Joint Air & Space Power Conference 2018

THE FOG OF DAY ZERO

JOINT AIR & SPACE IN THE VANGUARD

9–11 OCTOBER 2018

READAHEAD

Joint Air Power Competence Centre

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

READAHEAD

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

Joint Air and Space Power Conference 2018

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

Esteemed Colleagues,

It is my privilege and pleasure to serve as the moderator for this year's Joint Air and Space Power Conference, which will be hosted by the Joint Air Power Competence Centre (JAPCC) 9–11 October 2018 in Essen, Germany. As you have already noted from the cover of this read-ahead, the theme of this year's conference is:

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

The expression 'Fog of Day Zero' is a concept used to indicate that in modern warfare it is not always clear at what point in time there actually is a state of war. The days of nations formally declaring war on one another are past. The uncertain situation is caused by the fact that a modern adversary (who does not even have to be a state actor) can already commit actions which could be seen as a hostile act, but which may not be immediately recognized as such by the victim. For this reason, the expression 'Day Zero' is also not well defined in time. It is not a specific point in time nor does it imply a specific length of time.

What 'Day Zero' does imply is a situation of uncertainty: is there an attack going on, if so who is the attacker, what are his intentions and does this mean there is a war on? This situation of uncertainty is very often denoted as 'fog'. Unlike the NATO-USSR stalemate in past decades, a modern adversary has many options to inflict damage, cause casualties, cause confusion and thus influence the strategic and tactical situation, without overt military action, and perhaps without the target being aware it is under attack. An example of unclear hostile acts are cyber-attacks. Cyber-attacks may cause a lot of damage to infrastructure in areas such as energy provision,

public transportation, money traffic etc. and be very difficult to attribute to the party responsible. Another option for the attacker is 'fake news', which on occasion might be supported by 'real live coverage of events taking place' in order to aggravate and destabilize the population and in turn the nation or Alliance. A good example is what is now known as the Ukrainian crisis. Initially, it was not clear whether the 'rebels' were in fact dressed-up Russians soldiers … Now there is more clarity, and it is also clear that cyber warfare did play a significant role in this conflict.

Contrary to the situation in the 1990s and 2000s, where NATO was largely unopposed as the sole military superpower on the globe, recent years have seen the re-emergence of near-peer and even peer competitors. The competencies of these Near Peer opponents in cyber, electronic and information warfare, and in some cases space, are known, and growing, and thus so is the complexity of the associated challenges.

Also in NATO countries, a lot is invested in topics like cyber, EW etc. At the same time there is also a strong dependency on electronics and computers, and therefore 'vulnerability'. The situation in space in that regard is very interesting. A lot of the national systems used by NATO, including some weapon systems, are dependent on electronic provisions like GPS-navigation and timing. If the opponent is able to effectively jam or even take out the GPS, those systems may well be rendered useless.

Satellites are also used for ISR, which has a significant role in information gathering. What is the situation if all of a sudden, reliable information provided by those satellites is no longer available? Should that lead to the conclusion that there is a war on and is it possible to determine who the opponent(s) is/are?

Day Zero, although not well defined, does require that not only the military, but also the civilian population are prepared. This requires resilience to act

in uncertain situations, but also to be able to cope with cyber-inflicted damage and disruptions. For the military, it is important to look at weak spots that may have developed over the years. An example is the dependence on contracted civilian companies to provide crucial support. With respect to dependencies, we should consider communication networks, transportation, maintenance and repair and stockpiling. There may not be a problem, but it is certainly worthwhile to take a close look at these subjects and determine how robust and resilient our Alliance is in this regard. Force protection deserves special attention since this may prove to be the game changer in the 'Fog of Day Zero' and crucial in preserving our fighting capabilities in the onset of war.

To prepare for the above-described situations requires training and education. People should be trained to follow procedures, but also to think out of the box. They should be trained to think in situations where significant loss of capital assets has taken place, where the opponent's intentions and manoeuvers are unclear and where even the position and movements of friendly forces may be blurred. And of course, this should be done in a joint manner. Air assets and Special Forces may be the only means available to react quickly to a hostile act; this implies that in training these assets, the colour of uniforms should be irrelevant!

In the following chapters, you will find articles that address aspects of the various topics mentioned above, intended to provide food for thought and to generate critical questions about the way ahead for our Alliance. It will be interesting to see and hear the various introductions during the conference, but also the hopefully lively discussions on these topics. This is your opportunity to contribute and we look forward to seeing and hearing from you in Essen in October!

André van Koningsbrugge (M. Sc.)
Commodore (WE) RNlN (ret.)

Table of Contents

Moderator's Foreword ..... **V**

I **Threat Awareness** **1**
The Not-So-Stable Stability 1
Geophysical and Space Dimension 2
Electromagnetic Dimension 3
Information Including Cyber Dimension 5
The Hybrid and 'Asymmetric Bird' Dimension 6
Non-conventional Dimension 8
In Conclusion, the Alliance is Challenged 9

II **Baltics Beware: Russia's Conventional Forces Outgun NATO Near its Borders** **15**
The Atlantic Alliance is ill-prepared to Deter Russian Aggression 15

III **Potential Counter-Space Scenarios on Day Zero** **19**
Introduction 19
Step 1: In Preparation of Day Zero 20
Step 2: The Fog of Day Zero 21
Step 3: Day Zero and After 22
Conclusions 25

IV **Cyberspace and Cyber-Enabled Information Warfare 29**
A 'Fog' Machine in Modern Conflict 29
Introduction 29
Russian Information Warfare 30
Cyber-enabled Information Warfare and the Ukraine 33
Cyber-enabled Information Warfare and Joint Air Power 34
Conclusion 35

V **Force Protection on Day Zero 39**
Setting the Scene 39
Deterrence 41
Deterring 41
Delivering Deterrence 42
Enhanced Forward Presence at the Rear 44
Summary 45

VI **Resilience: A Core Element of Collective Defence 47**
Virtual Vulnerabilities 47
Civil Preparedness 49
Five Specific Areas Come to Mind 51

Table of Contents

VII **Outsourcing Logistics. One Step Too Far?.....59**
Conclusion.....63

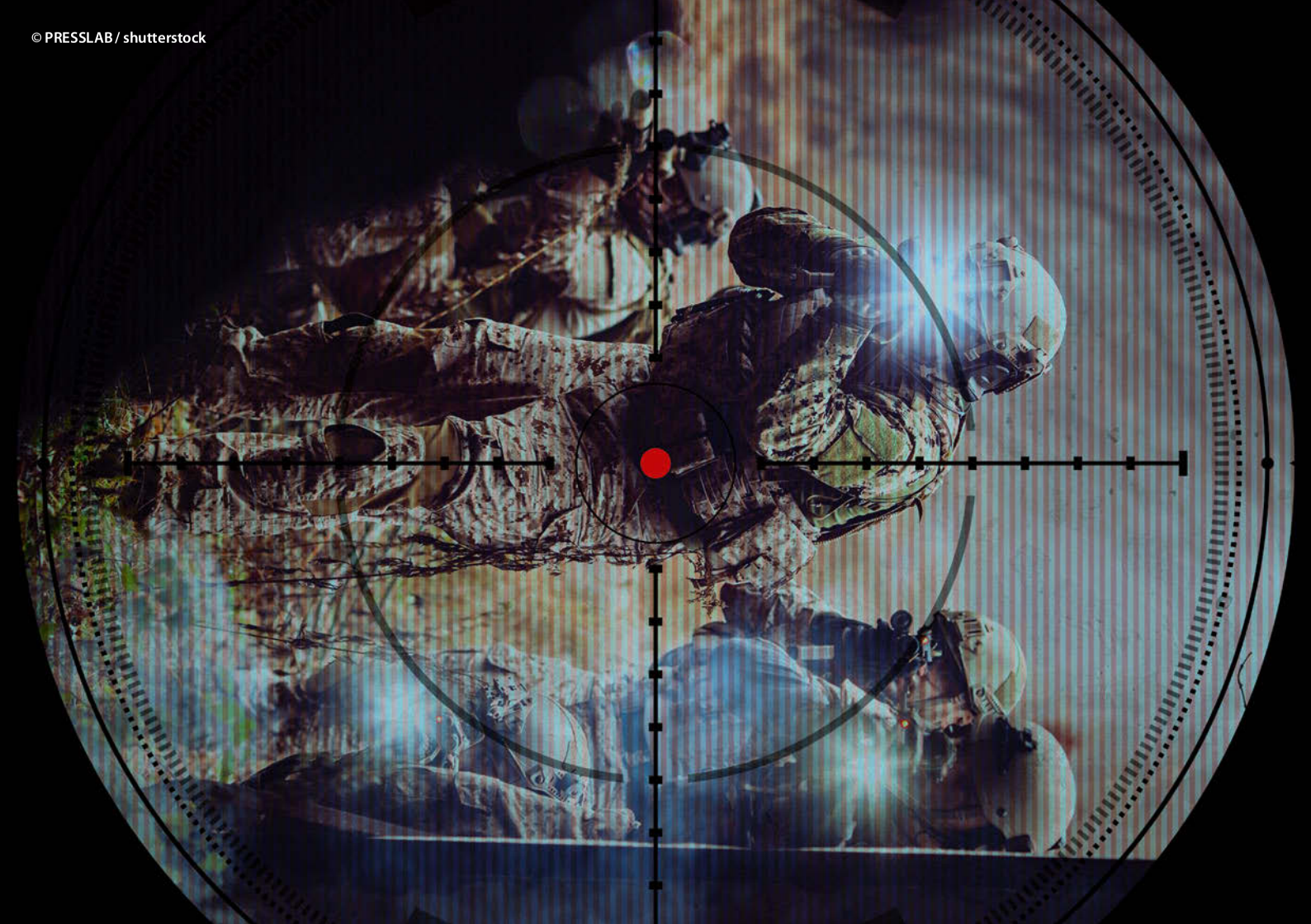
VIII **Exercises and Training Preparing for Day Zero.....67**
Introduction.....67
What Does Not Work?.....69
Joint Challenges require Joint Solutions.....70
What Does Work?.....71

IX **Joint Project Optic Windmill and Day Zero Operations?....75**
Introduction.....75
Multinational Integrated Air and Missile Defence
Exercise Joint Project Optic Windmill.....76
JPOW and Day Zero Operations.....78

X **NATO-EU Relations and Day Zero Challenges.....83**
Introduction.....83
The NATO-EU Joint Declaration and Proposals.....85
PESCO.....87
Conclusion.....89

XI **The Significance of Day Zero.....93**
The Executive Director's Closing Remarks.....93

Conference Itinerary.....98


© PRESSLAB / shutterstock

Threat Awareness

1

Lieutenant Colonel Panagiotis Stathopoulos, *GRC, Air Force*

The Not-So-Stable Stability

In the 2016 Warsaw Summit, the Heads of State and Government (HOS/G) clearly declared in its statement[1]: 'the Alliance faces a range of security challenges and threats that originate from the east and from the south; from state and non-state actors; from military forces and from terrorists, cyber, or hybrid attacks. The greatest responsibility of the Alliance is to protect and defend our territory and our populations against attack. And so renewed emphasis has been placed on deterrence and collective defence'.

Last year's confrontation between North Korea and the United States over Pyongyang's nuclear program, a strained NATO–Russia relationship, the Iran nuclear deal, advancing nuclear modernization programs around the world and the India-Pakistan nuclear arms race dominated world headlines. Even though global power is shifting from West to East, many factors[2] such as asymmetric demographic change, increasing urbanization and polarized societies (especially in the developing world), easy access to Commercial Off the Shelf (COTS) emerging technologies, and economic and resource globalization are shaping a rapidly

changing, complex environment, which subsequently increases the potential for instability.

Additionally, state and non-state actors are deploying non-attributable tools, such as hybrid and cyber activities, to impact the global security environment under the threshold of conflict.[3] This latter edge of this so-called 'grey zone' is the threshold between peace and crisis or war, and for the scope of this paper could be defined as 'Day Zero' of Alliance operations towards a conflict. NATO forces may be required to engage offensively and defensively with any emerging threat during the 'Day Zero' of an armed conflict. Which begs the question, "Is NATO aware and prepared to engage any emerging threat in the 'fog' of early armed confrontation?" To answer that question this article is going to articulate a general awareness and consideration of certain state and non-state actors' capabilities from the East and from the South, which could challenge NATO readiness at 'Day Zero'. Food for thought is also going to be provided by considering the physical and non-physical operational domains, as well as asymmetric and non-conventional aspects.

Geophysical and Space Dimension

Over the last decade powerful state actors from the East, mostly Russia and China (less so North Korea), have developed and refined robust military capabilities in the traditional domains of land, maritime, air and space to deter opposing forces. Information operations, strategic and long-range air operations, advanced integrated air defence systems, precision strike capabilities from air, land and sea weapon systems, and broadband and very low observable multipurpose platforms could be considered major components of their arsenals, all of which can be networked and under centric command.

The term 'Anti Access / Area Denial' (A2 / AD) can be used to describe the effect when many of these key military enablers are combined / overlapped

to create heavily defended 'bastions', in which it is extremely difficult for outside forces to gain access. Even though A2/AD is often presented as a defensive capability, these same capacities could also be employed in conducting or supporting offensive operations as well.[4] Today, there are A2/AD bastions arrayed in the Asia-Pacific region[5] as well as on NATO's eastern and south-eastern flanks, such as Syria, Crimea and Kaliningrad[6], where a blend of command-centric air defence systems, advanced air operations capabilities, powerful electromagnetic operations and capable ballistic-cruise missiles could repel most third-party military operations.

It is important to note that modern warfare is increasingly reliant on information, particularly from space sensors. Because of the expansion of their military operations (both in terms of geography and precision striking information requirements), Russia[7] and China[8] have developed a significant constellation of orbiting satellites with almost the same capabilities as NATO. Their military space capabilities are a key component of strategic deterrence, enabling armed forces to fight 'informatized' local conflicts (i.e. high situational awareness of dispersed forces), likely countering any military third-party's intervention in the region of conflict and supporting operations aimed at protecting the state actor's emerging interests in more-distant parts of the world. It is apparent that the space domain can be used to support and strengthen Command and Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities. Therefore, it is likely that state actors in the eastern and southern regions of the globe will develop and/or modernise their space capabilities towards military purposes[9].

Electromagnetic Dimension

Although the Electro-Magnetic Environment (EME) bridges the geophysical, space and the information environments, success in EME operations is

often a precursor to success in the other operating domains. Indeed, Electronic Warfare (EW) is expected to be a force enabler and multiplier in future conflicts. Russia has consistently invested in EW modernization since 2009, with modernised EW systems entering service across strategic, operational and tactical levels to augment military capabilities[10]. At the same time, Beijing is improving its EME capabilities, which they see as key components of strategic deterrence and as essential to deterring or fighting modern, information technology-enabled warfare[11].

Considering the aforementioned eastern military powers' EME capabilities, NATO military offensive or defensive operations are likely to be challenged in the event of a conflict. Russia's and China's EW capabilities are an integral part of their A2/AD configuration and are clearly tailored to target NATO's C4ISR. In particular, Russia is developing a diverse package of EME operations systems to address a broad set of frequencies and systems of the Alliance. To put it simply, Russia and China have developed offensive and defensive electromagnetic systems which are under joint, highly automated, central command and control[12] [13] [14].

Although EW assets of Russia and China are under joint command and control (C2 of EW), many of these systems are deployable in Unmanned Aircraft Systems (UAS), rendering them low observable, highly mobile and agile, and making adversaries' ability to target and neutralize them more complex and challenging. The aforementioned EW systems not only may deploy an electronic attack but also might support Russia's and China's C4ISR operations in a robust manner. These EW assets are often an integral part of A2/AD configurations, bridging and linking geophysical and space domains, in particular signal intelligence (SIGINT), air defence and precision strike[15].

