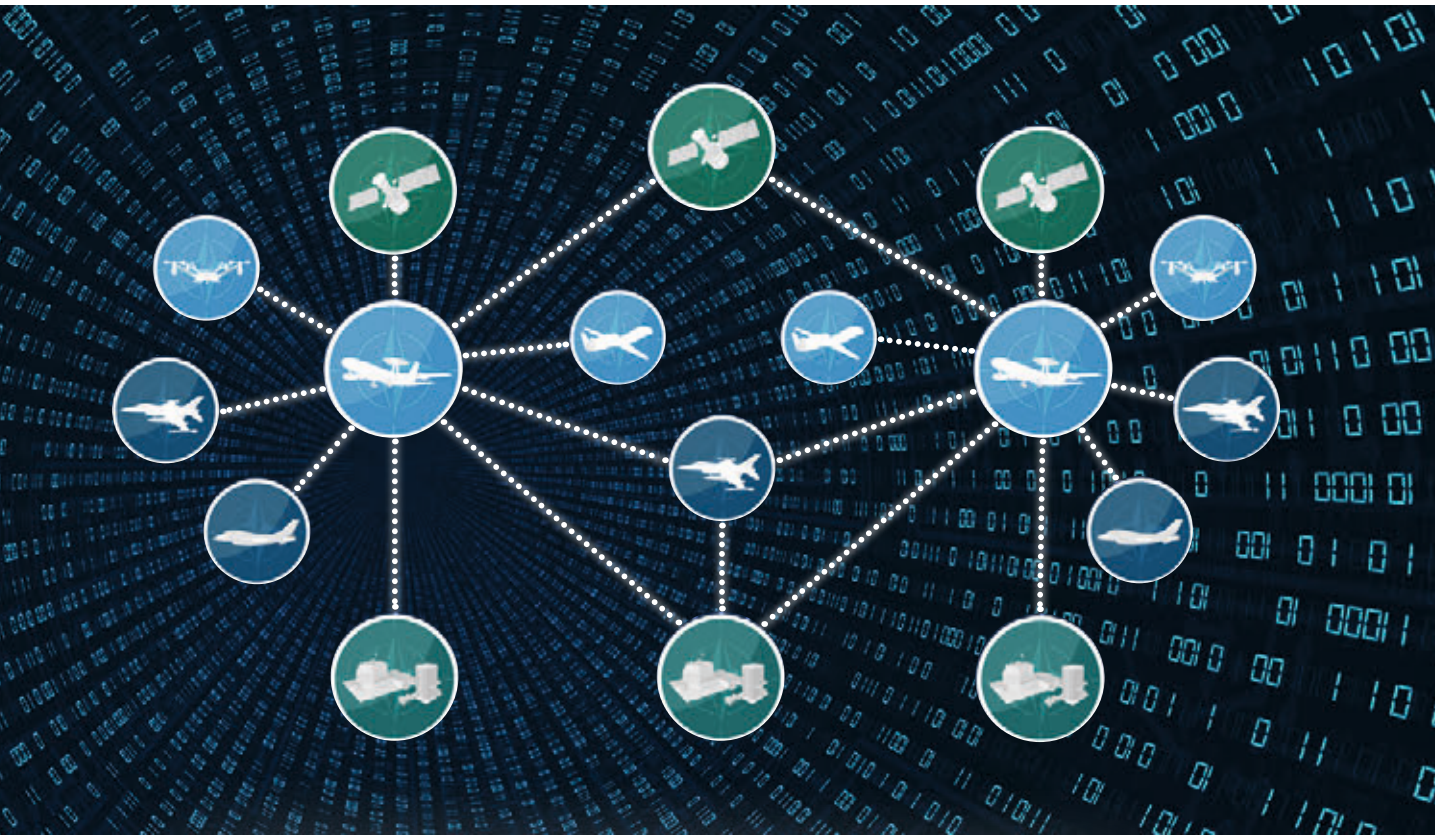
November **2017**



NATO Joint Air Power and Offensive Cyber Operations

Joint Air Power Competence Centre

Cover picture Ⓜ © NATO (Figure), © SaidAuita/shutterstock (Background)

Disclaimer
This publication is a product of the Joint Air Power Competence Center (JAPCC). The views and opinions expressed or implied in this work are those of the author. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO), and is designed to provide an independent assessment in the field of Offensive Cyber Operations and Joint Air Power following the 2016 NATO Summit in Warsaw.

