Joint Air & Space Power Conference 2016

Preparing NATO for Joint Air Operations in a Degraded Environment

4–6 OCTOBER 2016

READAHEAD

Joint Air Power Competence Centre

This page intentionally left blank.

Preparing NATO for Joint Air Operations in a Degraded Environment

This page intentionally left blank.

READAHEAD

Preparing NATO for Joint Air Operations in a Degraded Environment

Joint Air and Space Power Conference 2016

Joint Air Power Competence Centre

Acknowledgements
This read ahead is a JAPCC product realized in collaboration with the authors of the essays contained herein. The JAPCC would like to thank the numerous authors who took the time to contribute to this product in an effort to advance this topic for discussion within NATO.

Disclaimer
This publication is a product of the JAPCC. The views expressed in this work are those of the authors. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO), and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

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

[M] Denotes images digitally manipulated

Moderator's Foreword

Dear Reader,

It is my great privilege and pleasure to act as the moderator for this year's Joint Air Power Competence Centre (JAPCC) Conference, which will take place over the period 4–6 October 2016 in Essen, Germany. The theme for this year's conference is 'Preparing NATO for Joint Air Operations in a Degraded Environment.'

This is a broad topic and is one that has perhaps not had the visibility it deserves in recent years. Recent contemporary operations in Iraq and Afghanistan have been conducted in environments where our adversaries, though lethal and innovative in some areas, lacked the technical sophistication to deny us the full spectrum access we need in order to successfully bring air power to bear. Put simply, modern air power is a high tech business and it is utterly reliant upon the ability to gain unrestricted and assured access to the entire electromagnetic spectrum, space, and, increasingly, cyberspace. Environmental degradations, be they imposed by an adversary or created by natural phenomena, have a massively debilitating effect on the ability to successfully project air power across all its roles.

When I began my military flying career during the Cold War, NATO took its air power preparedness extremely seriously. We anticipated degraded operating environments, both in regard to electronic counter-measures and to the potential need to continue to operate in a nuclear, biological or chemical environment. We equipped our forces accordingly and trained for the worst case scenario. After years of coalition operations in uncontested (and uncongested) environments, we must now ask ourselves if NATO has taken its eye off the ball in this regard.

In the pursuit of this question and in preparation for the upcoming Conference, the JAPCC offers the following food-for-thought pieces for your consideration. Designed to provoke thought and incite debate, the essays are written by leading thinkers from the military, industry, NGOs and academia and address various themes that should underpin any thorough discussion of preparing to operate in a degraded environment.

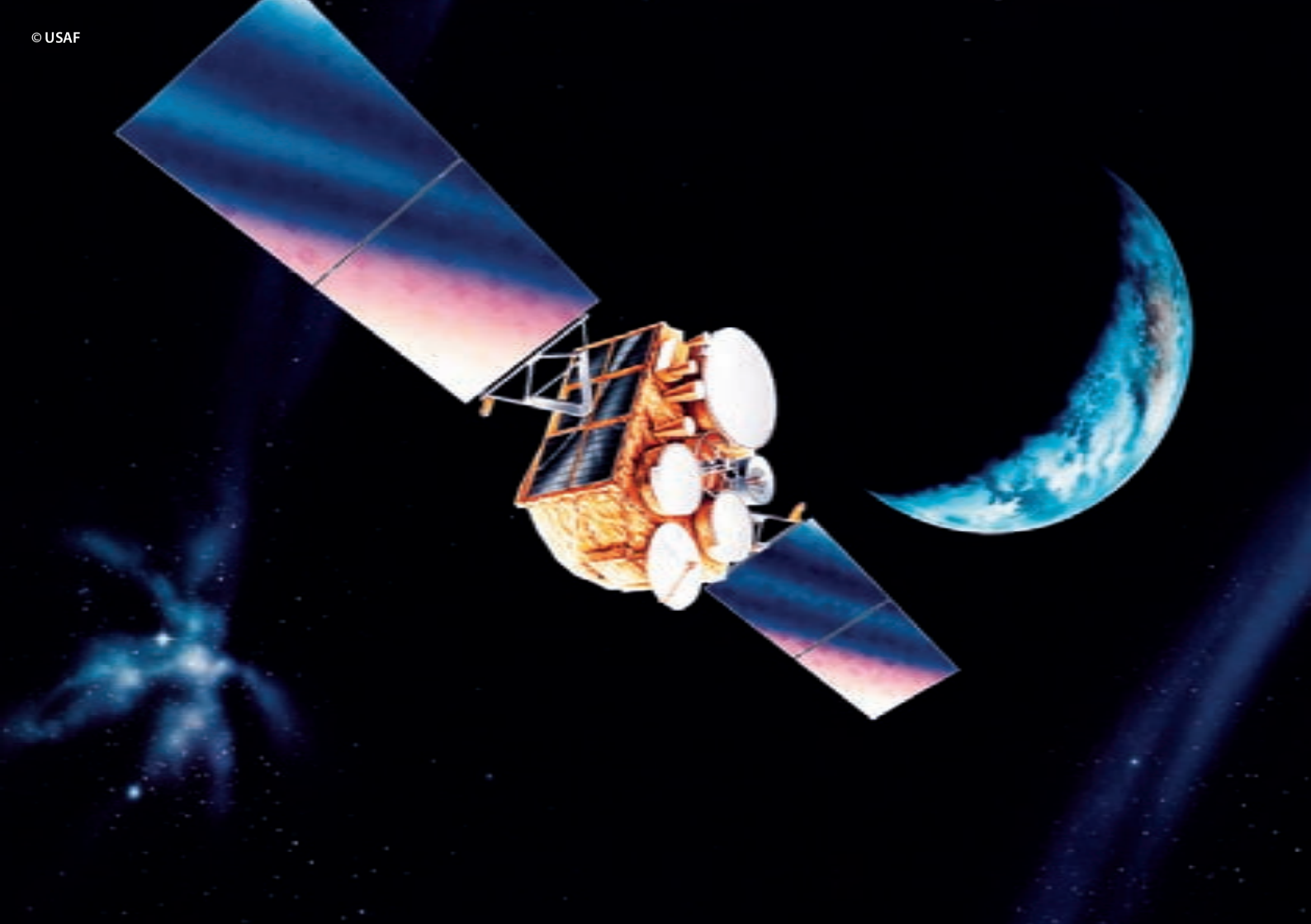
In seeking to address the constraints NATO's air power assets might face in a degraded environment, the JAPCC staff has also assembled a multi-disciplinary, multinational team of distinguished speakers and panellists for this year's Conference. Crucially, the conference seeks to consider what NATO could and should do to improve its preparedness in this regard. This is your opportunity to contribute!

I very much hope you will join us at Essen in October for what promises to be a fascinating and important two days.

Ian Elliott
Air Commodore (ret.), GBR AF

This page intentionally left blank.

Table of Contents


© USAF

Are We as an Alliance Prepared to Operate in a Degraded Environment?

1

Lieutenant General Joachim Wundrak, DEU AF

Since we have been involved in Afghanistan, we have unintentionally let certain aspects of our overall mission capability degrade as we've focussed on developing those skillsets we needed to be successful in that environment. Specifically, I do not think NATO is training as hard as we used to for situations that will require us as Airmen to be flexible and innovative to counter the challenges of a near-peer adversary.

When the JAPCC team briefed me about the topic for the upcoming Air and Space Power Conference, I was very supportive of the proposal. If we do not address our ability to operate in degraded environments through equipment procurement and by training at the most realistic levels we can manage, we may find future conflicts do not end favourably for our way of life.

You could ask why are we addressing preparing for degraded environments instead of contested environments or why not look more specifically at the concept of preparing to defeat an Anti-Access/Area Denial (A2/AD) environment. While both these are essential conversations, from my perspective, A2/AD is a subset of contested, which itself is a subset of degraded. So, an environment could be degraded as a result of an adversary

contesting that environment. That adversary could use an A2/AD strategy to contest the environment. The use of degraded as opposed to contested opens the discussion to situations potentially caused by a wide variety of factors, not just those caused by enemy actions. However, as a senior NATO air commander, I am personally focussed on the impact that A2/AD might have on our ability to operate and think we need to pay particular attention to the A2/AD challenge.

The term A2/AD itself is relatively recent, but the concept of controlling access to a battlespace or controlling an enemy's freedom of movement within battlespaces is as old as human warfare. I won't go into a long history of A2/AD here, but I do want to briefly address why today's A2/AD is not what our predecessors dealt with. From an air perspective, the modern A2/AD area is built on the foundation of an Integrated Air Defence System, or IADS, and uses associated systems to extend their range. Modern IADS have ranges in the hundreds of miles and are supplemented by long-range surface-to-surface weapons and non-traditional weapons (such as cyber-attack) that can reach well beyond this distance. Thus, the adversary now has the ability to hold at risk our assets deep inside our territory without ever leaving their territory. This is Regional A2/AD, or A2/RD – an ability to deny access and control action across an entire region, which is a greater problem by several orders of magnitude.

What concerns me about A2/RD is that we may not have superior technology available to us – stealth and precision weapons may not be enough, even when coupled with the most modern TTPs we can employ. The A2/RD 'bubble' is so large that our current long-range weapons are simply not long-range enough or are too easily defeated by modern systems. Of particular note, the threat is not static – it is persistently adapting to match our capabilities. We cannot remain complacent and assume that our capabilities will remain effective against the changing threat.

Regional A2/RD is here to stay and, as those charged with the collective security of our Alliance, we must be ready to counter its effects.

What is the way forward for the Alliance? How do we ensure we are ready to counter the effects of A2/RD? We must start now to prepare to operate in an environment that features A2/RD as the centrepiece of our adversary's posture. Preparation, in my mind, has two key facets – personnel and equipment. Of course, these two are intrinsically linked – you must have the right equipment for the personnel to use and they must be capable of using that equipment to create the desired effects.

At the core of the problem is NATO's failure to continue to develop and acquire the technology required to counter modern IADS and related systems. Of course, industry is primarily charged with the development of such systems, but we as NATO's militaries have not asked them to give us solutions to this problem in recent years. Without a demand signal, industry will not invest in the necessary systems development. Without investment in research and development, the technologies we need will not be available to us. Of course, the question then becomes 'What technologies will defeat the A2/RD systems?' However, there are many other questions that must be addressed: Manned or unmanned platforms? Cyber or real-world weapons? Large numbers or highly technological? Or a combination of the two and, if so, in what ratio? How do we handle increasing levels of automation in weapons systems? How do we make systems resilient?

The other side of preparation is the personnel. I believe that we in NATO have the most capable and motivated airmen in the world. Given the proper equipment, resources, and sufficient training, they will not let us down. It goes beyond buying the enough of the right equipment – our personnel need to have the right kinds of training to be effective with that equipment. The questions that have to be answered in terms of personnel are also significant: How many personnel and in what kinds of

organisations? What ration of combat versus support forces? Whose responsibility is supporting deployed forces in the event of a conflict? How much live versus how much virtual training? How much training versus how much exercising? How do we make personnel resilient?

Of course, some of the questions I have raised here are not specific to the A2/RD environment but they are all questions that must be answered if we are to succeed in countering the A2/RD threat. As NATO's air leaders, we must debate these and other questions and determine what the right answers are to ensure our collective security while facing an A2/RD world. I don't even know all the right questions, but I know if we don't take the opportunity this 2016 JAPCC Conference brings to start this conversation, we may not be ready when the moment comes.

Lawfare: Lowering Legal Thresholds Because of a Degraded Environment?

11

Colonel Dr. Joop Voetelink, NLD AF

In accordance with the principles of the rule of law, all military operations have to be carried out in full respect of national and international law. The growing focus on legal aspects of operations has paved the way for a practice referred to as lawfare: the use or misuse of law as a means of achieving military objectives. Although today misuse of law is a common tactic in asymmetric conflicts, it can be utilized in traditional warfare as well and can ultimately lead to a situation in which an opponent is denied effective use of its advanced sensors and weapon systems. The question then is, given the degradation of the operational systems, do we still have to comply with the law, in particular with the Law of Armed Conflict (LOAC)?

Of course, the answer is clear and simple: even in a degraded environment, LOAC continues to apply in full and legal thresholds will not be lowered. Degradation may, however, impact the application of certain rules. This paper takes the rule of law as starting point for explaining the nexus of law and the conduct of military operations. It then focuses on the instrumental role of law and the practical use of LOAC in the targeting process.

NATO-member states, like many other modern sovereign states, are built on the principles of the rule of law, as the preamble of the North Atlantic Treaty affirms. Even though the rule of law concept will sound familiar to most of

us, it may be hard to give a clear description of it. Perhaps not surprising, if one cares to take a closer look at the UN Secretary General's definition:

The rule of law refers to a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.[1]

That one hurts, does it not? Let me put it in more simple terms: rule of law means that a state must enact laws and that the state itself, its government and officials, just as its citizens, are accountable under these laws.

