Joint Air & Space Power Conference 2018

THE FOG OF DAY ZERO
JOINT AIR & SPACE IN THE VANGUARD

CONFERENCE
PROCEEDINGS

Joint Air Power Competence Centre

Disclaimer
The Joint Air Power Competence Centre (JAPCC) Conference Proceedings is a product of the JAPCC. It is produced to provide a summary of the Joint Air & Space Power JAPCC 2018 Conference and subsequent proceedings. It does not represent the opinions or policies of NATO and reflects independent analysis, opinion, and the position of its authors.

Release
This document is approved for public release. Portions of the document may be quoted or reproduced without permission, provided a standard source credit is included.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

Table of Contents

The JAPCC Conference 2018

Sponsor Recognition

GENERAL ATOMICS AERONAUTICAL

IBM

LEONARDO

LOCKHEED MARTIN

THE VALUE OF PERFORMANCE.
NORTHROP GRUMMAN

SNC SIERRA NEVADA CORPORATION

THALES
Decisive technology for decisive moments

ThalesRaytheonSystems

The JAPCC wishes to thank all sponsors for their contribution to this year's Conference and for helping to make it a great success.

Klaus Habersetzer
Lieutenant General, DEU AF
Executive Director, JAPCC

This book contains the proceedings of The Joint Air Power Air Power Competence Centre's annual conference held at the Messe Essen, Germany from 9–11 October 2018. The theme for this year's conference was:

'The Fog of Day Zero – Joint Air and Space in the Vanguard'

In this edition of the conference proceedings, we have captured and themed the results, rather than publishing a chronological recounting of the panel discussions. We hope this makes it easier for our readers to identify the key takeaways.

We thank those of you who joined us for your contributions to the discussion, and hope that those of you who were unable to be there will find this wrap-up informative and thought-provoking.

If you wish to provide feedback on these proceedings, or the conference on the whole in order to help us increase the value of the event, please send us your feedback at conference@japcc.org.

Thank you and good reading!

The Joint Air Power Competence Centre (JAPCC)

The Fog of Day Zero
Joint Air and Space in the Vanguard

Opening Address by the Director, Joint Air Power Competence Centre.

'Since NATO's establishment almost 70 years ago, mutual trust, respect and the pledge to collectively defend ourselves when threatened have held this Alliance together.'

Introduction

From 9 to 11 October 2018, the Joint Air Power Competence Centre (JAPCC) held its Annual Air and Space Power Conference in Essen, Germany. The conference was attended by more than 280 participants, including four NATO Air Chiefs and 55 General Officers, Flag Officers and senior civilian executives. Attendees also included members of several NATO organizations, representatives of non-governmental organizations, academia and defence industrial partners. In total, 25 different nations were represented, a true cross-section of the Alliance and European partners which fostered meaningful and fruitful discussion. The format comprised four panels designed to address the following issues: defining the threat environment, Air Power's role in that environment, whether NATO has the right mindset to operate in this environment and how NATO can use Air Power to address these challenges.

The theme of this conference was 'The Fog of Day Zero', a concept to describe the uncertainty of the environment and/or an adversary's activity, experienced prior to the start of hostilities or the declaration of war. This uncertainty is often a result of modern adversaries, be they state actors, non-state actors or Violent Extremist Organizations (VEOs), committing hostile actions which remain largely below the traditional 'armed attack' threshold of war and may not be easily recognizable as such by the victim. In fact, modern warfare is not necessarily characterized by a definitive declaration of war, rather it may emerge through a succession of seemingly uncorrelated events. For this reason, the expression 'Day Zero' does not refer to a specific point in time or a specific length of time, rather it describes a situation of uncertainty about whether there is an attack underway, the identity of the attacker, their intentions and whether the hostile actions constitute an act of war.

'The clarity of the bi-polar Cold War world, where some of us began our service, is long gone.'

After the Cold War NATO was engaged in various campaigns, and confronted adversaries who lacked the capabilities to challenge NATO Air Power. This led to a period of complacency where many in the Alliance took for granted that NATO Air Power would always prevail and do so without significant losses. This complacency, combined with a global economic crisis, led to significant reductions in NATO forces, equipment and capabilities. Misplaced self-assuredness and a sense of superiority, continues to be the reason that, during exercises, Alliance forces are always assumed to be superior, suffer few losses and always win. In recent years, however, NATO has witnessed the re-emergence of near-peer competitors. Although these competitors would not be in a position to win a full-scale military conflict with NATO at this time, they have the means to attack NATO's vulnerabilities indirectly, such as by employing cyber, strategic communication, electronic warfare (EW) and space capabilities. NATO's military, as well as civilian population, is highly dependent on many of these systems and domains for communication, precision navigation, weather information, financial transactions, and civilian infrastructure services to name a few. Over the course of the Conference, three main themes dominated discussions: How does NATO define an attack? What is NATO's current readiness to respond? and How should NATO prepare for the future?