Comments and queries on this document should be directed to the C4ISR & Space Branch, JAPCC. Please visit our website www.japcc.org for the latest information on JAPCC, or e-mail us at contact@japcc.org.

Author
Lt Col Paul J. MacKenzie (RCAF)

Special thanks to the following people for providing clarification and recommendations during the drafting of this document:
Clare Lain, NATO Cooperative Cyber Defence Centre of Excellence
Wg Cdr Rob Smeaton, SHAPE HQ JCyber
Maj Ron Werkman, NATO Command and Control Centre of Excellence
John Gwinnup, NATO Intelligence Fusion Centre

Release
This document is releasable to the Public. Portions of the document may be quoted 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

Telephone: +49 (0) 2824 90 2201
Facsimile: +49 (0) 2824 90 2208
E-Mail: contact@japcc.org
Website: www.japcc.org

Ⓜ Denotes images digitally manipulated

FROM:

The Executive Director of the Joint Air Power Competence Centre (JAPCC)

SUBJECT:

NATO Joint Air Power and Offensive Cyber Operations

DISTRIBUTION:

All NATO Commands, Nations, Ministries of Defence and Relevant Organizations

The successful projection of Joint Air Power relies heavily on Cyberspace for complex mission systems, C4ISR and Space Support to Operations. Assets operating in the air environment must have freedom of movement, literally and in Cyberspace, to effectively project power and, ultimately, secure Air Superiority, without which there is a grave risk to mission accomplishment.

As a vital component in the projection of Air Power, Cyberspace has surpassed its mark as an enabler, now recognized as not only critical to mission assurance but a Domain of operations in itself. Consequently, it is critical that the systems operating in Cyberspace be secure, reliable and available and establishing these criteria by employing defensive measures alone may be insufficient. It may be necessary to exploit the ability to attack those systems attacking NATO, to include an adversary's mission systems, and even as part of a joint effort to accomplish the mission. Ultimately, we must ask ourselves whether Defensive Cyberspace Operations (DCO) alone are sufficient, or whether this posture inhibits the adequate projection of Joint Air Power. A strong argument can be made that NATO must be able to request and/or exploit offensive Cyberspace effects.

In this White Paper, JAPCC looks back at the evolution of Cyberspace within NATO, from the initial use of IT/CIS for basic digital communications needs, through to the declaration of Cyberspace as a Domain of operations. Lessons learned from key events as well as research papers are cited in an assessment that asserts offensive Cyberspace operations and effects are required to have the most effective Cyberspace posture, suggests how they might be applied in Joint Air Power scenarios, and offers that structural models already exist for how this capability might be incorporated into the NATO organization and processes.

Joachim Wundrak
Lieutenant General, DEU AF
Executive Director, JAPCC

JOINT AIR POWER COMPETENCE CENTRE

Joint Air Power Competence Centre | centre de compétence de la puissance aérienne interarmées
von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar | Germany/Allemagne | Tel +49 (0) 2824 90 2201 | Fax +49 (0) 2824 90 2208 | www.japcc.org
NCN: +234 or 239 2201 | **E-Mail:** contact@japcc.org

TABLE OF CONTENTS

NATO JOINT AIR POWER AND OFFENSIVE CYBER OPERATIONS

NATO JOINT AIR POWER AND OFFENSIVE CYBER OPERATIONS

Introduction

The declaration by NATO at the Warsaw Summit of July 2016 that cyberspace is a domain of operations[1] represents a significant milestone in the evolution of cyber policy in the Alliance. First appearing officially on the NATO agenda in the Prague Summit of 2002 with an entirely defensive focus[2], cyberspace has risen in prominence steadily to now reach the forefront of priorities and share, if only in policy and not yet in practice, the same stature as the maritime, land and air operational domains. Yet NATO forces are hindered in that current NATO policy, conforming to its 'raison d'être' as a defensive alliance, remains focused on Defensive Cyber Operations (DCO) and has not yet embraced Offensive Cyber Operations (OCO)[3]. The implications of pursuing OCO and the decision to maintain a defensive posture have been the focus of extensive analysis by NATO cyberspace and legal experts and any change to this posture in the foreseeable future is forecasted to be very slow. The same handicap is not shared with the other domains, excluding those prohibitions imposed under the Law of Armed Conflict (LOAC), within which our military