It is also highly likely that Russian and Chinese EME operations will fuse with cyber operations, allowing EW forces to corrupt and disable computers and networked systems as well as disrupt use of the electromagnetic

spectrum[16]. In particular, NATO must understand that Russia and China have integrated their EME capabilities within all domains of operations, especially cyber, and they may exploit the electromagnetic spectrum in a broad area by conducting and supporting many types of operations, even asymmetric or hybrid conflict ones.

Information Including Cyber Dimension

Although cyber, electronic and information warfighting domains are 'siblings', they are also distinctive. Cyber warfare is about exploiting the challenges of the 'wired' electromagnetic spectrum, while EW is managing the challenges of the 'non-wired' electromagnetic spectrum[17]. However, certain state actors such as Russia and China believe that weaponization of the information dimension[18] [19], including cyber, and employing the latter in times of peace, crisis and war, are a strategic enabler across the spectrum of conflict. Indeed, it implies an intent to become a dominant player in 'grey zone' conflicts by controlling their domestic populations and influencing adversary states.

Considering the 'Russian way of warfare'[20] it's likely that cyber, fused with electronic warfare operations, will be one of Russia's key elements to disrupt, degrade, deny or neutralize adversary command and control and enemy power projection capabilities. Cyber activities could also be an offensive operations tool of non-state actors such as DAESH / ISIS[21] and Al-Qaeda. Cyber operations have the potential for very insidious effects on military operations, in particular during the grey zone threshold of operations in the fog of 'Day Zero'. Several features of cyber weapons such as increased variety, no need of physical proximity, intrinsic data attribution, lack of persistent traces, easiness of concealment, and implementation of delayed effects can contribute to the difficulty of cyber warfare attribution, which are not as readily apparent as traditional means of armed conflict[22].

Similarly, China identified cyberspace as one of its four 'critical security domains' alongside the far seas, space, and nuclear domains[23]. However, cyber tools are not only a weapon of large-scale and capacity state actors such as Russia or China. Over the last few years North Korea has resorted to cyber activities in order to affect its adversaries, with increasing capacity and scale. For example, during the March 20, 2013 cyber-attack on major South Korean banks and broadcasting agencies[24] Pyongyang clearly demonstrated its intent to utilize cyber-attacks as a tool during a crisis.

In addition, the armed forces of Russia and China have developed complex and highly automated networks which may provide fused and high accuracy targeting information to any of their kinetic (and non-kinetic) systems. Their military (and even civil networks) are layered, overlapped and resilient, making their targeting and their denial or neutralization a very difficult task for any adversary.

However, cyber tools can be powerful weapons of any small-scale state actor, as well as non-state actor. NATO planners must be aware that state and non-state actors may employ cyber activities during a peace, crisis and/or war phase of operations. In particular, in the fog of 'Day Zero' offensive cyber activities, fused with EW and information warfare, may be employed insidiously in order to influence adversary armed forces and domestic populations.

The Hybrid and 'Asymmetric Bird' Dimension

When the Russian Army invaded Crimea in 2014, the initial denials of involvement broadcast from Moscow convinced virtually no one, especially since Russia was the neighbouring state and invaders were speaking Russian. Similarly, when artillery munitions strike beyond the forward line of troops, the ballistic trajectory can be traced, the adversary usually can be identified, and a conflict might be attributed to the guilty party.

On the other hand, a low flying 'bird' over a NATO armed force during peacetime could be a scenic and natural condition; it could also be an adversary's biomimetic[25] robotic drone, employing nanotechnology (nanotech)[26] in support of opponents' military aims. In effect, the combination of very low observability and nanotechnology, bridged together with cyber, electromagnetic and information war domains, may prevent attribution of adversary actions and consequently allow the 'scenic bird' to continue its assigned task. This vagueness of attribution is just one challenging element of hybrid warfare, which can be used up to and beyond 'Day Zero'.

Information operations, cyber, proxy groups, economic and political influence, and clandestine measures are just some of the military and paramilitary tools of Russian hybrid operations. Moscow seeks to use hybrid warfare and indirect action to ensure compliance on a number of specific geopolitical strategies; to divide and weaken NATO; to subvert pro-Western governments; to create pretexts for war; to annex territory; and to ensure access to European markets on its own terms. In particular, Russian hybrid warfare strategy objectives are to capture territory without resorting to overt or conventional military force; to create a pretext for overt, conventional military action; and to use hybrid activities to influence the politics and policies of countries in the West and elsewhere.

However, these hybrid capabilities aren't the sole purview of large states. Particularly for non-state actors, access to today's COTS technology may allow adversaries to exploit recent technological innovations in order to deploy indirect or asymmetric actions and the use of asymmetric tactics in hybrid warfare domains are within reach. For example, even as the US and its allies carry out large-scale aerial strikes in Iraq and Syria, their target, the Islamic State (ISIS), may be able to retaliate on another front (e.g. cyber, small UAS, etc.). Even if ISIS may not currently have the capability to carry out large cyber-attacks in an asymmetric war, it is unlikely to find it difficult

to recruit followers with the requisite expertise, such as Al-Qaeda and other similar organizations have done in the past.

NATO military decision makers and planners must be aware that in the grey zone of 'Day Zero' certain state and even non-state actors may employ many kinds of tools in order to support an armed conflict against the Alliance or to support their interests. Hybrid and/or indirect means of fighting can be subtle, but still dangerous, means of warfare.

Non-conventional Dimension

During the March 1, 2018, annual address to the Russian Parliament, the Kremlin leader Vladimir Putin said Russia has developed a new, 'invincible' nuclear-capable cruise missile with 'unlimited' range that is capable of eluding air defence systems[27], thereby highlighting the idea that nuclear power and intercontinental ballistic missiles (ICBM) might be the most reliable and effective means of strategic deterrence. Not only Russia, but China, India, Pakistan and North Korea have modernized their nuclear capabilities so that they maintain prestige and power in the world order.

Apart from strategic nuclear weapons, the aforementioned state actors also have active stockpiles of non-strategic nuclear weapons and warheads. These non-strategic nuclear-capable weapons include air-to-surface missiles, short-range ballistic missiles, gravity bombs, and depth charges for medium range bombers, tactical bombers, and naval aviation, as well as anti-ship, anti-submarine, anti-aircraft missiles, and torpedoes for surface ships and submarines.

Although nuclear weapons are clearly the greatest concern for the Alliance, chemical-biological weapons (CBW), and calibrating how CBW and conventional weapons factor into the current military standoff or raise the

threat of war, are as important today as they have been since the end of World War II. Even though most of the world's state actors[28] have signed the Chemical Weapons Convention (CWC), certain state actors such as North Korea have yet not joined in the Organization for the Prohibition of Chemical Weapons (OPCW). In particular, North Korea is believed to have a varied and robust chemical and biological weapons arsenal.[29] As seen in the last 20 years, such as the Iraq campaign and recent terrorist attacks, the control of CBW is very difficult in an unstable environment and the risk of non-state actors to use CBW is recently increasing.

Even if CBW weapons and their control are not so achievable and traceable, NATO policy makers and planners should be aware that nuclear and biological-chemical weapons are always Weapons of Mass Destruction (WMD), and they might even be employed by small-scale state actors, rendering them high priority threats for the Alliance in the fog of 'Day Zero'.

In Conclusion, the Alliance is Challenged

Aristotle (384-322 BC) said that even the improbable could always be done. All of the threats above warrant enduring vigilance, as many state and non-state actors have proven many times that they can surprise the international community with rapid advances in military capabilities. NATO policy makers and planners should be aware that in the fog of 'Day Zero' any potential state or non-state adversary may employ various kinds of tools in order to achieve its strategic interests and national priorities, as well as to deter any Alliance offensive action or even employ offensive operations.

In the fog of 'Day Zero', NATO Joint Air Force power should be prepared to be engaged with an adversary which might be very capable to fight in any

dimension of operations, challenging NATO readiness and its military capabilities' effectiveness. Even more so, Russia and China have developed vast underground facilities, and their armed forces rely on means of denial and deception in order to obscure and conceal their military actions, ensuring their decision makers and armed forces a high level of survivability, and multiplying their effectiveness.

In these days of not-so-stable stability, certain factors such as increased polarization, power politics and competition, cyber and hybrid tools' employment from state and non-state actors may impact global security, further deepening uncertainty, disorder and complexity. Consequently, NATO is faced with a broad spectrum of evolving threats and must prioritize its efforts to ensure success. These efforts, at least but not limited to, may be focused on:

- **Acknowledging the reality of the threat.** Certain state actors have displayed an incredible leap forward with their military capabilities, making them 'near peers' with various NATO nations in many functional areas. Even more, non-state actors have demonstrated non-lethal capabilities which could be employed through asymmetric (or hybrid) warfare against the Alliance. Therefore, these existential threats should dictate that NATO realistically plan, train and exercise against worst-case foes, and not merely those threats that are easily handled by the Alliance's current force structure and readiness.
- **Enhancing Electromagnetic (EM) spectrum activities' effectiveness.** The increasing mobility and affordability of EM devices necessitate that Alliance EM users should leverage the inherent 'Jointness' of EM devices in order to increase the effectiveness of active and passive electromagnetic operations through all operating domains. Robust mechanisms should be established in order to coordinate and increase effectiveness of all EM activities, including EM Spectrum Management, Cyberspace, Space and (J)ISR in achieving the Alliance's operational objectives.

- **Enhancing 'Jointness' across all operating domains.** NATO has developed the Defence Planning Process (NDPP) in order to identify capabilities and promote development and acquisition by Allies so that it can meet its security and defence objectives. However, NATO's capability to operate in Joint environments has not been fully developed but offers great opportunity to create synergies of effect. Consequently, the NDPP should also ensure that 'Jointness' is enhanced across all domains in order to fully realize the combined / joint capabilities of NATO member nations.
- **Pre-emptive information strategy.** Acknowledging the speed of current and future threats, NATO should not merely rely on reactive information operations, but develop pre-emptive strategies in the information domain, including cyber, in order to effectively counter threats to the Alliance. Employing ISR across all domains, including information / cyber activities, often offers the best opportunity to gain strategic advantage over adversaries in a rapidly changing environment. As a result, NATO could pre-empt its opponents in myriad ways, and could repel or defeat a perceived imminent offensive shortly before that attack materializes.

In summary, in the future the Alliance may be called to manage many crises, which could necessitate that NATO be engaged with a wide range of actors and conditions. The capabilities in which the Alliance chooses to invest are extremely important because, at the end of the day, NATO must be ready to fight, and win, in the fog of 'Day Zero'.

Lieutenant Colonel Panagiotis Stathopoulos (HAF) is an experienced F-16 instructor and functional check flight pilot. He has also served as director of operations and as commander subsequently in the 341 Fighter Squadron from 2012 till 2016. He is currently serving as the Electronic Warfare (EW) including SEAD Operations SME at the JAPCC.

Endnotes

1. Lieutenant General J. Wundrak, et al, 'Joint Air Power Following the 2016 Warsaw Summit: Urgent Priorities', An Allied Command Transformation Headquarters Study conducted by the Joint Air Power Competence Centre, Kalkar, Germany, 2016, https://www.japcc.org/portfolio/airpowerafterwarsaw/, (accessed May 2018).
2. Allied Command Transformation (ACT), 'Strategic Foresight Analysis', Virginia, Norfolk, 2017, http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf, (accessed May 2018).
3. Ibid. 2.
4. Lieutenant Colonel A. Schmidt, 'Countering Anti-Access/Area Denial', The Journal of JAPCC, II (23), Kalkar, Germany, 2016, pp. 69-77, https://www.japcc.org/countering-anti-access-area-denial-future-capability-requirements-nato/, (accessed May 2018).
5. US DoD Office of the Secretary of Defence, 'Military and Security Developments Involving the People's Republic of China 2017', Virginia, 2017, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF, (accessed May 2018).
6. US Defence Intelligence Agency (DIA), 'Russia Military Power', Washington D.C., 2017, http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf, (accessed May 2018).
7. Ibid. 6.
8. K. Pollpeter, et.al, 'The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations', RAND Corporation, Santa Monica, 2017. https://www.rand.org/pubs/research_reports/RR2058.html, (accessed May 2018).
9. B. Preston and J. Baker, 'Space Challenges, in Strategic Appraisal: United States Air and Space Power in the 21st Century, edited by Z. Khalilzad and J. Shapiro, RAND Corporation, Santa Monica, 2002, https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1314.pdf, (accessed May 2018).
10. R. McDermott, 'Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum', A report of the International Centre for Defence and Security (RKK/ICDS), Estonia, 2017, https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf, (accessed May 2018).
11. M. Chase and A. Chan, 'China's Evolving Approach to Integrated Strategic Deterrence', RAND Corporation, Santa Monica, 2016. https://www.rand.org/pubs/research_reports/RR1366.html, (accessed May 2018).
12. Ibid. 6.
13. Ibid. 7.
14. Ibid. 11.
15. Ibid. 10.
16. Ibid. 6.
17. US Army FM 3-12, 'Cyberspace and Electronic Warfare Operations', HQ US Army, Washington D.C., 2017, https://fas.org/irp/doddir/army/fm3-12.pdf, (accessed May 2018).
18. Ibid. 6.
19. Ibid. 5.
20. S. Boston and D. Massicot, 'The Russia Way of Warfare: A Primer', RAND Corporation, Santa Monica, 2017, https://www.rand.org/pubs/perspectives/PE231.html, (accessed May 2018).
21. It is an acronym for the Arabic phrase al-Dawla al-Islamiya al-Iraq al-Sham (Islamic State of Iraq and the Levant).
22. N. Rowe, 'The Attribution of Cyber Warfare', in Cyber Warfare: A Multidisciplinary Analysis edited by J. Green, New York, Routledge, 2015.
23. Ibid. 5.
24. bbc.com, 'North Korea behind South Korean bank cyber hack', 3 May 2011, http://www.bbc.com/news/world-asia-pacific-13263888, (accessed May 2018).
25. Biomimetics or biomimicry is the imitation of the models, systems, and elements of nature for the purpose of solving complex human problems.
26. The manipulation of matter with at least one dimension sized from 1 to 100 nanometres, is defined as nanotechnology.
27. N. Hodge et.al. 'Putin claims new "invincible" missile can pierce US defences', CNN, 1 Mar. 2018, https://edition.cnn.com/2018/03/01/europe/putin-russia-missile-intl/index.html, (accessed May 2018).

28. Member States of the Organization for the Prohibition of Chemical Weapons (OPCW), https://www.opcw.org/about-opcw/member-states/, (accessed May 2018).
29. J. Parachini, 'Assessing North Korea's Chemical and Biological Weapons Capabilities and Prioritizing Countermeasures', RAND Corporation, Santa Monica, 2018. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT486/RAND_CT486.pdf, (accessed May 2018).

Baltics Beware: Russia's Conventional Forces Outgun NATO Near its Borders

11

The Economist
Print Edition | Europe, 8 March 2018

Addendum: *This following article 'Baltics Beware: Russia's Conventional Forces Outgun NATO Near its Borders' (in Print Edition/Europe, 8 March 2018) can be sourced at: https://www.economist.com/*

This article has been removed due to licencing requirements.

This article has been removed due to licencing requirements.

This article has been removed due to licencing requirements.


© Andrey Armyagov / shutterstock

Potential Counter-Space Scenarios on Day Zero

III

Lieutenant Colonel Tim Vasen, *DEU, Army*

Introduction

Today, all nations rely on modern technology, and Space systems in particular, for support that is fundamental to all our activities (consider the importance of satellite communications, the Internet etc ...). We must recall the critical support Space-based systems provide for military operations, such as communication (SATCOM), position, navigation and timing (PNT), intelligence (ISR) and early warning (OPIR[1]). Without these Space supported tools it would be almost impossible to safely and effectively conduct any military operation.

This article aims to stimulate thought about the importance of the 'resilience" of Space-based services, especially when considering NATO does not own any Space assets but relies on Space services provided by NATO member Nations.

This article is based on the experiences of US strategic simulations of threats against Space systems and the consequences on warfighting and civil life with reduced capabilities. It will analyze a possible scenario in three steps, starting from all possible actions accomplished by a Near Peer opponent in preparation of 'Day Zero', through the 'Fog of Day Zero' and,

in the last part, analyzing the scenario of an armed conflict where the Space domain and services are highly affected by the opponent.