In seeking to address these challenges posed by 'The Fog of Day Zero', the JAPCC's intention was to stimulate debate amongst the various participants. The following proceedings consolidate significant points from the keynote addresses, the panel discussions and attendee contributions to form a summary of the event and to highlight areas for future consideration and development. The document does not record the minutes of the Conference, rather it highlights the major themes and draws together thoughts and ideas from all elements of the conference.

For a fuller understanding, readers are encouraged to read these proceedings in conjunction with the previously published Conference Read Ahead material.

In the spirit of the Chatham House Rule, no statements, opinions or ideas are attributed to any particular individual within this record.

THEME 1: What Defines an Attack?

A representative of a potential near-peer adversary recently stated 'We will never be able to compete with 10 American carrier battle groups, or field aircraft that have the degree of stealth of an F-22, nor do we have the ambition to. We will simply take out your satellites, radio links, and computers.' This could be done using the full range of hybrid warfare tools: from 'little green men' to 'big green rockets', to 'fake news' and even cyber and electronic attacks. The initial results could include loss of space-based ISR, GPS, Link 16 and computer-based mission planning systems, and the effects

would likely continue. This could seriously undermine both the perceived and actual effectiveness of NATO Air Power. NATO is not accustomed to suffering losses on a grand scale, which might well happen on Day One if we are not properly postured.

Perhaps the best-known article of the Washington Treaty is Article 5. This article states that an armed attack against one member state is an armed attack against all. Nations may respond using their inherent right of self-defence or they might act individually, or collectively, in accordance with Article 51 of the U.N. Charter. Each NATO member state will provide such assistance to an attacked member state as the supporting member deems necessary. There are two key aspects in the wording of Article 5: 'armed attack,' and 'as it deems necessary.' This begs the question: 'What is an armed attack?' Under international law there is no definition of an armed attack, nor is there one in the NATO glossary, leading to the possibility of confusion and slowing down the decision making process. The second interesting aspect in Article 5 is the wording 'as it deems necessary'. This implies that it does not necessarily mean military force. The assistance provided by a NATO member state to an attacked nation can be of a different nature; it can be moral, financial, it can be by imposing sanctions, and so on and so forth.

'It is important to know what constitutes an armed attack before Day Zero. If NATO waits until Day Zero, it will already be too late.'

One of the challenges in determining whether or not an armed attack has occurred is assigning attribution. If the armed attack is a terrorist attack, for example, it could be dealt with by law enforcement agencies and not the military. The September 11th attacks, were responded to with military means after the North Atlantic Council consented that the United States of America had been subjected to an armed attack. Although the attack was conducted by a non-state actor, the key to it being considered an armed

attack under Article 5 was that it had been directed from abroad. Today it is more difficult to distinguish between State and Non-State actors.

When differentiating between State and Non-State actors one must consider the proxy. A proxy is a Non-State entity that is controlled by a State power. Proxies are not groups who act independently, those are Non-State actors. Actions by the so-called 'little green men' who act as uniformed military personnel but do not identify with a nation, supported by propaganda, misinformation and cyber-attacks, make attribution difficult.

Kinetic actions against NATO are easier to identify, and make the determination that an armed attack has occurred quite simple. However, NATO is facing attacks in new dimensions. Vulnerabilities in airbases, communication networks and infrastructure abound. Modern facilities are no longer hardened, and it is questionable how well they can be protected from CBRN attacks or swarms of inexpensive drones. As Italian Air Power theorist, General Giulio Douhet, pointed out it is far easier to destroy an enemy's eggs and nest on the ground than it is to hunt and kill the enemy's fighting birds in the air, therefore aircraft protection must be considered at home bases as well as transit locations. Space assets are also vulnerable, as space is no longer the unreachable sanctuary of a few select nations.

'The first target that we have to achieve in a peer competitor environment is to regain what we've been used to enjoying since day zero in the counterinsurgency environment which means gaining and maintaining control of the air.'

Likely adversaries have made it clear that they are developing, fielding, and expect to operate counter-space weapons. NATO must prepare for physical and cyber-attacks against ground stations and other space mission nodes; jammers and dazzlers to deny receipt of satellite signals and imagery, prevent navigation, intelligence, and communication links; or,

even worse, 'spoofers' that replace authentic space signals with misleading information. NATO's potential adversaries now have ground-launched weapons that would shoot down satellites and create debris clouds that would affect the ability to operate in space for decades. Those adversaries are also devising on-orbit weapons to rendezvous with space systems and destroy them in orbit. An attack in space is comparable to an attack against any air, maritime or land force assets, and also comparable to an attack against key cyber systems.

