The 12th NATO Operations Research & Analysis Conference Proceedings

Programme Committee Forward

It is our pleasure to publish the proceedings of the 12th NATO Operations Research & Analysis (OR&A) Conference co-organized by NATO Allied Command Transformation (ACT) and the NATO Science and Technology Organization (STO). The 2018 event brought together approximately 130 OR&A experts from NATO commands and agencies, national defence analysis and research organisations, Centres of Excellence, academia and industry as part of the continuous development of a NATO OR&A Community of Interest building on the success of previous OR&A Conferences and Workshops.

The 2018 Conference offered an exceptional mix of senior military engagement, sharing of OR&A best practices and training in OR&A tools. Senior NATO leaders from ACT, STO and our Croatian hosts warmly welcomed conference attendees and noted how a robust OR&A capability would be a key enabler in defence capacity building and in supporting operations. It is therefore that strengthening OR&A is an essential part of the recently approved NATO Science & Technology Strategy. Three diverse streams were supported by keynote speeches from Brigadier General Armin Fleischmann (DEU, Cyber and Information Domain Command), Mr Roy Hasson (Amazon Web Services) and Professor Rommert Dekker (NLD, Erasmus University Rotterdam).

The conference also offered hands on training with the aim of promoting professional development and making the Conference more accessible to early career analysts. Workshops were provided on the simulation software SIMUL8, Alternative Analysis and Communicating the Benefits of OR&A. It was gratifying to see from the size and diversity of the audience this year that this initiative continues to add value to the Conference.

As always, the Conference continued to act as an essential centre of gravity for NATO's OR&A Community of Interest. Should you have any questions on the conference or its programme contents, please reach out to the program committee chairs:

Han de Nijs
Branch Head Analysis of Alternatives
Requirements Division
NATO HQ Supreme Allied Command Transformation
Norfolk, VA 23551-2490, USA
johannes.denijs@act.nato.int

Jacqueline Eaton
Office of the Chief Scientist
NATO Science & Technology Organization
NATO Headquarters
B-1110 Brussels, BELGIUM
eaton.jacqueline@hq.nato.int

1.0 BACKGROUND

On the 15th and 16th of October 2018, Croatia hosted the 12th NATO Operations Research and Analysis (OR&A) Conference in Zagreb, organized by the NATO Allied Commander Transformation (ACT) and the NATO Science and Technology Organization (STO).

This event built on previous OR&A conferences and workshops as part of the continuous development of a NATO OR&A Community of Interest. The conference aimed to coordinate and improve the contributions of OR&A to NATO operations and capability development to solving NATO's challenges. It brought together the analysis community from NATO commands and agencies, national defence analysis and research organisations, centres of excellence, academia, and industry. Over the years, the themes of the conferences have spanned the domains of operations and capability development, and both looked back to lessons learned and forward to new technologies, techniques and emerging challenges for the Alliance. Each conference has offered opportunities for nations and NATO commands and agencies to present new work and new methodologies.

The central theme for the 2018 conference was ***Tackling Complexity in NATO Operations in Contested and Degraded Environments***. The conference was organized around three themes:

- Understanding and Operating in the Cyber Domain;
- Challenges and Opportunities of Rapid Reinforcement & Force Mobility and its Logistics Aspects;
- Sense Making Through Analytics.

In addition, the conference offered the opportunity to attend hands-on training workshops on simulations, alternative analysis methods and marketing OR&A.

The conference had a high level of attendance continuing the trend from the previous years and confirming that it provides the NATO OR&A community with an essential platform to discuss ideas and concepts to improve and modernize the analytic support available to NATO.

2.0 WELCOME

The conference kicked off with a welcome by co-chairs Mr. Han de Nijs of NATO ACT and Ms. Jackie Eaton from the Office of the Chief Scientist in STO. They also provided an overview of the structure of the conference sessions, training, and workshops. Ms. Eaton introduced the new Awards process started this year to recognize the best paper contributed to the conference.

Mr. de Nijs introduced BGEN Poul Primdahl, Assistant Chief of Staff Requirements NATO ACT, who highlighted the main theme of the conference: Tackling Complexity in NATO Operations in Contested and Degraded Environments. This included three streams that the conference focused upon: Sense Making through Analytics, Understanding and Operating in the Cyber Domain, and Challenges and Opportunities of Rapid Reinforcement & Force Mobility and its Logistics Aspects. Finally, the General encouraged attendees to use this conference as an opportunity to find new ideas and solutions for challenging environments and enable Alliance decision makers to think differently about these challenges.

Dr Tom Killion, NATO Chief Scientist spoke next. Dr Killion shared with the audience the recently approved NATO Science & Technology (S&T) Strategy in which analytic advice to decision makers is a critical component of defence S&T. Dr Killion noted that analytics are at the heart of Big Data challenge and that NATO is dependent on the critical analysis of the OR&A community. He then welcomed the three

Keynote speakers: Brigadier General Fleischmann to provide a military perspective, Amazon Web Services representative Mr. Roy Hasson to provide an industry perspective, and Dr Rommert Dekker to provide insights from academia.

Colonel Slobodan Čurčija, the Dean of the Croatian Defence Academy, welcomed all attendees on behalf of the host country. The Colonel noted that Croatia is "an old nation living in a new country," but with a firm institutional commitment to science and technology, deep appreciation of the S&T community, and an undisputed need to cooperate with NATO allies and partners. Colonel Čurčija observed that interoperability begins with S&T. He noted that the 2018 Croatian Strategic Defence Review highlighted the growing indirect approach of adversaries, as well as Zagreb's commitment to meet NATO's guideline of 2% Gross Domestic Product (GDP) defence spending. Colonel Čurčija recognized the growing importance of S&T related education for his country but also the associated funding challenges. He closed his remarks by noting the need for "smart defence", referencing 2016-2018 strategic documents highlighting ties between defence, academic and industry communities.

3.0 KEYNOTES & PLENARY

The keynotes focused on each of the three themes.

3.1.1 Keynote 1: Operations Research on a Cyber Perspective, Brigadier General Armin Fleischmann, Cyber and Information Domain Command, Germany

Brigadier General Fleischmann provided the first keynote address. The General began by paraphrasing Clausewitz, noting that the nature of war has not changed, but the means and goals have. Territory and resources (singular) have changed to information and knowledge, and digitalization is a game changer. The General observed that the military systems updates every 30-40 years, as opposed to 3-5 years in industry. In the future, NATO operations will be increasingly characterized by hybrid warfare, whole of government approach (particularly in democracy), and the blurring of inner and outer boundaries. He noted the consistent trends of rising vulnerability, and decreasing costs across the S&T enterprise, as well as the lack of a code of conduct in the Cyber domain. In this era of ambiguity, attribution is difficult and underscores the need for well-trained personnel, and the challenge of distinguishing between true and false information. For example, generally 200 days are required to detect intrusion and update the systems. The general noted that potential Actors include criminals, whistle-blowers, spies, hacktivists, terrorists and governments.