Although the scenario uses realistic and established capabilities, only those published in unclassified publications were used. The actions that ultimately bring about war in the Space domain could be seen as a blueprint for actions around Day Zero of a technically highly developed opponent, determined to reduce NATO's technical advantages in warfighting. Another source, included experience from the NATO Trident series exercises of the years 2016 to 2018 and, again, the information was from unclassified publications. Finally, the findings from the same sources are referenced with respect to the dependence on and vulnerability regarding Space-related services.

Step 1: In Preparation of Day Zero

When a Near Peer Opponent comes to the point where to enter into conflict with a NATO country is imminent, it will most likely start by using pre-deployed Space-based ISR systems to prepare the battlefield, collecting data to gather information about infrastructure and armed forces as well as for mapping purposes. These actions, if they do not include orbital manoeuvres and rely mostly on passive sensors, are not detectable by NATO member states.

The Near Peer Opponent is capable of using several Counter Space actions against NATO Space-based and Space related infrastructure. Knowing that NATO member states also have the option of Counter Space actions, it will increase the training and education in standby systems and actions to get an advantage on the battlefield when no Space support is available.

It could be observed that a higher launch rate restores or replaces older Space systems or capabilities. It is possible that in larger constellations, like

PNT systems, spare satellites are launched. All these actions will be supported by media and political statements that the new systems are only for national purposes or go in line with planned commercialization. It is unlikely at this time, prior to Day Zero, that orbits especially designed for the upcoming battlefield would be used.

If the Near Peer Opponent has launch on-demand systems, equipped with mostly ISR payloads, the production rate will be raised to have several systems available to either restore damaged or destroyed capabilities in a short timeline or to intensify capabilities over the battlefield using specially designed orbits for that purpose.

Particular forces, regular (Special Operation Forces (SOF)) as well as irregular (unmarked and known as 'little green men' or partisans), are trained and equipped with special jamming and spoofing capabilities to be used inside the attacked NATO country.

Step 2: The Fog of Day Zero

SOF teams infiltrate the targeted country. Some of them are equipped with PNT spoofing systems to target critical lines of communication and try to cause accidents and casualties by altering navigation positions. Commercial shipping or civil air travel could be the initial target.

In parallel, irregular forces locate positions where the use of PNT or SATCOM jammers could cause the greatest possible disturbance to civil life. There could be attack plans prepared against Space related ground infrastructure to be executed on order.

If the Near Peer Opponent has, for its own defence, the option to establish strong Anti-Access / Area Denial (A2 / AD) bastions, highly capable PNT

jammers will be included, to prevent the use of precision-guided ammunition and to hinder NATO operations.

Some military satellites of the Near Peer Opponent in GEO[2] and LEO[3] release small satellites that are declared as inspector satellites to observe possible damage to foreign systems that have been detected by the Near Peer Opponents' Space surveillance network. They execute orbit changing manoeuvres and bring themselves in co-orbital positions to threaten potential NATO and commercial satellites.

Cyber-attacks against Space related infrastructure are initiated.

Step 3: Day Zero and After

With the start of the border crossing operation by the Near Peer Opponent, massive jamming and dazzling campaigns are launched across the full spectrum. In the area of operation, GPS PNT signals are jammed in all frequencies, suppressing the whole service. NATO forces that have to use the GPS service, by doctrine, can no longer operate effectively. Meanwhile, the Near Peer Opponent can rely on its own PNT system because it uses different frequencies. The same goes for the SATCOM services; Jamming is intended to disable these communication systems while cutting the C2 of the NATO Armed Forces. If there are no redundant radio or cable-based systems available, the impact is significant. To deny the use of ISR satellites, Synthetic Aperture Radar (SAR) sensors are jammed and Electro-Optical (EO) sensors get dazzled by low power, directed energy weapons. The Cyber-attacks against Space related infrastructure and services are increased.

Meanwhile, the forward-deployed spoofing systems as well as the PNT jammers operated by SOF and irregular forces, are used inside the attacked country. In particular, the small PNT jammers, used by irregular

forces in or near cities, airports or military-related logistical facilities, have a major impact on civil life. These impact financial transfers, use of ATM machines, credit cards as well as traffic control, because these services are controlled and coordinated by the GPS PNT system. To enhance the disruption, a massive media campaign as well as political campaigns are initiated to slow down the political processes.

According to the reaction from NATO in the Space domain, all Counter Space actions remain reversible at that time. Reversible in this case means that all the used counter-Space actions do not cause permanent damage to Space systems, the impacts are only temporary and timely as well as regional discriminated.

The absence of Space-based ISR data causes a capability gap. Intel information acquired through Space systems is not available to the decision makers. At a critical moment, the reduced Space services have a significant negative impact on the decision-making process as well as on the planning and executing of military operations. Additionally, the time to prepare decisions increases. Commercial imagery services have to be consulted but could be affected by Counter-Space means as well. The situation is the same for the communication services. Proven procedures for national, military and security data transfer are no longer available. Civilian life is also impacted as communication system services are reduced. The standing backup procedure is to use commercial assets or capacities for national purpose but this is challenging because the commercial market tries to fill its gaps first. The massive effects on civil life and inevitable economic impacts from the degraded Space services result in a 'battle' for the remaining capabilities. Attacks are also carried out against the GPS PNT system, which is degraded in several areas and not usable for precise military actions. The lack of accuracy of the GPS system could also cause the first casualties by friendly fire due to unsafe use of precision-guided ammunition as a result of spoofing. While NATO weapon systems rely,

doctrinally, on the GPS navigation system, the proven standards will not work. The advantage is gained by the Near Peer Opponent for a short to medium time period, but this could very likely lead to a successful military operation and gaining a strong position for the upcoming political and military actions.

To leave nuclear deterrence as the last resort, there will be no attacks nor even jamming / blinding or other attempts on the OPIR architecture of NATO by the Near Peer Opponent, as long as their own OPIR infrastructure is not targeted. From the perspective of deterrence, and in accordance with doctrine, the attack on OPIR infrastructure could be interpreted as comparable to a 'nuclear' attack.

When NATO also uses Counter-Space actions against the Near Peer Opponent's Space infrastructure, with the exception of OPIR, to reduce the advantage, the near Peer Opponent will likely conduct irreversible Counter-Space actions. That means the already deployed co-orbital satellites attack the threatened NATO satellites, likely disable them. There will be also directed energy weapons and missile based interceptors used against NATO and commercial satellites, supporting NATO, aiming to damage and destroy them. All these actions will additionally create a large amount of Space debris that threatens all satellites because of a higher risk of collision. Pre-planned attacks against ground infrastructure, by irregular forces, SOF or even precision-guided ammunition (as long as PNT services are available) could be expected. Cyber-attacks and media campaigns are ongoing. To fill the gap to acquire relevant, intelligence products for decision-making, the Near Peer Opponent uses its launch on-demand services to get back the initiative against NATO for a short or special timeframe.

Meanwhile, the Space war engulfs the whole world when the interruption of PNT services causes a lot of major disruptions of all worldwide traffic- and traffic management systems. The general public recognizes

the situation by their degraded TV and mobile phone services and non-functioning ATM machines. There will also likely be major impacts on stock markets as well as on global trade.

Conclusions

From the NATO perspective, Space Support to NATO operations is essential, which means that the loss of capabilities or services could have a major effect on NATO operations. NATO as an organization does not own any satellites, it has to rely on services, provided by national assets of member states. All Space assets will remain under national control by doctrine. However, the assets are also used for national purposes and normally respond to national requirements first. The 'guaranty' of Space related services for NATO operations, when required, is not fixed by negotiations or memorandums in general. Currently, the Spacefaring NATO member states have agreed to provide Space services, but it has to be negotiated for every new operation. Furthermore, concepts such as 'coordination' and 'redundancy' need to be carefully considered, negotiated and potentially applied by NATO and NATO Nations. NATOs role in order to build 'resiliency' throughout all Space-based services is to find a way to establish a guaranty of service.

This article describes a worst case scenario and should serve as a 'heads up' to what is possible and what could be expected. Although Space Support to operations plays a significant role, backup services have to be developed and exercised. According to the role of NATO, it should encourage its member states in improving the technical and organizational resiliency of its Space systems.

Finally, consideration should be given to any possible action taken by an entity in order to limit / disable NATO member states Space assets. Once

identified that an action has been taken by an entity, it should be determined whether it is a hostile act against a NATO Nation, significant enough to invoke the Article 5 of NATO Treaty. Should NATO reconsider Article 5 as it pertains to Space assets in particular?

References:

- W. Scott, M. Coumatos, and W. Birnes, 'Space Wars: The first six hours of World War III', Forge Books, Apr. 2007.
- W. Scott, M. Coumatos, and W. Birnes, 'Counter Space: The next hours of World War III', Forge Books, Oct. 2009.
- J. Patrick and F. Giudice, 'The key role of Space Support to NATO Operations', in Three Swords Journal, Joint Warfare Center (JWC), Jul. 2017.
- Author's personal experiences during execution of Trident Javelin 17 exercise, as well as supporting Trident Juncture 16 and preparation of Trident Juncture 18.

Lieutenant Colonel Tim Vasen (DEU Army) is a Subject Matter Space Expert at the Joint Air Power Competence Centre. He has a broad background in several ISR and Intel positions. In his previous positions he was responsible for Space Intel at the German Space Situational Awareness Centre (GSSAC).

Endnotes

1. OPIR: Overhead Persistence Infrared
2. GEO: Geo-stationary Earth Orbit
3. LEO: Low Earth Orbit


© Toria/shutterstock

Cyberspace and Cyber-Enabled Information Warfare

IV

Lieutenant Colonel Paul J. MacKenzie, *CAN, Air Force*

A 'Fog' Machine in Modern Conflict

Introduction

When considering military power, the elements that immediately come to mind for achieving operational objectives are the forces within the traditional Maritime, Air and Land Domains. Events in the Ukraine and Crimea, however, demonstrate that modern operations can be conducted below the threshold of war, so not to incite a military response, yet achieve operational effects all the same, through successful employment of actions both through cyberspace and against cyber targets and controlling information in and about the battlespace.

Control and manipulation of information for strategic and operational purposes, Information Warfare (IW), is nothing new. But, the explosive expansion of Information Technology (IT) and Computer and Information Systems (CIS) in the past few decades has acted as a force multiplier, and when exploited by a highly capable state, can prove instrumental in achieving political/military objectives; Russia is a prime example. Russia

does not treat cyberspace as a domain. Rather, it categorizes attacks/exploitation through, and of IT/CIS as a component of IW.[1] There is no direct correlation to what NATO refers to as the cyberspace domain, the closest equivalent term in Russian doctrine is 'information-technology warfare'.[2] As a consequence of the significant overlap of IW with cyberspace, analysts have adopted the term 'Cyber-enabled IW' (C-IW).[3]

This article focuses on cyberspace and the C-IW campaign in modern conflict with the aim of preparing participants of the JAPCC Conference (2018) by stimulating thought and promoting discussion, specifically with respect to the impacts on the projection of Joint Air Power.

Russian Information Warfare

Given NATO's overall superiority in conventional arms, President Vladimir Putin's philosophy is that Russia's military approach must be based on 'intellectual superiority.'[4] Russia will pursue information superiority as a key enabler to victory in future conflicts, employing a mix of military and non-violent means including political, economic, information technological and environmental elements, where mass media and computer networks globally will be exploited,[5] a practice which NATO's critics claim is synergy the Alliance lacks.[6] Furthermore, Russia will employ these measures through the spectrum of international relations, from peacetime (reconnaissance, espionage) to war (cyber-attacks on military systems and civilian infrastructure),[7] to achieve national, strategic objectives. In this respect, because there are varying degrees of cyberspace activity underway continually, there is no real 'Day Zero' in cyber conflict, with the possible exception of an unlikely attack causing severe injury or death, or extensive material damage to reach the threshold for justifying a conventional response by NATO or to trigger an Article 5 declaration.[8]

Conducting operations through cyberspace and against cyber infrastructure, Russia aims at subversion and destabilisation (long-standing practices now enhanced for the Internet age) to undermine confidence, disrupt relations, discredit and weaken authority and government / administrative structures.[9] Through C-IW, including effective use of the Internet, the employment of conventional military resources can be reduced and to a point, as some senior Russian military personnel have indicated, that armed intervention may be avoided altogether. [10]

An excellent illustration of how to execute IW is highlighted in Keir Giles' Handbook on Russian IW, in which he cites Russian Doctrine in a short synopsis of the principle objectives when exploiting the mass media:

- 'Direct lies for the purpose of disinformation both of the domestic population and foreign societies;
- Concealing critically important information;
- Burying valuable information in a mass of information dross;
- Simplification, confirmation and repetition (inculcation);
- Terminology substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events;
- Introducing taboos on specific forms on information or categories of news;
- Image recognition; known politicians or celebrities can take part in political actions to order, thus exerting influence on the world view of their followers;
- Providing negative information, which is more readily accepted by the audience than positive.' [11]

Creating misinformation and confusion by broadcasting these IW 'tools' through modern IT / CIS serves to intensify the ever-present 'fog of war' so common to all conflicts and with which one actor exploits the ambiguity

and through which the opponent is left to sift and navigate to ascertain the most accurate picture of realty. The Russian military exploit the expanse of the Internet to not only create confusion but to attack an adversary's decision-making and command and control networks. Extensive interconnectivity also allows penetration of a state's entire information network with potentially devastating consequences. The explosion and exploitation of social media that catalysed destabilization activities in the Middle East (Syria) and Africa (Libya) are cited by Russian authorities as perfect examples of the existential threat posed by unregulated control of the Internet.[12]

Of course, cleverly packaging press releases to win the IW campaign or designing and initiating cyber weapons to take over the IT / CIS in order to control the message is completely unnecessary if one side is capable of taking physical control of the Internet infrastructure, which was done in the initial phase of the annexation of Crimea. Russian forces seized control of the Simferopol Internet Exchange Point and altered the connectivity / cabling to the mainland and achieved total information dominance on the peninsula.[13] The significance of cyberspace as an enabler in modern operations is further evidenced by Russian SOF employment of telecommunications experts within their ranks. The reader should not be deceived into believing the extent of the influence is limited to tactical, unit-size targets, as Russia is increasing investigation into foreign Internet infrastructure and of international undersea telecommunications cables.[14]

In explaining the sense of urgency, Keir Giles quotes the US Director of National Intelligence writing 'Russia is assuming a more assertive cyber posture based on its willingness to conduct operations even when detected'[15] and supports the warnings in NATO's Framework for Future Alliance Operations that NATO nations must be ready to function in the event of loss or degradation of cyber infrastructure, from servers to undersea

cables, and where access to Internet services may be completely denied.[16] Not to be excluded is Russia's Electronic Warfare (EW) capability, also considered an element of IW in their doctrine, which was deployed in eastern Ukraine to spoof and jam GPS signals and defeat navigational and guidance systems. All this to say, NATO must be prepared to operate under conditions of degraded communications. Even Russian generals conceded that their own officers required retraining after becoming too dependent on IT / CIS and were unable to a conduct 'low tech' war. [17]

Cyber-enabled Information Warfare and the Ukraine

The successful operations by Russia against the Ukraine in 2014 'both included and relied upon cyber'[18] and direct lines of correlation can be drawn to the doctrinal concepts explained above. While the West is resistant and philosophically divided on whether and how to exploit cyberspace militarily, Russia has many strategies and tactics where cyber is integrated to within a 'whole of government approach'.[19] It has been proposed that two distinct effects of cyberattacks were demonstrated in the Ukraine conflict, the strategic effect of reducing the will to fight (i.e. through impacting mass opinion) and the tactical effect to reduce military capability (i.e. interrupting service to military systems).[20] There are conflicting opinions among Western cyber analysts as to whether the conflict in the Ukraine even constituted cyberwarfare. For instance, while the conflict revealed a plethora of cyber activity including espionage, defacements, hacktivism and denial of service attacks, in their entirety they do not constitute cyber warfare as currently defined by some Western cyber security analysts.[21] This is in contrast to the assessments of other experts who referenced physical and digital attacks on servers, mobile phones and internet accounts, cutting of cables, commandeering and compromising infrastructure as phenomena characteristic of cyberwarfare.[22] Another practice common in a cyber campaign is for states to carry out operations through

proxies in order to permit plausible deniability. Yet, proxies played a very minor role in the action in the Ukraine,[23] further evidence that Russia is not at all apprehensive about detection.