Russia and Belarus are seen as possible 'peer-state' actors, as there are similar kinetic force capabilities in northern Europe and in Russia's Western Military District and Belarus. Russia has created a strong and very challenging high-end, advanced and multi-layered defence environment around Kaliningrad. As a result, were the Baltic States to be quickly isolated from the rest of the Alliance, they might be difficult to liberate. In comparison to the Baltic States, Russia has the advantage in fixed and

rotary wing assets, ballistic and cruise missiles, Ground-Based Air Defence (GBAD), and nuclear capability. Moreover, Russia has plenty of space to manoeuvre within her borders and, therefore, operational depth. The Baltic States have scarce resources, are not in a position to build up equal power nor do they have sufficient operational depth. Furthermore, Russia conducts espionage, subversion, information and electronic warfare including cyber actions. They are constantly evaluating NATO air surveillance and readiness by conducting aggressive flight operations. It may not be Russia's intent to enter into war with NATO, but they might use a favourable opportunity to cut off a small piece of NATO, particularly if they think they can do so without shots being fired, as they did in the Ukraine with Crimea. For this reason the Alliance must demonstrate its readiness to respond, and to clearly and unambiguously demonstrate that every member nation will be protected and defended equally.

Russia has a new means of exploiting the vulnerabilities of the West: cross-domain coercion. Russian doctrine states that the Federation's main task in deterring and preventing use of military force is 'to neutralize possible military actions and military threats using political, diplomatic, and other non-military means.' Although the limited use of nuclear weapons to deescalate a conflict is absent in this doctrine, it remains a serious option. The National Security Strategy of Russia as of December 2015 is more explicit regarding strategic deterrence. It mentions 'interrelated political, military, tactical, diplomatic, economic, informational and other measures which are being developed and implemented in order to ensure strategic deterrence and the prevention of armed conflict.'

'An adversary can be successful in a sub-Article 5 situation if they are really capable in undermining political and societal cohesion in a country.'

This concept of strategic deterrence merges coercion with deterrence and can be applied in times of peace and war; in the West this is labelled hybrid

warfare, but it is much more than this. Day Zero could happen now, or may be happening already, and this really depends on how Russia implements this doctrine. Recently, the concept of 'soft power', coercion through non-military means, was also included in Russia's strategic deterrence doctrine. It includes disinformation and cyber-war to block information on what is going on in Russia. Soft power is primarily aimed at the civil societies of the West and could be strengthened by the use of technology. This concept of soft power was introduced in the Russian Foreign Policy Concept of 2013 and is also linked to the concept of 'controlled chaos'. This concept was presented by President Putin around 2012, when accusing the West of using various methods for destabilizing Russia.

Russia will continue to exploit NATO vulnerabilities, like social and/or economic issues, while using Strategic communication and disinformation to manipulate public opinion through a combination of deception, surprise, and higher responsiveness. They could seek to impose the burden of escalation on the Alliance. That burden of escalation would be political and psychological, as much as operational. NATO has to accept that deterrence will be harder to maintain in the face of a capable and resolute near-peer adversary. Therefore, NATO at Day Zero may find itself in an adverse situation, irrespective of what the overall advantage might be on paper in terms of capabilities, capacity and tactics.

NATO considers deterrence the tool of choice for contentious actions below the Article 5 threshold. Those actions, however, should be seen as shaping operations, preparing the battlefield in the context of strategic deterrence. This concerns not only NATO, but because this is about disinformation, taking out economic systems and creating divisions in societies and political systems, it also concerns the European Union, and individual nations. This effort is about cross-domain coercion, the use of different instruments of power to achieve political objectives. Although it may include military power, it is also an effort to distort a society as a whole, such as through offensive cyber operations aimed at economic, industrial, political, and utility service targets. Cross-domain

operations are difficult for NATO to address, and especially upon which to gain consensus, when they do not include a clear military action or armed attack.

NATO today faces a hybrid threat from enemies that can range from a Violent Extremist Organization to a peer or near-peer State competitor. Hybrid tactics can offset the lack of military capability. Terrorists, like ISIS, use effective Strategic communication, are decentralized, use short decision cycles, have no political restraints, use a multidimensional strategy, and are adaptive and resilient. In addition, NATO's potential adversaries use technology that makes it difficult to recognize that NATO is under attack.

During the Wales-summit, NATO member states agreed that malicious cyber activity can be as harmful as an armed attack. A cyber-attack against a bank or robbing a bank using conventional weapons would not be considered an armed attack, but a criminal act. Individuals trying to meddle in the democratic process of one of our member states however, could be assessed differently, as could cyber-attacks that disrupt infrastructure and supporting utilities such as electricity or water for large population centres. If conventional force is seen as an armed attack, an alleged cyber-attack on the democratic processes of the member states could be seen as an armed attack on that nation's sovereignty. The problem of attribution is increasingly difficult with cyber-attacks. Because of this difficulty, how the Alliance perceives such an attack and what sort of consensus it might achieve in terms of action will be difficult.