In Germany, Cyber, viewed as the fifth domain of operations, overlays air, land, sea, and space. The new Cyber and Information Domain Service (CIDS) integrates all relevant capabilities such as Military Intelligence, Electronic Warfare, Information Technology services, and Meteorology. For the Bundeswehr, CIDS' main pillars include: secure and maintain operation of IT system (standing mission), Intelligence and Effects, geographical information, intergovernmental cyber security.

Next, the General discussed three use cases pertaining to Cyber Security: 1) computer security to include protection of computer systems from theft/damage, 2) Emergency Response (in real life) citing as an example the requirement in Afghanistan for the mission thread medevac rescuing within 30 minutes, 3) Emergency Response "in digital life." The General talked briefly about ongoing studies, including the "Gamification" of Cyber Defence/Resilience; increasing role by non-state actors, exploitation of info environment; and Cyber decision-making and response as well as Artificial Intelligence ongoing activities like AI in the cloud and augmented reality.

Regarding Big Data Analysis, the General described the "Three V's" of Volume, Velocity, and Variety. Additionally, he cited two new "Vs": Value and Veracity, and about ongoing activities include Geo data layers, and creation of a Fusion Centre to fuse data and extract anomalies.

During the Questions and Answers (Q&A) period, the General took questions on the topics of entities inside or alongside the CIDS organization, ways of dealing with legacy services, which experiences in his

previous careers have prepared him for the current role, and the distinct political and military implications pertaining to cyber warfare. A participant asked if, considering the "Napoleonic" structure of our current organizations (e.g., 2/3/5 shops), we would be able to avoid fighting the last war. The General cited the importance of a new generation of training and education, including things like table top exercises, innovation, convincing "old guys" to change their mind. A final question related to the interplay between NATO and individual nations, because every nation has their own cyber-related organization, how can they interact. Therefore, the General said, that it is necessary to encourage nations in NATO and EU to cooperate more between their cyber communities.

3.1.2 Keynote 2 - Analytics and Data Lakes by Roy Hasson, Amazon Web Services

The second keynote presentation, *Making Sense of Data in a Few Simple Steps*, was given by Mr. Roy Hasson, a global business development manager at Amazon Web Services (AWS). Mr. Hasson's talk began with an overview of evolving customer requirements, the use of "data lakes" on AWS to store big data and enable analytic services. He noted that the US Central Intelligence Agency has decided to use AWS. Amazon S3 is in essence a highly scalable hard drive; the key is the integrated aspect of S3. Tools include "Glue," a means to automatically discover and categorize data to make it searchable; generate code to clean, enrich and move data; and run on an automated server. Other tools include "Athena," an interactive query engine that makes it easy to analyse data, and EMR, a big data toolbox. Mr. Hasson discussed several AWS data lake examples to manage disparate sources of data—including the US Department of Energy's Pacific Northwest National Laboratory, the US Census Bureau, and the US Financial Industry Regulatory Authority (FINRA). Mr. Hasson next discussed services developed through Amazon's long (20+ years) heritage of machine learning, including "Recognition" image and video analysis, "Transcribe" for automatic speech recognition, "Translate" machine translation, "Comprehend" to extract insights from text and conduct topic analysis. During the follow-on Q&A session, topics included Amazon tools' compliance with European General Data Protection Regulations (GDPR) regulations and requirements; whether Amazon looks at customers' data and patterns of use; authorities, protections, and restrictions involving facial recognition capabilities; and availability of data centres in certain regions.

3.1.3 Keynote 3 - New Developments in Logistics and Data Science, Professor Rommert Dekker, Erasmus School of Economics, the Netherlands

Professor Dekker's keynote to start the second day of the conference was devoted to the field of logistics. During the presentation, he discussed trends influencing the logistics area as well as new developments in logistics and especially those where data science and optimization play an important role. He discussed service logistics, control towers, 3D printing, predictive maintenance and container logistics. Civil research on logistics yields interesting ideas for the military, some of which are already being pursued in military operations. Following the presentation, the questions pertained to the applicability of commercial logistics approaches in military operations and the need to understand fully the military operations in order to provide scientific advice.

3.1.4 Plenary – Operational Analysis Support to Development of NATO Global Support Hub Concept, Mr Scott Joyce, NATO Communications and Information (NCI) Agency

Following Professor Dekker's keynote, Scott Joyce, a logistics subject matter expert on the NATO Defence Planning Process (NDPP) from the NCI Agency presented in plenary. He presented an Operational Analysis study conducted in support of the development of the NATO Global Support Hub Concept (GSHC). Mr Joyce provided an analytic perspective of methodologies and tools used to support the development of a Global Support Hub Concept. Through the use of a multi-phased approach, NATO worked on developing GSHC in 2013-15. Identification of potential hubs for staging areas was followed by the technical evaluation

of infrastructure and initial selection, in preparation for a final selection based on political factors, which in the end was not undertaken due to revised strategic priorities. Mr. Joyce reiterated and tied back to the first keynote speaker on the importance of speaking the same language as the key stakeholders.

4.1. STREAM SUMMARIES

4.1.1 Stream – Cyber 1 (Chaired by LTC Björn Seitner)

This stream had three presentations. The first presentation, *Understanding Strategic Level Decision Making in the Cyber Domain*, was given by Ms. Melanie Bernier from Defense Research and Development Canada. Ms. Bernier introduced the results of SAS-116, which was designed to enhance linkages between the technical and strategic levels in cyber defense. Topics included strategic level decisions in cyber, state of the art of decision-making in cyber, decision-making in the cyberspace domain and information requirements to support decision making. The research activities included literature review, interviews with member nation stakeholders, and qualitative analysis. She identified six features of an operational domain that are present in cyberspace. Specific characteristics of the cyber domain include being man-made and malleable, decision making is different due to time and speed, uncertainty, transparency, situational awareness. The team developed 12 use-cases of high-level decisions, mainly by interviewing decision makers in member nations (this report is available on the NATO website), observation of military exercises, and focus-group workshops. She closed with issues and areas for improvement, which are mostly related to information—especially the sharing and communication thereof. General Fleischmann started the discussion by asking about the need for trust in sharing of information. Ms. Bernier pointed out that most of current sharing is based on memorandums of understanding (MOUs), and there is a need for more substantive frameworks. Another question focused on methodology- how did the team manage the challenge of time factor in focus groups (in just half a day)? Ms. Bernier admitted the difficulty in getting time and the need to be extremely focused and expressed the hope that ACT or NCIA in the future could look at case studies.