Cyber-enabled Information Warfare and Joint Air Power

In times of crisis air power assets are first to respond, the vanguard, due to their speed, reach and precision, and air power is in more demand today than ever because of the reluctance of deploying ground forces.[24] Consequently, air power is a primary target for NATO's opponents during an IW campaign and its significance is increasing. NATO's adversaries typically claim that NATO is the aggressor, contravenes international law, bombs indiscriminately and kills innocent civilians, all with the intent to drive a wedge between the public and the Alliance and weaken NATO's unity, determination and resolve to act.[25] Unchallenged, an opponent's campaign against air power can progress and develop rapidly, even to the extent where the international community can be convinced to develop laws restricting the use of some forms of Air Power weaponry. The 2010 Treaty banning the use of cluster munitions is such an example, where a rapid campaign was launched under the guise that the ban would save lives, while valid counter arguments that the use of alternative weaponry could result in greater loss of civilian lives were not equally debated. Consequently, most Alliance Air Forces can no longer use a weapon that would be of great use in a conventional war.[26] Numerous mediation measures have been proposed and centre on the theme of establishing a robust and rapid counter-IW campaign plan. One Doctrinal Recommendation, to cite an example, includes quickly declassifying Bomb Damage Assessment (BDA) imagery and posting it to a website for the public.[27] Achieving this is a challenge even within our own Alliance IT / CIS, but accomplishing this outside of NATO's AOR in an operational area where the adversary has achieved information superiority

and control over cyberspace would be unlikely. Critical to success will be NATO's ability to maintain control over its Cyberspace infrastructure and defend its systems and networks, in accordance with the Enhanced NATO Policy on Cyber Defence[28] and the Revised Cyber Defence Action Plan,[29] as well as Alliance member nations honouring their commitment to defend their national Cyberspace, as described in the Cyber Defence Pledge of 8 July 2016.[30]

Conclusion

Ultimately, the primary objective in a C-IW campaign, as part of a comprehensive approach to warfare, is to influence the minds of the masses, and though the role that media plays (mass and social) must not be understated, Cyberspace is the principle enabler in this Internet-era. As an Alliance we must recognize that a well-executed C-IW Campaign can achieve strategic and operational effects that historically have been considered possible only by the employment of conventional forces. These campaigns are sustained by controlling (exploiting and attacking) Cyberspace. So, while the Alliance must be ready to deliver its own message to counter the opponent's IW tools, it must also safeguard its cyberspace infrastructure, the primary means by which its message is promulgated, while at the same time being prepared to operate in a highly degraded environment if it fails.

Questions for consideration:

1. Is the Alliance capable of adequately synergizing military and non-violent means to achieve a holistic approach, including Cyber effects, or are its critics correct in saying NATO lacks this synergy? If that is the case, what must be done to bridge this gap?

2. Reconnaissance and espionage are generally acknowledged as accepted practices of statecraft (when done for purposes of national security only). Have we the indicators to be able to recognize when an opponent's C-IW campaign has progressed beyond these accepted practices into subversion and even destabilization and are we, as an Alliance, ready to respond in kind?

3. Is NATO doing enough to counter opponents' IW 'Tools' particularly in that Keir Giles cites many as Doctrinal practices and what the Alliance should expect to see in future conflicts?

4. NATO agencies commit a great deal of resources to defend our Systems and networks from Cyber-attacks. Do we work close enough with our civilian agencies to be able to understand that they do the same and are we aware of the degree to which nations are honouring the Cyber Defence Pledge, not only from a Cyber Security but a Physical Security / Force Protection point of view as well?

5. Do our militaries accurately understand the dependence on cyberspace, enough to prepare be able to operate effectively in a severely degraded environment? Assuming the answer is currently 'No', should we be training and exercising for this scenario? What will it take for us to conduct exercises with degraded IT/CIS? Should we consider project options in the future that include retrograding vice upgrading the cyber systems we depend upon? Is Joint Air Power more dependent on Cyber and, therefore, more vulnerable to a degraded environment and does this exacerbate the vulnerability of the Alliance overall?

Lieutenant Colonel Paul J. MacKenzie (RCAF), JAPCC Cyberspace SME, examines the many facets of Cyber as it relates to NATO Joint Air Power and from a defensive perspective through to the potential in exploiting offensive effects.

Endnotes

1. K. Giles, 'Handbook of Russian Information Warfare', NATO Defense College, NDC Fellowship Monograph Series, Rome, Nov. 2016, p. 8.
2. Ibid., 9.
3. J. Wirtz, 'Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy', in 'Cyber War in Perspective: Russian Aggression against Ukraine', Geers, Kenneth (Ed.), NATO CCD COE Publications, Tallinn, 2015, p. 36.
4. Ibid. 1, 3.
5. Ibid. 1, 6.
6. Ibid. 1, 7.
7. Ibid. 1, 10.
8. P. McLeary, 'NATO Chief: Cyber Can Trigger Article 5', https://www.defensenews.com/home/2015/03/25/nato-chief-cyber-can-trigger-article-5/, (accessed 14 Mar. 2018).
9. Ibid. 1, 11.
10. Ibid. 1, 18.
11. Ibid. 1, 47.
12. Ibid. 1, 43.
13. Ibid. 1, 49.
14. Ibid. 1, 65.
15. Ibid. 1, 67.
16. Ibid. 1, 67.
17. Ibid. 1, 68.
18. Sakkov, Sven, 'Foreward' to 'Cyber War in Perspective: Russian Aggression against Ukraine', p. 8.
19. Giles, Keir, 'Russia and Its Neighbours: Old Attitudes, New Capabilities', in 'Cyber War in Perspective: Russian Aggression against Ukraine', p. 21.
20. Lewis, James Andrew, 'Compelling Opponents to Our Will: The Role of Cyber warfare in Ukraine', in 'Cyber War in Perspective: Russian Aggression against Ukraine', p. 40.
21. Libicki, Martin, 'The Cyber War that Wasn't', in 'Cyber War in Perspective: Russian Aggression against Ukraine', p. 50.
22. Pakharenko, Glib, 'Cyber Operations at Maidan: A First Hand Account', in 'Cyber War in Perspective: Russian Aggression against Ukraine', p. 61.
23. Maurer, Tim, 'Cyber Proxies and the Crisis in Ukraine', in 'Cyber War in Perspective: Russian Aggression against Ukraine', p. 86.
24. J. Corum, PhD., 'Mitigating Disinformation Campaigns Against Air Power', Joint Air Power Competence Centre (JAPCC), May 2017, p. 20.
25. Ibid., 172.
26. Ibid., 45.
27. Ibid., 182.
28. 'Enhanced NATO Policy on Cyber Defence (NR)', NATO, PO(2014)0358, 27 May 2014. Only unclassified information has been quoted.
29. 'Revised Cyber Defence Action Plan (NR)', NATO, PO(2017)0077, 10 Feb. 2017. Only unclassified information has been quoted.
30. 'Cyber Defence Pledge', NATO, https://www.nato.int/cps/en/natohq/official_texts_133177.htm, (accessed 14 Mar. 2018).


© metamorworks/shutterstock

Force Protection on Day Zero

V

Wing Commander Jez Parkinson, *GBR, Air Force*

Setting the Scene

Introduction. Many conflicts have been decided by the ability, or inability, to hold vital ground[1]. Rommel was defeated in North Africa because his lines of supply were cut and the British lost Crete because they failed to recognize the importance of Maleme Airfield and to protect it accordingly.

'When one comes to consider that supplies and materiel are the decisive factor in modern warfare, it was already becoming clear that a catastrophe was looming on the distant horizon for my army.'

General Erwin Rommel

Context. The second half of the twentieth century was a bipolar world dominated by the Cold War between the United States of America/NATO and the Soviet Union. However, those days are gone and the world is now a far more complex place. Put simply, NATO is now surrounded by threats *(to include within the Cyber Domain)* so, if there are 360-degree threats, the Alliance must respond accordingly. NATO still has to be capable of holding vital ground as well as deterring an adversary, but what it has to hold, how and from whom, is now a more significant challenge.

Threat. It is easy to be overwhelmed by the current discussion of global threats but, in its most basic form, for any adversary to pose a threat, they have to have both the *capability* to do NATO harm and the *intent* to do so; without both components, there is no credible threat. When discussing how to respond to potential threats, by considering the threat posed by each adversary in turn, allows a list of responses to be developed. Some measures will be appropriate for all adversaries whilst certain adversaries, will require tailored responses. Irrespective of the threat-actor it is suggested that there are several inevitabilities going forward. Firstly, at some point an adversary will 'get lucky'. NATO has to be prepared for a successful attack and have immediate response, recuperation and business continuity plans in place at all locations. Second, traditional geographic boundaries are irrelevant; there is no such thing anymore as a 'rear-battlespace'. Air and Space Power is the Alliances strategic advantage so, why confront the latest platforms in the environment where their performance is optimized? Far better to destroy them at their home base if that is where they are least protected. An attack on the Homefront, will also likely have a very different impact on the will of member states to react. Finally, in a world with 24-hour news, much has been made of the concept of the 'strategic corporal[2]'. The same concept applies to our adversaries; a lone actor, with access to resources could have a huge impact. Also considered in this category, the reality of an 'insider threat[3]' within Alliance territory.

Question: *Is sufficient emphasis being placed on the threat posed by non-state actors?*

Question: *Why would any adversary choose to confront capability in the environment where it performs best?*

Question: *Is the so-called 'Homebase' correctly protected? What is NATO Air and Space Power's weakest link?*

Deterrence

Deterrence Made Simple. Deterrence Theory is complex and no single definition exists. However, for the purposes of this short piece, the simplest way to consider Deterrence is as a basic cost versus benefit analysis. Specific to preventing an adversary from launching action designed to seize territory, Deterrence can be considered to have two facets. First, the defender's acknowledged ability to meet any attack with an immediate and decisive counter-attack. The second, to create a situation where a potential aggressor weighs possible options, and realizes that the costs far outweighs the potential benefits[4].

Deterring

Contested Space. A question that should be considered is that in the areas where its presence is contested, does NATO have a sufficiently robust, flexible and sustainable footprint in order for it to be seen as a credible deterrent? Robust, flexible and sustainable are inseparable, critical facets:

a. Robust. NATO forces need to be sufficiently robust to do significant damage to a lightly equipped, rapidly deployed adversary force. It is offered that the adversary force would necessarily need to be lightly equipped, in order to move swiftly, which in turn would be required to maintain the element of surprise. Further, surprise would need to be a key element of an adversary plan, as allowing the Alliance sufficient time to respond would inevitably lead to defeat.

b. Flexibility. Flexibility is required to counter adversary action across a broad spectrum of activity. In other words, have the ability to deliver a rapid and decisive counter-punch unhindered by time, distance, climate or geography.

c. Sustainable. Peer or near-peer competitors will recognize that a force can be neither robust nor flexible if it cannot be sustained for a sufficient period of time to be assured of success.

Understanding Cost. Much is made of the premise that we exist in a resource constrained environment and there are a multitude of competing priorities and Defence is often a long way down that list of priorities. However, there is a simple but stark choice to be made at the NATO Summit in Brussels. The Alliance is at a critical juncture and must modernize or, face the real possibility of humiliation and subsequent collapse. Deterrence is expensive, however, the cost to NATO of *not* deterring a competitor is exponentially greater; Deterrence is actually the cheapest option.

Question: *What would be the true cost to the Alliance of a failure to effectively deter a competitor?*

Strategic Communication. A competitor may see 'reinforcement' measures by NATO as escalatory. However, part of any 'modernization' initiative(s) needs to incorporate the development of more effective messaging; reinforcement needs to be demonstrated as being purely defensive. Similarly, there is a need when considering confrontation with a peer or near-peer competitor to acknowledge the role of the previously thought out-dated concept of Passive Defence to include physical protection of facilities, dispersal and redundancy.

Question: *Can NATO communicate, quickly and effectively to counter adversary messaging and is NATO prepared to defend high value civil or/and military objects of interest through renewed investment in passive defence?*

Delivering Deterrence

Reality. In short to medium-term, NATO has no peer competitor that can hope to prevail over NATO in a protracted conflict. This is something that

is regularly *not* discussed but, is something that NATO does not, in the immediate future, have to contend with. Furthermore, it is offered that not all states on the periphery of the Alliance are under equal threat; some are simply too large to be challenged by any likely competitor. This provides the Alliances with its first advantage in that any competitor has to achieve both a quick win *and* be sure that having achieved such advantage, NATO will not respond because the concept of Deterrence becomes reversed i.e. NATO cannot respond because the politically perceived cost of doing so far outweigh the benefit.

Focus. Identify where the true risk lies and respond accordingly. The focus for Deterrence needs to be on doing what is required to prevent a quick and what is realistically likely to be an irreversible 'land-grab'[5], which in turn, then undermines NATO credibility and cohesion[6]. This needs to be done whilst simultaneously protecting assets within Alliance Territory from the more likely terrorist-style attack. It would be too easy to say that all areas where NATO has currently deployed an Enhanced Forward Presence (eFP) are equally under threat. Those areas most at risk are those that are small enough to be over-run rapidly, with the commitment of a relatively small force and, as a result, where NATO would then have to confront the issue of Deterrence from the completely opposite perspective i.e. Nations having to consider whether the benefit of having to mount an operation at scale to eject an invader was worth the cost.

Question: *How strong is NATO Cohesion – has the Alliance over-expanded and in an increasingly complex world, is it time to re-think the approach to European Defence?*

Real Presence. Where the risk of a 'land-grab' is identified as being possible, NATO should plan to position forces sufficient to remove from any adversary the option to take swift and decisive action. By doing this, NATO creates a state where a competitor has to acknowledge that in order to

achieve their objective(s), the only option would be to confront NATO forces with mass over time.

Question: *What scale of Joint Force would be required to deliver 'real presence'?*

More Balanced Forces. So how should NATO deliver Deterrence in those areas where it is necessary? The proposed answer is to develop the current concept of eFP into a more robust, flexible and sustainable force. Key to such development would be to develop a balanced force. One that is able to operate across all domains, with components able to switch seamlessly from the supported to the supporting role. In the future, eFP needs to be delivered in a truly Joint manner, underpinned by a broader Comprehensive Approach.

Understanding what is Vital. To be successful, a competitor will need to focus his actions on vital ground be this airfields, seats of government, ports, main supply routes etc. Therefore, NATO needs to protect these assets using both active and passive measures and pre-position sufficient operating stocks with these protection forces to enable them to hold for a protracted period until relieved. In other words, eFP needs to deliver enhanced protection to those assets that are vital for success.

Enhanced Forward Presence at the Rear

Threats without Borders. The title above may appear an oxymoron but, the reality is that the Alliance is facing 360-degree threats. How these threats will manifest themselves at different locations over time will vary, however, the inescapable challenge is that every location needs to be adequately protected against the specific, identified threat. This development has greatly increased the complexity of Force Protection requirements from when there was a clearly defined front line.