1. Warsaw Summit Communiqué, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 15 Mar. 2017.
2. Prague Summit Declaration, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/official_texts_19552.htm, accessed 20 Mar. 2017.
3. North Atlantic Treaty Organization, 'Cyber Defence', http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 20 Mar. 2017.

personnel are highly skilled and experienced at planning across the full-spectrum of operations. This shortfall makes the already complex subject of cyberspace that much more difficult for planners who are charged with integrating cyberspace into operational plans and mission execution. Air forces, in particular, rely heavily on cyberspace's Computer and Information Systems (CIS) and Information Technology (IT) to carry out their missions. From the strategic to the tactical level and from Command and Control (C2) systems to mission systems, air forces are, arguably, both more vulnerable to breaches in their defences and greater benefactors of successful attacks on adversaries' systems. This leads one to question whether cyberspace doctrine, policies and procedures lacking direction and guidance regarding OCO have an adverse impact on NATO forces operating in the air environment and, if so, how OCO might benefit NATO forces during the planning and execution of the projection of air power.

Definitions

It is important to understand what is meant by OCO and what distinguishes it from DCO. There are no universally accepted definitions of cyber terminology among NATO nations.[4] Therefore, there are many varied interpretations which make both distinguishing between the two and recognizing where they overlap somewhat challenging. It is beyond the scope of this

4. Cooperative Cyber Defence Centre of Excellence, Cyber Definitions, https://ccdcoe.org/cyber-definitions.html, accessed, 5 Mar. 2017.

© Toria/shutterstock

paper to provide a detailed explanation of offensive and defensive cyber operations. For the purposes of clarity the following simplified definitions will suffice. DCO are considered those actions undertaken to ensure the confidentiality, integrity and availability of NATO systems and/or data. OCO are those activities undertaken, via digital means, to infiltrate, reconnoitre, exploit, disrupt, deny access to and/or destroy the adversaries' systems and/or data. Furthermore, since the focus is OCO as they pertain to Joint Air Power it is necessary to understand Joint Air Power as the 'synergistic application of air, space and information systems from and for all services to project military power' and includes the 'use of military force in air or space by or from an air platform or missile operating above the surface of the earth'.[5]

Background

The defence of its CIS/IT has always been one of NATO's principle responsibilities in order to protect its ability to connect the Alliance, support projects, and conduct operations and missions. The overall responsibility to protect NATO's CIS/IT was shared for decades among several agencies up until 1 July 2012 when the NATO Communication and Information Agency (NCIA) was formed from the amalgamation of several agencies, principally: the NATO Consultation Command and Control Agency (NC3A), the NATO CIS Services Agency (NCSA), the NATO Air Command and Control Systems (ACCS) Management Agency (NACMA) and the Active Layered Theatre Ballistic Missile Defense (BMD) Programme office.[6] From the initial introduction of CIS/IT, such as basic e-mail and web page capabilities, through to today's complex C2 technology for BMD, ACCS, Joint Intelligence Surveillance and Reconnaissance (ISR) and the Federated Mission Network (FMN), CIS/IT has rapidly evolved from being a simple data communications system, to an enabler, and thence to being critical for mission assurance. This evolution has seen not only steady transformation at the unit and organizational levels but an increase in prominence within the Alliance's political agenda. First mentioned at the 2002 Prague Summit where the Alliance committed modestly to 'strengthen our capabilities to defend against cyber-attacks',[7] the Alliance has steadily increased the role of cyberspace within its mandate to where, at the Warsaw Summit in July 2016, the Alliance recognized cyberspace as a domain of operations, to share the status with the traditional domains of maritime, land and air.[8]

'… most crises and conflicts today have a cyber dimension …'