The second presentation was *A Knowledge-Based Model for Assessing the Effects of Cyber Warfare* by Clara Maathuis, a PhD researcher in Cyber Operations at Delft University. Ms. Maathuis gave an overview of her team's new Cyber Operations Analysis Model, a knowledge-based model for assessing the effects of cyber warfare. The Model looked at real-life case studies including Georgia in 2008, Stuxnet, and Ukraine, as well as virtual scenarios. Her team proposed limiting the number of effects to 5-10 effects in order to maximize the benefit to military commanders. Q&A discussion included methods used to distinguish between adversaries' intended and collateral effects; the problem of establishing targeting identities for the actual and virtual scenarios; the use of AI in the model discussed by Ms. Maathuis; how to convey the meaning and insights of the model for actual decision makers and the potential application of the Model to a predictive approach.

The third presentation was *A Collateral Effect Estimation Framework for Non-Munitions Targeting Analysis* by Dr. Ahmed Ghanmi, a principal analyst at Defense Research and Development Canada. Dr. Ghanmi began his presentation with a definition of Targeting, the Collateral Effects Estimation (CEE) Study, a key aspect of non-munitions targeting. He discussed the Joint Non-Munitions Effect Experiment (JNEX-2), which focuses on integrated cyber operations into the Canadian Armed Forces' joint targeting cycle. CEE Drivers included Persistence (permanent, temporary, and transient), Extent (global, regional, national, etc.) Severity, and Likelihood or Probability of a collateral effect. Cyber Layers include physical, logical, and

personal. The Decision Tree Analysis looked at Effect Metrics in relation to CEE Questions. The team developed a systematic approach combining decision tree and risk analysis methodologies to estimate CEE for non-munitions based targeting. Q&A discussion included consideration of the number of targets and the length of time required in the CEE cycle; the challenge of controlling effects with regard to the CEE framework; the possible future use of subject matter experts and proven analytic methods in CEE; prioritization of the effects in CEE; the challenge of understanding known unknowns and indirect effects in the targeting process and the range and differing levels of severity of impact.

4.1.2 Stream – Logistics 1 (Chaired by Mr. Tom Baldwin)

This stream had three presentations. The first presentation, *Strategic Lift Modelling within the NATO Defence Planning Process (NDPP)*, was given by Ms. Roxanne Evering from the NCI Agency. Developing requirements within the NDPP consists of an initial structural phase to identify a pool of capabilities, followed by a second phase where scenarios are used to 'iteratively stress test' the pool. The result generates what is called a Minimum Capability Requirement (MCR). The second phase is supported by analytical requirements modelling. The NDPP has an established methodology to analyse the quantitative requirements for strategic air and sealift capabilities needed to deploy forces into theatre. However, given the current strategic security environment, there is an increasing emphasis on the use of Inland Surface Transportation (road, rail, inland waterways), to support strategic deployments within SACEUR's Area of Responsibility. The NDPP methodology is therefore being adapted to address this newer and more relevant aspect of strategic deployments. There were questions about the return or output from the program. It seemed the return was "defined by the capacity of the operation – and not a detailed practical assessment." Additionally, questions remained about the purpose of NDPP. It seemed that the end goal was to validate the capability level of a given country – but not always.

The second presentation, *Gamification of Integrated Logistic Support Training*, was given by Dr Altan Özkil from Ankara Atilim University in Turkey. Contested and degraded environments have created a whole new set of considerations for logistical support. Integrated Logistics Support (ILS) is one of the key methods for calculating the real cost of logistical aspects of operations. NATO countries have two major ILS needs. First, increasing the cooperation, awareness, and dissemination of ILS workforce training. Second, analyses ILS considerations for Rapid Reinforcement & Force Mobility in contested and degraded environments. The panel drew on extensive audience experience in this field. They helped identify the future needs surrounding ownership and training requirements. They also identified challenges in working across generational differences and the importance of making the training organic.

The third presentation, *Logistics analysis for resilience of an army equipment in initial operations*, was given by Mr. Daniel Kallfass from Airbus, Germany. Making sense of complex systems is difficult because of their nonlinear, multi-dimensional, and interdependent nature. Modelling and simulation with subsequent analytics may be one suitable means to facilitate the sense making process. With the aim to investigate the resilience of an army equipment in e.g. an initial operation logistic Discrete Event Simulation (DES) has been developed. In order to cope with different operations from a permissive to a contested or degraded environment a campaign generator was integrated. A substantial basis for this simulation is logistic data, e.g. data concerning maintenance times and loss rates by battle damage of the regarded army equipment. The challenge caused by the non-availability of these data can be solved by adapting data coming from a combat simulation or expert judgement, for example. The aim is to indicate, under which circumstances, the resilience of the army equipment can be achieved. The results could serve to prepare, future missions in the above-mentioned environments, and to provide recommendations for future equipment, training, logistic processes, maintenance capacities, or stocking of spare parts. Discussions revolved around real world stories and data to show the applicability of this information and program. Users are considering data farming and broader applications in order to prevent any spurious results or conclusions.

4.3.3 Stream – Other 1 (Chaired by Ms. Sylvie Martel)

This stream had three presentations. The first presentation on *Analytic Wargaming* was given by Ms. Sue Collins from NATO HQ Supreme Allied Commander Transformation (SACT). Ms. Collins began by providing various definitions of wargame, emphasizing the requirement that the game provide valuable data and evidence to support decisions on NATO's most difficult problems. She presented a case study of the military implications of Urbanization, involving a future "smart" but overcrowded city of "Archaria" in 2035. The wargame involved a "green" team consisting of civilian representatives including a city manager, International Committee of the Red Cross (ICRC), academics. There was also a strong "red team" to represent the adversary and threat. The wargame pushed analysts to consider second, third, and fourth order effects. Key results of the wargame were that the conceptual framework was validated, capability requirements were refined, recommendations for improvement were generated—and most importantly, the results received stakeholders' acceptance and buy-in. Wargame challenges from an analytical perspective include cognitive bias, the use of data collection as a checklist, proper use of qualitative data, achieving balance between detailed guidance and free-thinking, and thinking into the future. Ms. Collins concluded by outlining the future of wargaming for NATO. Q&A discussion included the qualitative vs. quantitative aspects of the wargame modelling and the application of the MARVEL model during the wargames.