The concept of the rule of law is important to the armed forces as they are key state organs, tasked with providing security. In addition, many present-day crisis management operations even include rule of law elements tasking the participation forces to support the rule of law in the host state. E.g. in 2011 NATO established the NATO Rule of Law Field Support Mission (NROLFSM) in order to support rule of law activities in Afghanistan.

In terms of the conduct of international military operations, the rule of law requires all military action to have an adequate legal basis under international law and, subsequently, that all activities are carried out in accordance with the law, e.g. LOAC and/or human rights law, depending on the type of operations. NATO operations are all carried out within this broad legal framework as is reflected in policy, as well as operational documents, such as the Oplan and Rules of Engagement, which, inter alia, further detail the legal aspects of a specific operation.

Obviously, law and in particular operational law matters to the military and permeates every level of contemporary operations, even to the extent that it can become instrumental in carrying out a mission. The latter notion was captured in the term lawfare, which is described by a former US Air Force lawyer as: 'The strategy of using – or misusing – law as a substitute for traditional military means to achieve an operational objective'.[2] The Counter-Insurgency operations ISAF carried out in Afghanistan provide a telling example of conduct of lawfare using law as a means to achieve a certain goal. As this type of operation focuses on the civilian population, it is critical to create a safe environment. Consequently, military commanders were instructed to transition from combat operations to law enforcement as quickly as possible and, based on experiences in Iraq, ideas were developed to criminalize the insurgency. Insurgents were, if possible, to be captured and then transferred to the Afghan criminal justice system for prosecution. In this way, Afghan law was a tool to remove insurgents from the battlefield while at the same time making clear to the local population that insurgents were ordinary criminals under their national laws.[3]

Misuse of law to achieve a military objective is a common tactic in asymmetric warfare by weak or technologically less advanced parties to armed conflicts. Generally, they try to level the playing field by exploiting their opponent's commitment to comply with LOAC. For example, they know their opponent will not easily attack a dwelling as he knows it is a protected object under LOAC and fears that even lawful destruction of that property and possibly civilian casualties may suggest he operates in total disregard of LOAC.

Emerging technologies may offer new opportunities for equally advanced warring parties to leverage the LOAC in traditional warfare. For example, suppose a party to a conflict is capable of intercepting data received by and sent from their opponent's surveillance or GPS satellites and, subsequently, can stealthily manipulate that information so that a protected object under LOAC, like a hospital or church, appears to be a genuine military target. It

may cause the other party to refrain from using the satellites and other connected systems out of fear of being accused of deliberately breaking LOAC.

Not all tactics and techniques that have the potential of degrading the opponent's operational systems can be labeled as lawfare, of course. They may, however, seriously affect the ability to gather sufficient and detailed target information and to launch a precision attack. Today NATO's whole targeting process explicitly builds on reliable information and precision-guided munitions. LOAC is part and parcel of that process. This raises the question whether degradation of the operational systems lowers any legal thresholds. In other words, do we still have to comply with the full range of LOAC-rules when systems have become compromised to the point they are unreliable and cannot guarantee the object to be attacked is a lawful, military target?

The starting point for answering this question is the knowledge that LOAC had been around for quite some time now and is built on well accepted, general principles, such as humanity, military necessity, distinction, and proportionality. Furthermore, the bulk of the conventional rules relating to the targeting process are set out in the 1949 Geneva Conventions and the 1977 Additional Protocols. So, even if degradation of our operational systems sets us back a couple of decades, the same set of rules continues to apply. The Falklands War (1982) and the Gulf War (1990–1991), for instance, were both fought within a legal framework that is not much different from the one that is applicable right now in the fight against ISIS. Of course, new conventions impacting air operations have been drafted, such as the 2008 Convention on Cluster Munitions, and customary law has further developed, but the targeting process at large is still governed by the same core principles and rules.

In addition, it must be acknowledged that armed conflict is all about forceful submission of an opponent. It is inevitable that people perish in

the course of wars, even innocent civilians. Something that is implicitly accepted in LOAC: there is no unconditional rule penalizing incidental death of civilians. Nevertheless, there is a clear distinction between the civilian population and combatants and between civilian objects and military objectives (the principle of distinction) and the civilian population and their property must be respected and protected at all times. As a consequence, they may never be the object of attack and parties to an armed conflict 'shall direct their operations only against military objectives' (Article 48, Additional Protocol I, the Basic Rule). This rule has been at the heart of our targeting process for decades.

Although civilians cannot be the object of an attack, they can become victims of an attack directed at a military target. Under LOAC this is acceptable, but only to the extent it is proportional. Therefore, warring parties have to reduce collateral damage, which requires that an attack is cancelled if it is expected to cause civilian casualties or damage to civilian property which would be excessive in relation to the concrete and direct military advantage anticipated (principle of proportionality).

This principle is the reason we conduct an elaborate proportionality analysis using the Collateral Damage Estimation methodology to reduce the likelihood of civilian casualties. It is clear that when technology fails us the risk of collateral damage will increase significantly. That does not necessarily mean attacks are forbidden on principle. The next step for a commander is to balance the potential collateral damage with mission accomplishment, or in legal terms: with the concrete and direct military advantage anticipated. A host of factors come into play, such as the availability of specific munitions, the type of conflict, weather condition, etc., which all have a different weight.

At the end of the day, a commander may have to come to the conclusion that, because of the necessity to take out a specific target and a lack of capabilities, a higher number of civilian casualties has to be accepted

under the specific circumstances. Although that decision may well be lawful under LOAC, it will be a hard sell to politicians and the public who have all grown accustomed to extremely low levels of collateral damage. It may even result in a prohibition on attacking certain targets, as happened during the Vietnam War, when the White House set strict limits on the bombing campaign against North Vietnam.[4]

As our armed forces are part of societies built on the rule of law we are, rightly so, extremely conscious of law in general and of LOAC in particular. That latter field of law obliges us to respect and protect civilian life and property even in times of armed conflict. Nevertheless, LOAC accepts collateral damage and incidental civilian casualties as long as it is not excessive. Since Operation Desert Storm, precision weapons have become widely available and are continuously being improved resulting in an ever decreasing number of civilian casualties. Protection of civilian life is paramount now to a degree it even seems unethical to accept any loss of civilian life. Opponent are exploiting that commitment, making military commanders as well as politicians even more reluctant to accept civilian casualties. System degradation will cause us to reconsider the whole question of proportionality within the existing legal framework, possibly resulting in a sharp rise of collateral damage. Although lawful, it may be hard to convey that message to the public.

Colonel Voetelink is Associate Professor of Military Law at the Netherlands Defence Academy. Colonel Voetelink has previously served as a Ground Operations and Personnel Officer at Air Force units in Germany and the Netherlands. After completing Dutch law training, he served as a lawyer in various legal positions at the Royal Netherlands Air Staff. In 2012 he obtained his doctorate on this subject at the University of Amsterdam.

1. UN Doc. S/2004/616, Report of the Secretary-General on the Rule of Law and Transitional Justice in Conflict and Post-Conflict Society.
2. Charles J. Dunlap, Jr., 'Lawfare Today', Yale Journal of International Affairs 2008, p. 146.
3. Joop Voetelink, EvBO: Evidence-Based Operations How to Remove the Bad Guys from the Battlefield, Journal of International Law of Peace and Armed Conflict 4/2013, p. 194–201 <papers.ssrn.com/sol3/papers.cfm?abstract_id=2400965>.
4. Frans P.B. Osinga & Mark P. Roorda, From Douhet to Drones, Air Warfare and the Evolution of Targeting, in: Targeting: The Challenges of Modern Warfare, Asser Press 2016, p. 42.

© NATO

© US Air Force, Master Sgt Ben Bloker

An Italian Perspective on Preparing NATO for Joint Air Operations in a Degraded Environment

III

Lieutenant General (ret.) Leandro De Vincenti, ITA AF

Despite there being no clear and/or approved definition of the term 'Degraded Environment' in any military glossary, there is nevertheless a strong – albeit rarely voiced – awareness of the potentially negative impact and disruptive effects that such a 'condition' may have on Joint Air Operations by almost every Political/Military leader. Even though the term 'Degraded Environment' is largely undefined, the general understanding of the potential 'Threat' posed by it is conceptually absolutely clear, in that the ability to continue Air Operations as planned is compromised, thus potentially jeopardising the accomplishment of the entire mission.

Degraded environment threats are undefined and there are a variety of reasons why they may arise in the operational arena, from those caused by enemy actions to those caused by natural factors and which can impact in all operational fields. What is clear is that, despite being undefined, unpredictable and in some way unknown, a 'Degraded Environment' always represents a threat that will undoubtedly impact and affect military operations across the entire spectrum of warfare. Therefore, 'How to prepare NATO for Joint Air Operations in a Degraded Environment' is complex and there are no easy and unique answers.

This paper offers some possible considerations from where to start the discussion of where and how to prepare the NATO Command and Force Structure for such operations.

Recent contemporary operational experiences (Afghanistan, Libya, Iraq, Syria…) have already forced NATO to move away from its 'classical' approach to Operations and have driven the redevelopment of Tactics and Doctrines. New 'types' of combatants have entered into a completely 'new' and 'chaotic' operational environment where opponents feel free to follow unusual and unexpected 'lines of operation'. This can disrupt previously consolidated tactics, procedures, rules, protocols and international 'conventions' and can limit and condition freedom of action and manoeuvre for 'official governments' within a coalition. This trend will likely continue to accelerate, driving a need for new Doctrines as a result of the large variety of possible means of degradation in operational scenarios.

The unavailability of a Satellite network would, of course, have a negative impact on many individual capability areas such as Strat Com, C2, Civil Military interaction, Space domain, but, if coupled with a degradation of the Electro-Magnetic spectrum and in the Cyber domain, the resulting dramatic reduction in environmental quality seems very likely to be capable of causing the collapse of all previous classical 'assumptions' about the use of Air Power and related weapons.

So, how to approach the 'preparedness' of NATO?

To consider and study, individually, the very long list of possible areas likely impacted by a Degraded Environment situation, whether caused by specific enemy action and/or by any other natural environmental factors, would be a 'mission impossible'! Rather, it may be better to consider a different way of 'how' to approach the Planning Process of the Operation

from the very beginning, reintroducing additional and incremental planning factors similar to those in use before the advent of modern Information Technology. This might be considered as some sort of a 'back to the future' game.

In aiming to 'mitigate' rather than to 'solve' the wide range of possible negative impacts, a first tentative option might be to pre-plan an equally vast range of preliminary measures when starting the mission planning process.

In fact, the availability of a more robust and more comprehensive Rules of Engagement Catalogue, taking into consideration a wider range of different options related to different levels of environmental degradation, may set the conditions for a preliminary acceptance of possible higher risk of friendly losses and civilian casualties because of precision and accuracy reductions in a degraded environment. This might prevent, or at least limit, the subsequent effect on StratCom messaging and the natural political aversion in this regard. Such Rules of Engagement should be proposed by Operational Commanders and approved by political Authority after much deep legal assessment.

Redundancy in pre-planning and prioritization of backup plans as part of the operational planning process may also help mitigate unexpected situations which arise in a Degraded Environment, especially if combined with a significant reconsideration of the balance between deliberate and dynamic targeting. In fact, while the first (deliberate targeting) involves the generation of an extensive detailed Target Folder, possibly prepared well in advance and when still in an unconditioned and uncontested EMS/EW and Communications environment, the second (dynamic targeting) strongly demands significant last minute ISR&COMM capability because of the lack of a detailed Target Folder of 'unpredicted' new targets.

Additionally, a different approach to the formation of the Joint Prioritized Target List (JPTL), including a different and wider list of Targets combined with different types of Weapons to generate a sequence of 'graduated' backup JPTLs, would offer an additional possibility to select a set of TGTs and related Weapons according to the different levels/types of degradation. Doing this would help sustain the Air Operation, even if with some limitations.

For example, shortening the C2 chain and relying on different standing orders may be an additional technique to maintain the basic principle of Air Power, which strongly demands Centralized Control-Decentralized Execution. Prioritized action and alternative courses of action, developed well in advance, may also provide effective mitigation to some degradations.

What we can assume is mandatory is the investment of additional effort and the formation of a new mindset in approaching and performing the Operational Planning process; this must take into consideration the many possible different options which arise from scaled levels of Environmental Degradation. Nevertheless, none of the above mentioned mitigation measures will alone represent the solution. A combination of all the above mentioned proposals could represent a starting point to approach the way to prepare NATO for thinking about a new Doctrine on how to prevent the potential constraining of Air Operations in a Degraded Environment.