The increase in prominence of cyberspace on NATO's political agenda was inspired primarily by two seminal events – the cyber-attacks on Estonia in April 2007 and the conflict between Russia and Georgia in the summer of 2008, in which cyber was a significant component to Russia's 'Hybrid Warfare' tactics. The attacks on Estonia prompted NATO to develop a policy on cyber defence in January of 2008. After the conflict in Georgia, when it became clear that cyberspace had 'the potential to become a major component of conventional warfare' and that 'most crises and conflicts today have a cyber dimension',[9] there was a succession of responses undertaken by NATO, the more significant of which included the adoption of a Strategic Concept (November 2010), the integration of cyber defence into the NATO Defence Planning Process (NDPP) (April 2012), the establishment of NCIA (July 2012), the endorsement of the current Cyber Defence Policy (June 2014), the approval of the new Cyber Defence Action Plan (September 2014) and the Technical Arrangement on Cyber Defence between the NATO

5. Concept for the Joint Air Power Competence Centre (JAPCC) MOD Bonn, 31 Jul. 2003, p. 3.
6. NATO Communications and Information Agency (NCIA), http://www.nato.int/cps/en/natolive/topics_69332.htm, accessed 28 Mar. 2017.
7. Prague Summit Declaration, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/official_texts_19552.htm, para. f, accessed 20 Mar. 2017.
8. Warsaw Summit Communiqué, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/topics_78170.htm, para 70, accessed 15 Mar. 2017.
9. North Atlantic Treaty Organization 'Cyber Defence', http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 20 Mar. 2017.

© Rawpixel.com/shutterstock, Screen Layout: © JAPCC

Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU). All these activities were developed within the framework of NATO's mission and core tasks of collective defence, crisis management and cooperative security.[10]

Doctrine

Despite the Warsaw Summit declaration that cyberspace is a domain and that 'cyber-attacks could be as harmful as a conventional attack and present a clear challenge to the security of the Alliance', member Heads of State and Government (HOSG) reaffirmed their commitment to 'follow the principle of restraint towards international peace, security and stability in cyberspace'[11] and so maintain focus on defensive activities. In July 2016 the NATO Military Committee Joint Standardization Board (MCJSB) tasked the Allied Joint Operational Doctrine Working Group (AJOD WG) to develop the Allied Joint Doctrine for Cyberspace Operations – AJP 3.20. The current estimate for completing AJP 3.20 is sometime in 2018.[12] Based on the Doctrine Task document and the assessment of feedback to the Working Group, it could be expected that the AJP 3.20 would 'exclude comments relating to the need for future capabilities to

10. North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/topics_133127.htm, accessed 24 Mar. 2017.
11. Warsaw Summit Communiqué, para 70.
12. NATO Standardization Office, Military Committee Joint Standardization Board, 'Doctrine Task (DT) for Allied Joint Doctrine for Cyberspace Operations – Allocation of Study Number and Detailed Tasking' (14 Jul. 2016).

the extension of NATO into offensive operations'[13] and maintain focus on defence within cyberspace. However, the DRAFT version of AJP 3.20 (of 1 January 2017) introduces OCO within NATO doctrine and was being circulated for review and feedback at the time of writing this paper.[14]

'… cyber-attacks could be as harmful as a conventional attack …'

The Law of Armed Conflict

As debates and discussions continue with respect to identifying where changes must and/or can be made to NATO Policy in the way ahead, the absence of approved direction and guidance specific to OCO is misinterpreted by many to mean that NATO is prohibited from exploiting OCO in any manner. While there is no treaty that specifically deals with Cyber Warfare, International Law Applicable to Cyber Warfare has been established and it encompasses the international law both governing the resort to force by states as an instrument of their national policy, and regulating the conduct of armed conflict as they apply to cyberspace. The legal restraints and constraints, or 'Rules' as they are titled, of which there are 95 in total, apply to the conduct of cyber operations and they are, for the vast majority, similar in principle as those that apply to the traditional domains (maritime, air, land) which aim to protect civilians from being impacted by military operations, such as those dealing with Necessity and Proportionality, Self-defence, Prohibition on attacking civilians/civilian objects, Indiscriminate Attacks, and the Choice/Verification of targets. In fact, it may be surprising to some military planners today that in those situations where 'cyber operations would in most cases be less likely to cause collateral damage, they would be required by law in lieu of kinetic alternatives'.[15]

The Best Defence Requires Offense

Irrespective of whether OCO are permissible if/when done in accordance with the LOAC, NATO Force Structure does not include resources to conduct OCO, nor is it likely to in the foreseeable future. Having declared cyberspace a domain of operations without preparing to conduct OCO or being able to generate offensive cyberspace effects presents a rather unique conundrum. The armies, air forces, navies and special forces of modern nations defend and deter through employment of their capabilities to achieve both offensive and defensive effects. It can be argued that cyberspace operations are no different in principle from the traditional domains and this raises the question whether the lack of policy regarding OCO in NATO doctrine represents a capability gap. In cases such as these, the military turns to lessons learned from previous experiences and to the research and development of the defence scientists to assist in the development of new policies, direction and guidance in order to forge ahead with new and/or evolving concepts/technologies. In the case of cyberspace, experience and analysis demonstrate that it is at least more efficient, if not critical, to employ both offensive and defensive capabilities together and, preferably, within a single entity in order to properly execute cyber operations.

