environment." This conference provided an opportunity for international and Alliance CD&E practitioners to meet face-to-face, work together in workshop venues, and collect outputs for current programmes of work and products. There were 232 conference delegates, from 35 nations, including representatives from the North Atlantic Treaty Organization (NATO), NATO Partner Nations, the European Union, and various industry representatives.

The conference is of great value to the Alliance and partner nations providing a unique opportunity for the international community to discuss the most current issues relating to CD&E in the process of capability development. The discussions and interactions established reinforce the relationships between HQ SACT, Joint Staff J-7, attendees and those in the community of interest for current and future collaborative work.

Keynote Address

General Paul Selva (USAF), Vice Chairman of the Joint Chiefs of Staff

General Paul Selva (USAF), Vice Chairman of the Joint Chiefs of Staff, welcomed the NATO Member and partner countries' delegates, highlighting military innovation, great power competition, and how

Gen Selva steps off the stage to answer NLD LTC Jos Hekking's question.

disruptive technology is changing warfare. On October 30, 1953, President Eisenhower approved the National Security Council Directive 162/2, laying out America's nuclear strategy. NATO could not outmatch the Soviet Union's conventional power; the ratio was around 10:1. We could not answer that threat without nuclear weapons. The Red Army then rebuilt itself around nuclear and conventional weapons.

Looking at our experience in Vietnam, we needed better precision and stealth. The 1970s brought about Air Land Battle and Global Positioning System (GPS) allowing for precision position, navigation, and timing—this asymmetry was in our favor.

The keyboard—it's the future! Most who saw it thought it was a fancy typewriter. It is an input/output device. Gen Selva related, as a lieutenant colonel, he was tasked as a group of eight to research what data meant to modern warfare; knowledge-based, distributive warfare. If disruptive technology is out there, what does it mean? Exquisite knowledge, how do you use it to act faster; what tools

and weapons do you need? Russia is looking at how to make humans better through man-machine teaming. The Chinese are looking at speed, speed, speed. In 1996 we were looking at asymmetry and the impact of warfare.

"Light warfare" is now (war at the speed of light) high speed computers, high speed weapons; it's all about speed. None were developed specifically for the military. We built nuclear, stealth, and GPS for military applications. We were told to share GPS. Cloud computing is for Big Data, 4G and 5G speeds, artificial intelligence (AI), and 3-dimensional manufacturing. Commercial industry outpaces Department of Defense spending in these areas 1000:1. We didn't invent it, we need to bring these people in. Not a unifying technology, but democratizing technology. The Cloud allows us to be different. My data is mine, your data is yours. How do we work as an alliance if we will not share data? Cloud competition allows us to have this dialogue. If we cannot share data, we can't collaborate, we have segmented data. If my picture of world battle space is different from an ally's, then it is a vulnerability. Counter AI can exploit this.

Gen Selva shared the fact that he does not have any social media accounts. His photo was posted to Facebook and through its Facial Recognition Photo Tagging, Gen Selva was tagged as his brother. He used this anecdote to illustrate when AI is used, the results may not be correct; we need to have confidence that the calculated results are accurate. Understating what AI is and isn't is very important to our efforts: Why it works, or doesn't; what to do to break it down, to make it work. We need an advanced concept, the best tools in the hands of our Soldiers, Sailors, Airmen and Marines. Are we asking the right questions? Is a keyboard just a fancy typewriter, or a window into the future? We need to think critically to break the cycle, with the best method for development via experimentation, not on the battlefield.

Welcome Remarks

Mr. Donald Morse (USA Civ), Chief, International Force Development Division JS J-7, made his 9th and final appearance as Master of Ceremonies. The two co-sponsors, Major General William Hickman (USA A), Deputy Chief of Staff, Strategic Plans and Policy, HQ SACT and Rear Admiral Andrew Loiselle (USA N), Deputy Director Future Joint Force Development, JS J-7, set the stage for the next three days in their welcome remarks. It was noted that the conference allows us to design our force based on the future of our capabilities and concepts that we have developed here. The take-away challenge to the group was to be ready to interact, be part of the plan, participate, and share experiences. This will allow focus on the task at hand to assist in definition, complexity, structure, people development, and the influence of concepts.

RDML Loiselle welcomes the delegates.

Guest Speakers

Mr. Paul Scharre
Senior Fellow and Director, Technology and National Security Program and
Center for a New American Security
Topic: Ethics

Drones are simple robots. Mr. Scharre asked, "Are we comfortable delegating life and death decisions to machines?" There are legal and moral questions. We have boat drones, but who decides to fire the machine guns? We're not there yet. If you lose communications, what happens? What if it is under attack; can it attack? What about new pop-up targets? A human chooses the target, but a pop-up threat changes the flight pattern. Currently we have human-supervised defense weapons to counter fast targets (e.g., counter missile, counter mortars).

The Israeli Harpy drone is more like an autonomous weapon since it is a loitering missile, as compared to the quick-strike High-speed Anti-Radiation Missile. Loitering weapons are feasible, but until now we have not trusted them and could not recover them. Questions raised are, will it be a waste of an asset, what about white shipping, and what is the usability of the weapon? Many new systems are reusable. What about swarms? There was a test battle of drones, acting in swarms, they launched got to altitude and fought each other. Each team had a computer, they both hit the enter button and after that, the drones flew autonomously.

Mr. Scharre highlights ethics and the use of autonomous drones.

There is mayhem to fight hacking in computer security. What is legal, what is moral, what is ethical? Legally, humans are not required for war. The Law of Warfare is about effects on the battlefield. Robots are not legal agents and humans are responsible. Are these immoral? What is legal and what is right? Decisions are made at machine speed.

The United Nations Convention on Certain Conventional Weapons seeks to prohibit or restrict the use of certain conventional weapons which are considered excessively injurious or whose effects are indiscriminate.

Paul Scharre's new book, *Army of None: Autonomous Weapons and the Future of War,* is available on Amazon: *https://www.amazon.com/Army-None-Autonomous-Weapons-Future/dp/0393608980.*

Dr. Ulrike Franke (DEU Civ)
Policy Fellow, European Council on Foreign Relations
Topic: Autonomous Weapons

Autonomous weapons might cause a revolution in military affairs. Citing Andrew Marshall of the US Department of Defense's Office of Net Assessment, Dr. Franke defined a revolution in military affairs as a "major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts, fundamentally alters the character and conduct of military operations."