In addition to external threats, NATO has to cope with insider threats such as theft of critical information or sabotage; system software hiding malicious logic that might be activated at any inopportune moment; and hackers seeking to degrade command and control networks, infrastructure, and other key space/cyber terrain. It is simpler and much more efficient to manipulate information than it is to destroy it or to force it through sophisticated cybersecurity firewalls.

The use of refugees to achieve political goals is seen as an aspect of controlled chaos. A refugee crisis has a huge effect on public opinion in NATO and EU countries. In March 2016, General Breedlove stated before the Armed Services Committee of the United States Senate that Russia and Syria were indiscriminately bombing Syrian civilian targets in order to increase the stream of refugees. In this way the crisis and the need to respond were brought to a higher level of urgency in the public eye, while simultaneously creating economic and internal security challenges in the nations to which the refugees were being driven. Some have termed this 'weaponization of refugees' and it is a growing challenge for the Alliance and other destination nations.

The migrant crisis led to a discussion between Russia and the European Union; the European Union expected Russia to shift migrants to northern Europe. Migrants arrived at the Finnish-Russian border, which could be seen as a statement from Russia that Finland should be very careful when considering a partnership with NATO or participating in certain exercises and European sanctions. It was also part of an attempt to get concessions from, or even cause cracks within, the European Union. The refugee crisis causes politicians in the West to balance the desire to help with the humanitarian emergency with the pragmatic need to preserve economic and physical security for their own populations.

'Responding at the time, place, and manner of our choosing, which includes the choice of domains, the NATO Alliance has a diverse, agile and flexible array of forces that can do this extremely effectively.'

NATO must not allow its adversaries to define and set the conditions for Article 5 in new domains. NATO should work on strategies for the use of new technologies in emerging domains, and prevent others from defining too specifically what constitutes an armed attack in the space or cyber domains (to name two); doing so merely opens new doors for adversaries to exploit.

THEME 2: Is NATO Ready?

'Readiness means having ready assets, capabilities and realistic training.'

In March 2011 NATO entered a conflict in Libya. The North-Atlantic Council decided that measures to protect civilians and populated areas under threat of attack should be implemented in accordance with UNSCR (United Nations Security Council Resolution) 1973, and should continue until no longer required. In effect, UNSCR 1973 mandated NATO to conduct operations. However, at that time, NATO was not ready. The Alliance did not have the right mindset to assume a mission to monitor an arms embargo, enforce a no-fly zone, and protect civilians, because it had not prepared or planned to do so. There was not a synchronization of kinetic, non-kinetic,

lethal and non-lethal capabilities, nor an adequate number of staff officers trained to plan for combat operations; the focus had previously been on peace support operations, humanitarian assistance and disaster relief.

NATO learned a number of lessons from the experience of Operation UNIFIED PROTECTOR, and the Russian seizure of Crimea in 2014 increased the sense of urgency to return to a better state of preparedness for larger-scale conflict as opposed to the out-of-area peacekeeping and stability operations that dominated the late 1990s and early 2000s. As a result, the Alliance has been gradually improving the organization and training of the Joint Force Commands and their warfighting components over the last several years, in order to better prepare for the full spectrum of possible conflicts, but we aren't there yet.

'The force that we have postured is the one that will be engaging in Day Zero.'

The Washington Treaty delineates the actions and efforts NATO may take when faced with an attack. Under the terms of the treaty, NATO nations may provide military support to one another as they see fit. Article 3 will allow each member state of the Alliance to defend itself and come to the assistance of others. In addition to Article 3, Article 4 allows for multi-national consultation. If, in the opinion of any member state, the political integrity, territory, or security of another member states is threatened, any member state can call for Article 4 consultations. The obligation of the other 28 members is to listen, but not necessarily agree with, what is being said. Article 4 consultations rarely end with a decision made by the North Atlantic Council, but they do foster communication and support good decision making. Today, statements on discussions are made public. The main reason for doing so is deterrence, this is a public affirmation that NATO is aware of what is ongoing and demonstrates solidarity among NATO nations.

In response to threats, NATO must evaluate its readiness to respond. The clarity of the Cold War is long gone and the recent focus on VEOs can no longer be exclusive in a world that is almost all fog accompanied by friction. NATO does not know where or when Day Zero will come, or if it is already here, so how does NATO collectively prepare and make ready for conflict in this fog? The United States Air Force Chief of Staff, General David L. Goldfein, recently acknowledged that there are more warfighting domains than there used to be. This can be described by expanding Longfellow's phrase from 'one if by land, and two if by sea' to 'three if by air, four if by space, and five if by cyberspace'. The electromagnetic spectrum and information operations could be seen as the 'sixth' and 'seventh' of this multi-domain world. Perhaps it is most important to understand that these attacks will likely come in more than one of those domains and they will come simultaneously.