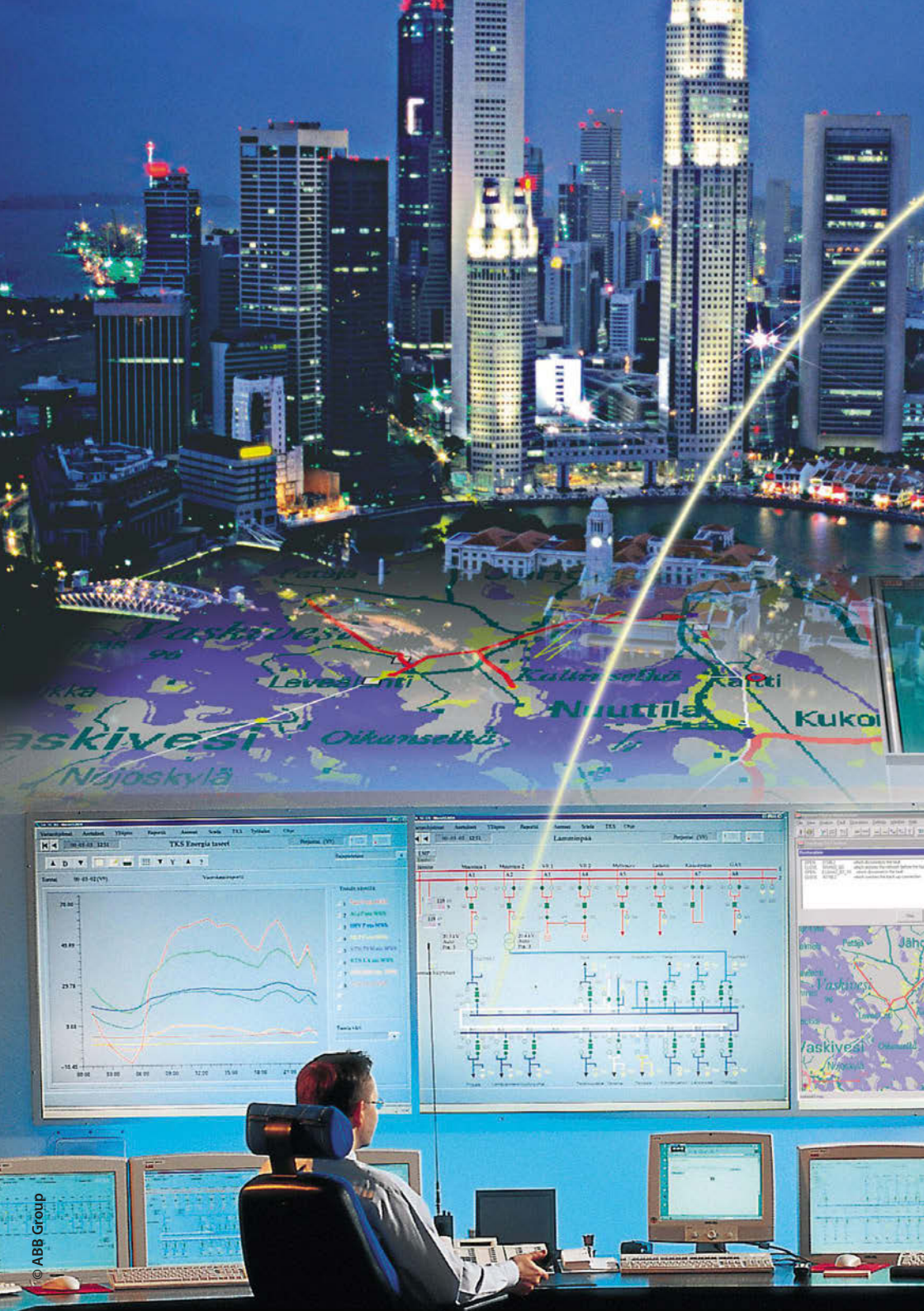
Summary

The reality is that NATO cannot hope to protect itself completely from all of the challenges that are currently possible. By understanding the concepts of threat and deterrence in their most basic forms and simultaneously applying a reality-check to who our competitors really are and what they are actually capable of, it is suggested that a way forward can be defined. As with many things, a 'balanced approach' is required. We need to adopt an approach that protects both the periphery and the core of NATO through a mixture of active and passive measures but, recognizing that whereas the concept of threat might be ubiquitous, the actual way in which a threat will manifest itself will be different, therefore, different location-specific approaches will be necessary.

Wing Commander Jez Parkinson is a RAF Regiment Officer with 32-years' Service; over half in the Multinational environment. He is the Author of NATO FP Policy, FP Doctrine for Air Operations and the current Custodian for Joint FP Doctrine.

Endnotes

1. In all domains to include the likes of shipping lanes and airspace and today, cyberspace.
2. The concept that very junior military leaders can make significant decisions. Tactical decisions that have strategic or even political implications. After Charles C. Krulak, 'The Strategic Corporal – Leadership in the Three Block War'.
3. In its simplest form, an insider threat is defined as a threat that originates from within the organization being attacked or targeted and is carried out by an employee, former employee, contractor or other such individual who has apparent legitimate access. An attack may be kinetic or non-kinetic (e.g. an attack with an actual weapon or through the introduction of malware etc. into the organizations systems).
4. H. Praks, 'Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics – the Case of Estonia', NATO Defence College, Research Division, Rome, Dec. 2015.
5. D. Shlapak and M. Johnson, 'Reinforcing Deterrence on NATO's Eastern Flank – Wargaming the Defence of the Baltics', Rand Corporation, Santa Monica, 2016.
6. As a result of creating a situation where a number of nations, as democratic societies, are simply unable to answer a call to arms under Article V as a result of domestic public opinion.


Vaskivesi
Nuuttila
Oikunselkä
Näjoskylä
TKS Energia tasot
Lammimpää
Jäh
Vaskivesi

Resilience: A Core Element of Collective Defence

VI

Jamie Shea, *NATO Deputy Assistant Secretary General*

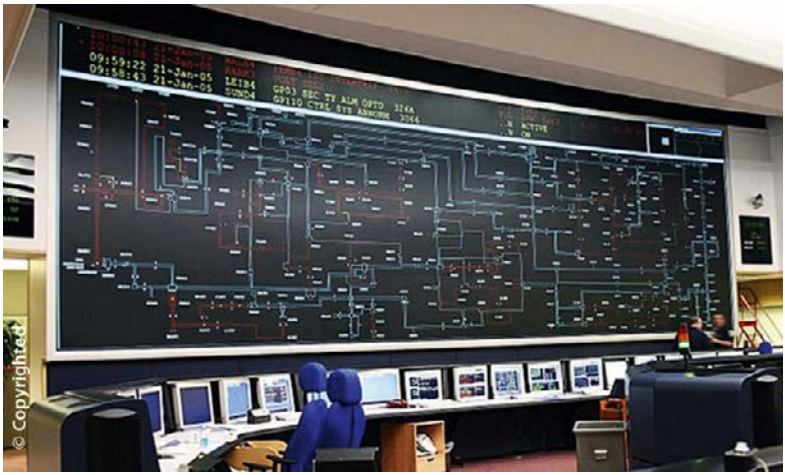
We live in an age in which more people have access to highly sophisticated technologies and almost every social, economic or military asset has become 'securitized' or vulnerable to disruption – whether temporary or more lasting – from an outside attacker or even an inside source.

In a globalised but also more confrontational and complex world, resilience will remain an ongoing concern for Allies, requiring constant adaptation as new vulnerabilities and threats emerge.

Virtual Vulnerabilities

Cyberspace is perhaps the most extreme form of this vulnerability as it interconnects the entire planet in real time, making it possible for anybody to attack any electronically operated target from anywhere at any moment. This vastly complicates the task of defenders, who can rarely know in advance that an attack is being launched, where it will strike or where it will originate. So the defender has to try to protect every important part of the national economic or military infrastructure all the time, while the at-

tacker can choose the individual segment or vulnerable fault line that he wishes to disrupt.



SCADAs – or automated control systems for electrical grids or energy pipelines – are just one example of how infrastructure that we depend on for the normal functioning of our lives is increasingly automated, remotely controlled or integrated into ever more complex networks, which are vulnerable to attack.

As we move from the internet of things to the internet of everything, more and more of the infrastructure that we depend on for the normal functioning of our lives is being automated or controlled from remoter distances or integrated into ever more complex networks. The SCADAs – or automated control systems for electrical grids or energy pipelines – are but one example. So are cross-border grids which means an energy blackout in Italy can immediately turn off the power in parts of Switzerland, or an overload at one transmission plant in India can plunge 400 million people into temporary darkness, to cite just two recent examples.

The globalisation of networks and the increasing integration of physical infrastructure into the virtual world, for instance the storage of data not in

machines but in 'clouds', has certainly brought about efficiencies and savings. But it has also greatly magnified the consequences of a disruption and the number of key nodal points and attack surfaces that malevolent actors can exploit.

Civil Preparedness

A second tendency increasing the sense of societal vulnerability is the state of civil preparedness within the Alliance. The delivery of forces and military capabilities that NATO needs to uphold collective defence or to project forces beyond its territory relies on civilian resources. During the Cold War, many of these, such as railways, ports, airfields, grids or airspace were in state hands and easily transferred to NATO control in a crisis or wartime situation. Today, by contrast, 90 percent of NATO's supplies and logistics are moved by private companies and 75 percent of the host nation support for NATO forces forward deployed on the territory of the eastern Allies comes from private sector contracts.

Similarly, when facing distributed denial of service cyber-attacks against its outward-facing networks, NATO has relied on cooperation from the telecoms sector and the internet security companies to filter and capture data, identify malware and provide extra bandwidth.

Without doubt the transfer of ownership and responsibility to the private sector has brought cost-efficiencies; but the quest to reduce costs and overheads to increase profitability has also led to less redundancy and less resilience. In addition, as hybrid threats below the threshold of NATO's collective defence clause (Article 5 of its founding treaty) blur the traditional distinction between peace and war, government special powers based on wartime emergency legislation have become less practical to implement or even obsolete.

As a result, NATO faces two distinct but inter-related resilience challenges: first, to ensure that it can speedily move all the forces and equipment required to any part of the Alliance facing an imminent threat or attack, ensuring full and unimpeded access to all the infrastructure it needs for this purpose; and second, to be able to anticipate, identify, mitigate and recover from hybrid attacks with minimum disruptive impact on the Alliance's social, political and military cohesion.

Civil preparedness is, above all, a national responsibility, in the same way that Allies must ensure adequate cyber defence for their critical information technology networks, especially the ones that NATO depends on for its own operations. This said, Allies' security relies on individual nations upholding this commitment; and NATO has an interest in obtaining as much transparency as possible so that it can assess potential vulnerabilities or gaps and accurately measure progress. Avoiding unpleasant surprises in crisis situations when the Alliance needs swift and reliable information and the capacity to analyse, decide and respond swiftly has to be the goal.

Consequently, the theme of 'resilience' – how to define it, assess it and enhance it across the Alliance – has become a leading topic for the NATO Summit in Warsaw, in July.

Resilience is increasingly seen as the corollary of deterrence and reassurance measures in the classical military sphere as part of a comprehensive security strategy for the Alliance. The seven baseline requirements to be assessed are:

1. assured continuity of government and critical government services;
2. resilient energy supplies;
3. ability to deal effectively with the uncontrolled movement of people;
4. resilient food and water resources;

5. ability to deal with mass casualties;
6. resilient communications systems; and finally
7. resilient transportation systems.

These seven areas apply to the entire crisis spectrum, from an evolving hybrid threat all the way up to the most demanding scenarios envisaged by Alliance planners.

So how can NATO make its contribution to improving resilience within its 28 Allied nations?

Five Specific Areas Come to Mind:

Cyber Defence

The first is cyber defence. NATO experiences 200 million incidents on its networks every day and around 200 more serious intrusion attempts every month. This level of hostile activity is also what Allies are experiencing as the 'new normal' in the cyber domain. NATO's first task has been to upgrade the protection of its own networks by giving the NATO Cyber Incident Response Capability (NCIRC) additional capabilities for earlier detection and more rapid response to cyberattacks. Two Rapid Response teams have also been created to assist Allies, as well as to manage incidents affecting NATO itself.

NATO has now moved on to help Allies improve their cyber resilience by introducing capability targets into the NATO defence planning process and devising a new memorandum of understanding between NATO and individual Allies to establish secure connectivity and arrangements for information-sharing and crisis management. A number of Allies have come together to develop specific capabilities in fields such as a malware infor-

mation-sharing platform, training and education, and systems configuration for effective decision-making.

The NATO Cooperative Cyber Defence Centre of Excellence in Estonia has helped NATO to organize state-of-the-art annual exercises to improve the skills of cyber operators using a cyber range that Estonia has transferred to NATO.

Finally, and given the importance of industry that owns 90 percent of the networks NATO and the Allies depend on, the Alliance is developing a NATO-industry cyber partnership to encourage information-sharing and best practices. This will give NATO a better grasp of the rapid pace of innovation in the sphere of information technology and how it can better integrate emerging technologies and new concepts into its cyber defence. The proposal to create an 'innovation hub' at the NATO Communications and Information Agency should facilitate this dialogue and mutual understanding between NATO and the small-and-medium-size technology providers that are often the most innovative in this area.

As the Alliance looks towards the Warsaw Summit, some further measures are on the table. One is a 'cyber defence pledge' or commitment to speed up national implementation of the NATO capability targets, which requires sustained national focus and adequate resources.

A second idea is to look into the political, legal and operational consequences of declaring cyber as a domain, as many Allies have done already in terms of their national cyber strategies. This reflects the increasing awareness that most conflicts and crises these days have a cyber dimension and that – as NATO increases the momentum of its military activities for collective defence – NATO commanders need the requisite tools and authorities to defend against advanced cyberattacks and to operate across the cyber spectrum.

Hybrid Threats

A second area of resilience is a strategy to respond to hybrid warfare which NATO foreign ministers approved last December. NATO is improving its intelligence-sharing and early warning processes in order to better anticipate and map hybrid warfare activities. It is developing in this respect a set of early warning indicators that can trigger a number of crisis-response options. This is because rapid identification of a hybrid attack (as opposed to an isolated or random incident) and speedy decision-making are essential to nip these attacks in the bud and block escalation.

Understanding hybrid threats. (Photo courtesy of European Parliamentary Research Service)

NATO ambassadors and defence ministers have held simulation and scenario-based exercises to fine-tune their situational awareness and responsiveness vis-à-vis threats, which are specifically designed to be ambiguous and difficult to attribute.

Effective strategic communications to dispel false information, propaganda, lies and myths is also an essential part of coping with hybrid attacks that seek to confuse public opinion, aggravate social tensions and undermine trust in governments.

All this does not mean that Allies are as vulnerable to a hybrid attack as Ukraine proved to be during Russia's illegal annexation of Crimea. However, Allies are now encouraged to map potential vulnerabilities that can arise from Russia's involvement in business, financial, media or energy concerns, for example, and to share the lessons learned from resilience stress testing more broadly within NATO.

Civil-military Readiness

A third area under discussion concerns NATO's ability to fully implement its Readiness Action Plan for the reinforcement and defence of Allies, whether to the east or to the south. NATO members have to adjust their territorial defence mechanisms and infrastructure to the new security environment and revive the planning fora that existed during the Cold War.

In particular, NATO planners require cross-border transit arrangements for the rapid deployment of the Very High Readiness Joint Task Force and NATO Response Force. As new Graduated Response Plans for detailed collective defence arrangements are adopted, the Allies must ensure that elements such as transport, flight corridors, civil-military airspace coordination, fuel stocks, pre-positioned equipment, port access and legal agreements are fully integrated into military planning.

Crisis-response measures to activate civil emergency measures will need to be updated and civil defence requirements will need to be given more attention, based on the military requirements for the Readiness Action

Plan and associated capability packages for its deployment. A more sustained dialogue between military commanders and national civil emergency authorities is now being established.

Stepping Up Cooperation with the EU

A fourth area is the relationship between NATO and the European Union (EU). The two organisations occupy different parts of the resilience spectrum but there is also considerable overlap in the middle. A joined-up approach based on a shared situational awareness and coordination of responses is key to a successful response.

Currently NATO is talking with the EU on enhanced cooperation in four areas: civil-military planning; cyber defence; information-sharing; and analysis and coordinated strategic communication to spot disinformation and communicate a credible narrative. One early deliverable is a technical arrangement between the NATO NCIRC and the EU Computer Emergency Response Team (EU CERT) for the exchange of information, which was concluded in early February.