A future example of an Autonomous Weapons Systems (AWS), is commonly referred as a "killer robot." Others, such as autonomous unmanned aerial vehicles (UAVs) and surface-to-air missile defense systems, are a reality today. The types of changes that arise from this new evolution of warfare include organisational and operational (military level), doctrinal/strategic (political level), and societal.

Dr. Franke discussing autonomous weapons.

Examples causing operational changes are: weapons faster than humans, advanced stealth, more precise munitions (causing fewer casualties), new military operations (such as swarming), so-called "weird" mistakes and biases (caused from AI systems learning wrongly from data), flash crashes (escalatory chain reactions), and automated cyberwars.

Organisational changes include shifts in the balance of power between those who build weapons and those who use them (i.e., between private companies and state governments). Doctrinal/strategic changes include new military doctrine (e.g., kill webs), non-state groups gaining access to autonomous weapons (ISIS already has UAVs purchased on the Internet), and the problem of attributability (it will become more difficult to figure out who's responsible).

Societal changes such as fewer soldiers in harm's way and ethical changes could be the most revolutionary element of AWS if and when humankind delegates to machines real life and death decisions, according to Dr. Franke. There are elements that can be considered revolutionary; if we allow machines to make life and death decisions, we will have a revolution in change.

Dr. Andrew Moore (USA Civ)
Dean, School of Computer Science, Carnegie Mellon University
Topic: Artificial Intelligence

The development of artificial intelligence systems has its origins in the late 1950s and early 1960s. At that time, the model for Artificial Intelligence (AI) systems was Perceive-Decide-Act. This development culminated in the 1996 defeat of world chess champion Garry Kasparov by an AI program. However, development stalled after this, mainly because the original model was flawed. The new AI model (or the "AI Stack"), Perceive-Learn-Decide-Act, incorporates machine learning concepts and enables AI systems to cover a broad range of capabilities and potential future uses. Machine learning allows AI systems to use aggregated data over time to better decide how to act.

Dr. Moore talks about the AI Stack.

Computer vision is now routine and has displaced other sensory modes and allowed autonomous decisions through machine learning (e.g., neural network for image detection). The next breakthrough is low-cost, low-power cameras, similar to the breakthrough in voice characterization/profiling. Layer on top of machine leaning is "Search, Plan, and Prove." In addition, future AI development must make use of concepts such as game theory in order to better decide and act in non-rule-based situations, in which some actors have information that other actors do not have; poker not chess. Improvements of machine learning on software development based on past data means, by the 2020s we will get to self-improving software (self-monitoring, fixing and development of software). The democratization of machine learning will allow non-experts to develop such systems in weeks—including by people with evil intent.

Town Hall Panel

Moderator: Dr. David Kilcullen (USA Civ), Author and Futurist
Panelists:
  o *Vice Admiral Paul Bennett CB OBE (GBR N), Chief of Staff Headquarters Supreme Allied Command Transformation*
  o *Brigadier-General Derek Basinger (CAN A), Director General Capability and Structure Integration (DGCSI)*
  o *Dr. Franke*
  o *Dr. Moore*

The Town Hall Panel discussed the challenges posed by the revolution in military affairs underway in the fields of autonomy and AI. The programme allowed attendees to engage the panelists on topics raised by the guest speakers and senior military officers. Discussions included: requirement for "human-in-the-loop" during lethal and non-lethal decision-making; the legal, ethical, and moral considerations involving autonomous weapons; and advancing "pieces" of solutions rather than trying to solve the whole issue at once. There was a consensus that all stakeholders—military,

technologists, ethicists, policy makers, lawyers, and philosophers—should contribute to the debate on design and use of autonomous systems.

The panel opened with the question, "What do we actually mean by human-in-the-loop when it comes to autonomous weapons systems?" The discussion ranged over how to define meaningful human control, the ethical, moral, and legal ramifications of lethal and non-lethal decision-making, and where in the chain and to what degree in that decision-making should be delegated to the machine.

Dr. Kilcullen addresses the panel consisting of (l-r) VADM Bennett, Dr. Moore, BGen Basinger, and Dr. Franke.

It was noted that from a technological standpoint, AI is not yet at the point that it can replace a human being in high-level and complex cognitive tasks. While current AI can function at the insect level fairly well and is better than a human in tasks such as assessing large amounts of structured data; its ability to operate at the human decision-making level is just not there.

Another question from the floor, that was debated, was the potential effects of AI and autonomous systems in terms of organizational concepts as the technology becomes more advanced and interwoven into warfighting. The term "strategic corporal" on the battlefield is familiar as shorthand for the devolution of command and control from the strategic and operational levels towards the tactical edge. In many ways, the current military force is structured on an industrial age model; what we call enablers today will be the "enabled" tomorrow (cyber, info operations, etc.). As is already being seen in the cyber realm, with more AI increasingly assuming traditional soldier roles, the soldier will need to change, becoming more technologically adept. The chain of command will need to evolve at the same time to reflect the redistribution of information flows and decision-making.

In summary, there was a consensus of the importance of an interdisciplinary approach to be involved in the ongoing debate on design and use of autonomous systems as the technology advances and new potential use cases come forward. Part of this process is educating non-technologists on AI in general. Additionally, it was emphasized that despite human failures in the use of technology in history, we can't ignore ethically considered warfare. While it may feel like a constraint at times, it is absolutely necessary.

Plenary Address

Mr. August Cole (USA Civ)
Author, Futurist and Senior Fellow, Atlantic Council's Art of Future Warfare Project

Mr. Cole discussed the value of using works of fiction to address potential challenges in the future. Identifying blind spots or viewing situations through a different lens are all benefits of studying fiction. It can be useful in helping us look at the world in a different way and understanding the globality of conflict, such as the role of hackers and Silicon Valley. We can gain insights to what is the impact of disruptive technology, what is going on and what is missing. He outlined his thesis through his acronym, FICINT (Foresight, Individuals, Community, Inspiration, Nuance, and Technology). Foresight can be used to answer, does this work?