'We have to have in our mind that the same peer state actor tries to affect or harm the entire Alliance in difference ways, from different directions.'

Currently, in order to operate, NATO responds quickly to perceived enemy action but is highly constrained. To complicate the issue, NATO's staffing processes are slow which causes friction. Therefore, there will not just be fog but also friction during Day Zero which will carry on through open hostilities on day one of conflict. To cope with this situation, NATO forces must organize, train, equip and prepare command and control processes using long-term planning ahead of time and supplemented with contingency planning.

To prepare for potential hostilities, accurate intelligence, situational awareness and indications and warnings are essential to enable an appropriate response. The question is how to detect and manage actions in the fog of Day Zero to prevent 'Day One'. The answer may well be deterrence. Deterrence, to be effective, must be based on facts and supported by

strong evidence. Deterrence implies readiness, which means ready assets, capabilities, realistic training and plans. Plans must be actionable and aimed at delivering effects. For deterrence to be effective, unambiguous Strategic Communication to potential adversaries is essential. The adversaries must be convinced that NATO is ready and that there would be a price to pay should they attack. Effective Strategic Communication implies that NATO has the political will, the plans, the assets, the capabilities and is ready to use them.

When looking at how NATO can address emerging security challenges using Air and Space Power, there are four realities to keep in mind. The first reality is considered the 'power reality', the ability to project power. The combined GDP of the NATO Alliance exceeds 36 trillion dollars, so there is no financial impediment to NATO's projecting military power. The second is the 'transition reality', the ability to transition from peace to conflict. When deterrence fails, prompt consensus is pivotal, and the

transition to collective defence must be decisive. The third is the 'threat reality', which is probably the most important with respect to Day Zero. There can be up to 30 different views of the threat, one for each Alliance member and still another of NATO's collective view. In conjunction, the enemy can choose to enter into war, this is a new situation for the Alliance; deterrence has always worked. Finally, there is the 'force reality', the reality that NATO forces must be ready, deployable, and sustainable to be fully combat capable.

'We live in a time of profound international challenge and change where we are seeing what would be described as a demonstration of differences, both political and military.'

Another problem facing NATO is that there is no existential threat perceived by the population nor by the politicians in the manner that was present during the Cold War. Nobody believes that even near-peers pose a threat to our existence or our way of life. Over the last 20 years NATO enjoyed the luxury of engaging in out-of-area counterinsurgency operations and hybrid conflict. Against a peer competitor NATO would not enjoy the luxury of using the ROE and caveats normally used in counterinsurgency operations. In addition, this shift may produce a different popular opinion of civilian casualties and collateral damage. NATO needs to adapt to regain relevance both in defence and regarding broader security matters. The danger of not adapting is twofold. The first danger is the possibility of an inadequate response due to lack of resources. It is extremely difficult to advocate for defence resources when taxpayers do not see clear indications of a threat against which to defend. This leads to the budget cuts, force reductions and failures to modernize that we have all witnessed firsthand. Secondly, and an even more challenging risk, is NATO's lack of adaptation to the new and ever-changing scenarios. Just like NATO, the general public must also prepare for Day Zero and adjust their mindset and threat assessment to that of a peer or near-peer

adversary (Sweden, as an example, has undertaken a campaign to educate and prepare their population just so). NATO has to be able to synchronize joint operations to achieve joint effects. Greater authority should be delegated to the military to conduct readiness and response exercises and realign forces, otherwise by Day One, time will have been lost and with it, potentially, the battle.

Protection of NATO assets must be at the forefront of planning. Logistics and reinforcement areas that were once considered secure, due to being positioned in isolated and inaccessible rear areas, can no longer be considered safe havens. Since the end of World War II, NATO has enjoyed relatively unchallenged supply lines whether moving forces domestically or around the globe. In the face of reinvigorated near-peer competitors with tools including cyber, counter-space, hypersonic missiles, etc … it is no longer safe to assume that Alliance lines of communication will remain uncontested. These 'rear areas' must be better protected and made more resilient. To address this, the Alliance established a new operational command to counter these threats, the Joint Support and Enabling Command (JSEC). Among the JSEC's tasks are ensuring mobility, providing force projection, providing logistic support, enabling of the AOR, cross-border operations, protection of critical NATO installations, and counter hybrid operations.

The JSEC also has to enable training and integration and is responsible for the RSOM process (Reception, Staging, and Onward Movement) of NATO follow-on forces. The objective is to ensure freedom of operations and sustainment in the rear area in support of Alliance operations. In crisis, JSEC will function at the same operational level as the Joint Force Command HQ. In peacetime, it will support any NATO Command Structure (NCS) entity during Baseline Activities and Current Operations (BACO). During the BACO period, the JSEC's main task will be establishing a solid network and coordinating between nations the processes and procedures for SACEUR's rear area that could, if interrupted, hamper the swift and effective reaction of NATO to a crisis situation. The important concept here is readiness. The plan is for the JSEC to achieve IOC in September 2019 and FOC in September 2021.