The second presentation was on *Mastering the Littoral* by Mr. Guido Veldhuis and Mr. Bas Keijser from TNO, Netherlands. Mr. Veldhuis began by identifying two key challenges in future littoral operations: 1) how to make sense of the complex urban littoral environment, and 2) how to plan operations in that complex environment across the three physical, information, and human landscapes. The first challenge requires a world view that thinks in terms of an ecosystem of flows (e.g., money, energy, and people) and resilience. The second challenge is to plan operations in that complex littoral environment involving adaptive, dispersed, and non-contiguous tactics to face the threat. Mr. Veldhuis concluded by soliciting the audience's views on whether his team is asking the right questions, and if they had existing works, thoughts, or examples to offer on his work. Q&A topics handled by Mr. Veldhuis, and his TNO colleague Mr. Bas Keijser, included the importance of graphic displays to facilitate engagement with stakeholders versus detailed modelling, the origin of the "ecosystem" concept, and potential application of "mastering the littoral" concepts to non-maritime (i.e. land and air) forces.

The third presentation, *Child Soldiers in the Cyber Domain*, was given by Dustin Johnson and Ben O'Bright of the Dalhousie University in Halifax, Canada. Mr. Johnson began by defining a cyber-child soldier and explaining why we should care about this phenomenon. Mr. O'Bright noted that child cyber soldiers are defined as a "wicked problem" for which the applicable international legal framework is still evolving, whilst the number of cyber-attacks—and role of children in them—is rising. Past cases include possible Russian youth group attacks on Estonia in 2007, ongoing terrorist recruitment online, and the recruitment of children via Internet by the so-called Islamic State. The presenters concluded with the need for more soft Operational Analysis (OA), qualitative approaches to study the issue. Q&A topics included the nature and quantity of data that currently exist on the issue, the age range of child cyber soldiers and if it would be worth establishing categories (e.g. below 15 years of age, and 15-18 years old), the need for additional research (and funding) on this issue.

4.1.4 Stream – SAS-110 Operations Assessment (Chaired by Mr. Andy Bell)

The first presentation was on *SAS-110 – Changing the Way We Look at Assessments* by Dr Adam Shilling. Although doctrine and best practices exist for conducting assessments in long-term stability operations, the complexities of conducting an operational assessment in a fast-paced decisive action fight involving conventional combat, such as that represented in an Army Warfighter Exercise (WFX), can be a challenging endeavour. This paper outlines a framework for an assessment method developed from NATO and national experience that assessors can apply as their organizations conduct decisive action operations. It explains principles to be applied across a warfighting staff with the purpose of assessing the operation's plan. This

method seeks to encompass the entire staff into the often least emphasized aspect of the operations process – assessment. The Q&A session highlighted a number of points. The primary purpose of assessments is to make operations more effective. Participants agreed that the while the assessment process has always been part of the staff environment, it is certainly more complex than it has been in the past. Questions on this brief revolved around ensuring that the assessment is closely connected to the commander's desires in order to bridge gaps in the organization's performance. Unfortunately, participants did not seem to think the example discussed was appropriate to their experiences and NATO operations overall. It would be a more effective to focus on unit accountability and prioritize questions more so than answers. The conversation then shifted to the difference between effectiveness and efficiency. Commanders need to ask whether they are doing the right things or doing the right things well. Each commander can probably point to an experience where their command performed their mission well, but perhaps they did not experience the desired effect.

The second presentation was given by Dr Ben Connable on *Gap Analysis in Operations Assessment Doctrine*. NATO conflict assessment methods have improved considerably since the expansion of the alliances' international security engagements in the early 2000s. However, our examination of published articles, reports, and doctrine suggests that there is a dearth of published literature on conflict assessment and lagging integration of advanced assessment techniques into NATO doctrine and practice. Despite the persistence of irregular warfare, humanitarian assistance requirements, and stabilization missions, there now appears to be less interest in determining the pathways and outcomes of these conflicts through structured assessment methods. More can and should be done to translate NATO's resident expertise into general knowledge and practical application for the alliance. Q&A brought out several points. There was general consensus that as a community we have done a poor job informing command and developing buy-in on the importance of OA. It will be important to provide evidence and theory to commanders in order to sell the assessment. Providing more detail in these scenarios will help commanders understand when they see feedback that they are not expecting or feedback that is difficult to hear. There were also comments surrounding the difficulty of working across classification levels and sharing information. There was a common appreciation of the fact that assessment needs more attention.

The final presentation was on *Red Teaming and Operations Assessment* by Dr Anton Minkow. The paper demonstrates that operation assessments are not confined to formal assessment staff groups, nor they are as centralized as previously thought. Commanders realized the limitations of centralized assessment products, based primarily on quantitative metrics, and sought other sources to augment these products. Decision-support Red Teaming is one such capability that can complement operations assessments. Since the main challenge to any assessment process is whether it is measuring the right things in the right ways, Red Teaming could act as the independent reviewer of critical elements of the assessment process. Methodologically, Red Teaming offers a range of qualitative and contextual analytical methods to decision makers. From the Q&A, the main concern with this presentation was ensuring the connection between execution and effectiveness. To what extent has there been a linkage between OA and course of action assessment in NATO? All participants agreed that in the past, things were more stove piped.

4.1.5 Stream - Other 2 (Chaired by Ms. Katie Mauldin)

The first presentation *Technology Assessment in future Alliance Operations (TAO),* was given by Mr. Gabriele Rizzo, lead scientist with Leonardo in Italy. Mr. Rizzo began with an overview of why and how NATO does technology trends forecasting, including the challenge of incorporating input from all 29 member nations. He described the methodologies and results for each of the two workshops. Workshop 1 used a 4-stage "tree growing" approach to generate new trend areas for the future. Workshop 2 focused on the 2035-2040 timeframe, and featured challenge discussions, introduction of new "ability card," and voting on the most compelling force generation of abilities. Challenges of the workshops included getting the full attention of the audience (especially military), leaving enough time for ideas to unfold, and achieving cost effectiveness. A key conclusion was that no single technology would win the day in future scenarios. Questions and follow-up discussion centred on the number of trend areas, new uses of technology, and

accounting for the combination and effect of multiple technologies.