Mr. Cole challenges delegates to use fiction in future thinking and concept development.

- o Individuals provide perspective and situational awareness to come up with solutions.
- o Community to provide the power of the narrative.
- o Inspiration, the ability to conquer the future, the tools and people we need to make it a reality.
- o Nuance on how we encounter AI to determine what is true and what is not.
- o Technology for first rate intelligence concerning two opposing points of view while maintaining cognitive capability.

As he walked the different terms, he used fictional movies and books to illustrate his points.

Daily SITREP: Experimentation in Trident Juncture Exercise 2018

Delegates received a daily SITREP on experimentation being conducted in NATO's Exercise TRIDENT JUNCTURE 18 (TRJE18) which was executing concurrently. TRJE18 provided an environment for the testing, refinement, and validation of new capabilities and concepts. Experiments from NATO entities, coalitions and Nations were integrated into TRJE18. Through risk management and extensive planning experimentation objectives were pursued while avoiding detriment to other exercise objectives. NATO ACT Operational Experimentation (OPEX) coordinated 21 experiments in the Exercise, ranging from discovery through to validation. Please visit www.act.nato.int/tj18 and access factsheets on each TRJE18 experiment. Find out more about OPEX here: https://www.act.nato.int/opex-fact-sheet.

Mr. David Beckwith providing the daily TRJE18 SITREP

NATO ACT PAO provides a glimpse of experimentation in TRJE18 exercises.

Endnote Address

Admiral Manfred Nielson (DEU N)
Deputy Supreme Allied Commander Transformation

Adm Nielson provides the Endnote address.

Admiral Nielson highlighted how Exercise Trident Juncture truly hit the mark. The conference theme "Confronting the Challenge of a Disrupted Security Environment" is not only extremely interesting but also extremely important. If we don't do CD&E right, we will put our credibility at risk which will maybe lead us to remain a dominant but probably irrelevant alliance in the future. We will need validated concepts, and this has to be done faster than ever before.

Highlighting his feelings on failures in experimentation and innovation, Adm Nielson reminded the delegates of his speech at the 2016 CD&E conference in Sofia, Bulgaria, where he stated, "Experimentation and innovation sometimes ends in a failure. Is this a problem? No, this is the risk we have to take!" Are NATO, the allies and the partners ready to take such innovation risks? We need to convince political leaders to invest in an unknown future, even if we do not know if something will happen or not. It means investing in fast concept development, consequently validation, make mistakes, re-try, stop or continue. During his opening remarks, our co-sponsor, Rear Admiral Andrew Loiselle described that the US National Military Strategy is seeking a balanced "boxer stance," ready for both, current and unexpected challenges, and able to adapt to future threats. That's a great advice for all of us! The numerous discussions explored a number of challenges, in particular the ethical question of decisions with lethal consequences in an environment enabled by AI and autonomy—the human-in-the-loop. The legal and ethical issues raised by the Lethal Autonomous Weapon System, have already been addressed during the Munich Security Conference in February 2018. The challenge will be not to limit the discussion. Our NATO alliance consists of like-minded nations committed to the principles of individual liberty, democracy, human rights, and the rule of law. A decision needs to be made in order to be able to use such technologies; our adversaries will not hesitate to use them against us.

Through the conference workshops, you have explored: 1) How new technologies in Autonomous Systems, Artificial Intelligence, and Data Analytics have the potential to provide capabilities that will radically change the operational environment—especially in the areas of Autonomous Vehicles, Cyber, C2 and Urban Operations; 2) Military implications of disruptive technologies such as directed energy systems, hypersonic weapons and railguns can complicate adversary decisions; 3) How networks (sensors, weapon platforms, C2) evolve in conflict; 4) Creative ways to look at problems (thinking wrong) and alternative narratives to escape the same as last time approach. General Paul Selva reminded you that fighting together as an alliance, enabled by the tools of AI, and Big Data, means we share our data to achieve a shared understanding of the battlespace. We will continuously work on our Disruptive Technology Roadmap, based on findings and outcomes of this conference, the NATO Industry Forum, and the Chief of Transformation Conference. We will set our Focus on the areas of Artificial Intelligence, Autonomy and Big Data Science.

2nd Annual CD&E Exchange

For the second year in a row the ICD&E conference held the CD&E Exchange that provided an informal environment for conference delegates to network, exchange ideas, and interact with CD&E projects drawn from across the globe. By adopting a mini-expo format, attendees learned about each NATO Centres of Excellence, the Multinational Capability Development Campaign and other important programs of work within Concept Development and Experimentation.

NATO ACT Deputy Chief of Staff Strategic Plans & Policy Major General Hickman and Mr. Mehmet Kinaci share perspectives on strategy.

USA CDR Alex Wright participates in the CD&E Exchange Protection of Civilians Virtual Reality demonstration.

Conference delegates networking at the CD&E Exchange.

Conference Workshops

Workshop 1 - From Disruptive Technologies to Capabilities: New Concepts for Autonomy, Artificial Intelligence and Data Analytics

Led by Colonel Robert Kraus (USA F) and Lieutenant Colonel Timothy Povich (USA A) NATO Science and Technology Organisation (STO); supported by Commander Joe Strassberger (USA N), HQ SACT Autonomy Programme

Background

New technologies in Autonomous Systems, Artificial Intelligence (AI), and Data Analytics have the potential to provide capabilities that will radically change the conduct of warfare—especially in the areas of Cyber, C2, and Urban Operations. To leverage these capabilities, commanders and planners must grasp the potential opportunities and risks associated with the application of these new technologies. The workshop explored the current status of technologies, potential capabilities, and opportunities for concept development.

COL Kraus kicks off the workshop.

The workshop consisted of three sessions focusing on different technologies. Each session included introductory briefs and expert presentations followed by small-group breakouts to discuss the technologies and their impacts on future operations. In the first session on autonomous systems, Dr. Jason Stack from the USA Office of Naval Research provided a thematic overview of the autonomy area. Mr. Arthur Holland Michel from the Center for the Study of the Drone at Bard College discussed counter unmanned aerial system (C-UAS) technology.