'… in those situations where "cyber operations would in most cases be less likely to cause collateral damage, they would be required by law in lieu of kinetic alternatives".'

General Keith Alexander (US Army), when Director of the US National Security Agency (NSA), in his interview with the US House Armed Services Committee in 2010 in the aftermath of Operation Buckshot Yankee (the response to a cyber-attack that impacted classified US military systems in the Middle East including

13. NATO Standardization Office, Military Committee Joint Standardization Board, 'Doctrine Task (DT) for Allied Joint Doctrine for Cyberspace Operations – Allocation of Study Number and Detailed Tasking' (14 Jul. 2016), p. B-I-3.
14. NATO AJP 3.20 Allied Joint Doctrine for Cyberspace Operations (DRAFT – 15 Jan. 2017), p. 33.
15. Schmitt, Michael N., 'The Law of Cyber Targeting', Tallinn paper no. 7, 2015, ***The Tallinn Papers,*** p. 18.

Book Cover
© Cambridge University Press 2013
Michael N. Schmitt (Ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare

Background
© ESB Professional/shutterstock

the SIPRNet and JWICS[16]) explained that in order to stop the ongoing harm being conducted by the virus they 'needed to bring together the offense and defense capabilities'.[17] More specifically, they needed to stop the virus from beaconing, and while the forensics teams focused on defence and determining attribution, it was an offensive cyber unit of the Joint Functional Component Command – Network Warfare that proposed the techniques to neutralize the malware.[18] General Alexander explained that it was not until the offensive and defensive teams were brought together that his unit began to make real progress in countering the threat. Indeed, the Task Force plans were to make greater use of offensive cyber capabilities to defend the systems in the future.

In his study explaining how the United Kingdom developed its approach to cyber, Group Captain Shaun Harvey (RAF) argued for the integration of OCO and DCO in order to exploit what he referred to as cyber 'equities', conditions where these two separate lines of effort are balanced in order to achieve the most effective operational results.[19] He offered the scenario where DCO personnel are committed to the correction of a vulnerability, but by doing so deny their OCO colleagues from conducting cyber intelligence gathering through allowing opposing forces to exploit the same vulnerability. This type of activity could only be successful if the offensive and defensive lines of effort are coordinated within a single command structure and while operating in unison.

In its Task Force Report on Resilient Military Systems and the Advanced Cyber Threat (January 2013), the US Department of Defense (DoD) Defense Science Board explained that, along with vulnerabilities introduced with third party manufacturing, Commercial-Off-The-