Up to the Warsaw Summit, NATO and the EU are continuing their discussions at the staff level, as the EU finalises its own strategy to respond to hybrid threats. The aim is to harmonise procedures and to support each other's efforts in responding comprehensively. The ambition is to identify pragmatic, flexible approaches which could be reflected in a joint declaration by NATO and the EU at the Warsaw Summit. NATO and the EU are also developing compatible 'playbooks' to ensure more participation in each other's activities, such as exercises and training.

It is also important that NATO and the EU work together to tackle other resilience challenges that do not result from deliberate attacks. The most

urgent of these is the migration crisis. NATO has recently deployed a maritime task force in the Aegean to work with Greece and Turkey and the EU border agency, Frontex, to monitor the flow of refugees and migrants and in this way help to curb the illegal activities of smugglers and traffickers.

Working with Partner Countries

Finally, NATO's partners can also help to improve the Alliance's overall resilience. Not only Ukraine but many other partners have been the victim of hybrid operations. Their experiences and lessons learned can help NATO to better understand the type and impact of hybrid tactics. More information-sharing and early warning can help NATO decision-makers to identify incipient attacks that could start in a partner country but rapidly spread to NATO territory.

Conversely, NATO's experience and expertise can help partners improve their own capacity for resilience. Unsurprisingly resilience areas like cyber defence and civil emergency planning are increasingly featuring in defence capacity building packages for partners such as Georgia, Moldova, Jordan and Iraq. In the Baltic region, Sweden and Finland – two of NATO's most active partners, which have enhanced opportunities for dialogue and cooperation – have also faced hybrid pressures from Russia. These Nordic partners have drawn closer to NATO through consultations, training and exercises, including the conclusion of host nation support arrangements for crisis assistance.

In conclusion, Allies need to adapt constantly as new vulnerabilities and threats emerge from non-state actors such as so-called Islamic State, as much as from state actors like Russia. Resilience is here to stay as a core element of collective defence. That is why NATO will stay focused on reducing its exposure to threats to its cohesion, independence and security.

Article from this page: https://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

Jamie Shea is currently serving as NATO's Deputy Assistant Secretary General for Emerging Security Challenges. He is a regular lecturer and conference speaker on NATO and European security affairs.

© MCD, Richard Frigge

Outsourcing Logistics. One Step Too Far?

VII

Lieutenant Colonel Joop Berghuizen, *NLD, Air Force*

As mentioned in chapter 6, 'resilience is a core element of collective defence'. Within the article several issues are clearly considered part of logistics, thereby making logistics an important component of collective defence. This paper will focus on one of the core issues mentioned in the article, the use of 'Contractor Support to Operations' (CSO).

As stated in the previous article 'The delivery of forces and military capabilities that NATO requires to uphold collective defence largely relies on non-military owned resources. During the Cold War, many non-military owned resources were in state hands and easily transferred to NATO's control during crisis or wartime situations. However, nowadays, 90 percent of NATO's logistics are moved by private companies, and 75 percent of the host nation support for forward deployed NATO forces on the eastern flank comes from private sector contracts.' In other words, NATO is relying heavily on so-called Contractor Support to Operations.

According to NATO policy[1] Contractor Support to Operations is the use of pre-planned and / or ad hoc commercial contracts which are specially developed and run by the applicable HQ (or through NATO agencies) entitled to perform such kinds of support activities. CSO enables commercial

entities and/or agencies to provide a portion of logistics support to 1) ensure materiel support is available for NATO commanders and the Troop Contributing Nations (TCN) and 2) to optimize the use of military resources and capabilities. The methods of contracting to accomplish this can be very diverse. They often include common technical and system support contracts, dormant contracts (where the execution is postponed until the requirements materializes), high-end assured-access contracts (providing a capability when needed) and Rapidly Usable Enabling Contracts (RUEC), which are a flexible array of pre-planned time and mission critical contracts at high readiness.

CSO applies to a wide range of logistic related functions[2] [3] and could include technical arenas, such as maintenance of weapons systems or Computer information systems services. CSO could also provide deployment and sustainment support (i.e. strategic support, Air to Air Refueling, operating an Airport of Debarkation, Air Traffic Control, Firefighting, fuel storage, etc.). In this day and age, CSO is an integral part of all major logistics areas.

On the positive side, the transfer of ownership and responsibility of support operations to the private sector has predominantly provided cost-efficiencies and is often used as a way to eliminate redundant capabilities. However, the redundant capabilities, ensuring resilience, might not be part of contractors' organization, where elements like leanness and efficiency might increase the risk of being less resilient.

To better understand this way of contracting and the consequences, imagine an emerging crisis that may require the immediate activation or transfer of certain civilian-led support elements. However, the required actions and authorities to do this reside in the Crisis Response Management System of NATO. That poses the following question in the case of a hybrid threat; Does NATO have sufficient indications and warnings to activate the necessary Crisis Response Measures (including support) for Collective Defence in time?

From an operational planning point of view, there are numerous considerations to take into account whether or not to use CSO because CSO entails risks. For example, how reliable is the contractor when faced with the possibility of taking casualties? Will the required level of support capabilities be available, especially in an appropriate level of readiness and quality across the full mission spectrum? With regard to our military capabilities, what about security and activities when host-country or third-country nationals are involved? How do we stay in control of costs? Should we for example activate a dormant contract for training and exercise? Is NATO and its member states able to sufficiently mitigate all the related risks?

To support operations like the enhanced NRF, contracts for critical supplies or services need to be placed on a higher readiness state with more formal contracts (RUEC and Assured access as mentioned above) which will result in higher costs. The question then arises if such support would not be more cost-effective if it was done by NATO and its member states? Likewise, is HN resilient enough to continue to support NATO logistics if it is faced with the choice of supporting NATO or its own people?

Another issue is border crossings[4] and the use of Lines of Communication (LOC),[5] both of which have been discussed in many NATO committees and is defined as Military Mobility project within the European Union's 'Permanent Structured Cooperation on Defence' (PESCO). Many items have to be resolved like the quality of infrastructure, accessibility of LOC in scenarios that include Anti-Access Area Denial (A2AD), and border crossings in the days preceding 'Day Zero'. Although they initially may not seem related to CSO, there are many correlated issues, e.g. civilian contractors from other nations and TCNs on privately owned toll roads, all of whom are transporting dangerous military goods. Will the contractors still be able to use the LOC and get access to the locations when and where NATO needs them?

In regards to requirements, the challenges associated with the integration of Command and Control for CSO is an element not to be underestimated. This integration will come with costs for operational interfacing and exercises. This is true not only for testing the procedures but also when deploying CSO personnel in exercises. So, is NATO willing to raise the costs of an exercise by enabling a huge number of CSO contracts? In context, these factors begin to cast doubt on the acclaimed efficiency of using CSO for NATO operations.

Because NATO has to be ready to operate across an entire spectrum of violence, force protection of contractors also has to be taken into account. Although contractors can be authorised to carry weapons for self-defence, it raises the question of whether arming them turns them into combatants and, if so, would it be acceptable for both sides (contractor and NATO). As an alternative, providing force protection to the contractors using NATO or TCN forces might not be possible due to the number of contractors that could be involved. For example, during recent US military operations in Iraq and Afghanistan, contractors frequently averaged 50% or more of the total DOD presence in-country. In effect, we are saving on logistics personnel but at the same time are laying a huge burden on the highly needed and limited available force protection units. So, is NATO able to protect contractors with the mentioned restrictions?

Considering all the questions raised above, there is a strong relation between and dependency on CSO and the readiness of the Alliance on Day Zero. After all, the Area of Operation is only fully enabled if all the components of logistics are readily available. Although risk mitigation can and should be done before Day Zero (and RUECs are a good solution), unforeseen requirements shall, by definition, result in increased costs and delays in deliveries of capabilities and thus hindering the response at Day Zero.

Possible alternatives, such as increasing stockpiles and the dispersal of storage locations, are an option we all know from the past, but many nations

don't have the ability or willingness to move their national stockpiles to a foreign nation. That being said, it should be pointed out that although stockpiling increases costs, at the same time it solves many of the border crossing and LOC problems and thus mitigates some of the risks that might come with CSO. Therefore, is it logical that the Alliance is using NATO common funding to improve NATO designated airfields but is reluctant to forward the necessary equipment and supplies to run the operations from those airfields?

Conclusion

The 'evolution' in logistics which relies more and more on the private sector, and subsequently changes our organizations from an effective to a more efficient one, is increasing NATO's risks by unintentionally dismantling an agile logistic backbone. The dependency on CSO makes NATO logistics more vulnerable and, therefore, a weaker link in NATO's deterrence. Nowadays, it seems that NATO is only looking for risk mitigation to solve the problems of CSO. However, does the costs of using CSO for support outweigh the negative effects on resilience and the ultimate effect on the effectivity of NATO operations? Looking at the limitations and risks linked to the use of CSO, should NATO not look for other options to overcome these limitations and risks and, by doing so, NATO could be better prepared to strengthen NATO deterrence and options for Day Zero?

Lieutenant Colonel Joop H. Berghuizen (RNLAF), JAPCC Logistic SME, supporting all levels and examines the many aspects of Logistics and Mobility in relation to NATO Joint Air Power. Before he was assigned to the JAPCC he served in several joined, national and international staff-positions.

Endnotes

1. 'NATO Policy on Contractor Support to Operations', AC/305-D(2016)0009-REV6, NATO, 2018. (Still under silence procedure).
2. NATO Logistics is the science of planning and carrying out the movement and maintenance of forces. It can also be understood through the core functions they fulfil which include but are not limited to: supply, maintenance, movement and transportation, petroleum support, infrastructure engineering, and medical support.
3. 'NATO Principles and Policies for Logistics', MC 319/3, NATO.
4. In general this are all the issues related to get approval to the sovereign territory of a nation for air, sea and inland surface movements in support of a NATO operation.
5. All the land, water, and air routes that connect an operating military force with one or more bases of operations, and along which supplies and reinforcements move.

Exercises and Training Preparing for Day Zero

VIII

Lieutenant Colonel Ed Wijninga, *NLD, Air Force*

Introduction

Since the end of ISAF operations in Afghanistan, NATO has been confronted with new conflicts on its Eastern borders with the Russian occupation of the Crimea peninsula and operations in the Ukraine as well as the increased military posture of Russia in Kaliningrad. Suddenly, NATO is faced with the possibility of an actual attack on a NATO member nation which could result in an Article 5 declaration and hence a Major Joint Operation on NATO soil. These developments require a renewed focus on both hybrid and peer-to-peer conflict. This has resulted in the Readiness Action Plan (RAP), the Very High Readiness Joint Task Force (VJTF), and an enhanced NATO Response Force (eNRF). With the three concepts now having been developed, NATO aims to train and exercise to employ these concepts to their fullest extent.

SACEUR has been very clear about the necessity to improve readiness for large scale conflict through enhanced training and exercising and wrote in his Annual Guidance on Education, Training, Exercises and Evaluation (SAGE19): 'I have instructed my staff to put large scale, high-intensity, all-domains warfare against a near-peer adversary at the very heart of all our training from now on, and I am prepared to assume some risk in other areas to achieve this.'

SACEUR considers Training, Education, Exercises and Evaluation to be key tools for the adaptation of the Alliance and in preparing it for this change. He also underlines the imperative for demanding and realistic exercises, tailored to improve and validate the Alliance's interoperability, operational concepts and planning, C2 arrangements, decision-making responsiveness and perhaps, most importantly, our ability to conduct operational art[1].

This new direction and guidance requires a review and update of existing exercise scenarios, a task NATO's Joint Warfare Centre (JWC) in Stavanger, Norway has already embarked upon with the further development of the SKOLKAN 3.0 scenario for exercise Trident Javelin 17 and the development of the all-new OCCASUS scenario for exercise Trident Juncture 18 and consecutive Trident Jupiter exercises, starting in 2019.

Based on a Letter of Agreement and starting with exercise Steadfast Jazz 13, the JAPCC has supported the JWC in the development, preparation and execution of exercises, providing Air & Space Power expertise by contributing with an Opposing Forces (OPFOR) Air team to various small- and large-scale exercises such as Steadfast Jazz 13, Trident Juncture 14-18, Trident Jewel 15, Trident Javelin 17, Ramstein Ambition 14-18 and (German national exercise) Kalkar Sky 15-16.

During the execution of all of these exercises, the JAPCC team has experienced that Training Audiences were frequently struggling with the scenario and, in particular, with the doctrines, tactics and capabilities of a very realistic and dynamic OPFOR. This despite the fact that Primary Training Audience (TA) Commanders can exert some influence on the scenario during its development and have at times tried to adjust the scenario a bit more to their liking. A recent example was the start of the execution of exercise Trident Javelin 17 at G+200, the start of the 'Restore' campaign, whereas the real problems facing the commanders, such as Anti Access Area Denial (A2AD) needed to be addressed right from the

start (Day Zero) of the campaign. Especially the initial stages of the conflict, where the Enhanced Forces Presence and the NRF might be engaged, where Headquarters need to be activated and forces deployed, meanwhile gaining access and securing lines of communication could be exercised.

In exercises, avoid the use of 'Fairy Dust' to make joint problems go away.

What Does Not Work?

The overwhelming issue that seemed to appear in all the exercises was a persistent lack of jointness. This already started during the planning and preparation phases of the exercise when the Joint Force Commanders and their subordinate components did not engage properly to embark on the Comprehensive Operational Planning Process. This is sometimes driven by the pre-occupation of staffs with day-to-day work, real-time operations, other priorities and so on. Fact is, that in previous exercises, especially the Comprehensive Preparation of the Operational Environment (CPOE) was not conducted in a joint manner. A proper analysis of the situation forms the basis for the overall Concept of Operations and the subsequent OPLAN for the Alliance's operations during the exercise. If not done jointly it results in several stove-piped 'mini-campaigns' and also has a marked negative effect on the Joint Targeting Process which has led to component commanders attacking OPFOR's capabilities on their own with little success but at very high cost.

This lack of joint thinking has also led to seams in the overall Air Defence Plan, especially in coastal areas where the Air Defence Plan should be a joint effort between the Air Component and the Maritime Commander. These seams are then exploited by OPFOR with sometimes disastrous results for the Alliance.

Joint Challenges require Joint Solutions

Based on experiences in the wars in the Balkans, Afghanistan and Iraq, many NATO men and women have adopted a culture of 'invincibility'. There is a clear adversity to losing aircraft, capital vessels or command ships, High Value Airborne Assets (HVAA), NATO's PATRIOTs, etc. This has led to, sometimes heated, discussions when OPFOR shot down aircraft or sunk NATO ships. Commanders were averse to accepting these results and did sometimes not accept adjudication results from the Exercise Control Organisation (EXCON) and insisted on a cap in the number of losses per day or restoring capabilities that had been lost the day before. Additionally, not every AWACS in the world can be in one exercise, and there cannot be more SCALPs in one exercise than ever produced worldwide. Every Tomahawk missile launched from a vertical launch system on a ship is one less Air Defence missile available (bearing in mind, the enemy can count too!).

There needs to be a culture change into making exercises more realistic and accepting that the 'enemy' truly does get a vote.

Major NATO exercises not only serve a training-purpose, they are also an important and proven instrument for conveying a Strategic Communication message that NATO is prepared, able and willing to face any conflict should the need arise. Major exercises always include a Distinguished Visitors Day (DV-Day) where it is important that the commanders are able to show some level of success in the current campaign. However, the preparations for these DV days seem to pre-occupy commanders and their staffs during exercise execution and sometimes conditions need to be changed to show a more favourable picture on DV-day. Leaders (mostly) get this, but staffs sometimes create roadblocks to exercising these challenges because, in some cases, they are culturally conditioned to 'look good' in exercises. This jeopardises exercise execution and is frustrating for both the

Training Audience and EXCON, and it has a marked negative effect on the conduct on these very expensive and time-consuming exercises.

Exercises do not need to LOOK good, they need to BE good!