In the second session focused on AI and Data analytics for military decision making and cyber defense, Dr. Sanjeev Mohindra, Assistant Group Leader, Intelligence and Decision Technologies Group at the Massachusetts Institute for Technology (MIT) Lincoln Laboratory, provided a brief on the role of AI in the data-to-decision cycle. Mr. David Martinez, Associate Division Head Cyber Security and Information Sciences Division at MIT Lincoln Laboratory, followed with a presentation on the use of autonomy in cyber operations. The third session focused on Autonomous technologies in support of Urban Operations. Captain Tim Hulme from the Development, Concepts and Doctrine Centre, UK gave a broader perspective on how disruptive technologies will change operations and their impacts in urban environments. Dr. Robert Davis, Chief Scientist, Geospatial Research and Engineering, US Army Engineer Research and Development Center focused on specific technologies that provide Soldiers with better situational awareness in urban environments.

Key Outcomes or Future Implications

The immediate impact of the workshop was that participants gained a stronger understanding of these potentially disruptive technologies and the capabilities they could provide. The second impact was that participants walked away with a better knowledge of the ongoing efforts in all of these areas across NATO which will help synchronize advancement in these areas. There were a number of key ideas that came out of the sessions.

Session 1: Autonomous Systems and C-UAS

*MG Hickman interacts with one of the four breakout groups.*

CDR Joe Strassberger provided an overview of the HQ SACT Autonomy Programme to start the session, highlighting the current efforts underway within ACT. Dr. Stack then highlighted 17 focus areas identified within the STO in which work is still needed to implement autonomous capabilities. One of his focal points was the human-machine interface and he addressed the question of where to draw the line between human and machine and emphasized that trust must be developed between human and machine. Another focus was the development of systems such as swarms.

One of the biggest risks we face is not moving quickly enough to outpace our adversaries. While significant technical hurdles exist, there are substantial legal, ethical, and policy issues to be worked out before we can leverage the capabilities provided by autonomous systems. In response to a question about how well nations share data, Dr. Stack emphasized that there is a willingness to share, but the issue is more about what can be shared and how to share it. Hurdles to solving this issue are often technical rather than policy. Collaboration can be done at the NATO Secret level but some countries still work in a close-hold environment. One solution is to continue to conduct demonstrations of the systems at larger exercises, getting them in front of people who need them.

Mr. Holland Michel's brief focused on the issues inherent in the rapid growth of C-UAS. Most nations are still in the experimentation phase of C-UAS development and there are many different approaches to the technology, but none are 100% effective. As such, a system-of-systems approach that incorporates various different C-UAS technologies in one system is generally the most popular current solution. Near-future advances in small UAS technology that make the aircraft harder to target, including increased autonomy, miniaturization, and enhanced connectivity will further complicate the C-UAS problem-set.

Session 2: Artificial Intelligence and Data Analytics in Support of Decision Making and Cyber Operations

Dr. Mohindra gave a brief overview of the state of AI dominance in the world, and how it has become a race to create the most effective AI systems. The underlying theme of the brief was the "canonical AI framework for data to decisions" (see figure). He explained the differences between the commercial and national security uses for AI. While there are potentially many uses for commercial systems in national security roles, there are gaps that commercial systems do not or cannot fill. Understanding these gaps will be important for the development of national security AI systems.
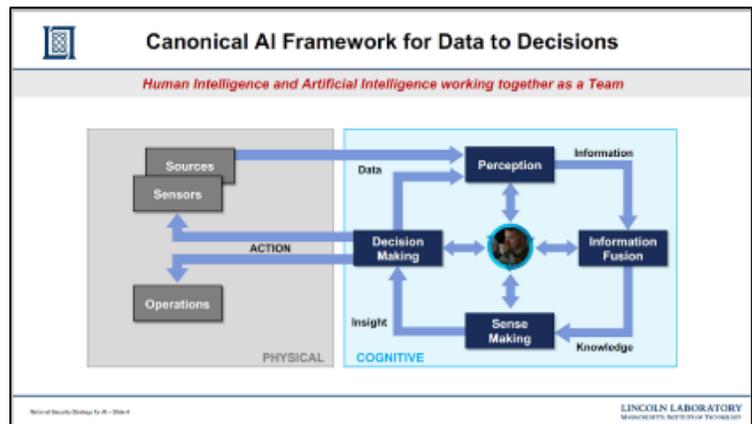
Mr. Martinez provided information on the application of "narrow AI," artificial intelligence developed for specific problems, in cyber security. Using machine learning, AI can be used to prioritize the

protection of vulnerabilities in a network and can also be used to identify counterfeit hardware in a system. By effectively teaming human analysts with machines, AI technologies can reduce human workload and expedite the decision-making process. One of the major challenges is advancing capabilities while rapidly inserting them into operational use.   The solution to this involves establishing a culture of innovation, rapid experimentation and deployment and focusing on capabilities across all elements of the AI canonical architecture.

Session 3: Autonomy in Support of Urban Operations

LtCol Jozsef Bodnar started the session by providing an update on HQ SACT's Capstone Concept "Joint Military Operations in an Urban Environment" and highlighted new capabilities needed in future urban environments.   Captain Hulme presented a wider perspective on the use of Autonomy in urban environments. His main thrust was that users of autonomous systems will not be "technologists" or experts but, rather, the average individual in the field. Therefore, we need to get better at moving the technology out of the lab and into the field. Autonomous systems and AI are also democratizing the battlefield, giving low-budget actors access to high-tech warfare in an increasingly uncertain battlespace. In sum, we must take a comprehensive approach to the implementation of autonomous and AI systems that includes the human aspect as well as the purely technological aspect.

Dr. Davis focused on autonomy supporting the soldier. Operations in urban environments will likely be conducted by small teams of technologically augmented soldiers. Autonomous technologies and AI should be able to provide them with 'leap-ahead' situational awareness, reinforced with appropriate training. The military will have to make use of already-available technologies to integrate with dismounted operators in the same way that the technologies have already been implemented in commercial vehicles. The emerging spectrum of AI-enabled context-aware computer systems and recommenders are promising tools for adoption for small units operating in urban environments.

Way Ahead and Recommendations

There were several key themes that arose from the discussion groups.