The second presentation, *Rethinking the Assessment of NATO Operations*, was provided by Igor Fainchtein from Joint Force Command (JFC) Brunssum. Mr. Fainchtein discussed a proposal to change Operations Assessment (OPSA) to reflect NATO's new focus on high-intensity warfighting instead of previous emphasis on Crisis-Response Operations (CRO). Specifically, he argues that there is a need for higher levels of command to build on OPSA of lower-level headquarters and not duplicate it. There is a mistaken emphasis on quantitative data at the expense of valuable qualitative data. The addition of Confirmatory Questions balances quantitative and qualitative data, and provides a more flexible decision-making architecture. Commanders should be making decisions based upon a degree of Wisdom, the highest level of the Data-Information-Knowledge-Wisdom (DIKW) Pyramid. The Q&A period included discussion of the strong enduring need for qualitative data, and the historical and predictive elements of OPSA.

The third presentation was *Threatcasting: Preventing Strategic Surprise* by Colonel Andrew Hall, Director of the US Army's Cyber Institute at West Point. Colonel Hall gave an overview of the "threatcasting" methodology, which is a framework and process that enables multidisciplinary groups to envision threats 10 years in the future and then plan what organizations and individuals can do to disrupt, mitigate, and recover from these threats. The process involves science fiction prototyping and "back-casting" to identify gates or flags that could be seen on the way to a future event. Threatcast scenarios to date include vulnerabilities of complex and efficient systems, identifying AI weapons factories, detecting and defeating chemical weapons attacks. Threatcasting has produced graphic novels (comic books) to illustrate and explain scenarios. Q&A topics included the challenges of getting non-US/non-Western ideas into Threatcasting, and marketing graphic novels to senior military leaders.

4.1.6 Stream – Analytics 1 (Chaired by Dr Ben Taylor)

The first presentation was on *Data Collection & Management (DC&M) for Analysis Support to Operations* by Ms. Jackie Eaton. Extensive trusted datasets are essential for analysis to successfully support military decision-making. In today's interconnected technology-enabled world, the volume, variety and velocity of data being generated is enormous. Advanced algorithms, such as those developed by Google or Amazon, make this data available to everyone in support of their everyday decision-making. Military leaders are demanding the same from their decision support systems. However, current approaches to military DC&M are inadequate to provide the trusted datasets necessary for this level of support. Data is often collected on the fly with little consideration for its reuse and analysts are forced to spend disproportionate amounts of time searching for and preparing data for analysis. For operational analysts to provide the comprehensive and timely decision support for today's complex operations, military leaders need to implement substantial changes to the people, processes and tools in their HQs. During the Q&A session, one issue identified was that within the same NATO headquarters facility, there are several contracts - often with the same company - for the same product. Good for the company awarded the contract, but not an efficient or responsible use of limited NATO time, funds, or expertise. Contracts should be consolidated to avoid such overlap and the focus should remain on supporting the warfighter rather than chasing down data. We can see examples of this poor data management in the case of Afghanistan. One participant described poor knowledge management and archiving procedures resulting in individual countries departing theatre and taking their data/information and lessons learned with them – resulting in a loss for NATO as an organization. In addition, knowledge management is always an issue in a complex and diverse work environment. We must all be stewards of the data and information we gather and not forget to set up future deployers – and generations – for success by passing along what we have learned. The challenges in addressing these problems should not be underestimated. The study identified that the standard staff structure in the headquarters was one factor contributing to the duplication and fragmentation and that existing policies were not being followed. These point to a cultural and organizational challenge that is unlikely to be resolved by the deployment of new technology or the introduction of new processes.

The second presentation was on *Getting Grip on Big Data with Autonomous Multi-Source Analysis* by Dr B. Van der Vecht, Dr A.C. van den Broek, Mr. Riccardo Satta and Mr. F. Bomhof. Continuous monitoring of open information sources produces enormous amounts of data containing sparse relevant information. Available sources on the internet contain unstructured text (e.g., social media, blogs, news sites), imagery (e.g., photo, video, satellites), or structured data (e.g., traffic information, geospatial information) and more. It is not feasible for human operators to process all data. Therefore, including these sources in the intelligence analysis requires automatic processing to produce answers to relevant intelligence questions. A framework is proposed in which autonomous information collectors with scraping, crawling and explaining capabilities are responsible for monitoring specific sources. They trigger cues for other collectors to direct their searching process. Using confirmations or contradictions, the data from multiple heterogeneous resources are fused. The results may activate pre-defined, higher-level indicators that alarm a human analyst, who is provided with insights, information and traceability functions. As such, open big data sources can be included in intelligence analysis. During the Q&A session, questions were raised about the nature of the data collected. Specifically, participants wanted to know more about whether big data could be biased or if, by its vast and seemingly random nature, it was immune to biases. Additionally, there were questions about use of software in creating large data sets. Participants were concerned that biases in, for example: language translation software, could bias conclusions drawn from Big Data. In addition, exploiting this kind of approach by linking automated data collection and analysis to automated decision making raises further questions as to how far automated systems can be allowed to act without human supervision and whether human decision makers in the loop will always remain a limiting factor in the speed of response.

The third presentation was on *ORBAT Planning by Methods of Operations Research* by Major General (retired) Georg Nachtsheim and Ms. Alexandra M. Friede. Over the past 20 years, NATO has utilized multiple force generation processes as part of its operational planning for real world crisis response operations. Today, NATO enters a new phase of its response planning. NATO needs to be able to generate multinational formations, ready for quick response, credible for any potential adversary and sufficiently dominant for operations in potentially very challenging operations and Article V nation state warfighting environments. However, national and NATO force planning continues to lack standardization and interoperability. Furthermore, high value assets, not least in the fields of Command, Control and Communications (C3), recce and intel, indirect effects or Special Operations Forces (SOF) are insufficiently distributed amongst NATO members' force pools. This puts an even heavier burden on the shoulders of national and NATO force and operational force planners. Germany has launched the Framework Nations Concept (FNC) initiative to help overcome this situation. As a FNC framework nation, Germany has committed itself to leverage multinational joint capabilities for NATO's Article V nation state warfighting purposes. By now, 16 FNC participating nations are trying to develop coherent harmonized planning to overcome deficiencies, to improve synergy effects, to achieve the highest possible operational effectiveness through common DOTMLPFI and, complementary to the NDPP efforts, in the long run, to achieve at least converging force planning. German academics and military insiders of the Helmut-Schmidt-University/University of the Federal Armed Forces have developed a working tool, which can assist these efforts. Furthermore, inspired by the NDPP Capability Codes, a data bank was programmed with all known or available force and capability data of European member states. Today, it is feasible to simulate all possible combinations of Multinational (MN) force contributions within the FNC context, to compute the force composition thus identifying venues for remedial action and even to assist decision makers in how to further shape cooperation agendas and harmonized force planning. During the Q&A session, there were several questions revolving around the hurdles of the NATO defence planning process. Participants identified challenges associated with the fact that the process is meant to cover 3-4 years; presumably, the concern here is that the needs on the ground will have changed in much shorter order. Additionally, there seems to be a gap between the concepts of national force planning and operational objectives. This gap creates a space where strategically significant concepts such as the future nature of cyber warfare, differences between conventional, hybrid and asymmetric warfare, and future coordination tactics can be overlooked. Classic concerns about manpower and financial constraints experienced by all nations were also mentioned, but the conversation did not present recommended solutions to these legacy issues. In the end, participants were

faced with the reality of limited time and resources. While operationally focused military commanders will continue to deal with these constraints, it is up to the academics to study these issues and propose solutions.