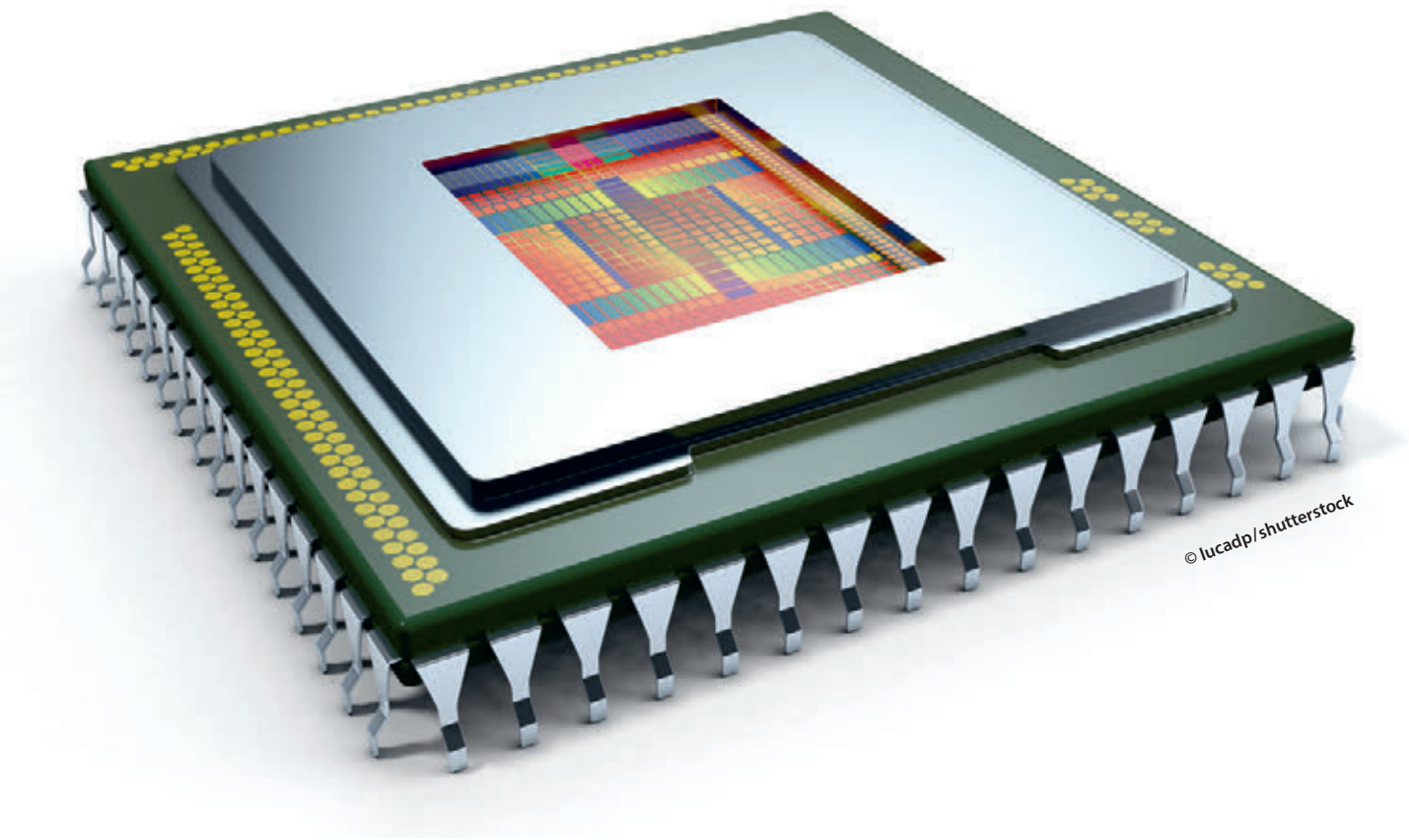
16. The USA's Secret Internet Protocol Router Network (SIPRNet) and Top Secret, Joint Worldwide Intelligence Communications System (JWICS).
17. Gridal, Karl, 'Operation BUCKSHOT YANKEE', from Healy, Jason, Editor, ***A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*** Cyber Conflict Studies Association publication, 2013, p. 210.
18. Ibid., p. 209.
19. Harvey, Shaun, Group Captain RAF, 'Unglamorous Awakenings: How the UK Developed Its Approach to Cyber', from Healy, Jason, Editor, ***A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.*** Cyber Conflict Studies Association publication, 2013, p. 257.