What Does Work?

What is required to improve the major NATO exercises and ensures that Training Audiences, from top to bottom, go through a steep learning curve thereby making sure that they meet SACEUR's goals? This starts with the acceptance and trust that commanders need to have in the quality and fidelity of exercise scenarios that are currently being developed. There is no requirement to assert influence on the development of the scenario. No real enemy will ever ask NATO's commanders how he wants to fight the war! This means that the TA should be confronted with doctrines and tactics at all levels and need to experience these as they come. Freedom of Manoeuvre needs to be earned, not assumed. The TA needs to accept assessments/adjudication by EXCON to improve the protection of NATO's critical assets and critical enablers. The TA should ensure that the Targeting Process is conducted in a joint manner and needs to focus on a steep learning curve (fail, assess, adapt, improve). The TA also needs to learn to accept to lose (high-value) ships and aircraft in an exercise as a result of flaws and errors in their own plans. Exercise scenarios also need to start at Day Zero in order to confront planners and commanders with an entirely new situation where the complexity of activating the NATO Command Structure and deploying forces while, at the same time, being engaged in battle challenges the Training Audience realistically.

An example of how to improve exercises and Training Audiences performance are the Joint Project Optic Windmill (JPOW) exercises where the Concept Development and Experiment (CD&E) phase allows the TA to experiment and test several different approaches to a pre-defined and specific

problem. This allows the TA to make mistakes, to recover, adapt the plans and respond to the challenge in a different manner. It also helps to better understand the complexity of the actual threat and how to jointly overcome it.

It is better to lose in a simulation than explain in real life that losses were a result of poor training and poor execution.

Single Component actions or single weapon systems are not the solution to complex joint problems, such as A2AD. Firing Cruise Missiles into Multi-Layered Defence systems is not the answer. It can be part of the answer. Addressing these joint issues requires a joint, multi-component effort by both Special Forces, Cyber, Land, Maritime and Air. Staffs need to work together, not independently. Degrading these systems requires the approach of 'peeling an onion', layer by layer and this will take weeks, not hours. It probably also requires commanders to accept more risk because the Alliance might need to operate under the opponents' umbrella or conduct operations in a contested and congested battlespace. Synchronization, Integration and Prioritization are key words here to achieve success. Reflecting this jointness and planning in an Operational Design is an operational art and needs to take into account the mutual dependency between components.

NATO must continue efforts to be more joint in it's thinking.

There are several ways to improve the current culture. Develop plans which execute missions simultaneously, or sequentially in a timely manner, with a common effect in mind. Commanders and staffs need to be prepared (and agile enough) to respond when (partial) success is achieved and exploit the situation immediately. Components should understand each other's doctrines, especially where areas or capabilities overlap (such as Coordinated Air Sea Procedures (CASP)). Realise what their impact is to the wider plans and what the implications are to joint and component objectives. Components should better understand the implications of

supporting and supported commander relationships. Also helpful would be a re-establishment of the standing liaison elements that have been deactivated in 2010. This deactivation has led to stove-piped planning and further limitations on the understanding of the needs, challenges and capabilities of others. Joint Table-Top exercises, including experimentation, could be organised to address a specific problem for commanders for them and their staffs to work on and gain joint experience.

There are many opportunities to improve very quickly. It only requires a mindset change.

Points for Discussion:

- To 'train as you fight' requires a different approach towards planning, preparing and conducting our exercises, how do we achieve this?
- How can we improve jointness?
- How can we improve understanding of each other's components abilities and TTPs?
- How can we restore the Liaison Element system that was abolished in 2010?
- Would Table-top exercises to challenge commanders specifically be helpful?
- How do we change the mindset towards accepting higher risk?
- Should commanders influence scenario development?
- Do we need to LOOK good or BE good?

Lieutenant Colonel Ed Wijninga (RNLAF) is currently serving in the Education, Training, Exercises and Lessons Learned Section. He has supported the Steadfast and Trident NATO CPX exercises as Chief OPFOR Air for the past six years.

Endnotes

1. SACEURs Annual Guidance on Education, Training, Exercises and Evaluation 2019 (SAGE19).

© MCD, Hille Hillinga

Joint Project Optic Windmill and Day Zero Operations?

IX

Lieutenant Colonel Berry Pronk, *NLD, Air Force*

Introduction

NATO exercises generally focus on the 'main game' (i.e. major land-component operations) time in conflict, starting at D+100, or beyond. Although recent exercises tend to move closer to a 'D+0' starting point, they still commenced at a day well beyond the onset of hostilities. While beginning exercises on a post 'D+0' (or 'Day Zero') operational construct may benefit certain components and exercise objectives, the dearth of 'Day Zero' exercises has come to reflect an institutional avoidance of the particular (difficult) problem sets that the Alliance would likely face when pitted against near-peer adversaries. Nonetheless, there dawns a move towards exercising in such a construct. For example, during the last Trident Javelin exercise the term 'Day Zero Operations' surfaced almost daily as an acknowledgement that at least some future exercises should start at the 'Day Zero' of a theorized conflict.

Discussions about the exercise Joint Project Optic Windmill (JPOW) often lead to definitions of what it is **not,** such as **'not** a Field Training exercise' or **'not** a Command Post exercise'. As a matter of fact, it is an exercise that can facilitate adequate room for experimentation and which can enable great

training possibilities that are shaped for optimal knowledge enrichment. JPOW is a Computer Aided Exercise where participants can train with their real systems, i.e. hardware in the loop, or simulators or even computer models of their capabilities. All of this exists in one exercise network loop, along with a simulated air threat. In the past, there have even been exercise combinations that paired with real air operations (such as time-sensitive targeting).

This paper will describe the exercise JPOW in general and its possibilities and opportunities in the context of 'Day Zero'. JPOW takes into account that one of the most challenging missions for NATO is IAMD, primarily because this complex mission expands through all domains, involves all services, and requires flawless cooperation and collaboration between multiple nations and NATO entities. Since 'Day Zero Operations' aren't universally defined, and therefore 'Day Zero Requirements' for exercises aren't well identified, an attempt will be made to show how JPOW itself or the general construct of JPOW can be utilized as a valuable base for training Integrated Air and Missile Defence (IAMD) and other NATO forces for this critical timeframe.

Multinational Integrated Air and Missile Defence Exercise Joint Project Optic Windmill

After the first post-Cold War mission (Desert Storm 1991), where Theatre Ballistic Missile Defence (TBMD) played a significant role, the lack of sufficient TBMD training opportunities in NATO, especially at the tactical level, was recognized by air defence communities in the Netherlands, Germany and the USA. In 1996, a dedicated team of experts from the Royal Netherlands Air Force, the German Air Force and US European Command (US EUCOM) took the initiative to organize a small-scale Theatre Missile Defence exercise, complementary to the larger US and NATO TMD exercises, called 'Joint Project Optic Windmill'. The initial goal of this initiative was to bring TMD operations to the lower tactical level, to exercise and to maxi-

mize the interoperability potential between the (in those days) three main Patriot users: the United States Army, and the German and Netherlands Air Force. JPOW '1' proved to be an immense success, and the filling of this need in the existing exercise calendar was widely appreciated. As a consequence, JPOW became a recurring event. Throughout the years, JPOW evolved and expanded its scope to Air & Missile Defence, and matured from a small scale tactical level initiative to a leading Integrated Air & Missile Defence exercise for both the tactical and operational level in Europe.

JPOW distinguishes itself from other exercises by including a concept development and experimentation (CD&E) phase in the overall exercise set-up. This segment, which precedes the execution phase, offers the participants the unique opportunity to demonstrate, practice, evaluate and validate different IAMD programmes and concepts. Doctrine, Techniques, Tactics and Procedures (DTTP) can be developed, tested, validated, improved upon and tested again in a testbed environment. The implementation of lessons identified (from the CD&E phase) in the execution phase allows for immediate feedback and, subsequently, a steep learning curve.

Currently, JPOW is a bi-national DEU-NLD led exercise which enjoys strong support from US EUCOM. JPOW has already proven to be a valuable tool in supporting NATO air operations by improving planning and C2 procedures throughout the domain of IAMD. The last iteration of JPOW provided IAMD training for over a dozen NATO and partner nations.

Because it is forged by corresponding IAMD stakeholders for their own exercise participants, JPOW offers important training opportunities and consistently reflects relevant IAMD issues. Furthermore, NATO regularly expresses its appreciation for JPOW, particularly because the flexible set-up of the exercise enables new ideas and concepts to be validated or tested. A considerable part of NATO's IAMD procedures, as well as parts of its current Command Structure, were developed and evaluated during JPOW exercises.

JPOW and Day Zero Operations

While JPOW is a flexible means to create training opportunities the concept of 'Day Zero Operations' is relatively new and, as stated above, not well defined. Hence, it is quite difficult to build an exercise dedicated to this purpose. In short, 'Day Zero' is difficult to define and hard to fight. Therefore, the simplest answer has been to avoid the topic entirely and move on to easier paradigms.

However, this dilemma dovetails into what makes JPOW special among other exercises. While most exercises cannot accommodate vague starting conditions and potential failures by the 'blue team', the isolated run capabilities of JPOW satisfy these special criteria and can be easily accommodated within the CD&E phase of the exercise. For example, during the CD&E phase, specific problem areas could be explored and/or tested. Bigger challenges can be chopped into more defined problems to be explored, analysed and then tackled under controlled circumstances. In addition, JPOW contains a Combat Enhancement Training/Force Integration Training (CET/FIT) phase where 'Day Zero' academics can be briefed and discussed to enable a common understanding before the start of the exercise.

The organizers of the next edition of JPOW (JPOW 19) are considering designating the transition from peacetime to conflict as the starting point of the exercise. However, the anticipated time required for the stand up of a wartime Air C2 structure would consume all available exercise time. Therefore, the exercise planning groups are using the flexibility of JPOW 19 to amalgamate parts of the transition (towards a JFAC), the mix of standing NATO peacetime missions and wartime NATO procedures, as well as initial entry operations.

Of note, JPOW does not support actual large troop movements, nor strategic deployments, but could create circumstances that can still challenge

logistics planning and Command and Control procedures. Also, the scenario can be specifically shaped in a way to better identify necessary conditions for day 1 operations, which will support the definition process of Day Zero operations (e.g. shape I&W needs, identify necessary ROE and units available for certain circumstances) or create/improve DTTPs.

The concept of having a starting phase of an exercise with a more experimental character, like JPOW, could be highly beneficial for other exercises as well. This is especially true for exercises like Trident Juncture/Javelin, which are currently used as evaluations of Joint Force Commands. Unfortunately, evaluation exercises are (generally) not the time for exploration and optimization since the allowance for failure is drastically minimized. These kind of ventures are good for exercising identified Best Practices but leave little room for creativity. Consequently, an 'allowance for learning' would need to be instituted in these type exercises in order for them to effectively support a JPOW-like ideal.

Overall, a JPOW-like structure, where there is emphasis on experimenting with ideas (as a whole or as single scenario vignettes) that can be tested without the pressure of an evaluation, would be beneficial to test a 'Day Zero' construct. The exercise should embrace a mindset of 'Trial and Error' to get better, rather than a pass-fail scorecard that stifles creativity and honest introspection.

The combination of academics and experimentation, a flexible CD&E phase, and an actual exercise construct that has proven to be highly effective during JPOW can do the same for exercises that test various scenarios and training audiences, including 'Day Zero'. Instinctively, in today's environment, many within the Alliance feel that changing circumstances require an adapted and creative exercise process to remain fruitful and successful for tomorrow's conflicts. Therefore, it might be beneficial to scale down the evaluation/certification segments of some exercises and use

the regained time for experimentation, which will allow the participants to experience trial, error and then learn from their mistakes. Not every exercise should be changed into a JPOW-like structure, but where there is a need to exercise 'Day Zero' scenarios, the JPOW paradigm will likely pay the most dividends.

Lieutenant Colonel G. W. 'Berry' Pronk (RNLAF) has been working over 30 years in the domain of Surface-Based Air and Missile Defence. Besides his broad tactical experience he worked in several joined, national and international staff-positions. Currently he is the Subject Matter Expert for SBAMD at the JAPCC.

© NATO

NATO–EU Relations and Day Zero Challenges

X

'NATO doesn't have the luxury of choosing the security threats we face. We must be ready and able to operate decisively across all operational domains – land, sea, air and cyberspace.'

NATO Secretary General, Jens Stoltenberg[1]

Major Victoria Thomas, *USA, Air Force*

Introduction

Despite individual differences and myriad challenges, the North Atlantic Treaty Organization (NATO) and the European Union (EU) have remained mostly unified in their commitment to peace and security among and between their member nations. In keeping with their founding principles, the 28-member EU focuses mainly on economic issues while the 29-member NATO Alliance continues to be mostly defence-oriented. Over the years the aperture of each organization has expanded, prompting both champions & critics to highlight areas where the two organizations could and should cooperate better. The necessity of working more closely was magnified as the world recovered from the 2008 financial crisis amid resurgent global actors and unprecedented migration flows which were the result of weak governments,

a spread of violent extremist organizations, and climate change. Simultaneously, unconventional threats like cyber-attacks on financial institutions and foreign elections became de rigueur. The ability of either organization to address security challenges before they become existential threats can only be achieved through a strong NATO and a strong EU that cooperate on a day-to-day basis and not only when urgent or convenient. During the 2018 Joint Air and Space Power Conference, panellists will examine air power's role in the ambiguous period preceding a possible armed attack, and will refer to this time, including initiation of armed hostilities, as 'Day Zero'. Theoretically, the necessary cooperation, collaboration and communication needed to navigate the fog of Day Zero should not be that difficult to achieve. NATO and the EU share a majority of member nations & have basic overlapping values, principles and interests. Twenty-two nations belong to both organizations and in recent years, executive leadership of both have loudly touted the benefits of working together. Just as each organization is greater than the sum of its parts, integrating parallel work strands would allow NATO and the EU to meet objectives even more efficiently & effectively. Nonetheless, differences do exist and in some cases they have resulted in serious barriers to aligning programs of work, reducing costs and shortening program timelines. Unfortunately, project hoarding and petty vying for ownership of particular projects by individuals, nations or even the EU and NATO undermine the many success stories of NATO-EU cooperation. In order for civilian and military personnel to differentiate between threats and challenges, and prepare appropriate responses should deterrence fail, the two organizations will need to leverage both their differences and their similarities. The world has now experienced the 'longest period of peace and stability in Europe's written history'[2] – more than 70 years. Unfortunately, peace now does not guarantee peace forever. Successfully navigating the fog of Day Zero will require an integrated NATO and EU accustomed to practicing active engagement at every level.