Lt Gen (ret.) Leandro De Vincenti served as Commander of the NATO 5th Combined Air Operations Centre, Poggio Renatico, ITA. During Operation Unified Protector, he served as Chief of Staff, Joint Force Command, Naples. In addition to accruing many years of flying experience in the Typhoon and AV-8B, EH-101 and NH-90, he has also served as the Chief of Staff, NATO HQ Naples and has commanded the 9th Wing of Grazzanise in addition to multiple staff tours in various Headquarters.

Agile Command and Control in a Degraded Environment

IV

Rear Admiral (LH) Thomas Ernst, DEU N,
Commander, Maritime Air NATO

The Allied Maritime Command (HQ MARCOM) is prepared to deliver Command and Control (C2) of the full spectrum of joint maritime capabilities. MARCOM is a static headquarters, and plans, conducts and supports joint maritime operations of the Alliance. It maintains comprehensive situational awareness throughout NATO's maritime area of interest and is ready to execute C2 of a maritime heavy Smaller Joint Operation (SJO-M), and to act as the Maritime Component Commander (MCC) to support a Major Joint Operation (MJO). These generic requirements set the stage for how MARCOM must operate in order to deliver effect. From a maritime air perspective, we are dealing with several inherently challenging intersections with regards to C2. We are interacting daily with national entities and assets that operate under national command. This removes the flexibility that comes with having assets under NATO OPCON. We are also dealing with the intersection between NATO intelligence interests and national intelligence interests – which are mostly the same, but exist under different release criteria.

However, piercing through these challenges, it is the ambition of COMMARAIRNATO to be able to execute clear C2 from the static HQ MARCOM,

interacting with the other entities of the NATO Command Structure (NCS) such as AIRCOM, LANDCOM, and Joint Force Commands, with NATO Force Structure (NFS) elements such as NATO Airborne Early Warning & Control (NAEW&C), STRIKFORNATO and other maritime High Readiness Force Headquarters (HRF(M)), further out to the respective national headquarters, and finally out to the maritime air assets flying within the national and NATO areas of interest. This communication must be carried out through a degraded environment at MARCOM, as well as in degraded conditions for our assets operating in the respective areas. This constitutes a major challenge for an agile command and control – in any type of condition and environment.

Degraded Environments

The conference will focus on operations in a degraded environment that results from conditions imposed on us by an opponent that aims to contest that environment. Such environments are coming to the forefront of operational planning based on recent experiences as well as new technologies. One emerging focus consists of doctrines and technologies under development and employment that facilitate Anti-Access and Area Denial (A2/AD) strategies. These become apparent through new types of warfare and weapon systems. In a maritime sense, we see the employment of submarines and mines for area denial, and the operational and strategic placement of Coastal Defence Cruise Missiles (CDCM) for anti-access. In the maritime air domain, Alliance assets will be vulnerable to new and capable Surface-to-Air Missile (SAM) systems along the coast, impeding the efficient execution of maritime air operations. The revival and emergence of hybrid warfare is also shaping plans and capabilities. From a maritime perspective we see extensive underwater research programs underway that can lead to disruption of underwater communication cables, we see the use of civilian and merchant vessels for mine laying and obstruction of harbours, and we see civilian fishing vessels carrying

SAM threats. These factors are shaping and hindering our maritime and maritime air operations in times of crisis and beyond. Additionally, after more than a decade of Alliance operations in Afghanistan, we became accustomed to operating without air threats against a materially inferior opponent. In the future, we must also prepare to meet a peer opponent. A degraded environment can become evident through degraded or absent satellite navigation, through executing ISR missions with an opponent jamming all-weather Synthetic Aperture Radar (SAR) sensors, and of course, the degradation of communications with our opponent significantly hindering the effective and efficient use of the electromagnetic spectrum through advanced Electromagnetic Warfare (EW) operations. These are just some of the conditions NATO is likely to face, on a small or broad scale.

ACO Forces Standards

The ACO Forces Standards Volume I (General) states the generic requirements for Alliance operations and entities, through the Main Capability Areas (MCA). This short paper focuses on the centrepiece of these, namely Command and Control (C2).

NATO has clear and explicit standards that must be met in order to execute C2 in Alliance operations to meet NATO's level of ambition. Alliance headquarters must be ready to exercise C2 for Article 5 contingencies, to contribute to efficient conflict prevention, and to execute crisis management including Non-Article 5 Crisis Response Operations (NA5CRO). NATO operations will encompass high- and low-intensity combat and any environment: we will operate in extreme conditions, to include desert and arctic areas of operations, in areas contaminated by Chemical, Biological, Radiological and Nuclear (CBRN) weapons and waste, NATO will operate in spite of cyber-attacks and whilst experiencing Electronic Warfare (EW) degradation. Albeit a non-exclusive list, these factors are only a few of the

challenges we must be ready to meet from a maritime and maritime air C2 perspective. Not only will the maritime component interact with the other components, specifically and likely more regularly with the air component than with any other, but also integrate our forces closely for the establishment of an Integrated Air and Missile Defence (IAMD). As an additional example, the maritime component will work in close collaboration with the air component in the Targeting Process, which demands close coordination and exchange of sensor information, and an overall integration of assets and information for a seamless common operational picture. As a maritime headquarters we are required to ensure communications stability, interoperability and coverage to other relied upon entities. This leads to demand for secondary and tertiary communication solutions facilitating ongoing operations, as well as sound operational contingency planning for future operations.

More specifically for maritime air units there are requirements for secure and interoperable voice communications – HF, VHF and UHF – in accordance with established standards in MC-195. Modern aircraft are also required to be able to transmit sensor information through secure satellite communications. The Alliance demands a wide array within the sensor portfolio for maritime aircraft, in order to mitigate the various conditions at sea and to facilitate a collaboration of sensor information in cases where one sensor is not sufficient for various reasons – for example having the sensor partially or fully degraded by the opponent (e.g. SAR jamming).

So What Does This Mean to Our C2?

Operations in a degraded environment as already described will be a challenge. The ambition is simple and focused, but hard to achieve, and the requirements are challenging to meet in such a likely operational environment.

The goal for MARCOM is to execute C2 of its forces in any environment, even if degraded conditions for the HQ exist at its static location. In order to mitigate this, an alternate operations centre has been set up for redundancy, with backup communications systems. COMMARAIRNATO has the ambition to execute C2 through his established 'Maritime Air Network' as described in the Alliance Maritime Governance paper of 2016, and will interact closely with all national maritime air entities. The inherent dispersal of units and the diverse geographic location of the Maritime Air Control Authorities (MACA) will likely mitigate a specific effort to degrade C2 message traffic and communications in the maritime air domain. There is a weakness that runs through the entire NCS, namely the dependence on NATO Secret Wide Area Network (NS WAN). However, by executing C2 through the respective national entities, if required through our basic message handling system, COMMARAIRNATO hopes to overcome this dependence, although a concerted deconfliction and coordination will be much more challenging should the overall Wide Area Network be subject to a sophisticated cyber attack.

The requirement to execute C2 from the Alliance headquarters to the respective assets in spite of a degraded framework for communications is absolute. Most naval airborne assets are equipped with High-Frequency (HF) radio(s), which are harder to jam and degrade than communication carried out over higher frequency bands. This will help in a degraded EW environment. Also, the inherent autonomy with which many maritime air operations are being carried out relaxes the need to communicate often with any other unit. This means that aircrew will find mitigating strategies and tactics to execute maritime air operations without having to rely on communications with another unit or a command entity ashore.

The potential complexity of future military operations must not be underestimated. Threats from a peer opponent throughout the spectrum of hostilities, new, advanced, and capable weapons systems, and the

potential for operating in a degraded environment all complicate planning, systems procurement and preparations for future operational challenges. So, how can we best prepare ourselves in order to mitigate the challenge of operations in a degraded environment?

There are some factors that stand out as potential avenues to pursue in order to be prepared:

Infrastructure. We must have a robust and redundant infrastructure. We are highly dependant on Information Technology (IT) and the already mentioned Wide Area Networks. We must have the robustness demanded from a modern IT system to withstand sophisticated cyberattacks. We must be capable of establishing a common situational awareness without a total dependence on shared IT applications. This points towards a second factor worth mentioning, which is competency and knowledge of common and standardized procedures.

Procedures. The Alliance consists of 28 nations with various operational experiences from the different regions of the organization. This knowledge has led to common tactics, techniques, and procedures to which we must adhere, keep updated, and constantly challenge and improve. Common procedures stand out as the backbone of mitigating against loss of communication and IT systems during operations.

Training. Training is another mitigating factor that will facilitate the complex joint operations of the future. Common basic and advanced training, leading into basic and then complex exercises, is paramount for a coherent effort between the Alliance partners. Our peacetime operations and complete freedom to manoeuvre can quickly evolve into operations in a dense threat environment with degraded communications. This is where the shared procedures, training, and exercises will help to facilitate the common effort necessary to accomplish the Alliance's objectives in

spite of the degraded environment. In short, we must regularly exercise our common procedures.

Pre-Planning. A fourth factor that will help sustain operations in degraded environments is the proper pre-planning of such operations. Operational experience shows indeed that 'the plan is nothing – planning is everything' – the better we have prepared and thought about potential courses of action of our opponent, the better chance we have of operating in environments that are sub-optimal, and where core communications and movements are being challenged.

In the present financially austere environment where we see cutbacks to budgets and the down-scaling of military organizations, we must be able to think outside the box, spend our resources wisely, and utilize our assets efficiently.

Rear Admiral (LH) Thomas Ernst is the current Commander Maritime Air NATO, under Allied Maritime Command. After years of operational experience flying the Tornado, Rear Admiral Ernst has served as Chief of Staff to State Secretary Dr. Wichert at the Ministry of Defence in Bonn and Berlin and the commander of the Marineschule Mürwik. While in command at the Naval Academy, he served as DCOM EUNAVFOR Atalanta at the EU Operational Headquarters in Northwood, GB.

© UN Photo/Rick Bajornas

A Quick Glance from the German Macro-Political Perspective

V

Mr Christian Motzer, DEU

In US or British discussions on military strategy, the scenario of a cyber war may play a certain bigger role – 'strategic novels' like Singer's and Cole's Ghost Fleet even make it into airport book stores. In German everyday politics, however, as well as in the consciousness of the general public, the subject generally plays a smaller role. Connoisseurs of the German security policy landscape will hardly be surprised by that: Military debates are normally conducted by experts over here, with little intensity among the general public. If they reach the public at all, it is through the media in a mostly-scandalized form.

The guidelines for the German security policy are laid down by the so-called 'White Books' drafted by the Federal Ministry of Defence, which normally have very long publication cycles. As this is being written, a new White Book is approaching completion. Its predecessor dates from the year 2006. However, the attention paid to this significant document of Germany's security policy is rather minor outside expert circles. Even more specialized publications in the field – like the overall airborne strategy dating from December 2015 – are regularly ignored outside the apparatus.[1]

A cursory analysis of joint air operations in a degraded environment from the perspective of German politics can be logically separated into two aspects:

1. The negative perspective: The political consequences of military operations in a degraded scenario.

Should it become necessary to conduct military operations in a degraded environment – which consequences would this have for the German public and for German politics? Are such operations with their potentially far-reaching public consequences at all controllable? Can such a conflict even be conducted anymore?

2. Danger prevention as the means of choice Better safe than sorry: Is the problem of degradation an integral part of German political discourse? With what means do they choose to prevent degradation or alleviate its effects? What advice can be given to military leaders?

Regarding 1: The political consequences of military operations in a degraded scenario.

To be frank: The perspectives for the German Federal Republic in the case of a conflict in a degraded environment are rather sobering.

'Parliamentary Forces' and Security 4.0[2]

To start with, the German armed forces are controlled by the Bundestag ('parliamentary forces') – parliament needs to legalize every single armed operation by German forces. In the case of a cross-party consensus, this procedure can happen swiftly. However, in a possibly less-obvious strategic situation, such as a cyber attack on navigation systems, a harsh political debate in parliament is conceivable. What also has to be kept in mind is that in cyber conflicts foreign and domestic security may be hard to separate. In cases where the critical civilian infrastructure also experiences failures – energy systems, the internet, mobile phone services, the civilian traffic infrastructure on rails and in the air, civil GPS, the financial system –

the political system would have to operate under much less favourable conditions both technically and politically and with a much heightened demand on civil-military coordination.

Exercises (called LÜKEX) by the German Interior Ministry, which is predominantly responsible for cyber security, have in the past also simulated cyber attacks. These exercises made the magnitude of the challenge posed by such scenarios to a society and its preparation in this area very clear. Indeed, many measures have been adopted in the Federal Republic of Germany to strengthen defence capabilities in this field in recent years. Still, the challenges that cyber security poses to integrated and highly developed national economies like the Federal Republic are manifest.