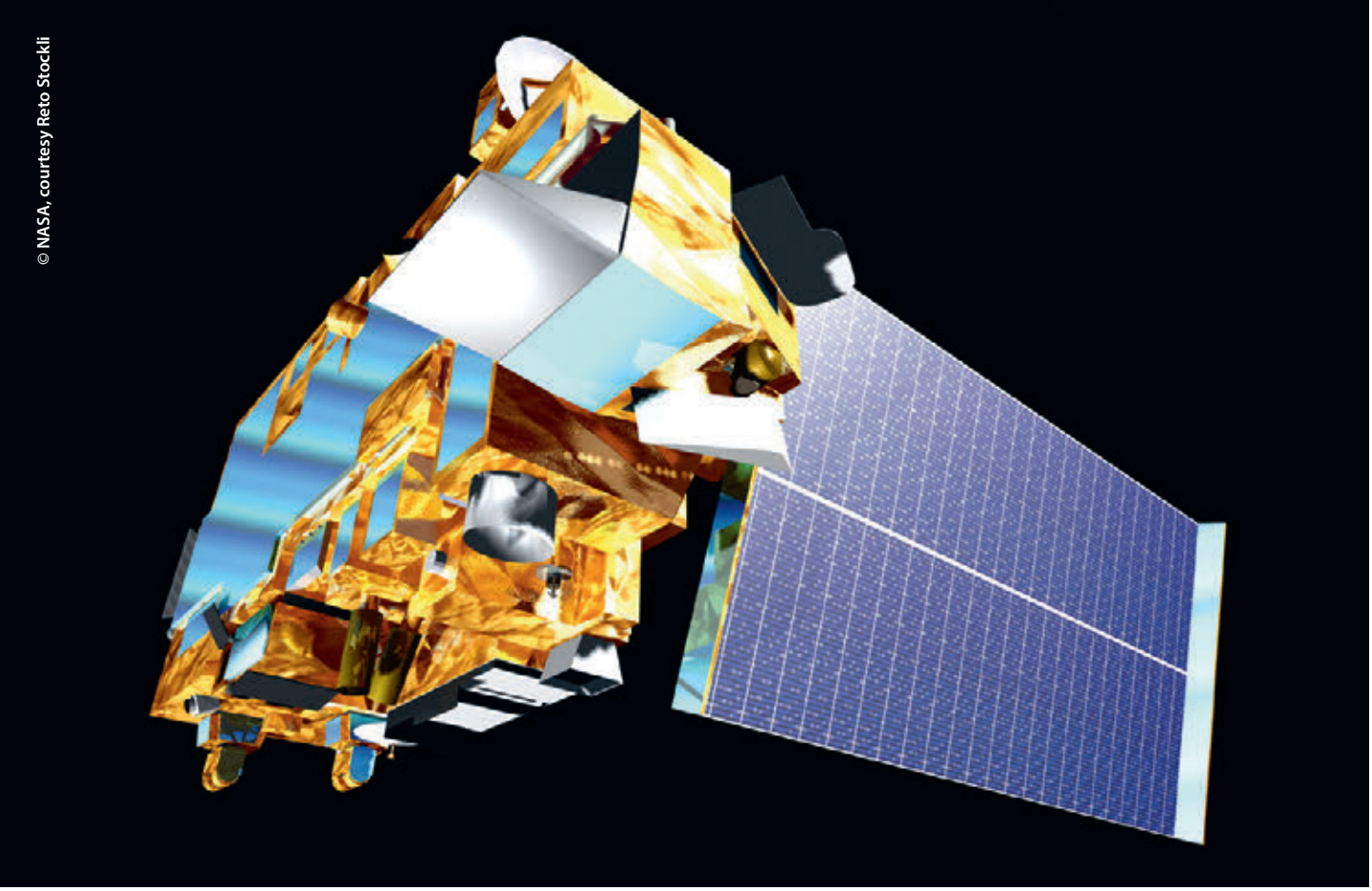
Shelf supply, offshore development and the inherent vulnerability of the Internet, that 'the complexity of modern software and hardware systems makes it difficult if not impossible to develop components without flaws or to detect malicious insertions' in order to defend completely against cyber-attacks.[20] The report elaborates by explaining many commercial operating systems have nearly 50 million lines of code and that complex integrated circuits have over 2 billion transistors; consequently, it is impossible to test such software and hardware completely for vulnerabilities. The report adds that while cyber defence alone may help protect from less sophisticated threats, well-resourced state actors have the ability to create significant cyber capability so 'defense only is a failed strategy', and that there must be a mix of offensive and defensive cyber capabilities.[21] The report added that 'the best (cyber) defenders will be those who understand what can be accomplished from an offensive point of view … (and that) creating cyber warriors with expertise in offensive and defensive cyber skills should be encouraged'.[22]

'… many commercial operating systems have nearly 50 million lines of code … complex integrated circuits have over 2 billion transistors …'

Lessons learned from operational experience and detailed research and analysis support the integrating OCO effects to have the most effective cyber defence posture. However, the full potential of OCO in the cyberspace domain extends well beyond the layered defence of NATO's IT/CIS to include not only the

20. Defense Science Board, Department of Defense, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan. 2013, p. 26.
21. Ibid., p. 29.
22. Ibid., p. 64.