4.1.7 Stream - Logistics 2 (Chaired by LTC Björn Seitner)

The first presentation, *Optimized Spare Parts Inventory for Military Deployment*, was presented by Professor Armin Fügenschuh. He introduced a mathematical model to support the German Armed Forces to find an optimal mix of spare parts that would enable a quick reaction in case of a NATO Response Force (NRF) deployment. This approach focused on spare parts for vehicles to ensure mission survival with the highest period of time in an attempt to determine the optimal selection of spare parts and how many systems are functionally required during high/low op tempo. Using mixed Integer Stochastic programming (a two-stage mixed-integer optimization), the goal is to make the best decision with uncertain input data. Advanced Integrated Multi-dimensional Modelling software is the system designed for modelling and solving large-scale optimization and scheduling problems. This model has been applied to a real world and a simulated dataset. The analysis shows that a relatively high service grade is possible even with a small weight capacity. The analysis also showed the importance of missing data. It also appears that a moderate number of scenarios provides stable solutions that are also representative for a new failure scenario that was not part of the optimization The Q&A topics pertained to probability of failure and survival, volume data and management of the warehouse capability

The second presentation, *Recommendations on the adoption of Modelling and Simulation for analysis and decision making support for Deployment Planning*, was presented by Dr Pilar Caamano from NATO STO Centre for Maritime Research and Experimentation. She discussed logistically contested environments, deployments planning capacity, adoption and integration of Modelling and Simulation. By definition, modelling is a representation of a system or process while the simulation is the execution of these models over time. The implementation of the proposal is intended to provide logistic planners a new approach based on simulation and data which could enhance the iteration among stakeholders in the decision making process. So far, the team has identified the need for sustainment to support qualitative and quantitative analysis in the assessment of deployment plan feasibility, robustness and resilience. The Q&A topics included the need for an integrated system and operational analysts' involvement.

The final presentation in this stream was *Rail Gauge Logistical Challenges in the 21st Century Rapid Deployment and Reinforcement*, presented by Nicholas Myers the President of War Vs Peace. He discussed the rapid deployment and reinforcement of forces during crisis that pose timeliness challenges on logistics. Through the use of Operational Analysts to understand Soviet deployment times, the briefing suggested that modern NATO militaries could learn from this evolution to Soviet military thought to inform plans to deploy troops as a potential defence of continental Europe from the Far East. The Q&A topics included Baltic state reaction, frequency changes to increase the barrier and the ability to transfer rail cars in East Germany.

4.1.8 Stream – Analytics 2 (Chaired by Mr. Han de Nijs)

The first presentation was provided by Dr Mohamed Ibnkahla on *Internet of Things and Machine Learning for Information Operations Targeting*. The Internet of Things (IoT) and Machine Learning (ML) have been extensively used in several civilian domains including Intelligent Transportation Systems, e-Health, and Smart Electrical Grid, leading to spectacular results in these fields. However, the deployment of IoT and ML in the military context is still new. Planners can use the IoT and ML algorithms developed for industrial and business applications to address some of the data aggregation and analytics problems in military applications, including Information Operations Targeting Analysis, Joint Lessons Learned Analysis, and Joint Doctrine Development. During the Q&A session, there was a common agreement that the next war will be fought in cyberspace. Based on this recognition, the conversation shifted to shaping the soldiers of the future to be prepared for this new battlefield. Starting with unmanned platforms across air, land and sea, now with the advent of AI, we are seeing humans increasingly removed from the warfighter's decision-making process.

Despite this trend, conference leaders highlighted the importance of military commanders. Ultimately, decisions will be left to the soldier vice machines. UN is investigating the rights of collecting IoT data and what is ethical. Nothing in the military will be done until this is ironed out.

The second presentation was on *Concept of Conventional Threshold* presented by Dr Jaan Murumets, Estonian National Defence College. The problem of how a small country can make the threshold for a potential attacker as high as possible (within the limits of affordability) is of high relevance in the contemporary security environment in Europe. Stemming from conceptual thinking in Scandinavian countries, an analytical framework of the Conventional Threshold appears a promising way to address the problem of the weak deterring the strong – to include the role of deterrence and resilience, and the importance of creating favourable conditions for Allied assistance. One closely related problem involves the practical application of the Threshold Concept within the routine policy-making and defence planning process. Leaders must consider to what extent it can be utilized via generic planning tools (planning assumptions, policy guidance, missions and tasks, and required capabilities). For the purposes of collective defence, the analytical process must be standardized and compatibility of results across nations ensured. To prove the validity of this approach, two generic strategies were assessed against the functions of a threshold, strengths and weaknesses discussed, and findings developed. The study proves that the concept of conventional threshold is applicable within, and using tools of, Western defence planning methods. Q&A revolved around the nature of the security environment assessed during the study. Participants in the session wanted to know whether there was a contained or protracted conflict underway as well as get a clearer sense of each side's motivation. These questions are a reflection of the changing nature of warfare in the 21st century. Future strategies require smaller countries punch back hard – upping the ante so that outside assistance comes sooner.

The final presentation was on *Tackling Combinatorial Explosion in Force Design* by Dr Ben Taylor, Defence Research and Development Canada. Force Development at the strategic level is about planning the evolution of a military force into future decades. One of the challenges is to manage the complexity of the options space. Creating a portfolio of high value-for-money options through traditional optimization tools is computationally demanding and risks a force with no coherent design, as these tools do not account for a higher-level vision. Equally, offering senior leadership a small number of customized thematic future force options may not offer real choice, as they may in reality be limited to a number of extreme models and one compromise model, which will inevitably by the preferred option. To address this problem, a novel approach has been implemented in a high-level prototype model. This approach allows the utility of a force structure in meeting policy objectives to be explored, while working within financial, personnel and/or structural constraints. The prototype model can be taken as a starting point by any nation and implemented with different tools and/or in increased levels of fidelity to meet specific decision maker and/or national needs (such as whether force options are military units of capital assets or using it to develop just naval force options rather than whole of force options). The approach allows rapid development and evaluation of future force options to support Force Development decisions makers in their efforts to achieve national policy goals, whilst avoiding unnecessary levels of detail and complexity. The intent is to provide a tool to allow force developers to scope the solution space before launching more detailed examination of potential "sweet spots".