'Post Heroic Age'

Even more specific to Germany is the great degree of skepticism towards the use of military force resulting from the country's history in the 20th century. It is by no means inconceivable that this skepticism might have an impact even where a degraded scenario is comparatively contained: it is well possible that the German public would react with particular vigor to rising numbers of casualties amongst German personnel due to degradation effects. In addition, the perspective of killing non-combatants caused, for example, by a navigation failure, would further reduce the apparent legitimacy of operations in a decisive manner. The Kunduz air strike that took place in September 2009 and the political debate that followed may serve as a prime example of this effect. On the whole, debates regarding security policy tend to cause fear regarding the misuse of military means. This fear sometimes prevents the necessary differentiation in strategic debates. Another highly important debate connected with the future of German military aviation – the purchase of unmanned aerial systems – is much affected by these reflexes.

It can thus be concluded that from a political point of view the sum total of their negative effects makes conflicts in degraded environments particularly hard for the Federal Republic to conduct. This would presumably apply especially in the hypothetical case where a non-contained scenario starts affecting the civilian infrastructure at home. All the more the emphasis must be put on controlling cyber threats and/or alleviating the effects of degradation.

Regarding 2: Prevention as the means of choice. On April 26th, 2016 the president of the United States, Mr Barack Obama, once more reminded the Federal Republic in his speech at the opening of the Hannover trade fair that the country should raise its defence budget from the current 1.2 percent of GDP to the 2.0 percent that NATO requests. This already characterizes the situation most clearly: As with other countries a number of various possible conflict scenarios compete for limited budgetary means. The German armaments concept dubbed 'width before depth' ('Breite vor Tiefe') tries to account for this task.

Defence Against Cyber Threats

With regard to equipping and financing the German armed forces, there has been a recent reversal of the formerly negative trend towards the positive.[3] This also applies to the long-term financing perspective – the GDP share of defence spending is likely to increase further – especially for the cyber security sector. In the debate surrounding key military capabilities, Germany has come to recognize the importance of countering cyber threats, of strengthening cryptology, and of gaining information. The coalition agreement of the current federal government dating from November 2013 has already highlighted this. The aforementioned Military Aerial Strategy 2016 by the Defence Ministry is calling cyber attacks 'a trend among risk evaluation' stating that: 'The rising dependence of weapons systems on IT systems as well as

heightened dangers in cyberspace mean that it is of fundamental importance that weapons and other systems are robust and safe from an IT point of view. […] In order to facilitate this effectively we must make sure that the necessary bandwidth is provided for open and encrypted data traffic.'[4] The White Book which is to be published in summer 2016 is also going to put a focus on cyber security. It follows that cyber threats and the problem of degradation are well recognized politically. Expert politicians and the federal government are deliberating strategies and their realization. The Federal Ministry of Defence is cooperating closely with the Ministry of the Interior, which is predominantly responsible for IT security.

Action by Federal Ministry of Defence

Federal minister of defence, Dr. Ursula von der Leyen, also shows that she is aware of the task at hand. Recently she announced a 130 bln. Euro programme for research and modern material for the Federal Defence Forces through 2029. Concerning cyber defence, she created a new large organizational entity within the Bundeswehr at the beginning of this year, following the example of other NATO Allies. This entity consists mainly of units formerly belonging to other sections of the forces. It will be used to encompass all cyber capabilities. A core group consisting of three hundred cyber experts in the ministry is then going to lead more than 13,000 soldiers and employees in the areas of cyber defence and information – considering the overall size of the Federal Defence Forces, that is an impressive number. The leading heads in the defence ministry including, above all, State Secretary Katrin Suder, also stand in favour of a successful change in the culture of German security policy. This is also a good sign for the air force in order to prepare it for the challenges posed by cyber conflicts. As concerns the public at large, however, the discussion regarding this special threat looks rather typical: The public remains largely untouched by it. As in other areas of

security policy, continued information and communication activities are therefore needed in order to convince the public of the requirements of the scenario and the resulting political – and possibly financial – necessities.

Conclusion

As a highly developed national economy, the Federal Republic is exceedingly dependent on modern technology – militarily, domestically and economically. In the case of a conflict, it should be considered even less likely than with other members of the Alliance that the public will rally around the flag once effects of degradation make themselves felt. In order to allow politicians to help prevent or alleviate the effects of degradation in possible conflicts they rely – like with other strategic questions – on the factual input of the responsible military leaders. Politicians can then inform the public and bid for public understanding.[5] As usual, military leaders should seek the dialogue with the political realm and use the proven military-civilian channels: The Federal Ministry of Defence, the defence committee of the Bundestag, security and alliance bodies including possibly, in Germany, the Parliamentary Ombudsman for the Forces ('Wehrbeauftragter des Bundestags').

The debate may prove strenuous from time to time but it is surely worth the effort. Since an advanced persistent threat was identified nesting in the IT structure of the German Bundestag in 2015, there should be a certain sensitivity to the subject, particularly in Berlin that can be relied upon. Countering this threat slowed down parliamentary proceedings for a while and put the legislature and government in a state of considerable alarm.

Expert meetings like the JAPCC Conference are the indispensable first step of the information cascade, particularly for cyber conflicts and degraded.

Endnotes

1. Bundesministerium der Verteidigung (2015): Militärische Luftstrategie 2016, Berlin
2. 'Security 4.0' (German original: 'Sicherheit 4.0') is the title of a noteworthy article by the defence spokesman of the CDU/CSU parliamentary group in the German Bundestag, Mr Henning Otte MP, in: Newsletter Verteidigung, SPECIAL 08. 8th May 2015.
3. Compare: Gädechens, Ingo (2016): Die Einsatzfähigkeit der Bundeswehr. In: Europäische Sicherheit und Technik 4/2016. p. 10.
4. Bundesministerium der Verteidigung (2015): Militärische Luftstrategie 2016, Berlin, p. 13.
5. Due to the strong skepticism regarding unmanned aerial systems in this country it could make sense in Germany also to explain an apparent contradiction: Why do German forces need UAS despite the fact that this heightens dependency on technology?

Mr Christian Motzer is a senior staffer with the Christian Democrat party group in the Bundestag working as personal aide to its chairman, Volker Kauder MP. He has previously worked for a large international public affairs network. His master thesis concentrated on public opinion and the overseas deployment of the German Federal Defence Forces.

© USAF

Air Operations in Contested Environments

VI

Brigadier General Mehmet Yalinalp, TUR AF

The basic paradigm for air operations in a permissive environment is evolving. The long-term enjoyed benign environment has swiftly transformed into an unpermissive, contested environment with major challenges and problems, far more problematic than have been seen in recent previous conflicts.

The main cause behind these challenges and complications is the proliferation of high edge information/cyber technologies, surface- and air-launched precision-guided weapons, and advanced situational awareness capabilities. Non-western militaries have been continuously observing and adapting to the manner in which western militaries apply their advantages in technology, weapons, training and doctrine. In time, they have been able to adapt their policies and defences. This adaptation reveals itself in many forms; certainly the most prominent adaptation lies within Anti-Access (A2) and Area Denial (AD) spaces.

The challenges in contested environments can be subdivided into two sets of complementary terms; Anti-Access and Area Denial. Anti-access environment challenges access, complicates entry and makes force posturing very difficult. Area denial environment limits movement and maneuver of our forces. Air and space power faces both challenges in contested environments.

A2/AD Capabilities and Challenges in Diversified Domains of Warfare

A2/AD capabilities exist in all domains of warfare (Air, Space, Maritime, Land and Cyber) and exert cross-domain challenges to all services. Adversary capabilities and different challenges arise in many forms within an A2/AD environment. One of the areas in which this difficulty arises includes the Integrated Air and Missile Defence System (IAMDS). An opponent's well integrated and advanced IAMDS constitutes a focal adversary capability for anti-access and area denial operations. The modern IAMDS, with its highly capable and cutting edge technology and double-digit SAMs, presents a considerable challenge to friendly aircraft.

Added dangers have arisen from evolving technology in today's non-western fourth- and emerging fifth-generation fighters. Extended range air-to-air missiles pose a highly lethal threat as they are highly competitive against their Western peers. Additionally, evolution of the ballistic missile has resulted in a high precision, GPS guided, short to medium-range ballistic missile, with the ability to reach and rain into forward bases and deny force projection and posturing.

Counter Space Opponent attacks in space and cyber domains could deny many of the enablers for air and space power, including satellite communications, space ISR and Global Positioning System (GPS) based navigation and precision systems. Some countries have already shown that they possess capabilities to attack space targets. Anti-satellite weapons have been tested, validated and proven to be effective. These concepts extend into the realm of the electromagnetic spectrum; an essential extension of space and cyberspace domains which is also an intensely contested environment. The electromagnetic spectrum can be exploited by jammers to inhibit weapon solution/ISR collection, network-centric operations and ISR collection.

Especially common today are cyber-attacks, network exploits, malware-based attacks exerted to disrupt, deny, and steal information or sometimes to take control of the friendly strategic cyber capabilities. The physical elements of cyberspace, which comprise fiber optic cables, cell towers, computers and servers, are also vulnerable to adversary attacks. As a consequence of these cyber-attacks, we may become more vulnerable than the Land domain. Thus giving adversary rockets, artillery, and short/medium-range surface-to-surface missiles can target land forces before they can disperse from air, maritime and surface points of debarkation, where they are most vulnerable. Opponent AD tactics in the Land domain may also include minefields, use of chemical biological and radiological agents and special operations tactics.

Long-range A2/AD capabilities against naval vessels, including aircraft carriers, may comprise coastal or afloat antiship cruise missiles (sometimes low-observable), precision-guided ballistic missiles, and silent (diesel) submarines and advanced anti-ship mines.

Impact of A2/AD Capabilities on Operations

In the contest for Air Superiority, an A2/AD SAM shield prevents friendly forces from attaining air dominance or air supremacy, and makes it very difficult to obtain and, even if obtained, difficult to sustain air superiority. Long-range double-digit SAM coverage, which sometimes extends into friendly territory, gives the opponent an initial 'status quo' Air Superiority from the beginning. It should also be noted that in the A2AD environment, airborne C2 and ISR collection can be very difficult without significant risks to the high value platforms. Thus, intelligence preparation of the battle-space, persistent situational awareness and decision-making processes will suffer significantly.

One of the basic outcomes of operations in an A2/AD environment is high attrition rates on friendly air forces, because fighters, bombers, ISR

platforms and cruise missiles are extremely vulnerable to the advanced SAM systems. As fighter aircraft cannot be deployed to areas already under significant threat coverage, they will be based in the rear areas of joint area of operations. This will create a massive reliance on air-to-air refuelling aircraft.

It must be taken into consideration that if the opponent's territory is beyond a large sea or even an ocean, forward basing options will be very limited, some of the deployment/operation ports and bases might be exposed to surface-to-air, air-to-surface and surface-to-surface weapons of the opponent. Anti-Access Shield against friendly Long-Range Weapons and modern SAM systems have critical capability against long-range stand-off weapons and cruise missiles. Moreover, there will be an increase in Theater Ballistic Missile Threat (TBMT), as high precision, GPS guided, short- to medium-range ballistic missiles of the opponent can reach and rain into forward bases and deny force projecting and posturing. Thus, robust and persistent Theater Ballistic Missile Defence (TBMD) must be established prior to deployment of the aircraft and forces.

It is also imperative to understand the consequences of degradation in space capabilities or losing space support, as this would complicate ISR operations, precision navigation and weapon solutions and space-reliant information service. In terms of the electromagnetic spectrum, it is an essential extension of space and cyberspace domains, becoming an intensely contested environment due to air, sea and ground-based high-tech jamming systems.

Adversary A2/AD operations in cyberspace can range from the tactical level to the strategic level. At the tactical level, adversaries can use cyberspace to disrupt satellite ISR/information systems and data links. At the strategic level, an adversary can attempt to take control of, or exploit, friendly information systems. Increase in Force protection in a contested environment, protecting forces, units, installations and C2 nodes against infiltration, sabotage, and direct attacks will be a major concern.

A major risk in the realm of the Contested Land Domain is the proliferation of precision-guided short-/medium-range ballistic missiles, long-range artillery and mobile rocket launchers, as they pose a major threat to Reception, Staging and Onward Movement (RSOM) areas, such as ports and airfields. Adversary SAM systems can limit Army aviation, including airborne ISR, airborne assault, and air drops. Contested Maritime Domain maritime power projection and command of the sea would be hampered by coastal or afloat antiship cruise missiles, precision-guided ballistic missiles, and silent (diesel) submarines and advanced anti-ship mines.