In addition to rear area security, there remains the ongoing requirement to deploy, defend, receive forces, fight and continue to operate. This means that protective structures on NATO air bases must be reinforced. Aircraft are now parked in hardened aircraft shelters of 1980 vintage, designed to withstand a nuclear blast. Some of the protection they offered may still be relevant, but the threats are changing. Today parked aircraft must be protected against threats such as swarming UAVs including those with CBRN elements or capable of generating electronic warfare effects. Directed energy weapons and high-performance microwaves could cripple electronic systems. Cybersecurity is another critical aspect due to modern systems' dependence on information technology and computer and information systems. Ground-based air-defence (GBAD) must also be modernized. Ground-based personnel must also be able to work under CBRN conditions.

Space-based capabilities provide critical information on a daily basis for commercial, civil, humanitarian, diplomatic, and military activity. Space used to be a sanctuary, unreachable to all but a few nations, but that is no longer the case. Despite the rapidly expanding number of actors who can access or affect space, and the inescapable dependence on space-based capabilities, NATO appears slow and perhaps reluctant to acknowledge that space has become a warfighting domain, and this is a concern. The potential threats to NATO space capabilities are complex and the list is long.

THEME 3: What is NATO's Response?

'Since NATO's establishment almost 70 years ago, mutual trust, respect and the pledge to collectively defend ourselves when threatened have held this Alliance together.'

The third and final theme of the Conference centred on NATO's Response, what can or should Air and Space Power do in the fog of Day Zero. Responsiveness means being able to swiftly execute pre-planned options because there is no time to initiate planning once the peer competitor attacks. Additionally, it includes when, where, and how NATO will respond. In 2018, the United States published a new National Security Strategy, followed quickly by a National Defense Strategy. In these strategies three lines stand out: a commitment to lethality, the importance of alliances and partnerships, and the acceleration of acquisition. The United States specifically highlights the two near-peer powers Russia and China, as well as Iran and North Korea, clearly indicating a shift in national thinking to more full-spectrum combat and the A2/AD environment. At the same time, NATO held two summits with three key and recurring points: first, 'NATO is a defensive Alliance'; second, the strategic concept of 'collective defence, crisis management, and cooperative security'; and third, the reaffirmation that 'as long as nuclear weapons exist, NATO will remain

a nuclear Alliance.' This sets the stage for the future environment wherein NATO must adapt to operate more effectively.

During recent Summits, nations have agreed to increase their defence spending and to procure new systems. However, new systems alone are insufficient; more realistic training is required to ensure these new systems will be used most effectively. In addition to increased funding and additional training, several other recommendations were put forth to address emerging security challenges. First, NATO needs to develop a comprehensive list of indication and warning (IW) systems, driven by the political leadership, to focus the Alliance. Second, a standing mission should be initiated to fuse the information of all ISR assets – persistent, non-persistent, and episodic – to directly support these IW. Third, a standing, fully functional processing, exploitation, and dissemination (PED) architecture and a targeting centre need to be established to act upon the information

gathered. Finally, NATO should establish a standing, fully manned Air Operations Centre to ensure the proper command and control (C2) of NATO missions. This future C2 structure must be in place, trained and ready to act. These measures will ensure that all 29 Allies have the ability to use all necessary information and to conduct targeting as required.

'We need to ask ourselves now how many of the tactics that we are employing today, the way in which we train to fight, are a hangover from a time in the past rather than an absolute grasp of our understanding of the future.'

In the next decade a robust mix of 4th and 5th generation fighters in Europe should comprise the bulk of tactical Air Power of the Alliance, while different 6th generation systems are being studied, for operational fielding somewhere in the 2040s. The key to success is the ability of these weapon systems to interoperate. One of the critical systems is the data link that allow them to capitalize on their respective strengths when networked together in a multi-domain C2 architecture. Ensuring the reliability of the hardware, the integrity of the links between these systems, and the resistance of the command centres to interference is challenging. This ability will depend heavily on cyber and space-based systems.

NATO is highly dependent on electronic and, in particular, space assets to support C2, provide data, and enable precision strike operations. If those capabilities are denied, NATO units will have to revert to old techniques and in some cases, legacy or abandoned technology. When faced with degraded performance it is common to blame the equipment, the operator and/or even the weather. This leads to an acceptance of the idea that some systems and some capabilities are unreliable, when in reality they may be under attack. We need to improve critical analysis of service interruptions and recognition of malicious activity. NATO operations will be affected by the loss or degradation of space and electronic assets and, therefore, there must be alternatives to these capabilities when degraded or denied.

'Do you understand how dependent you are on space systems and space capabilities?'