- o There is a need for more robust CD&E to bring in and experiment with new autonomous technologies as they develop to speed up the process of leveraging these continuously evolving technologies

- o "Narrow AI" is currently being used in many commercial applications and could be ready for defense applications such as filtering, extracting and identifying key information from large amounts of data for applications in intelligence collection and fusion.

- o There is a general lack of knowledge of AI technologies; more testing and experimentation of the technologies for defense applications should be done to assess their capabilities and build trust in the technology, partnering with academy and industry could help facilitate this.

- o Sufficient, common data is vital to implementing AI technologies. Data sharing and management in complex adversary environments and across national boundaries will be the major challenge to turning AI into a capability.

This workshop continued the exploration that is ongoing within the Nations as well as in NATO ACT and STO in these technology areas. The workshop outputs will be shared with ongoing NATO programs and will help inform HQ SACT Autonomy and Urban Operations efforts. The outputs will also contribute to the development of the STO research themes of Autonomy, AI and Big Data for Military Decision Making and Operations in Complex Urban Environments, which are focused on developing more collaborative research in these areas, through integration into the STO Plans and Programs Workshop in February 2019.

Workshop 2 - Concept Development Management in NATO: "Future Collaboration"

Led by Commander Stefan Meyer (DEU N), Concept Development Branch Staff Officer, HQ SACT; supported by Lieutenant Colonel Uwe Willert (DEU F), Concept Development Branch Staff Officer, HQ SACT

CD&E defines a concept as a solution-oriented transformational idea that addresses a capability shortfall or gap. To facilitate the development and ultimate execution of CD&E concepts, a newly revamped CD&E Handbook was developed and is located in CDE365, through TRANSNET, https://portal.transnet.act.nato.int. The newest iteration enhanced processes within CD&E while highlighting the need to improve the management process.

Cdr Meyer outlines the New CD&E Handbook.

The Development Management in NATO: "Future Collaboration" workshop brought together delegates from Centres of Excellence (COEs), Joint Forces Training Centres (JFTCs), Nations, and industry to gain diverse perspective on CD&E Collaboration. Changes briefed included the establishment of the Campaign Steering Board (CSB) as a decision making body for direction and guidance, recognition that a CD&E Working Group can be an effective tool but needs reorganization to include COEs as standard members (vice optional), and the importance of introducing project management throughout the process. Prioritizing concepts throughout NATO and partners is currently ambiguous and will require dedicated management and engagement to optimize.

Another area of attention is gaining understanding on the focus of the 25 COEs; semiannual reports are delivered but lack standardization in approach of content and format. Workshop participants were split into three syndicates, each addressing the same topic of how best to collaborate CD&E between COEs, Nations, and other entities without duplicating efforts.

The first syndicate identified three Lines of Effort (LOE) in order to resolve the CD&E management problem. These LOEs are improved communications, enhanced processes, and assurance of relevance in developed products. In the first effort, communication paths and patterns must be clear and transparent for all POCs and stakeholders, with their roles and responsibilities plainly defined.

For the second effort, a System Approach to Training (SAT) was identified as a model to consider, with increased COE involvement in the process. The final effort is best exemplified when a bottom-up idea obtains support from leadership and becomes a top-down request with the commensurate support. The syndicate concluded that CD&E has the tools necessary to collaborate; but, with surmountable implementation gaps, must not reinvent the wheel.

The second syndicate identified three main themes of focus: tools, leadership/direction, and Information Knowledge Management (IKM). The group's main need identification was for a shared space for the COEs to exchange information on concept development including an individual space for each centre. The group concluded that there were many tools available but most of them needed updating. The final recommendations were to reinvigorate conferences and workshops, improve and enhance IKM, TRANSNET, and the CDE365 webpage to better support the exchange of ideas. Additionally refine reference terms and enhance direction/guidance for the CD&E management structure for all stakeholders.

The third syndicate identified a lack of distributed information during the intermediate and final stages of the CD&E process. Using the "ends, ways and means" approach, the group determined that a central repository for all concepts needed to be established. ACT already has a Concept Development and Experimentation Management System (CDEMS) that houses experimentation information; but, at present, it is not set up to include concept development. The group determined that a viable solution is available by building on the existing database with the appropriate resources and high level support. Finally, advertising to all partners the efficiency and benefits of the collaboration tool will support its success.

A representative from each syndicate briefed the group's recommendations to DACT and DCOS SPP on future CD&E work that would improve direction and guidance to COEs, and collaboration between nations, ACT and NATO. Increasing awareness and training for the decision making bodies is key to process improvement within CD&E. The review and adaptation of MCM 0056 defines the major roles and responsibilities of those involved in CD&E process. The reorganization of the CD&E Working Group and the revitalization of the terms of reference will ensure the COEs are included in the discussion of these change. Identification of the Campaign Steering Board (CSB) as the decision making body for direction and guidance assisting internal ACT processes on enhancement of the decision making of CD&E will also be vital. Lastly, more focus on the implementation of the CDE365 webpage and the securing of a collaboration platform for CD&E use in future updates and maintenance is recommended to continue firsthand awareness and transparency across the community.

MG Hickman and Adm Nielson receive feedback from the Concept Development Management in NATO: "Future Collaboration" Workshop.

Workshop 3 - Understanding the Military Implications of Disruptive Technologies

Co-led by Mr. Jeff Becker (USA Civ), JS J7 and Mr. Neil Chuka (CAN Civ), DGCSI

This workshop explored the implications of several emerging technologies on how military forces are structured and operated. The participants examined how these technologies may alter warfare, and the resultant challenges posed for allied militaries as well as ways to leverage any advantages. The workshop looked to mature and refine these implications, including steps required in the near-term to prepare for these changes.

Workshop leaders stated at the outset that emphasis would be on the implications for warfighting, instead of grand strategy and broad concepts. After an initial brief plenary session, members of the workshop were divided into two separate working groups—a US-led group on battle network competitions, and a Canadian-led group focused on maritime and naval issues.

Thread 1 (USA): Battle Networks

Topic 1: Battle Network Competitions
Mr. Bryan Clark (USA Civ), Center for Strategic and Budgetary Assessments (CSBA)

Mr. Clark gave a presentation on Battle Network (BN) competitions drawn from CSBA's 2015 study, What It Takes to Win: Succeeding in 21st Century Battle Network Competitions; copies of the study were provided to working group members. Mr. Clark defined a BN as a combination of target acquisition sensor, target localization sensors, command and control (C2) elements, weapons, weapon platforms, and the electronic communications linking them together. He noted that this combination includes all the elements of a force that contributes to a mission, the CONOPS they employ, and the metrics they establish; competition between BNs tends to accelerate and culminate, and then jump to a new mode.