Participants during the Q&A session identified interoperability concerns, as much of the software developed is country or coalition specific and will not work universally. There were also concerns about the degree of effort required to take advantage of these tools – will the reward received be worth the effort expended to achieve it? The best way forward seems to be to testing this software in order to gather more information and collecting/disseminating lessons learned to improve the software and increase applicability across the force. There are plans in place to test with the Canadian Defence Forces and information will be shared in the future.

4.1.9 Stream - Cyber 2 (Chaired by Ms. Sylvie Martel)

The first presentation of this stream, *How the NATO Alliance can become Operational in cyberspace domain,* was presented by Mr. Johnathan Searle of the NCI Agency. The purpose of this briefing was to discuss Cyberspace, which is now recognized as an Operational Domain by NATO, and highlight methods being used to help NATO operationalize Cyberspace. In order to achieve superiority within any domain NATO needs to be able to undertake both offensive and defensive operational activities. When it comes to cyber, NATO is purely defensive although some NATO members are developing offensive cyberspace capabilities, which may be voluntarily provided to support NATO-led operations. The presenter discussed the Operational Functional Services (OPS FS) Baseline Project, which uses a mission threads approach to support the identification of Command and Control (C2) requirements and interactions with other domains. The OPS FS Baseline Project and the mission thread approach is being used to support the integration of national cyberspace effects, the interaction with the Joint Planning and Joint Targeting process, and the integration of Cyberspace ISR. Q&A topics pertained to the work ongoing in ACT cyber branch and coordination with the work carried out within the OPS FS Baseline Project.

The second presentation, *Approaches to Implementing Joint Cyber Defence Situational Awareness* was presented by Mr. Torbjorn Kveberg and Mr. Torgeir Broen from the Norwegian Defence Research Establishment. The opening of the briefing highlighted the need to connect their initiatives on research in cyberspace with OR&A. Cyber Defence Situational Awareness (CDSA) is a tool to help the Commander understands and assesses the cyberspace situation, its relation to parallel operations, threats and infrastructure which is required for maintaining combat capability. CDSA helps move beyond the traditional computer security mind set to cyber defence. CDSA requires understanding of one's own Communication and Information Systems, requirements and adversarial activities. Given that cyberspace is contested it was emphasized that you need to be able to evaluate current Courses of Action (COAs), balance technological capabilities and understand risk. Q&A topics included modelling military operations, building scalable data models scoping cyber defence, highlighting redundancy through situational awareness, existing situational tools and working with sharing threat information with the international community.

The final presentation in the Cyber 2 stream was J*UMP Tactical Cyber Mission Planning* by Tim Dudman, Sowdagar Badesha and Marco Casassa Mont. The Joint User Mission Planning (JUMP) application is being developed in the UK and is a demonstration environment to show the impact of air, land and sea activities on the cyber domain for joint force missions using analytics and visualizations. JUMP provides research to the defence community using analytics and visualization, which can be implemented to best effect coherent mission planning as well as techniques to support a military commander. This application utilizes technologies that were originally developed for an approach to human interaction with cyberspace to increase military situational awareness. JUMP has been used for interactive Course of Action (COA) evaluation, mission analysis and cyber-attack analytics that provide insight into scenarios to bridge the cyber and physical domains. The current focus is to support socio-technical cyber risks and controls, electro-magnetic effects and optimizing task cost and time calculations for COA evaluation. Q&A topics included limitations pertaining to uncertainty, high probability events, similar tools, potential integration with other existing tools (e.g. the NATO tool TOPFAS), mission impact assessment and cyber terrain boundaries.

4.1.10 Stream – Analytics 3 (Chaired by Dr Ana Barros)

The first presentation was *Analysing Meta Models to Make Sense of Large Scale Simulations in a Military Context,* by Mr. Wouter Noordkamp. To provide decision support in a military context, such as to evaluate and assess new platform concepts and tactics, simulation models are required, among others, to model complex interactions between opposing forces. However, this may require a large number of simulation configurations, because of the variation and uncertainty of input parameters. Therefore, metamodels, approximation models offer an interesting alternative. In this presentation, the potential of the Kriging metamodeling method in terms of prediction error and computation time for an Anti-

Submarine Warfare (ASW) case is explored. The results show that Kriging is a promising method that achieves roughly 5% prediction error while reducing the calculation time by a factor of three and at the same time covers a larger solution space. The use of Kriging supports the evaluation of new platforms and sensor and weapon systems by carrying out more time-efficient simulations by decreasing the required number of variations. Moreover, it can support the development of tools for the provision of (tactical) advice in a real time operation.

The second presentation was on *A Method for Repeatable Data Collection and Assessment of Communications Interoperability,* by Ms. Elena Krupe. Ms. Krupe identified that the US Army lacks a standardized and repeatable methodology to process, identify, evaluate and organize communications interoperability among multinational mission partners. Her challenge therefore was to leverage and capitalize on data collected during exercises to be used to understand the current capability level with specific mission partners and manage operational knowledge related to Doctrine, Organization, Training, Materiel, Leadership/Education, Personnel, Facilities, and Policy (DOTMLPF-P) elements that limit or enable communications. Knowledge management during an exercise is a critical role for commanders and helps ensure documentation of lessons learned over the course of an exercise for future participants. In this way, we can avoid making the same mistakes over and over again and re-learning old lessons the hard way. She created a data framework based on unit structure, data elements and mission partners. This prototype tool is being currently developed and tested during multinational exercise events. One of the challenges encountered in this study was accounting for different nations' processes. To simplify the research and ensure applicability to future examples, she only collected data on common processes. In order to keep the data up to date, she uses observers during routine and frequent exercises in the United States to ensure the most current data updates.