The NATO-EU Joint Declaration and Proposals

Day Zero definitions vary by domain and perspective as do assessments about whether it has already passed. Some analysts contend that Day Zero is long behind us. Theories vary on how NATO and the EU should recognize, prepare for, and respond to threats in each domain. NATO's Secretary General has said that, 'a cyber-attack can trigger Article 5'[3] of the Washington Treaty[4] but has cautioned that 'it's also important to understand that cyber is not something that always triggers Article 5'.[5] The one thing that is clear is regardless of domain NATO and the EU must commit to greater cooperation in order to define threats, recognize indications and warnings, and determine next actions. While inter-organizational agreements alone do not guarantee action, they are a critical step toward cooperation. When taken at the highest levels, they give guidance to the operational and tactical-level action officers who innovate and implement. Furthermore, they send a strategic message to potential adversaries of unity and intention to act if necessary. At the 2016 NATO-Warsaw Summit, NATO and EU leaders signed an unprecedented Joint Declaration (JD) solidifying their commitment to greater cooperation in seven major areas:

1. Countering Hybrid Threats;
2. Operational Cooperation, Including on the Sea;
3. Coordination on Cyber Security and Defence;
4. Developing Coherent, Complementary and Interoperable Defence Capabilities;
5. Facilitating a Stronger Defence Industry, and Greater Defence Research and Industrial Cooperation;
6. Exercise Coordination;
7. Building Defence and Security Capacity and Fostering Resilience of Partners.[6]

Through the Joint Declaration the President of the European Council, the President of the European Commission, and the NATO Secretary General

acknowledged challenges facing both organizations and agreed to address them through information sharing, asset interoperability, and integrated exercise and training programmes. In December of 2016 the respective Councils released a 'Statement on the Implementation of the Joint Declaration'.[7] The Statement included 42 proposals explaining how NATO and the EU would cooperate, collaborate and coordinate across the 7 major areas. The majority of Proposals emphasize that NATO and EU personnel must identify inter-organizational counterparts and complementary programs. Then they must build capabilities to meet current and future challenges or threats 'through continued and intensified staff-to-staff contacts,' 'staff-to-staff sharing of time-critical information,' and 'a spirit of reciprocity'.[8] In some cases this is already happening. The NATO Secretary General and EU High Representative/Vice President hold joint press conferences and attend ministerial meetings at each other's organizations. Various lower level experts meet with increasing frequency, share lessons identified and align programs of work. With regard to countering hybrid threats, since 2016, 'EU and NATO [have been] implementing and operationalising parallel procedures and playbooks'.[9] Also in 2016, 'NATO and the EU concluded a Technical Arrangement on Cyber Defence to help both organisations better prevent and respond to cyber-attacks'.[10] More broadly, a Joint Progress Report stated that, 'Complementarity of multinational projects/programmes developed in the EU or NATO context is pursued with concrete results such as in the area of Air-to-Air Refuelling,'[11] a critical force multiplier for allies and partners. Progress was also reported in naval operations, combined hybrid threat response exercises, partner capacity building, and in aligning the NATO Defence Planning Process and the EU Capability Development Plan.

The JD and Statement have provided freedom of movement for personnel to initiate or continue cooperation. But not all personnel have been educated on the guidance and unfortunately some that are educated do not see its benefits and therefore do not contribute to its success. Further-

more, lack of specificity and lack of tools to measure success make it difficult to set goals or prove progress. Only 17 of the 42 Proposals list specific timelines and despite a requirement to publish a Joint Progress report every six months, it can be difficult for staffs to measure progress toward non-specific output requirements. Expanding the Proposals with specificity and measurements of success would make it easier to build roadmaps and track success. Furthermore, visible evidence of meaningful progress would validate to sceptical parties the need for cooperation.

PESCO

Most of the JD's 42 proposals list complementary NATO and EU programs already in existence that must integrate operations. Still, bureaucratic stumbling blocks like NATO consensus and EU majority voting requirements have encouraged nations to seek out smaller organizations of like-minded entities such as the EU's new Permanent Structured Cooperation (PESCO) in order to achieve goals more quickly. 'PESCO is a Treaty-based framework and process to deepen defence cooperation amongst EU Member States'.[12] Of concern to some is the appearance of duplication when compared to the Joint Declaration & its Proposals. PESCO's 17 inaugural projects aim to 'jointly develop defence capabilities and make them available for EU military operations'.[13] The projects span 3 areas which overlap greatly with the 7 focus areas of the Joint Declaration:

1. Common Training and Exercises;
2. Operational Domains (Land, Air, Maritime, Cyber);
3. Joint and Enabling Capabilities (Bridging Operational Gaps).

Twenty-five EU member states have signed on to at least one PESCO project. While PESCO will undoubtedly enhance Europe's ability to detect, deter and respond to threats, neither the EU nor NATO can afford to have

member states simultaneously contributing resources in full to duplicative projects. Though defence spending in NATO as a whole has increased, still only three European Allies reported 2017 expenditures as meeting the Alliance's required 2 percent or more of their GDP.[14] Nine European nations will act as the lead for one or more PESCO project, but only one of these nations currently meets the NATO spending target.[15,16] In his 2017 'Initiative for Europe' speech French President Emmanuel Macron championed PESCO as part of an effort to ensure 'Europe's autonomous operating capabilities, in complement to NATO'.[17] The challenge for nations will be to balance their resource allocation to projects and missions while contributing to cohesion rather than detracting from it. One way to do so would be to ensure PESCO projects are nested inside the JD's Proposals. This would foster trust while building capacity and capability in an unprecedented manner for both organizations. In a JD joint progress report, leaders stated, 'cooperation between the two organizations is now becoming the established norm, a daily practice, fully corresponding to the new level of ambition referred to in the Joint Declaration'.[18] Leaders in both NATO and the EU must embrace programs like PESCO while integrating them into preexisting initiatives to responsibly build capacity and capability. Doing so will further prove that cooperation is an intrinsic core value.

Finally, while one might conclude that a nation with dual NATO and EU membership would approach each organization similarly, this is not always the case. In 2015, the Brookings Institution wrote that, 'Today, member states often send separate and sometimes contradictory instructions to their NATO and EU delegations'.[19] 'The Fog of Day Zero' leaves little room for separation and contradiction. Indeed, any confusion or discord over allocation of forces to NATO vs. PESCO, or insistence by each organization on maintaining autonomy from the other in a crisis will create seams that any intelligent adversary will exploit to create strategic paralysis in nations and in turn, NATO. Also in 2015, the Clingendael Netherlands Institute of International Relations published a study outlining how NATO and the EU

should respond to new threats. In exploring why cooperation and sharing between two organizations with so much in common is so difficult the authors wrote, 'Much has to do with the past and with the behaviour of certain member states, which has little to do with substance but all the more with domestic political agendas'. [20]

Conclusion

The constructs of the EU and NATO provide established frameworks from which to share information and increase both capacity and capability. In March of 2018 NATO's Secretary General told reporters that 'NATO doesn't have the luxury of choosing the security threats we face. We must be ready and able to operate decisively across all operational domains—land, sea, air and cyberspace.'[21] It is obvious that this applies as well to the EU. Considering the wide array of multi-domain challenges to both organizations, neither can afford to waste another minute on resistance to cooperation. Furthermore, neither can afford duplicative programs. The Joint Declaration and Statement on Implementation were unprecedented first steps. But in order to fully capitalize on the successes already reached and prove their concepts, the 42 Proposals need more specificity and tools to measure success. Secondly, NATO and EU leaders must discourage divergent initiatives and make every effort to nest programs like PESCO within already existing constructs. NATO and the EU have individually effected major achievements for their citizens but the guidance from the top is clear. Now is not the time for resting on laurels or driving wedges. Future success of either organization depends of the success of both.

Major Victoria Thomas (USAF) is a NATO Air-to-Air Refuelling (AAR) Subject Matter Expert. She is also a founding member of the Global AAR Strategy Team which aligns NATO and EU AAR programs of work.

Endnotes

1. J. Stearns, 'NATO Members Post New Defense-Spending Increase', Bloomberg, 15 Mar. 2018, https://www.bloomberg.com/news/articles/2018-03-15/nato-members-post-new-defense-spending-rise-amid-trump-pressure, (accessed 4 May 2018).
2. 'The European Story: 60 years of shared progress', European Political Strategy Centre, http://ec.europa.eu/epsc/publications/other-publications/european-story---60-years-of-shared-progress_en, (accessed 4 May 2018).
3. Press Conference by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at the level of NATO Defence Ministers, 14 Jun. 2016, https://www.nato.int/cps/en/natohq/opinions_132349.htm, (accessed 9 Apr. 2018).
4. 'The North Atlantic Treaty', Washington D.C., 4 Apr. 1949, https://www.nato.int/cps/en/natolive/official_texts_17120.htm, (accessed 9 April 2018).
5. Ibid. 3.
6. 'Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization', EU/NATO, Warsaw, 2016. Online at http://www.nato.int/cps/en/natohq/official_texts_133163.htm, accessed 20 April 2017.
7. 'Statement on the Implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization', EU/NATO, Brussels, 2016, https://www.nato.int/cps/en/natohq/official_texts_138829.htm, (accessed 30 Mar. 2018).
8. Ibid.
9. Ibid.
10. 'NATO Cyber Defence Fact Sheet', NATO, Brussels, 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf, (accessed 5 April 2018).
11. 'Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016', Jun. 2017, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf, (accessed 5 Apr. 2018).
12. 'Permanent Structured Cooperation (PESCO) Factsheet', European Union External Action Service (EEAS), Brussels, 5 Mar. 2018, https://eeas.europa.eu/headquarters/headquarters-homepage_en/34226/Permanent%20Structured%20Cooperation%20(PESCO)%20-%20Factsheet, (accessed 30 Mar. 2018).
13. 'Permanent Structure Cooperation – PESCO: Deepening Defence Cooperation among EU Member States Fact Sheet', European Union External Action Service (EEAS), Brussels, 2017, https://eeas.europa.eu/sites/eeas/files/eu_factsheet_pesco_permanent_structured_cooperation_en_0.pdf, (accessed 5 Apr. 2018).
14. Ibid. 1.
15. Ibid. 1.
16. J. Barigazzi, 'New EU Defense Pact: Who's Doing What', POLITICO, 14 Dec. 2017, https://www.politico.eu/article/new-eu-defense-pact-whos-doing-what/, (accessed 30 Mar. 2018).
17. E. Macron, 'Initiative for Europe Speech', Paris, 26 Sep. 2017, https://www.diplomatie.gouv.fr/IMG/pdf/english_version_transcript_-_initiative_for_europe_-_speech_by_the_president_of_the_french_republic_cle8de628.pdf, (accessed 30 Mar. 2018).
18. Ibid. 11.
19. W. Drozdiak, 'Why Can't NATO and the EU Just Get Along?', The Brookings Institution, Washington D.C., 28 Sep. 2015, https://www.brookings.edu/blog/order-from-chaos/2015/09/28/why-cant-nato-and-the-eu-just-get-along/, (accessed 30 Mar. 2018).
20. M. Drent, R. Hendriks, and D. Zandee, 'New Threats, New EU and NATO Responses', Clingendael Netherlands Institute of International Relations, The Hague, Jul. 2015, https://www.clingendael.org/sites/default/files/pdfs/New%20Threats_New%20EU_Nato%20Responses_Clingendael_July2015.pdf, (accessed 4 Apr. 2018).
21. Ibid. 1.

© US Air Force, SSgt Kyle Van Der Wagen

The Significance of Day Zero

XI

Lieutenant General Joachim Wundrak, *DEU, Air Force*
Executive Director, JAPCC

The Executive Director's Closing Remarks

The issue of deterrence was raised extensively in previous JAPCC Conferences: 2015 in the context of 'Air Power and Strategic Communications', 2016 with regard to 'Joint Air Operations in a Degraded Environment', and 2017 under the headline of 'The Role of Joint Air Power in NATO Deterrence'. It is therefore entirely appropriate that this year's Conference is dedicated to examining the indicators of failing deterrence, along with the situation when deterrence fails and Joint Air & Space Power is needed as part of NATO's response to a crisis and/or war. Hence 'The Fog of Day Zero: Joint Air & Space in the Vanguard' was adopted as this year's Conference theme.

As the Executive Director of the Joint Air Power Competence Centre I want to offer my perspective on some issues which are, in my opinion, relevant in the context of our Conference theme.

'Day Zero' can be seen as the early phase of a conflict and not necessarily as a concrete day. The 'Fog of Day Zero' implies that there might be activities happening that portend a crisis or war and we don't realize it, and may

not be able to positively identify the instigator. This becomes evident in a hybrid threat environment, when a hostile actor intentionally exploits ambiguity. The evolution of the crisis in eastern Ukraine since 2014 is an apt example. Unclear situational awareness and uncertain situations may prevent or slow down NATO authorities' ability to reach a decision to respond to a threat. Besides a discussion of 'what is Day Zero' I expect the Conference to examine the decision making process within NATO and the capabilities and vulnerabilities of NATO's Joint Air Power: Are we prepared well enough to deal with such an unclear situation?

In the past NATO has continuously adapted itself to the changing security environment with the resources and the resolve to guarantee the Alliance's security. Since the 2014 Ukraine crisis, NATO's emphasis has returned to collective defense whilst taking a 360 degree approach to projecting stability and cooperative security given the wider understanding of interrelated crises and security challenges. Polarization within and between states, power politics and competition between major powers have increased the potential for instability. Other trends include state and non-state actors using hybrid and cyber tools to impact the security environment in the grey zone below the threshold of conflict. So today, the Alliance must engage in both collective defense and crisis management at the same time.

Russia's illegal annexation of Crimea in 2014 and its military build-up changed the Alliance's security environment completely. Since then Allies have implemented the largest reinforcement of our collective defense since the Cold War. To counter the Russian threat NATO has taken many decisions at the NATO Summits in Wales 2014 and Warsaw 2016 like the Readiness Action Plan (RAP), the Very High Readiness Joint Task Force (VJTF), the enhanced NATO Response Force (eNRF), enhanced Forward Presence (eFP) and others. However, if deterrence fails, for example if a Russian snap exercise like ZAPAD 2017 turns over into real military opera-

tions, it takes time for the Alliance ground forces to counter an attack. If Russian troops take the famous 'Suwalki Gap' and link up with Kaliningrad, the Baltic States will be cut off from NATO territory. There is no doubt that Joint Air Power would be NATO's first responder to such a situation, hence 'Joint Air & Space Power in the Vanguard'. This example raises numerous concerns that should be discussed during our Conference, including: NATO's rapid reaction capabilities; Air Command and Control; the A2AD problem; the quantity, quality and readiness of our air forces; air transport for our ground troops; ISR assets; interoperability; jointness; sustainability; and resilience.

This Read Ahead is not all-inclusive, it merely provides food for thought and a good starting point for discussion by addressing various aspects which are relevant for the Conference theme. The chapter on Threat Awareness describes a broad spectrum of evolving threats and how NATO should prioritize its efforts to ensure success. The article from The Economist 'Russia's conventional forces outgun NATO near its borders' gives an impression on the amount of combat power Russia can concentrate at very short notice in the Baltic region and why the Alliance is possibly ill-prepared to deter limited Russian aggression. Possible conflict scenarios in the space and cyberspace domains are described in subsequent chapters, necessary considerations are listed and a number of questions raised. The chapter about Force Protection highlights various aspects of the threat for NATO forces and comes to the conclusion that NATO cannot hope to protect itself completely from all the challenges that are currently possible. We have included an article previously published on www.nato.int which emphasizes that 'Resilience' is a core element of collective defense. Chapters on Logistics and NATO-EU Cooperation round out this menu of challenges.

I want to highlight the Training & Exercise chapter in this Read Ahead. It addresses the way we prepare our men and women for the new security environment and for a peer-to-peer or near-peer conflict. Exercises do not

need to look good, they need to be good! The article gives a very realistic description of today's exercise situation and I'm sure that the Conference will have an in depth discussion about mentality, training and exercises.

I invite you to visit our Conference website to further explore details regarding keynote speakers, panels and the registration process for this year's Conference: https://www.japcc.org/conference/

In closing, I hope that you have found the articles in this Conference Read Ahead informative and enlightening. My desire is that these articles will provoke thought and stimulate discussion about the role of Joint Air & Space power in the early phase of a conflict; and that they will entice you to join a broad group of international colleagues and share your thoughts and ideas with us.

I sincerely hope to see you this fall in Essen!

Joachim Wundrak
Lieutenant General, DEU AF

Executive Director, JAPCC

Conference Itinerary

9 October 2018
Icebreaker and Industry Showcase
Director and VIP Tour of Industry

10 October 2018
Keynote Speech
Panel 1: The 'Day Zero' Threat Environment: Modern Threat Vectors, Adversary Shaping Operations, and the Article V Threshold
Panel 2: Joint Air and Space Power in the Vanguard of NATO's Response: Capabilities, Vulnerabilities and Challenges
Director's Luncheon
Panel 3: Does NATO have the Required Mindset to Fight on 'Day Zero'?
Networking Dinner and Industry Showcase

11 October 2018
Keynote Speech
Panel 4: How can NATO Address Emerging Security Challenges Using Air and Space Power?
Discussion Session on Way Ahead
Wrap-up and Director's Closing Remarks
Networking Lunch

Joint Air Power Competence Centre

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