To illustrate the idea of BN competitions, Mr. Clark walked through examples from World War II. First, he showed how the evolution of new technologies such as active sonar and submarine snorkels transformed anti-submarine warfare (ASW) during the Battle of the Atlantic in WWII. Metrics included Allied shipping losses, German U-Boat presence and losses, and the Allies' increasing attempts to suppress U-Boats. Technologists and tacticians worked together to counter newly introduced technology and tactics by the other side. A second illustration from WWII is the Royal Air Force bombing competitions using radar navigation and chaff to overcome targeting by German fighters. New tactics and countermeasures were rapidly developed by each side, often within weeks or even days. A third case study is the "Rolling Thunder" bombing campaign of the Vietnam War as US bombers had to overcome an enhanced threat from Vietnam's deployment of the SA-2 missile system. The United States introduced air defense suppression aircraft and missions, but as many as 50,000 strike sorties were lost due to virtual attrition imposed by the introduction of the SA-2.

During the follow-on question and answer (Q&A) discussion, workshop participants were asked to consider four key questions: 1) How might the emergence of these technologies impact the course of conflict and the conduct of war? 2) How might these capabilities render current systems or ways of conducting war obsolete? 3) In what specific ways might our nations—or adversaries—use this set of technologies to gain a military or strategic advantage? and 4) What force-development actions should be taken in the near term to mitigate vulnerabilities or capitalize on potential? Key themes raised during the Q&A included: how to reduce our dependence on large monolithic platforms like the F-35 toward more "decomposed" platforms such as the MQ-9 UAV; the role of new tactics,

techniques, and procedures (in complement to the technology); the difference between a war of national survival (e.g., WWII) and less urgent conflicts such as the Cold War and current conflicts; the concept of "transparent oceans" as a disruptive development; appropriate metrics for multi-domain operations; the difficulty of an integrated approach; competition involving responses in different, non-correlated areas (e.g., responding to conventional strikes with cyber-attacks); ethical norms in the West; challenges of deterrence in the age of AI; finding ways to identify the discontinuities like the commercial sector does (where and when a trend ends); and standardizing innovation across the Alliance.

Topic 2: Lasers, Hypersonics, and Railguns
Dr. Carl Rehberg (USA Civ), CSBA

For this presentation, drew from his new CSBA study, Air and Missile Defense at a Crossroads. He opened by citing the 2018 US National Defense Strategy's call for a "lethal, resilient, and rapidly adapting Joint Force." Dr. Rehberg asserted that we are in the era of "salvo competitions," describing the dynamic between opponents that each have the ability to strike and defend against strikes with precision. Both sides seek advantages by continually increasing the size and survivability of their strikes, and the capacity and lethality of their defenses.

Dr. Rehberg discussing lasers and Hyper Velocity Projectiles.

Dr. Rehberg started with an overview of Chinese and Russian maturing air and missile defenses, to include advanced surface-to-air missiles (SAMs), missile defense, and underground facilities. Although many observers are focused on ballistic missile threats, Dr. Rehberg highlighted the threat from cruise missiles, hypersonics, and Unmanned Aerial Vehicles (UAVs); for example, China is currently building 41,000 UAVs and has many more cruise missiles than ballistic missiles.

The next topic examined was Directed Energy (DE), which consists of both laser and High-Powered Microwave (HPM) weapons. Dr. Rehberg cited a recent unclassified US Congressional Research Service report on Navy-related DE weapons; of US services, the Navy is furthest along on DE weapons development. Although currently conceived as defensive weapons, DE can also be used in an offensive capacity. DE weapon advantages include their theoretically near-unlimited magazine depth, lower logistics footprint, and high technology readiness levels. Disadvantages include the requirement for robust power thermal management systems, need for higher power levels and dwell time, and challenges of integration readiness levels.

With regard to hypersonic weapons, advantages include their rapid response time, the significant increase in survivability (with no known defenses), and medium- to long-range employment. Disadvantages include their limitations to mostly soft and stationary targets, potentially problematic updating of navigation, and the difficulty of seeker solutions. Like DE weapons, hypersonics will have an impact on the conflict and conduct of war and potentially render current systems and ways of war obsolete.

Regarding railguns or Hyper Velocity Projectile (HPV) weapons, advantages include lower cost for medium range attack and defense, increased magazine depth for salvo competitions, and rapid and safe reloading due to the lack of explosives. HVPs are normally half the range of railguns. Disadvantages include their heavy weight, high power requirements, and limited mobility on the ground. Like DE and hypersonics, railguns and HPVs will have an impact on the conflict and conduct of war and potentially render obsolete current systems and ways of war. Dr. Rehberg closed with a listing of current CSBA publications on the subject.

During the Q&A discussion, participants were again asked to consider the same four questions as Topic 1. Key themes discussed were legacy systems; pushing new systems through the defense bureaucracy; and the problem of using fewer expensive high-tech weapons against more numerous low-cost weapons (i.e., at times, quantity has a quality of its own).

Thread 2 (Canada): Overcoming Future Naval Challenges Using Disruptive Technologies

As in the first syndicate, participants were asked to keep in mind the same four key questions while discussing and analyzing the topics: 1) How might the emergence of these technologies impact the course of conflict and the conduct of war? 2) How might these capabilities render current systems or ways of conducting war obsolete? 3) In what specific ways might our nations—or adversaries—use this set of technologies to gain a military or strategic advantage? and 4) What force-development actions should be taken in the near term to mitigate vulnerabilities or capitalize on potential?

Topic 1: Maritime Disruptive Technology Overview
Scott Savitz (CAN Civ), Senior Engineer, RAND Corporation

RAND identified 23 technology areas that the Navy and Marine Corps can use to overcome enduring naval challenges and that potential adversaries can use to exacerbate those challenges. The highest priority went to unmanned vehicles, autonomy, advanced electronic warfare, and tactical cyber. Other priorities were AI, big-data analytics, human-machine teaming, signature modification, advanced distributed sensors, and compact inexpensive satellites.