NATO's space capabilities must be protected and this can be accomplished in several ways. The first method is diversification. Reliance on a single system is risky, and single points of failure are key targets for the opponent. Global positioning system (GPS), positioning, navigation, timing (PNT), and precision delivery of munitions and manoeuvre all depend on GPS. The European Galileo system provides a similar service that has comparable accuracy making it a very good option for redundancy. Likewise, celestial navigation was commonly used before GPS and there is no reason why that technique cannot be used today in an automated manner. Inertial navigation provides yet another viable backup. Voice and data communications should not rely solely on space-based capabilities, but instead follow the 'PACE' philosophy which requires securing Primary, Alternate, Contingency and Emergency systems spread across space, air and terrestrial modes. Another element that establishes diversity, or dispersal, is proliferation. Where in the past we have relied on a small number of large and complex space systems,

for practical and economic reasons, in the future we will employ larger numbers of small, inexpensive and easily replaceable spacecraft to provide NATO a more resilient space-based services posture.

The second category is developing space systems and capabilities that can physically protect or even defend themselves. The next generation of missile warning satellites will contribute to their own defence, and integrate into a larger architecture that includes surveillance, IW, C2, and intelligence specifically designed to defend those space capabilities against attack.

Thirdly, space systems must be enabled to defeat offensive activity. NATO must be prepared to find and destroy, or at least degrade, adversary offensive space systems when necessary before they can be used in an attack. This ability applies across every domain. The ability to do so will contribute to deterrence, especially when it is evident that NATO can respond in the time, place and manner of its choosing and not merely with reciprocal strikes in space. It is important to note that, while NATO depends heavily on space-based assets, many of NATO's potential adversaries do not depend on space capabilities in the same way. A reciprocated attack on their space capabilities, therefore, may not have the same level of impact that is does on us. To help alleviate any ambiguity or questions, NATO should openly state in policy that it will respond to an attack on space assets in any way, and in any medium it deems appropriate. Creating uncertainty about the nature and severity of possible consequences can put potential adversaries at a substantial disadvantage that ideally is enough to deter aggression in space or any other domain.

Offensive and defensive operations alone are not enough. NATO must also establish more rapid and effective cooperation in space. The United States is taking steps to promote this cooperation by making security classification guidelines more rational, reasonable and better-suited for combined, coalition and Alliance operations. Greater sharing will promote transparency that makes actions easier to attribute, and in turn influences nations to be less provocative, because they will no longer be

able to act with anonymity. As we increase cooperation, space-faring nations will need to establish a set of agreed-upon norms for behaviour in space and be prepared to challenge those who do not adhere to these norms with the full diplomatic weight of the Alliance.

'We need to take a 360 view of where the risks and threats are.'

In an effort to enhance response times, NATO is currently looking into the facilities and procedures available for aircraft cross-servicing and the use of Air Power in protecting reception, staging, onward movement (RSOM) and integration of reinforcements. In addition, modern technologies have blurred the distinction between the 'front' and the 'rear' in war, and, therefore, additional resources should include protection to logistical lines throughout NATO's area of operations.

As resources continue to grow within NATO, training should be focused on full-spectrum operations to include GBAD systems, degraded environments and the need for increased Strategic and Political participation. In the seven years since Operation UNIFIED PROTECTOR in 2011, exercises have been used to fix part of this paradigm, primarily in NATO Response Force training. Article 5 (collective defence) exercises have been, and in the future will be, organized like this year's TRIDENT JUNCTURE in Norway and the North-Atlantic becoming more complex and directed at achieving a better understanding and being better able to deal with the uncertainty, complexity and ambiguity and how to cooperate with civil authorities. More time should be devoted to training to capacity and on the Alliance's ability to operate seamlessly as a single entity.

In future, politicians need to be involved in wargaming, not just within NATO but also in individual nations because decision-making and threat perception vary greatly from nation to nation within NATO. The speed of modern aircraft allows little time to form committees or hold meetings to formulate a response. Those responsible must be decisive and agile. Therefore, politicians should join in the training at the strategic level to better understand the challenges and provide pre-approved criteria and guidelines for action to military leaders where possible. In addition to dealing

with threats from a Strategic and Political perspective, senior leaders should understand that Strategic Communications with both our populations and our adversaries are vital. Delivering the correct narrative will be critical to obtaining the public support vital to mission success.

An additional problem is the lack of tactical level training. Training is historically conducted based on past experience, from predictable scenarios and seldom against realistic and uncertain adversaries that we predict will roam the future battlefield. To combat this, a system is required which constantly scans the operational environment and makes changes to exercise scenarios based on current and developing trends, and that helps define the blue force's scenario and, thereby, developing Air Power more likely to be multi-domain, joint, combined, and inter-agency.