The last presentation was on *Tackling Complex Anti-Access Area Denial (A2AD) Environments using Multi-National Modelling and Analysis,* by Mr. Tom Baldwin. A2AD is an increasing threat to the alliance, and is defined as a family of military capabilities used to prevent or constrain the deployment of enemy forces in a theatre of operations and reduce their freedom of movement. To determine the potential impact of an A2AD environment on NATO operations and identify how best to mitigate them. This presentation illustrates how a multi-national collaborative modelling and analysis approach was used to assess the challenges of such a complex A2AD environment and identify how they could be overcome. This approach combined military judgement and the use of two different models: Synthetic Theatre Operations Research Model (STORM) and Joint Theatre Level Simulation (JTLS that simulates joint, combined, and coalition civil-military operations at the operational level. STORM is a US DoD model comprising air, space, land, sea and air battlefields. It is a stochastic, constructive, theatre-level campaign simulation used to inform force structures, operational concepts and military capabilities analysis. This study shows the need for a clear identification of the available OA & Modelling capabilities as well as need to develop a robust arrangement to facilitate the use of different modelling capabilities and facilitate multi-national collaboration.

4.2. OR&A TRAINING SESSIONS AND WORKSHOPS

For the second time, training sessions were held at the conference with the intent of educating and developing the attending analysts in different OR&A techniques.

4.2.1 Alternative Analysis (AltA) Training

This training on Alternative Analysis (AltA) was run by Ms. Sue Collins and Mr. Tom Baldwin of NATO ACT. An overview was given of AltA, which comprises of a set of simple techniques that supports the inclusion of independent, critical thought and alternative perspectives to support decision-making. Around 20 participants were then given the opportunity to put into practice AltA techniques such as star bursting, pre-mortem analysis and brain writing on example NATO problems.

4.2.2 SIMUL8 Training

Ms. Corinne Freeman & Mr. Liam Hastie from the SIMUL8 Corporation ran a training course on their simulation software. Around 20 participants were introduced to the SIMUL8 software using an example problem designed to reflect NATO challenges within Rapid Reinforcement, Force Mobility and Logistic Aspects. After being introduced to SIMUL8 objects, such as start points, queues, activities and resources, participants built a basic model, which was, ran with dummy data. The results were assessed to identify issues within the process, such as bottlenecks, and determine areas for improvement. Participants were taught how to use SIMUL8's functionality to make changes to the model to test potential improvements in the process.

4.2.3 Communicating the Benefits of OR&A

Ms. Jacqueline Eaton, S&T Advisor, STO Office of the Chief Scientist, offered an interactive session on how to communicate the benefits of OR&A to non-analysts. Working in small groups around 20 conference participants learned how to conduct a target audience analysis and refine the way they communicate their analysis results to make them more memorable and effective for decision makers.

5.0 AWARDS

During the conference several awards were presented to members of the NATO OR&A community.

Dr Tom Killion presented the NATO Chief Scientist's award for Contribution to NATO OR&A to:

- Mr John Redmayne for an outstanding 24-year career in NATO OR&A.

Dr Ana Barros, the NATO System Analysis and Studies (SAS) Panel Chair, presented the SAS Panel Excellence Award to:

- Mr. Ahmed Ghanmi on behalf of the SAS-109 task group on *Risk Analysis for Acquisition Programs*.

Mr. Han de Nijs and Ms. Jackie Eaton awarded the NATO OR&A Conference 2018 Best Paper Awards to the following individuals:

- Professor Armin Fügenschuh, and Lieutenant Leonie Johannsmann (in absence) *Stochastic Mixed-Integer Programming for a Spare Parts Inventory Management Problem*

- Mr. Guido Veldhuis and Mr. Bas Keijser, *Mastering the Littoral*.

6.0 CONCLUDING REMARKS

The 12th NATO OR&A Conference attracted a record attendance and provided the community with a platform to discuss ideas and concepts at the cutting edge of OR&A. Collectively, the presentations and discussion served to confirm that there is a wide variety of high quality and highly relevant OR&A occurring within NATO, in collaboration among NATO Nations and partners, and in industry and academia.

In the closing remarks of Dr Pavel Zuna, Director of the STO Collaboration Support Office, he encouraged the audience to be grateful to Mr. de Nijs and Ms. Eaton for their leadership of the conference and the greater NATO OR&A Community. Next, Dr Zuna underscored that interoperability is critical for NATO, ensuring that both large and small member nations remain capable of operating effectively together. Finally, Dr Zuna

thanked all members of the audience and their home institutions for sponsoring their attendance at the conference.

7.0 ACKNOWLEDGEMENTS

The Programme Chairs would like to acknowledge the following members of the 2018 programme committee and their organizations for their significant contribution to the success of the conference:

- Ms. Sylvie Martel, Chief Operational Analysis, NATO Communications & Information Agency (NCIA)
- Lt Col. Björn Seitner, Logistikzentrum der Bundeswehr (DEU)
- Lt Col. Timothy J. Povich, PhD (US Army), Executive - System Analysis & Studies Panel, NATO Science & Technology Organization
- Lt Col. Dr Marko Zečević, Branch Head – Strategic Planning and Analysis Branch, Croatian Defence Academy (HRV)
- Mr. Jeroen Groenevelt, Panel Assistant - System Analysis & Studies Panel, NATO Science & Technology Organization
- Mr. Andy Bell, Operational Analyst - NATO Allied Maritime Command
- Dr Ana Barros, Principal Scientist, TNO (NLD)
- Ms. Katie Mauldin, Senior Operational Research Analyst - NATO Joint Analysis & Lessons Learned Centre (JALLC)
- Mr. Tom Baldwin, Operational Analyst, NATO Allied Command Transformation
- Dr Ben Taylor, Leader – Strategic Planning Operations Research Team, Defence Research and Development Canada (DRDC)
- Col. Andrija Kozina, Officer for Sciences and Development, Croatian Defence Academy

LIST OF ACROYMNS

Acronym	Expansion
A2AD	Anti-Access Area Denial
ACT	NATO Allied Command Transformation
AFSC	Alliance Future Surveillance and Control
AI	Artificial Intelligence
AltA	Alternative Analysis
AWS	Amazon Web Services
CDSA	Cyber Defence Situational Awareness
CIDS	Cyber and Information Domain Service
CoA	Course of Action
DC&M	Data Collection & Management
DOTMLPFI/P	Capability Lines of Development: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Interoperability/Policy
FNC	Framework Nations Concept
GSHC	Global Support Hub Concept
ILS	Integrated Logistics Support
IoT	Internet of Things
JFC	Joint Force Command
ML	Machine Learning
NCI Agency	NATO Communications & Information Agency
NDPP	NATO Defence Planning Process
NRF	NATO Response Force
OA	Operational/Operations Analysis
OPSA	Operations Assessment
OR&A	Operational/Operations Research and Analysis
Q&A	Question & Answer
S&T	Science & Technology
SACEUR	Supreme Allied Commander Europe
SACT	Supreme Allied Commander Transformation
STO	NATO Science and Technology Organization
TNO	Dutch Defence Research Agency