Ensuring C2 in Contested Environments

Ensuring resilient, redundant and recuperable C2 contested environments will require change in concept, innovation, organization, training or acquisition in a complementary manner. Below are some examples:

- Firstly, mission assurance rather than information assurance, including the vulnerability analysis of friendly weapons, platforms and information/cyber systems in peacetime provides an opportunity to assess areas most susceptible to exploitation. The focus of analysis and follow on protection should be on mission assurance rather than total information assurance in the event of a cyber attack.
- Secondly, Dispersal, Hardening and Force Protection. Friendly forces may have to deploy to the bases which are within adversary A2/AD coverage. Hardening of aircraft shelters and operation centres, coupled with robust force protection against surface and air threats will increase the survivability our operational networks and assets.
- Thirdly, a Joint Approach. As no single service has sufficient capabilities to address all the challenges faced in contested environments, Joint concepts like Air-Sea Battle (ASB) and Joint Operational Access Concept (JOAC) are in development to overcome the difficulties of contested environments.

Innovative Methods in Air Operations

Primarily, operational planning and execution should concentrate on those adversary vulnerabilities with less or no protection so that adversary centre of gravity could be reached and attacked. With this, the Protection Reduction of Reliance on Vulnerable Systems should be kept in mind. For example, employment of high-altitude, long-endurance, and stealth ISR platforms could be an alternative to vulnerable space capabilities.

Aged but long practiced and widely understood deception and decoy methods should prevail again. Sometimes these methods could be the only way to gain a superior advantage against a near-peer adversary. Exploitation of Stealth with ISR sensors, high edge, command and control integration capabilities through state-of-the-art, high-capacity links systems, fifth-generation air platforms not only serve air domain but also serve and cooperate with other domains. Additionally, air, land or sea launched cruise missiles would require stealth capabilities to penetrate opponent IAMDS.

Ultimately, agility requires building robust networks which negate physical or cyber-attacks, resilient systems which provide redundant methods, responsive systems which work against stringent problems, flexible systems which cope with changing conditions, and innovative systems which offer new solutions. Agility could be divided into two parts:

Technical agility, including the protection of vital space-based platforms and cyber networks by reducing their vulnerability to attack or disruption and increasing resilience if an attack occurs.

Conceptual Agility, comprising emerging C2 concepts such as 'Centralized Command, Distributed Control and Decentralized Execution' and 'C2 forward'.

Lastly, Virtual and Constructive training and exercises should be exploited to develop and mature concept of operations in an A2AD environment.

Brigadier General Mehmet Yalinalp is the Deputy Chief of Staff (Plans) for Allied Air Command. After years of operational experience piloting the F-16, he commanded 141st Advanced Tactical Training Squadron and a 4th Main Jet Base Fighter Group consisting of three squadrons. He served at different posts at several Turkish Air Force Headquarters departments including Strategy and NATO Force Planning Officer of Plans and Policy Department, Special Staff Member of Air Force Commander for international, military and national security issues, Planning Coordinator of Chief of Staff and Secretary General of Chief of Staff.

© NATO

Introduction to a Degraded Environment

VII

Lieutenant General Claudio Gabellini, ITA AF

The term degraded environment means many different things to different people. In order to be able to speak of DE in terms of air warfare, it is necessary, first and foremost, to give it context and define what a Degraded Environment is:

If a Degraded Environment refers to a degenerate situation (which evolves from a low to medium intensity conflict towards a higher intensity or even international one) then the ratio between risk acceptance, rules of engagement and law of armed conflicts is conditioned above all by the Political Will which must be expressed by a UN and/or NATO mandate and also by the rules of Law of Armed Conflict (LoAC). In particular, the concepts of proportionately and military advantage characterizing the single operations must be stressed. Senior Leadership, in these cases, is called to clearly define both the risk acceptance level and the objectives. The political level, instead, often mistakenly believes that air power is invulnerable and that its capabilities require no specific support.

If, on the other hand, Degraded Environment refers to a situation in which accuracy or capability is lost (due to ISR limitations or difficulty to obtain a PID), then it must be clear that the boundaries dictated by International Right must not be violated due to such limitations. The use of force,

according to the principles of the LoAC, dictates that it is clear where and against whom force is employed. In a case in which the assumed actual situation is different from the foreseen or planned one, LoAC prescribes that precautionary actions are taken and that every engagement is suspended. In such an environment, Air Power employment should also be ceased.

In such a context, how do Rules of Engagement (RoE) change to fit a Degraded Environment? It cannot be denied that RoE are impacted by each change, since they are the expression of Political Will in operational terms. As an example, if the situation evolves towards a higher intensity conflict, Political Will should adopt RoE that are more effective (aggressive?), with the goal of better safeguarding friendly combatants and making military action more effective. If, instead, the situation worsens in the sense that it becomes more and more difficult to discriminate between combatants and civilians (either because of the type of conflict or the lack of proper intelligence), the use of force should be minimized to avoid collateral damage (not acceptable?).

A Degraded Environment should not be considered a problem but only a condition in which force is legally employed. In more detail, to discuss DE requires that at least three main scenarios be addressed, for which a few thoughts are expressed here. The problem is not approached from a merely doctrinal point of view, except for a few references and considerations to be used as food for thought. Conversely, the foundation of the reasoning is exclusively based on experience, learned during the Operation Unified Protector (OUP).

As mentioned above, DE can be discussed in three main scenarios, contextualized in a modern conflict with a high degree of asymmetry:

- Technical;
- Legal/doctrinal;
- Environmental.

'Technical' DE

Presence of an opponent who is capable of jamming C4 systems as well as satellite systems, with obvious repercussions on the employment of precise munitions. It is obvious that in modern conflicts, marked by the exclusive use of PGMs (exactly as OUP), some serious thinking must be done that goes beyond the technical aspects directly connected with NATO. Going back to the employment of so-called 'dumb' munition cannot be excluded, providing that, past the purely technical aspects, precautions and/or predispositions are put in place.

At any rate, in the case of a DE of technical kind, the solution must invariably be found in the technical field. It is necessary to identify procedures, waivers, risk management techniques, acceptance procedures and mitigation measures that are to be studied and accepted during peacetime. It is evident, then, that the Political/Strategic level will have to find a balance for Air Power employment in a technically DE.

'Legal and Doctrinal' DE

The first element of this kind of degradation is now a constant of our times. It is represented by the asymmetry of modern conflicts and the consequent distortion of the traditional centres of gravity. Another fundamental aspect is depicted by the difficulty related to a mandate which does not contain all the necessary aspects to develop an air campaign, for example the military end state and clear identification of the enemy being fought (see UN Res. 1973). In such a degraded situation, the effective employment of Air Power is clearly impacted: it loses its main characteristic, which is strategic dimension, and is relegated to non-better defined support roles (e.g. the protection of civil population). This type of DE is potentially dangerous because it affects operations at every level, depriving them above all of the strength deriving

from a clear mandate toward a specified objective which in turn can provide the public with a term of reference for the benefit of the operations and the progress in the field.

'Environmental/Contingency' DE

Last but not least, another possible scenario sees NATO involved in a coalition operation including non-NATO countries (e.g. PfP) or other countries traditionally far from the NATO world (e.g. Arab countries). It might appear as an easy feat, but finding a modus operandi that is valid and inclusive of C2 systems, sharing doctrine and publications, classified mechanics and dynamics typical of the NATO world is not simple at all as recent history proves. Furthermore, a huge obstacle is represented by the sharing of Intelligence, which alone is already an issue within NATO itself. Problems connected with the release of Target databases, the access to Joint Targeting System (JTS), the sharing of information that even indirectly hint at the Intel capabilities of both the single Nations and the Alliance belong to this last category. All of this is very difficult without:

- a unique, mission dedicated LAN (bare minimum technical prerequisite) capable of functioning both in the centre as in the periphery, reaching every actor effectively;
- an approved and shared Collateral Damage Estimation (CDE) methodology, as well the computation of the Civilian Casualties (CIVCAS) probability;
- mensurated coordinates computation and release;
- a unique, shared and effective STRATCOM.

Conclusions

From the above points, it is possible to list the fields in which a solution can possibly sought and found:

Technical DE: procedures/mitigation measures/risk acceptance/risk mitigation/training.

Legal/Doctrinal DE: to work on mandates, in other terms on limits, constraints, caveats, etc.; to train in finding a legal framework during uncertain phases, while maintaining a high-level effectiveness.

Contingency/Environmental DE: establish since peacetime the actions to undertake and the methodology to apply if NATO is forced to operate in a context that is not typically NATO, as well as investing on all STRACOM activities: during the first month of OUP, the Alliance/Coalition has been less than effective in countering the degradation factor put in place by the opponent via an effective counter information action.

In any case, solutions in the above fields must be sought during peacetime to ensure NATO is able to continue to conduct Air Operations as necessary. NATO must begin looking into the areas mentioned above now if we are to be ready to perform our collective defence mission.

Major General Gabellini is the Commander of Combat Air Forces in the Italian Air Force and will soon be the Chief of Staff at Allied Air Command. He has accrued years of operational flying experience on multiple aircraft, including the MB339, F-104 and Tornado. He was part of the planning cell within the Combined Joint Task Force Unified Protector HQ of Bagnoli, serving as the Targeting Directorate Chief. He has also served as Head of the Operational Planning and Generation Department of the Air Force Command and the Chief of Staff of the Air Force Command.

Joint Air Operations in a Degraded Electromagnetic Environment – An Operator's Perspective

VIII

Mr Ian Stuart Ead, GBR

The question has been asked as to how we can continue to conduct operations in a degraded electromagnetic environment; this paper puts forward a view of how the command chain can help tactical aircraft crews operating under such conditions to make decisions that accord with the Commander's Intent. And it should be acknowledged that this paper proffers that no new equipment or technology is required to do so. This paper will consider operations in a 'middle ground degraded environment' where electronic attack on NATO systems and sensors is effected using 'conventional' jamming aids and spectrum denial means against those air systems operating in the tactical scenario. In such a scenario the loss of systems, situational awareness, and inputs from other friendlies leads to a worsening state of isolation for the crews involved who are forced into making decisions as to the execution of their mission in a highly stressed environment.

The Operator's View

Degraded operations are really an attack on the opponent's ability to access tactically useful data through the electromagnetic environment. The obvious targets of such an attack are Command and Control (C2), Situational Awareness (SA), weapons and sensors. The operational pilot

has to consider at each stage of such an attack whether a go/no-go decision is required and, assuming a 'go', how can they complete their element of the mission.

Clearly, all electromagnetic systems may be affected by electronic attack. However, the main mission critical areas are likely to include the loss:

- of communications with C2, for example, package command;
- of communications with other formation elements;
- or degradation of, SA tools such as data links;
- or degradation of, own-ship sensors.

In isolation each of these will be significant. Cumulatively the impact on SA and the resultant pressure will have a significant impact upon decision-making.

Most aircrew will have, at some point, experienced a mission where the original plan has gradually collapsed. The pressure builds from a simple foundation of wanting to complete the mission (after all we are largely task focused) through to the perceived risk to life and limb. Back in the debriefing room, each decision is taken apart and it seems so obvious whether the decision was good or bad. So we should ask why this couldn't be managed in the air?

Well the good news is that there is a sound reason for this which is described in the following section.

Decision-Making

The subject of decision-making has been studied by psychologists, albeit not necessarily under exactly the same stresses as we would find in air combat operations. To understand how decisions are made it is neces-

sary to consider both the brain functionality and the decision-making processes.

It has long been known that the brain is separated into three distinct areas with the neocortex dealing with high level, analytical functions and the mid-level limbic brain being largely concerned with feelings and memory. The lowest level, the reptilian brain, deals with 'instinctive' behaviours. In normal operation, these three areas work in balance. However, it has been shown that, under stress, the brain shifts the balance of decision-making from the more ponderous neocortex to the swifter limbic or even reptilian brain.[1] When it comes to decision-making, there are as many theories as there are psychologists. With regard to complex decision-making under stress the cognitive continuum theory is generally seen as the best fit. This states that analytical strategies occupy one end of the cognitive continuum, with intuitive decision-making strategies at the other end. What are referred to as quasi-rational decisions sit in the middle.[2, 3] The categories are best defined by the studies of Rasmussen[4] and Roscoe et al[5] and can be paraphrased as:

- **Skills-based** or perceptual-motor. Behaviours that have been learnt over time. These tend to cater for relatively fast and unconscious decision-making. Skill-based behaviours don't consume many mental resources. An example would be flying the aircraft. These behaviours form the intuitive end of the decision-making spectrum.
- **Rule-based** decision-making is where defined responses are learnt in relation to given scenarios. For example, if condition 'X' is met, execute plan 'Y'. Contrary to some expectations, these decisions are typically based upon pattern recognition with limited analysis. This type of decision process is quasi-rational (i.e. some cues can be processed analytically and others in a more automatic manner).
- **Knowledge-based** These are the true analytical approaches involving knowledge or mental models which are more theoretical in nature. Decisions are based on conscious, analytical thinking and require a

considerable amount of mental resources and time. Klein and Klinger[6] have shown that that even under low time pressure, analytical strategies require extensive work and lack flexibility. In aviation these approaches are best suited to low-intensity phases of flight and are to be avoided in more dynamic regimes. The models and tasks formulated are usually singular, well-defined and straightforward.[7, 8]

You can probably see how the decision-making processes are rooted in different areas of the brain which makes it difficult to blur, for example, analytical thinking with rule-based decision-making as they are processed separately. However, all three areas are used simultaneously but the emphasis placed on each type is factored by stress, in particular time pressure and perceived risk. The latter is very significant as perceived risk invokes survival instincts which must be trained out in the combat aviator.