All of the following need consideration:

- *Next-generation IT capabilities which enhance analysis and decision making:* AI, big-data analytics, and autonomy
- *Collecting and disseminating information:* Advanced distributed sensors, novel modes of communication, and quantum information sciences.
- *Bridging the human-computer interface:* Human-machine learning, augmented reality
- *Platforms:* Unmanned vehicles, compact satellites, and interdomain connectors
- *Weapons:* hypersonic weapons, advanced undersea weapons, directed-energy weapons, advanced electronic warfare, and tactical cyberweapons
- *Material/energy enablers and manipulating matter:* advanced materials, additive manufacturing, signature modification and reducing energy dependencies

RAND examined disruptive technologies in the context of a theoretical fleet problem: a strategic competitor is trying to invade another nation in the vicinity of a confined waterspace. The US Navy and US Marine Corps are trying to counter the adversary's aggression, which may include targeting of its territory as well as its forces. Both sides have pursued disruptive technologies.

The following 13 enduring naval challenges were highlighted:

1) Conducting anti-submarine warfare against submarines and unmanned underwater vehicles (UUVs)
2) Conducting anti-surface warfare against numerous vessels with standoff capabilities
3) Conducting integrated air and missile defense against larger numbers of more capable aircraft, UAVs, and missiles
4) Countering growing numbers of more advanced mines and torpedoes
5) Conducting damage control against more advanced threats
6) Conducting amphibious operations despite distributed, effective threats
7) Countering increasingly numerous and capable adversary unmanned systems
8) Precisely targeting mobile and/or elusive adversaries in complex environments at varied ranges while minimizing collateral damage
9) Suppressing and destroying enemy air defenses and launch platforms
10) Sustaining mobility and reliability of complex systems across distributed forces
11) Maintaining Blue ISR capabilities in complex EW and cyber environments
12) Countering ubiquitous Red ISR
13) Surviving and fighting despite increasing adversary lethality

Follow-on Q&A discussion included the key themes of whether defense was a "fool's game;" survivability; the effect of the principles of war on the acceleration of disruptive technology; characteristics of the littoral today; and where and when to draw red lines with regard to disruptive technology.

Topic 2: The Changing Face of Mine Warfare – The Application of Advanced Sensing and Autonomy to Enable Robust MCM
Warren A. Connors (CAN Civ), Group Leader - Mine Warfare, DRDC Atlantic Research Center

Mr. Connors introduced the topic by defining naval mine countermeasures (MCM) as that which is concerned with the detection, classification, identification, and clearance of naval mines. The task is challenged by the environment in which the mines are laid; traditionally, ship-based assets conduct hunting or sweeping operations.

Recent advances in the robustness of autonomous underwater and surface vehicles has resulted in the application of robotics to mine warfare. These systems, in combination with advanced sensing, perception, computation power, robustness, and decision making have allowed for a revolutionary change in the manner in which we conduct MCM. Mission autonomy is an active research area to improve effectiveness in uncertain environments. Advanced platforms, sensing, and autonomy provide MCM units with a capability beyond offboard sensing. Robotics provide a revolutionary surge in capability, providing the possibility of effective MCM while decreasing the risk to the sailors in the threat area.

Mr. Connors discusses autonomous mine countermeasures.

Key areas include:

- o Concept of Operations: Robotics in MCM
  - Standoff MCM – keep the Sailor (almost) out of the minefield
  - Multi-phase MCM – different "specialist" platforms to fulfil the phases of MCM
  - Parallel MCM – vehicles cooperating together within a phase, and collaborating across phases
  - Covert MCM – no surface expression
  - Intelligence
- o Advanced Sensing – High-Frequency (HF) side scan sonar; paired sensing gets rid of blind spots
- o Synthetic Aperture Sonar – an enhancement on HF side scan sonar but with lower frequency/increased resolution
- o Increasing MCM effectiveness with autonomy (not AI)
- o Autonomy is critical in the underwater environment
  - Difficult to non-existent communications
  - Changing environment
  - Covertness
  - Increase robustness
  - 3 A's of autonomy – Automatic, Adaptive, and Autonomous
  - Challenges for effective autonomous MCM – Sensing, navigation, employment/performance, doctrine/tactics, trust

Q&A discussion topics included: onload and offload capabilities of robotic MCM vehicles; current threats in MCM, such as the homemade IED type device; and the future of submarines in a "transparent" ocean.

Both the Battle Network and Maritime workings groups came back together in plenary session for the final topics.

Topic 3: A "New Era" for Chinese Military Innovation: China's "First Offset" and the Future of Warfare
Ms. Elsa B. Kania (USA Civ), Adjunct Fellow at Technology and National Security Center; Center for New American Security (CNAS), PhD Candidate, Harvard University

Ms. Kania began with brief historical context and an overview of China's innovation strategy for economic development and military modernization. This strategy is characterized by a national strategy of "military-civil fusion" between the People's Liberation Army and commercial sectors, and opportunities to transform today's "informatized" ways of warfare towards future "intelligentized" warfare. Ms. Kania defined Artificial Intelligence (AI) as the ability to have machines learn from data and solve problems. In terms of recent well-known developments, she highlighted the success of AI in complex games such as that of "Alpha-Go" in the traditional game of Go. In terms of AI superpowers, the US ranks first and China second; China is working hard to catch up and surpass the US. By 2030, China aspires to be the world's premier AI innovation center. China's military sees AI as accelerating military transformation and leading to the next revolution in military affairs. Other areas of exploration include human-machine integration and enhancement. Challenges for China include competition for skilled talent, training and continual learning requirements, and the management of high volumes of data.

Major themes discussed in the Q&A sessions included the ethics of AI; the relative advantages and disadvantages of China's relatively closed and homogeneous society; and China's AI priority areas.