In order to achieve battlefield superiority, streamlined decision making, realistic training and safe and secure lines of communication both in space and on the ground, it is important to exploit technology. The fourth Industrial Revolution will help innovate our operational logistics support enabling a 'just-in-time' supply chain. This supply chain will have a very small footprint, with spare parts readily available that do not need warehousing, and is achievable with little investment. Technology, for example, could also permit a maintainer, located anywhere, to send data to a 3D printer, perhaps collocated with an aircraft, to build required parts anywhere in the world. This same maintainer can then follow the maintenance or repair action virtually and even certify the maintenance actions using Blockchain. Industry plays a vital role in making this scenario a reality.

One agency that can assist in leveraging technology is the NATO Industrial Advisory Group (NIAG). The NIAG is working on ways to speed up acquisition processes and is able to reach back to approximately 5,000 companies in various member states and provide advice with a turn-around time of weeks instead of months or years. This has the potential to help eliminate extended acquisition programs such as those for the Alliance Future Surveillance and Control replacement for the E-3A, and the NATO Air Command and Control

System (ACCS). These systems share a flaw common in military procurement, the development and fielding takes far too long. In fact, many of the software engineers who conducted initial development for ACCS have already retired, which will present sustainment challenges going forward. The NIAG is more agile and accessible because it is already within NATO, so external contracting processes do not slow down work.

Conclusion

'We don't know when Day Zero will come, we don't know how it will come, we don't know where it will come or whether it is already here.'

Only through in-depth and focused examination can we begin to try and disperse the Fog of Day Zero and assess where Air and Space Power contribute to the solution. From the panel discussions we can conclude that, as ready as NATO is, there is still work to be done. NATO must focus on three areas: defining threats and attacks, increasing NATO's operational readiness, and protecting forces to enable an appropriate response.

NATO must better define effects, conditions and criteria that enable malicious non-kinetic activities to be classified as an armed attack and be able to respond using all the instruments of power, at a time and place of its choosing. NATO must continue to devise ways to ensure that Day Zero does not become Day One, or if deterrence fails, be ready to act on Day One with an adequate and proportional response.

An appropriate level of readiness is more achievable when we conduct more realistic exercises. The exercises must address challenges, such as operating in a degraded environment, relying less on centralized C2 and on defending NATO assets and territory from both peer competitors and VEOs, and everything in between. NATO must reassess its Force protection posture, the hardening of facilities and dispersal of assets and capabilities for greater survivability and resilience. Additionally, NATO must also develop methods of providing cybersecurity to ensure networks, networking and networked assets are survivable and redundant. Finally NATO must improve, as well as shorten, logistical tails and acquisition timelines by leveraging our industry partners and embracing technology.

The advantage NATO forces previously enjoyed over near-peer competitors is no longer as wide as it once was. NATO's ability to respond quickly to,

and be successful in, an Article 5 confrontation that could start one second from now is better than it's ever been before, but it's just not fast enough. NATO must strive to regain the capability advantage and reduce response times to prevent the significant losses that could occur in a campaign by failing to recognize that hostile activity is underway.

NATO must continue to improve how it conducts joint operations, including embracing new domains (such as cyber and space) as they mature. NATO must also adapt to a threat that is not unidirectional, as in the Cold War, but rather multi-dimensional. The current threats facing NATO come from outside and within the Alliance's borders, from space and cyberspace and target areas ranging from traditional military strongholds to critical infrastructure and soft targets in our homelands. Cyberspace has been recognized by the Alliance as a warfighting domain; it is time for Space to be as well. Modern adversaries particularly peer and near-peer competitors, are building Space and Counter-space capabilities, so Space will become a warfighting domain whether NATO wants to acknowledge it or not; the longer we wait to do so, the farther behind we will be in defending the broad set of capabilities upon which we have become inextricably dependent.

After decades of counter-terrorism and small-wars, NATO must execute a paradigm shift. The enemy might not attack 'force on force', or even kinetically at all. Attacks are more likely to take place in the information domain, against the financial sector or on any of a number of critical services or combinations thereof. An effective response from NATO will depend on early recognition and rapid countermeasures to defeat them before they cause irreparable damage or the death of Alliance citizens, or weaken NATO against armed confrontation. The ability to execute detection, prevention and defensive counter-action will depend more than ever on the cohesion of the North Atlantic Council and the delegation of appropriate authorities to SACEUR. This may require some high-level discussions in Brussels about the interpretation of the Washington Treaty Articles in light of new technologies and threat vectors, and our Alliance would be well-served if those discussions began sooner rather than later.

JAPCC invites you to attend the:

2019 | AIR AND SPACE POWER CONFERENCE

Shaping NATO for Multi-Domain Operations of the Future

8–10 October 2019, Messe Essen, Germany

Reserve the date in your calendar!

Watch out for Conference Updates: www.japcc.org/conference

Joint Air Power Competence Centre

von-Seydlitz-Kaserne
Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org/conference