It stands to reason that we want the aviator to make mission-based decisions that satisfy the Commander's Intent for the sortie. As they respond to each system degradation, it is assumed that they will consider the Commander's Intent in their response.

Commander's Intent

So why the consideration of the Commander's Intent? After all, it is a basic NATO tenet that:

'*The intent defines the end-state in relation to the factors of mission; … As such, it addresses what results are expected from the operation … and how, in broad terms, the Commander expects the force to achieve those results …*'[9]

This enables all participants to understand the role that they have in achieving the plan. NATO missions encapsulate the Commander's Intent in the OPLAN and lower level briefs will usually contain a derivation of

the SMEAC 5 paragraph order set[10] outlining this intent as part of the Execution phase.

In general, NATO's doctrine and orders are excellent at providing what Pigeau and McCann[11] define as explicit intent: this being the public statement of the aim within the confines of doctrine, orders, and tasking. This is modified by theatre specific data contained within rules of engagement, airspace coordination plans, 'SPINS' (SPecial INstructionS) and so on. This mass of data and procedures sets a frame of reference within which the pilot will make decisions in response to any change in the airborne environment.

A second strand is what has become known as implicit intent. This is more concerned with the perceived expectations as to how operations should be conducted. This tends to be developed over a longer period and is often 'absorbed' as a cultural behaviour rather than one that is written down. An example would be remaining within the law of armed conflict. Farell and Lichacz[12], show that implicit intent is open to interpretation based upon the role and experience of the subordinate. Within the military domain the implied intent will, unless specifically addressed elsewhere, include issues such as the degree of risk (both personal and mission) that the crew is expected to take.

So, armed with a definite understanding of the Commander's (explicit) Intent, and an appreciation of the implicit intent with which this should be managed, the crew are ready to go and commit aviation. Now this is where we need to consider that bit about how aircrew members think and make decisions.

So How Can We Help?

If we consider the situation of our crew participating in a NATO air operation we can assume that they have been well trained in flying and fighting in their aircraft (skills-based training), have been exposed to scenario

training through exercises whereby a variety of situations and responses have been shown (rule-based data). Finally, crews will have been briefed on theatre induction, rules of engagement and so forth (analytical data). Brilliant, what more could they want?

We can assume that we can do little to affect core training. Therefore, we are only able to affect the rule-based and analytical decision-making processes. As a mission progresses from low-pressure ground preparation and transit phases into the more pressured operating area elements the bias of conscious decision-making shifts from being analytically to rule-based. Analytical decisions will still be made, perhaps relating the current 'air picture' to the mission briefing, but pressure is increasing the reliance on the ability to match cue 'A' with response 'B'.

This is where decision-making in degraded operations comes in. Under optimal conditions NATO aircrew would expect to benefit from a number of SA tools including the use of datalinks and secure communications. Data from long-range sensors and other tactical platforms will be displayed on the data link to augment their own-ship sensors. In general, we have become used to, if not dependent upon, a data and communications heavy environment.

As we strip each of these away, the crew must react and, in general, the pressure will rise. Because of the environment will they be thinking logically, dragging up pages from dusty volumes that they read some weeks ago? This cannot be assured. It is most likely that the crew will be reliant on quasi-rational decisions. That means that they will be mentally searching for a response that matches the cue in front of them, whether it is a go/no-go or an engagement decision.

At present the Commander's Intent is described with the following caveat: *Its focus is on the force as a whole. Additional information on how the force will achieve the desired results is provided only to clarify the Commander's intentions.*

Similarly, the use of the 5-Paragraph style brief tends to relate back to the OPLAN level. Do these approaches truly help the warfighter to frame decisions on a daily basis? It is suggested that ensuring that the commanders offer explicit direction to crews as to what is required at all levels of the campaign will allow operators to make decision when operating in degraded environments as part of their mission standard Operating Procedures (SOP). These SOPs will need to cover numerous eventualities, too many to list here. However, it could include, for example:

- A definite directive as to where and when bogeys and bandits should be prosecuted. This explicit intent would remove any doubt from the mind of the pilot.
- The last point at which untargeted bandits ('leakers') should be engaged.
- What fire control order set should apply under what jamming conditions.
- How does the degradation of NATO capabilities change the Rules of Engagement.
- And many, many more.

But, surely we already have all of this in the extant plans, policies and doctrine documentation for an operation? Well, by and large, yes we – but not always in a format that fits the way in which aircrew think, especially when aircrew are forced into rule-based decision-making. Framing the policies in terms of for situation 'A' perform 'B' would allow for crews to use data readily from Day 1 rather than developing such matrices for themselves as they become more experienced in the theatre of operations. Who has not experienced a debate on the Rules of Engagement or Commander's Intent during the question and answer part of mission brief? Ever had a satisfactory decision at the end of such a debate? I am not so sure.

Finally, having developed a more user-friendly set of SOPs for operating in degraded environments, then crews must be allowed to practice operating under these conditions in peacetime training. This is not so much to put them through the misery of operating without all the support that they would normally expect but rather to prove to them their decision-making abilities and their ability to follow guidance in order to adequately execute missions under degraded operations within the realms of the Commander's Intent. This will mean conducting exercises whereby AWACS and datalinks are taken away from the crews at critical phases of the mission, and communication and other jammers are used in an integrated manner to test this decision-making ability. Training to fight and fighting as you've trained is, after all, a common adage for NATO in peacetime. I know it sounds a little 'Cold War Warrior' but that was a situation where crews fought without such aids …

Oh, and what about the 'smart Alec' in the debrief … just remember that he has the benefit of thinking analytically on the ground when you were reacting quasi-rationally in the air!

Following a 26 year RAF career as a navigator on Tornado bombers and fighters, interspersed with tours in intelligence and at the Fast Jet Test Squadron, the author is currently working as an aviation consultant, mainly in aviation safety management and electronic warfare. In writing this essay, he was greatly assisted by his wife, a trained psychologist.

Endnotes

1. Mason, J. L Stress and Decision-Making: Avoid Expensive Mistakes. Forensic Magazine Dated 29 Oct. 2013. Internet resource accessed on 27 May 2016 at http://www.forensicmag.com/articles/2013/10/stress-and-decision-making-avoid-expensive-mistakes.
2. Hammond, K. R., Hamm, R. M., Grassia, J. & Pearson, T. (1987). Direct Comparison of the Efficacy of Intuitive and Analytical Cognition in Expert Judgement. IEEE Transactions on Systems, Man and Cybernetics, 17 (5), p. 753-767.
3. Hammond, K. R. (1988). Judgement and Decision-Making in Dynamic Tasks. Information and Decision Technologies, p. 14, 3–14
4. Rasmussen, Skill, Rules, Knowledge: Signals, Signs and Symbols and Other Distinctions in Human Performance Models. IEEE Transactions on Systems, Man and Cybernetics (SMC-13)3. p. 257–266, 1983/
5. Roscoe SN, Jensen RS, Gawron VJ. Introduction to Training Systems. Ch in Aviation Psychology. Roscoe SN (Editor). First edition, Ames: Iowa State University Press; 1980: p. 173–181.
6. Klein, G., & Klinger, D.(1991). Naturalistic Decision-Making. CSERIAC Gateway, 2 (1), p. 1–4.
7. Hammond, K. R. (1988). Judgement and Decision-Making in Dynamic Tasks. Information and Decision Technologies, p. 14, 3–14.
8. Rouse, W. B., & Valusek, J. (1993). Evolutionary Design of Systems to Support Decision-Making. In G. A. Klein, J. Orasanu, R. Calderwood, & C. E. Zsambok (Eds.), Decision-Making in Action : Models and Methods. Norwood, NJ : Ablex Publishing.
9. NATO (2010) AJP-01 - Allied Joint Doctrine.
10. SMEAC = Situation, Mission, Execution, Administration and Command /Signal. This is the common application at unit level (see for example US Army Field Manual 5.0). Within the NATO HQ planning domain the acronym Situation, Mission, Execution, Service Support and Command Arrangements is strictly more appropriate (see AJP-01(D), paragraph 0549).
11. Pigeau, R. and McCann, C. (2000) Redefining Command and Control. In: R. Pigeau and C. McCann, (eds.) The Human in Command: Exploring the Modern Military Experience, 2000, New York, NY, USA: Academic/Plenum Publishers, pp. 165–184.
12. Farrell, P.S.E. and Lichacz, F. Measuring Common Intent During Effects-Based Planning. Canadian Forces Experimentation Centre (Command and Control Research and Technology Symposium), 2004. They cite the example that, if Explicit Intent is 'to capture the hill', then Implicit Intent might be 'to capture the hill with minimal battle damage' or 'to capture the hill with Air Force assets only.'
13. NATO (2010) AJP-01 - Allied Joint Doctrine.

Special Operations in Degraded Environments

IX

Lieutenant General Brad Webb, USA AF

Special Operations Forces (SOF) are no different from other forces who are challenged to conduct operations in degraded environments, yet some distinct peculiarities can be highlighted. Since the smallest study on this topic would fill entire volumes, the boundaries of this primer will be set as follows. First, considerations will span the far ends of the typical spectrum of Special Operations, starting with low-key and relatively low threat Military Assistance to indigenous forces, often in prolonged, austere and remote conditions. The other end of the spectrum implies deeply penetrating Direct Actions or Special Reconnaissance against technologically advanced adversaries. Secondly, we will consider degradation of the natural environment when induced by human actions, then look into the impact of the electromagnetic spectrum on communications and positioning, arguably the two most prominent factors during operations[1]. Emphasis will be given to SOF air operations and air-land integration.

Degradation is Our Friend

In many ways, SOF have consistently welcomed extreme environmental conditions which degrade sensorial perception in order to gain an advantage over an adversary unable to operate due to lower capability. Of

course the demarcating line in this distinction is thin and perilous. Aviation assets are the perfect example of how it takes exponentially extra training and resources to improve capabilities by a small margin. Being able to fly a little lower, on a little darker night, and a little closer to the enemy calls for absolute dedication and uncompromised investment on the quality of our units for the sake of getting that strategically relevant mission done.

Moreover SOF are, and must continue to be, pioneers in the use of breakthrough technologies to maintain the advantageous edge[2]. A great example is the fusion of sensors to provide a progressively wider multispectral view, to literally cut through all fogs of war[3]. Also, innovative 'smart' sensors and passive defences, such as reactive opacity materials, do help in negating the effects of enemy-made sensorial degradation (e.g. through the guided application of laser and light). As an important by-product of this demanding necessity, particularly in the case of aviation, technological advantages can be battle-proven in small quantities by lean and driven organizations, to be incorporated later by conventional forces. Nations that adopt and exploit this model usually report distinct benefits to both forces (SOF & conventional) and industry. In essence, the successful conduct of Special Operations greatly depends on the capability to operate deep into environmentally degraded situations, but the required sensorial 'edge' demands increased investment in training and equipment.

To Be More, Bring Less

SOF could be the first and only military presence in remote and/or austere scenarios like disaster relief operations and unconventional warfare. The winning factors in these cases are a light footprint, self-reliance, and inventive ways to leap the next hurdle. Translated for the Airman, this means specialized and unorthodox approaches to the well-established mantras of conventional maintenance, flight safety, airworthiness and crew rest. In Special Operations, punishing limitations of otherwise comfortable and

sound procedures must be mitigated with specific selection, training, broader experience and risk management. The finishing touch is provided by a highly mission-driven and adaptable attitude some call 'the SOF mindset'. Therefore, personnel selected to become SOF should have extensive conventional mission experience and have exhibited exceptional operational flexibility. This will ensure that, once they have completed their SOF specific training, not only will they be accustomed to genuinely austere environments but they will also be accustomed to the unique challenges they may encounter in a space, cyber or electro-magnetically degraded battlefield which denies technological aids.