Topic 4: Quantum Rules of Engagement: How Burgeoning Access to Fundamental Laws of Physics Will Alter the Field of Play
Dr. Peter C. Mason (CAN Civ), Chief Scientist for Electromagnetics, Defence Research and Development Canada

Dr. Mason began with a brief description of the difference between classical physics and quantum physics. He asserted that "rules matter" since they make up a typical organizational decision-making process, but they have the disadvantage of inefficiency. Dr. Mason described "Quantum 1.0" as the devices available today which are fundamentally reliant on the effects of quantum mechanics (QM). Examples of these include the transistor and the laser. "Quantum 2.0" is a class of devices that actively create, manipulate, and read out quantum states of matter, often using the quantum effects of superposition and entanglement. An example of Quantum 2.0 is the quantum "gyroscope" or lab bench. For purposes of position, navigation, and timing (PNT), quantum optical gyroscopes offer magnitudes of greater accuracy over mechanical and optical counterparts. Quantum radar holds the promise of reducing or removing "noise" and simultaneously reducing the signal, providing the advantage of lower detectability. In the area of communications, quantum encryption prevents eavesdropping and spoofing, and allows for detection of intercepted communications. Quantum gravimetry, which can measure tiny changes in gravity, is currently being employed to build extremely accurate clocks. Quantum magnetometry offers the promise of greater detection of metals and electromagnetic fields.

In terms of military applications for QM, potential short-term applications include PNT in denied areas, submarine detection, identification of underground facilities, change detection, and counter-mines. The greatest potential long-term application is quantum computing, but that also is one of the biggest challenges. Dr. Mason summed up the QM opportunity by asking what if we could sense almost anything and communicate without ever being heard. On the other side of the coin, he asked, how do we operate in the open?

Q&A discussion included the themes of QM and deterrence; timelines of when we might see QM-related technology in operational use; trust and "quantum assurance", the need for new strategy to accompany the new technologies; challenges of explaining the 'so what' of QM and AI to leaders and decision makers; and a call for action to include more "hands-on" engagements (e.g., war gaming, exercises) in future CD&E conferences.

Workshop 4 - Disruptive Thinking: Think Wrong Blitz and Executive Seminar

Led by solve/next: Mr. Chris O'Keefe (USA Civ) and Mr. Greg Galle (USA Civ); supported by ACT Concept Development Branch Head, HQ SACT

The Think Wrong Blitz and Executive Seminar introduced NATO delegates to the Think Wrong Problem-Solving System—a flexible system for defining and developing concepts and running experiments. Through a mix of short talks, stories, and hands-on drills, participants learned new language, frameworks, tools, and techniques for conquering the status quo and creating bold concepts to solve today's and tomorrow's vexing problems. The workshop promoted and explored disruptive thinking, alternative analysis, and problem formulation techniques. It supported the HQ SACT personnel development and staff training which emphasizes innovative thinking.

The Disruptive Thinking seminar, led by Mr. O'Keefe (center), takes advantage of the warm weather while running through a hands-on exercise.

Overview

The 1½ day Think Wrong Introduction Class and Executive Seminar introduced 35 NATO delegates to the Think Wrong Problem-Solving System—a flexible system for defining and developing concepts and running experiments.

Learning objectives:

- o Define bold aspirations for CD&E
- o Find fresh inspiration for CD&E
- o Let go of the assumptions, biases, and orthodoxies that limit what how CD&E is done and restrict vision of what NATO might do in leveraging its member nations and new technologies
- o Gain insight into how CD&E might be done and produce value for NATO
- o Discover what works, what might be improved, and what to avoid
- o Accelerate time to achieving the desired impact
- o Learn and apply practical tools and frameworks from industry in the CD&E process

Outcomes

- o Concept developers have an enhanced toolkit to leverage in developing new concepts
- o Shared language, tools, and frameworks for getting past NATO institutional barriers
- o An awareness and way forward for how to integrate disruptive technologies into NATO concepts and manage them in the context of a strategic military environment

Think Wrong Blitz Challenge Statement

How might NATO concept developers develop concepts in a way that exploits existing technologies so that we can leverage the combined technical advantage of the member and partner nations and keep pace with the rapid technological acceleration of the 21st Century?

Key Takeaways

- o Many barriers to concept development can be mitigated or managed by deploying the proper frameworks at the right time
- o NATO culture and human biology make it difficult to escape conventional thinking to develop radical new concepts
- o Rapid concept development incorporating disruptive technologies is possible

Selected concepts for potential future exploration and experimentation

ROU BG Dragos Iacob posts an idea to his group's board during a hands-on exercise.

Delegates generated hundreds of potential solutions to the challenge; the below concepts were selected as a sample by the delegates for further refinement and exploration during the workshop. A full report will be provided to ACT Concept Development with all concepts and outputs from this seminar.

NATbot
Climbing the horizon.
Creating experimental, NATO Robot-only Units,—explored various applications across intelligence, weapons support, and other systems, as well as the enabling infrastructure required to develop these units (C2 architectures, etc.).

Major AI
A(i) majority for success.
Cross-nation doctrine analysis and development using AI, coupled with majority versus unanimous approval process enables a shift from consensus to high-impact and majority approved doctrine.

BrainPower
Non-kinetic warfare.
NATO concept of non-kinetic warfare leveraging AI, nano-tech and neuroscience to inform and shape non-kinetic actions and avoid the high cost (financial, physical, reputational loss) of kinetic conflict.

FICINT
Science + Fiction = Next Generation.
Use science fiction to develop future scenarios that will attract, engage, and recruit the next generation of NATO leadership among students, focusing on humanitarianism, capacity building, technology, and the future character of war. NATO might leverage stories to attract leaders, then use young creative talent to shape the narrative. Allows for countering in gray and hybrid warfare.

N(AI)TO
Make NATO smart again.
Replace NATO with AI - use AI to develop concepts, rapidly develop solutions, aid decision making and prevent kinetic operations on both sides. Level of data sharing and common data model needed is high. Ultimately, replace both NATO and UN with AI.

SPACE Academy
Closing the space between us.
Unifying global initiative to join NATO and partner nations in developing rules, norms, and missions in space.

2019 International Concept Development & Experimentation Conference

Spain has graciously volunteered to host the 2019 ICD&E Conference. Attendees of the 2018 ICD&E Conference can expect an email in the Summer of 2019 with information and registration details.

For more information contact:

Maj Salvatore Falcone
HQ SACT
Lead Planner for the 2019 ICD&E Conference
cde-conference@act.nato.int