Keeping the 'OCOCDCAC' Loop Turning

We should all be familiar with Boyd's OODA loop (observe, orient, decide, act). The OODA loop is a very personal model which happens within a single entity. What our military need is to add a 'C' for communicate in between all of the phases. This will allow all fighting entities' OODA loops to be connected and synchronized for a successful job. But warfare will do everything to blur those 'Cs' and break team cohesion, with Electronic Warfare on the frontline to render our radio exchanges ineffective or even misleading. There is mitigation built into today's wide range of communication systems, over a huge spectrum of frequencies and capabilities. Yet, solutions abruptly narrow down when 'Beyond Line-of-Sight' (BLOS) is required. Due to a combination of remoteness, security, risk profile, lightness of burden and, therefore, dependency on many supporting assets, Special Operators are among the most demanding customers for BLOS. Again, investment in lighter and more sophisticated radios goes a long way but requires uncompromised investment in equipment and training. Alternative and creative techniques for bridges and proxies should be part of every operator's technical training but the real difference can be once again achieved in the human domain. Coordination and joint planning between forces must be elevated in order to fall back on solid mutual

understanding and well-choreographed practices. While the habitual relationship between ground and air SOF is easily recognized as a critical factor (yet not always practiced extensively), some nations have taken steps to strongly orient conventional air capabilities towards support of Special Operations, particularly with fast jets. A regular frequentation between apparently distant communities leads to personal relationship and professional understanding that can overcome many electromagnetic disconnections and lead to optimal results. The beneficial effects continue as personnel 'grow' together from the battlefield to the C2 structure, enabling unprecedented synergy.

You Are HERE

Global Positioning System (GPS) has provided an excellent service for the Allied soldier, sailor and airman for more than a quarter of a century. Frankly, it has been wonderful to have that 'big red dot' on our battle plan to navigate the perilous avenues of warfare. Yet, what had become addictive complacency in electromagnetically uncontested battles has been swept away in a puff by some of the jamming capabilities displayed in recent hybrid scenarios. As a sub-set target of communications jamming, space- and Ultra High Frequency-based GPS is one of the most vulnerable. For SOF, precision and swiftness of maneuver are a key factor to achieve relative superiority over a stronger force. In unconventional warfare scenarios, man-portable precise positioning is one of the thin advantage margins brought forward by introducing technology on an austere field. Its benefits are so much more impressive when it enables advanced joint fires and effects at the call of otherwise more primitive factions of combatants, with the bonus of an unmatched reduction of collateral damage. Against an advanced threat, very little margin is allowed for navigation errors and botched landings off the 'X', as well as the complexity of the mission calling for reliable and low maintenance systems to maximize attention to the fight. But, while in aviation and on vessels GPS has been coupled to inertial

navigation systems that nearly match its abilities, alternatives are not yet so rosy for operators in vehicles and are definitely uncomfortable for the dismounted[4] (even if interesting hybrid solutions are on the horizon[5]).

The development of man-portable, self-contained devices has not fully materialized, with viable solutions yet to be fielded. Therefore, all SOF should maintain a high level of proficiency in traditional positioning and navigation methods. Some may remember a paper map and a compass, with a fancy watch to match … luckily these basic tools are not alone, as advanced sensors such as the ones already mentioned do provide a great deal of assistance with visual (or cross-spectral in this case) navigation when a degradation of GPS, with little to no technological alternatives. It is true that the vast majority of aircraft benefit from the increasing quality of inertial systems, but little changes in the most dynamic and decisive phases of combat if there is no effective hand-over of precise coordinates from the surface. To preserve the huge advantage brought by air power to Special Operators who can tether to it, the same considerations on the habitual relationship made for communications are valid, with great mitigation in utilizing simple, well-rehearsed alternative reference methods which could restore a healthy portion of lost precision.

The Greatest of Evil

In our western cultures and in the way we conceive warfare, Chemical, Biological, Radioactive and Nuclear (CBRN) threats are the thing of nightmares and supervillains, with an incomparable power to coerce, destabilize and terrorize. SOF are often the military tool that could be called to pre-empt the fielding of such weapons, with the associated high risk of exposure and a requirement for no-fail specialization. Particularly for aviation forces, the most recent asymmetric conflicts (up to Operation Unified Protector) reduced the perception of the threat, luring numerous nations into savings on the expensive defences against CBRN. As a collective in NATO, we are

now facing rogue states and aggressively postured superpowers with capable arsenals, along with terror mongers with predisposition for the tragically spectacular. No matter the scenario, SOF and their aviation must be enabled to maintain the capability to achieve the mission in environments potentially highly degraded by CBRN to ensure the ability to target and neutralize vectors and facilities as well as to interface with other forces for a seamless handover of consequence management.

Working Under the Threshold

Special Operations are particularly effective, and cost-effective when they are utilized to understand and shape a crisis, well before it reaches a violent peak and an oversized international conundrum. SOF can give their unobtrusive best when helping to seam a torn political situation that could give way to the use of force. Especially within an Allied nation, SOF can understand, report on and defuse hybrid threats and prepare to counter the onset of hostile armed parties of any kind. But these uniformed capabilities must find a mechanism to seamlessly support the national legislation and law enforcement, legally and effectively. This is a fine wire on which to tread, but the rise in aggressive behavior around NATO borders calls for innovative and sensible approaches. As of now, the Alliance struggles to bring all of its combined potential to bear in support of an Allied or of a strategic partner since an elevated threshold of hostility is needed to grant national access to Allied military capabilities. In this scenario, a particularly smart opponent is free to progressively degrade the political, economic, social and security domains to favor its strategic goals, while denying NATO some of its most effective low yield/high payoff military options to strengthen security. More concerning, the same opponent will exploit the troubles artificially induced in society to use its forces as relief, thus gaining precious ground. NATO could consider enabling mechanisms of gradual response and pre-arranged, on-call connectors between national legislations and the use of SOF in order to

cohesively and appropriately respond to hostile human environment degradation that lurks below the threshold of gun-toting warfare.

Conclusion

In Special Operations, degradation of the environment does present opportunities as well as a need for NATO to reconsider its inner workings in the case of hybrid warfare degrading national security. The challenges of a contested electromagnetic spectrum can be more dangerous for SOF when compared to conventional forces, due to the necessity to achieve relative superiority through surprise, speed, precision and enabling supporting capabilities when numbers and firepower are not matched. Uncompromised dedication, habitual relationship down to the personal level and enhanced versatility through wider preparation and expertise are critical areas our nations must continue to prioritize, just as much as ground-breaking technology in small numbers.

Lieutenant General Webb is the Commander of NATO Special Operations Headquarters (NSHQ). NSHQ is the primary point of development, coordination and direction for all NATO Special Operations related activities, in order to optimize employment of Special Operations Forces. He has commanded the 20th Special Operations Squadron, the 352nd Special Operations Group, the 1st Special Operations Wing, the 23rd Air Force, and Special Operations Command Europe. His staff assignments include duty at Headquarters Air Force Special Operations Command, at the Joint Special Operations Command, and in the Office of the Secretary of Defense.

Endnotes

1. 'Defining Critical Technologies For Special Operations' by Maj. L. W. McLaughlin offers a somewhat dated but still very relevant insight from a technological point of view.
2. http://mil-embedded.com/news/army-special-operations-helicopter-pilots-to-use-synthetic-vision-from-rockwell-collins-to-navigate-degraded-environments/
3. NATO-sponsored research: http://www.aviationtoday.com/rw/military/attack/US-Army-NATO-to-Test-DVE-Systems_87501.html#.VzmL0zbQBD8
4. This example well represents how the search is still open: http://ustar.org/ustar-solicitations/handheld-dismount-kit-for-persistent-precision-navigation-in-gps-challenged-environments-for-military-operations/
5. Example: https://www.wpi.edu/Images/CMS/ECE/Paul_Olson_2012_Presentation.pdf

The End of an Illusion

X

Lieutenant General Ton van Loon, NLD A

'The only way forward is through cooperation.
The unity of all who dwell in freedom is their only sure defense.'

General Dwight D. Eisenhower

In 2014 Europe had to come to terms with the fact that not all neighbours are always nice. The Russian invasion into Ukraine and the shooting down of flight MH17 pointed out painfully that the illusion of eternal, and most of all cost-free, peace in Europe was just that: an illusion. Peace is not for free and requires hard work and financial commitment. In the words of Dutch defence minister Jeannine Hennis: 'I would like to underline that security comes at a price. And our need for security justifies paying that price. At some point, we may be forced to act militarily in order to remain secure on the European continent.'[1]

On the other hand, however, 2015 put the focus on another threat to European peace and stability. The influx of refugees and the impact of terrorist attacks (culminating in Paris) showed that security cannot be seen only in geographical terms. Instability and war, in the Middle-East and in Africa, has had an immediate impact on Europe. ISIS or Boko-Haram barbarism coupled with utterly corrupt and often equally barbaric regimes

have resulted in mass migration towards Europe. We could have seen this coming but we preferred to remain in a state of denial or in the words of Thomas Gray, 'ignorance is bliss'. The immediate impact of instability means we have to rethink how, but more importantly, the reasons why we get involved.

European interests are not merely geographic in nature and therefore its defence can also not be seen solely in geographical terms. Not only the refugee problem but also access to natural resources, freedom of navigation and of course terrorist safe heavens are all very legitimate security concerns that are not necessarily geographic in nature. The current vice chairman of the European Commission Frans Timmermans remarked in 2014 that if we fail to export stability, we will sooner rather than later import instability and if that happens it will not only threaten our economy but all of our values.[2] Even he, probably, did not predict the speed at which his comments became true. The consequence is that while until now, most missions outside NATO territory were seen as 'wars of choice', they are now turning into 'wars of necessity'. Nations have gotten used to doing crisis response operations out of choice and with a limited engagement in these missions, both in time and volume. To deal with the instability impacting our nations directly, it is very likely stabilization missions will be needed for a longer period of time and with much greater resolve. Politicians like to focus on solvable short-term problems but the speed at which instability is now being imported will force a discussion on longer-term solutions. After ISAF it was often heard that NATO (nations) have lost their appetite for such big involvement. That is probably true, but the choice is not ours anymore. We do not pick the crisis; the crisis affects us.

NATO, and especially its European nations, must realize that it needs military capabilities that can deal with both geographical, old school, threats but also with new school, complex threats. It is not a good idea to differ-

entiate between (national or collective) defence forces and crisis response forces. We need to have forces that can serve our security interest across the entire spectrum.

The biggest change in the European mindset that must occur is the understanding, not only in words but also in deeds, that Europe must invest in its own security to defend its territory but also its wider security interest. Si vis pacem, para bellum.

Geographical Threats and Degraded Environment

The aggressive Russian stance in the Ukraine has certainly resulted in renewed attention to the defence of NATO territory. One of the key problems here is that most of the discussion focusses on a potential area in which an incursion might take place. For instance: what if Russia invades one of the Baltic states. The use of air power to kick such an invading force out is not as easy as it has been in the era of crisis response operations. One problem is obviously the ability of this particular potential opponent to deny air access through A2/AD. In the words of General Gorenc: 'The advantage that we had from the air I can honestly say is shrinking, not only with respect to the aircraft that they're producing, but the more alarming thing is their ability to create anti-access/area denied [zones] that are very well defended by batteries of ground-based anti-aircraft missiles.' [3]

The problem here is that we still seem to think one dimensionally and most of all in a limited manner in our response to such an attack. If Russia attacks, let's say Estonia, our response should be to recognize that all NATO nations consider themselves under attack. This immediately would make A2/AD a lot more difficult. Defending against an invading force in a limited area, such as the Baltics, is possible but how do you defend the entire NATO Russia border? Even the best, most capable anti-aircraft

missile batteries cannot be everywhere. If we allow an invading enemy to choose the terrain on which to fight we give away a huge advantage. We should not. Fighting an enemy in a frontal assault in a very limited battlespace is not a good idea. French military theorist Ardant du Picq (1821–1870) puts it this way: 'Maneuvers are threats, he who appears most threatening, wins.'

During the Cold War NATO land forces stood shoulder to shoulder along the inner German border basically doing deterrence by denial. It is hard to see how we could do that today with the limited resources available. However, we could do deterrence by punishment. If a potential enemy is convinced the price to pay for aggression is too high, it is very likely he will reconsider. The most crucial element in collective defence is solidarity and cohesion. Article 5 of the North Atlantic Treaty revolves around the idea that an attack on one is an attack on all. During the Cold War no-one doubted this idea and that was the defining deterrent against an attack. In the 25 years since the fall of the Berlin Wall, Europe has been cashing in on the peace dividend. That not only resulted in declining defence budgets but also in a general reluctance to look at the big picture. Especially for air power, this desire to see even Article 5 attacks as a localized threat is very counterproductive. Air Power is most effective when its inherent flexibility can be exploited fully. There is nothing more maneuverable then air power!

In order to execute effective deterrence, capabilities must be convincingly demonstrated. Exercises should far more than today also focus on the message NATO sends to any potential adversary. Deterrence through training, however, cannot be limited to NATO spearhead forces (NRF, VJTF) without a credible buildup of much larger forces. In other words: the VJTF spearhead must credibly be followed by the rest of the spear, and, to stay with the metaphor, it will also only be effective with a strong athlete (or warrior) holding the spear.

Ultimately the degrading effects on NATO air power will depend on our (political) will to outmaneuver an invader. But far more importantly, we need to make sure that no-one believes they can get away with attacking NATO, not in the north- or south-east flank, nowhere.

Non-Geographic Threats and Degraded Environment

The reemergence of a geographical threat to NATO territory is however only one of the threats facing NATO countries. One could even argue it is not the biggest problem. The influx of refugees and the series of terrorist attacks have had an immediate impact on our societies. Comprehensiveness is the only way forward; as defence without development makes as little sense as development without defence. Hardcore defenders of strict separation between military and other actors need to realize that much more can be done by synchronizing efforts. The current refugee crisis cannot be dealt with by defending the borders, or by building walls, alone. At the height of the crisis, even last October, the UN World Food Program was not able to raise all the funds needed to feed the Syrian refugees in the region[4]. When refugees in the region are not receiving enough to survive, why are we surprised that they try to move somewhere else?

As such, this threat is maybe not bigger but certainly more imminent. Federica Mogherini, High Representative of the European Union for Foreign Affairs and Security Policy, in March 2015 at the EU Inter-parliamentary meeting in Riga, talked about 'the new security challenges posed by the so-called 4th generation's warfare, a hybrid war, which is manifested as a combination of a use of irregular and conventional military methods as well as elements from cyber, economic and information warfare, and political pressure'.

The consequence of the need for a wider context in which the military contribution must fit, is the fact that military action is dependent on

actions by others. If the building does not take place, the clear and hold cannot be very effective. The military then taking over the responsibility for the building as well is not a preferable solution. The PRTs in ISAF worked better when they had a strong civilian, development and diplomatic, involvement. On the other side of the spectrum, building something without creating and keeping a secure environment also does not work well. Development without security and especially spending development money without accountability can even be counterproductive[5]. The military can be the enabler for other actors but needs to realize that these other actors will provide the decisive effect.

A potential Russian threat to NATO would almost certainly also have a hybrid nature. It is very unlikely that Russia would use military force alone if it decided to attack us. In this sense, it is highly unlikely that the Cold War scenario will ever return. Dealing with such a hybrid threat would also involve other actors, for instance to deal with a dissatisfied Russian minority that could be exploited. Thinking about a comprehensive approach, and NATO contribution, is therefore not obsolete. On the contrary, it is more important than ever that we develop solid mechanisms for cross-domain synergy.

The new paradigm, therefore, is interdependency which requires a change in military culture. Military leaders need to understand that they cannot make decisions without involving others. Their effectiveness heavily depends on interaction with other, non-military, actors. In the words of General Mattis, USMC: 'if you cannot create harmony across service lines, across coalition and national lines, and across civilian/military lines, you really need to go home because your leadership in today's age is obsolete.'[6]

This is not necessarily a degraded but far more an uncomfortable environment. However, there is one crucial aspect that will degrade the

effectiveness of air power. Almost all recent conflicts have shown that our adversaries are very well versed at using messaging against us. Terrorism is all about creating fear. The actual action is only a tool to achieve that aim. It is not so much about the physical action as the perception of fear. We however usually respond with action supported by messages that often do not reach the target audience. The gap is significant. For instance, the Daily Mail online reported on 6 June: ISIS controls as many as 90,000 Twitter accounts which it uses to spread sick propaganda and radicalize Westerners.[7]

In that sense, the hostile media environment in most (if not all) COIN and CT operations must be seen as a degraded environment, especially for air power. In Afghanistan the Taliban became very versed in capitalizing on any civilian (collateral) casualties. Sometimes civilian casualties were even deliberately caused just to blame the ISAF coalition. The same can also be observed today in Iraq and Syria. Again it is all about the perception, not so much the physical casualties. The only way to deal with this problem is to fully synchronize our actions with our messages. Our motto should be: if you cannot explain what you are doing, you probably should not be doing it.

In dealing with non-geographic threats the degraded environment for air power is not so much about achieving air supremacy, it is far more about achieving pinpoint accuracy and proving just that. Avoiding collateral damage while striking the desired targets is however very difficult, especially if we allow our opponents to continue to control the (social) media.

C2 in the Complex Environment

Interdependency requires a different way of organizing command, changing from a vertical, command-driven approach to a more

horizontal, networked approach. Systems supporting such fundamentally changed thinking about command need to be much more open than today's systems. To work in a networked environment, we surely need to able to talk to each other. In the US military the development of a Mission Partner Environment (MPE) which replaces what was known as Future Mission Network (FMN) is a step in that direction. Based on the experiences in Afghanistan (Afghanistan Mission Network), the idea is to build a system enabling commanders to work with partners (other nations and other actors) in a common security domain.

It would be a big step towards real capabilities to combine forces in Europe if we could decide to build ONE functioning CIS system. Interdependence requires a change in mindset, away from national and military stovepipes. Of course, some things will need to remain secret but being able to communicate should not suffer from unnecessary secrecy.

Strangely enough, the European Defence Agency (EDA) actually has the mission to build just such a system. On the EDA website its says: 'The aim of the GovSatcom initiative is to provide its Member States and European actors with appropriate capabilities through an innovative and sustainable cooperation model. It further signals a new partnership not only between military and civil institutional actors, but also with industry in order to better contribute to the competitiveness of Europe.' That sounds perfect, why are we not using it?

White Papers

Predicting the future has proven to be very difficult. Attempting to define the threats and then calculating the capabilities needed to deal with those threats has not been very successful. For one because threats changed at such a pace

that planning ahead was just not possible. But often, risks that resulted in high costs were written down to accommodate yet another budget cut. The problem with defence is that it is very hard to explain why a capable military is needed when the enemy is not at the gates. But if the enemy shows up it is too late to build up the military. That fundamental dilemma will not go away. Authors and readers of white papers or strategic defence reviews, therefore, need to recognize that we can never predict exactly what is needed. Flexibility is, therefore, a cornerstone for any security policy.

The current German 'White Paper' process uses a series of meetings with stakeholders (participation meetings) in which the basis is laid for a broad public acceptance for an effective military. Interestingly, these stakeholder meetings look at defence from various angles, asking the question 'what do we want defence to do?' from different perspectives.[8] Asking this question could be a big step towards developing consensus on the capabilities we need. Broad discussion on this topic could also lead to a much better public understanding of the role of the military.

Today changes happen at such a high tempo that it is incredibly hard to plan ahead. A couple of anchor points remain however:

- Future military capabilities will have to rely on others. Joint, multinational and interagency must be elements of any defence development programme.
- Interdependency requires a fundamental change in mindset focusing much more on enabling then on commanding.
- Without enablers nothing works, military capability development must take that into account.

Perhaps the most important certainty is that having a credible military is the best guarantee we do not need to use one.

Endnotes

1. Speech during the Future Force Conference in Mar. 2015.
2. Free translation from Dutch of the HJ Schoo lecture by Frans Timmermans on 2 Sep. 2014.
3. Interview in Breaking Defense, Sep. 2015
4. http://www.wfp.org/emergencies/syria
5. See among others. Linda Polman, the crisis caravan, metropolitan books, Sep. 2010.
6. Quoted from http://www.dtic.mil/doctrine/fp/mission_command_fp.pdf
7. http://www.dailymail.co.uk/news/article-2982673/ISIS-controls-90-000-Twitter-accounts-uses-spread-sick-propaganda-radicalise-Westerners-terror-experts-reveal.html#ixzz4Ap8oDjXz
8. http://www.bmvg.de

Lieutenant General (ret.) Ton van Loon was previously the Commander of the International Security Assistance Force (ISAF), Regional Command South (RC-S) in Afghanistan. During this posting he conducted several operations and continued NATO efforts to implement the 3D (Defence, Diplomacy, Development) programme. He has operational command experience in Kosovo as well as having previously commanded the 43rd Mechanized Brigade and the 1st German/Dutch Corps. He has spent a significant amount of his career focused on German-Dutch military cooperation. He has also served on the Staff of the Royal Netherlands Army.

Preparing NATO for Joint Air Operations in a Degraded Environment

XI

The JAPCC Assistant Director's Closing Remarks

I sincerely hope you enjoyed reading the series of essays provided in our Conference Read Ahead; we asked the authors to write provocative pieces to stimulate your thoughts on how NATO might need to better prepare for future Joint Air Operations. I wanted to take this opportunity to offer my perspective as the Assistant Director on the essays of the Joint Air Power Competence Centre, highlighting many of the topics presented by our authors.

It will be challenging to generate the political will to respond to adversary actions short of war. Crossing the line from degradation which the affected population is willing to accept in order to avoid military conflict into that threshold which generates a cry for national response will be difficult to define and will likely be different for many nations. Even effective degradation to highly connected social structures and national economies may not exceed this threshold. In any case, it is imperative that the conversation between senior military and political leaders takes place in order to ensure the public is appropriately informed.

Building resiliency into NATO's C2 structure through procedures, training and robust information technology is imperative. Our information networks must endure through a degradation to a certain extent, and, if they

ultimately fail, we must retain the capability to effectively execute C2 in an offline or degraded mode. Shortening of the C2 chain, ensuring thorough understanding of Commander's Intent, development of standing operation procedures and pre-planned responses will result in the ability to maintain centralized control and decentralized execution even while experiencing some levels of degradation.

Civilian casualties and collateral damage will increase as the level of degradation grows more effective. Risk acceptance will need to evolve in an era of degraded precision weapons. Understanding that a level of collateral damage is part of any targeting process and that it is accepted under the Law of Armed Conflict is only part of the problem, it is convincing a world accustomed to near-zero-miss technology that the application of air power will be effected in a degraded environment. Developing the right communications method to generate awareness and ensure the understanding of the political leadership and public is fundamental.

Obviously, the technical challenges which will be experienced in a degraded environment will be frustrating, from nuisance level cyber intrusions to near blackouts of entire means of communication. This will traverse both the military command structure, the political sphere and the social structure of the general population. Application of military power will be effected by anti-access technology, not the least of which is the prevalence of double-digit SAMs which affect all domains (air, sea and land) and offer a level of air superiority to an adversary in areas which extend over friendly nations. Training will need to evolve to practice operating in a heavily contested and hostile environment, perhaps without unimpeded access to communications, or AWACS or GPS. In fact, with tailored tactics and procedures and vigorous training, we might even exploit this degradation for our own advantages as well.

The themes covered in these essays are certainly not all inclusive; at the conference our panel members will expound upon these themes as well as adding in additional thoughts from their field of expertise. I invite you to visit our conference website to further explore details regarding the panels, the topics and themes and the registration process for this year's conference: https://www.japcc.org/conference/

The end goal of this conference is not to present or develop solutions to the tactical challenges of how to prepare. That lies within the realm of Alliance commanders, at both the NATO and the national level. JAPCC hopes to open a dialogue among those senior leaders and their staffs, raising awareness of the challenges and considerations of operating in a degraded environment and setting the stage for a move towards the preparedness that NATO needs.

In closing, I hope you enjoyed the reading and that this has piqued your interest. There is much work to be done in order to better prepare NATO as a force to more capably conduct air operations within a degraded environment.

I sincerely hope to see you this fall in Essen.

Madelein Spit
Air Commodore, NLD AF
Assistant Director, JAPCC

Conference Itinerary

4 October 2016	
17.00–18.00	Registrations
18.00–20.00	Icebreaker and Industry Showcase

5 October 2016	
08.00–09.00	Registrations
09.00–09.30	Inaugural Session with JAPCC Director's Opening Address
09.30–10.15	Key Note Speech
10.45–12.15	Panel 1: 'Defining a Degraded Environment'
12.15–13.30	Lunch
13.30–15.00	Panel 2: 'Political and Strategic Level Considerations'
15.30–17.15	Panel 3: 'Degraded Air Operations and its Effects on Civil-Military Cooperation'
17.15–17.30	Closing Remarks
19.30–22.00	Networking Dinner

6 October 2016	
08.00–09.00	Registrations
09.00–09.30	Opening Remarks / Key Note Speech
09.30–11.00	Panel 4: 'How Does Degraded Air Capability Impact Joint Force Operations?'
11.30–12.00	Closing Session
12.30–13.30	Lunch

This page intentionally left blank.

Joint Air Power Competence Centre

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