© NASA, courtesy Reto Stockli

enablement of other traditional domains, but to independently generate effects at the tactical, operational and strategic levels. While addressing the role of OCO in NATO's collective defence, James A. Lewis writes that 'cyber techniques are essential for the kinds of combat operations that NATO forces may carry out in the future. No modern air force would enter into combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support … (and) offensive cyber capabilities will shape the battlefields of the future'.[23] He adds that offensive cyber actions will be conducted at the tactical and operational levels and that the 'most likely form of attack will be against command and control systems (including sensors and computer networks) and against the software that runs advanced weapons such as surface-to-air missiles or fighter aircraft'.[24] He also proposes that adding offensive cyber capabilities to NATO's doctrine and force structure will also strengthen its deterrence.[25]

Precision

Offensive cyber effects are not yet incorporated into mission planning, this includes the air campaign. Aside from the fact that NATO is a non-aggressive, defensive alliance, there is a general misconception within the organization that one of the principle reasons NATO refrains from OCO, apart from the resource bill, is the risk of causing collateral damage, of not being able to contain the effects and endanger civilians and/or the environment. This stems from a lack of understanding or appreciation for the precision with which offensive cyber effects can be applied. NATO would not risk violating the LOAC through OCO and moreover, nations possessing these capabilities have the technological prowess to reduce these risks to negligible levels. Since nations tend to safeguard both their weaknesses in cyber defence and their offensive cyber capabilities as a matter of national security, the preponderance of information that

23. Lewis, James A., 'The Role of Offensive Cyber Operations in NATO's Collective Defence', Tallinn paper no. 8, 2015, The Tallinn Papers, p. 3.
24. Ibid., p. 4.
25. Ibid., p. 2.

describes their precision is classified. Still, examples have been disclosed in the media that demonstrate the specificity to which OCO can be applied. In September 2007, Israeli Air Forces were able to penetrate Syrian Air Defence Radar coverage and remain undetected by the Syrian Air Defence Forces for the duration of an attack on a Syrian Nuclear facility. The specific details of the delivery vector and attack mechanism remain classified, but most experts agree that it was executed through a combination of airborne EW and OCO. [26,27] In another example, in June and October of 2008, the satellite control centre for the Terra Earth Observation System AM-1 in Spitsbergen, Norway was attacked. The investigation determined that in both cases the attackers 'achieved all steps required to command the satellite but did not issue commands'.[28]

'… adding offensive cyber capabilities to NATO's doctrine and force structure will also strengthen its deterrence.'

Perhaps the most celebrated case of an extremely precise cyber-attack is Stuxnet. This capability was highly specific, targeting only the industrial control systems for controlling the gas centrifuges used in the process of enriching uranium within Iran's nuclear research and development facilities. Many of the centrifuges were destroyed and Iran's nuclear programme was delayed by years.[29]

These few examples demonstrate that offensive cyber capabilities can be designed to be highly focused, even on well protected mission systems, and so avoid causing collateral damage and minimize the risk of contravening the LOAC.

It is important to recognize that creating offensive cyberspace effects of these types is considered a 'high art'[30] for which only a few NATO nations, the US and the UK for example, have the prerequisite 'elite cyber capabilities'.[31] However, the number of NATO member states developing OCO capabilities is growing. France has the ability to conduct OCO[32] and the Netherlands 'deploys offensive digital resources exclusively against military targets'.[33] Canada lifted its self-imposed restriction from conducting OCO in 2016 and is developing offensive cyber capabilities[34] and, on 1 April 2017, Germany established the Cyber Operations Command which will include an offensive element.[35]

Joint Air Power Gap?

Given that NATO recognizes cyberspace as a domain of operations, that OCO are not prohibited by international law (as long as the activity conforms to the LOAC), that combining offensive with defensive cyber operations (preferably under a single command) is necessary to be at the very least effective (if not critical), and that offensive cyber effects can be designed to be extremely precise, a capability gap is presented with respect to cyberspace operations, to include the exploitation of OCO effects in the projection of Air Power. Relying on cyberspace across the entire spectrum of military affairs from e-mail to complex mission systems, the potential for OCO applications is very broad. In assessing cyber targeting, Michael N. Schmitt attests that 'it is quite simply unimaginable that a contemporary conflict would not involve some manner of cyber

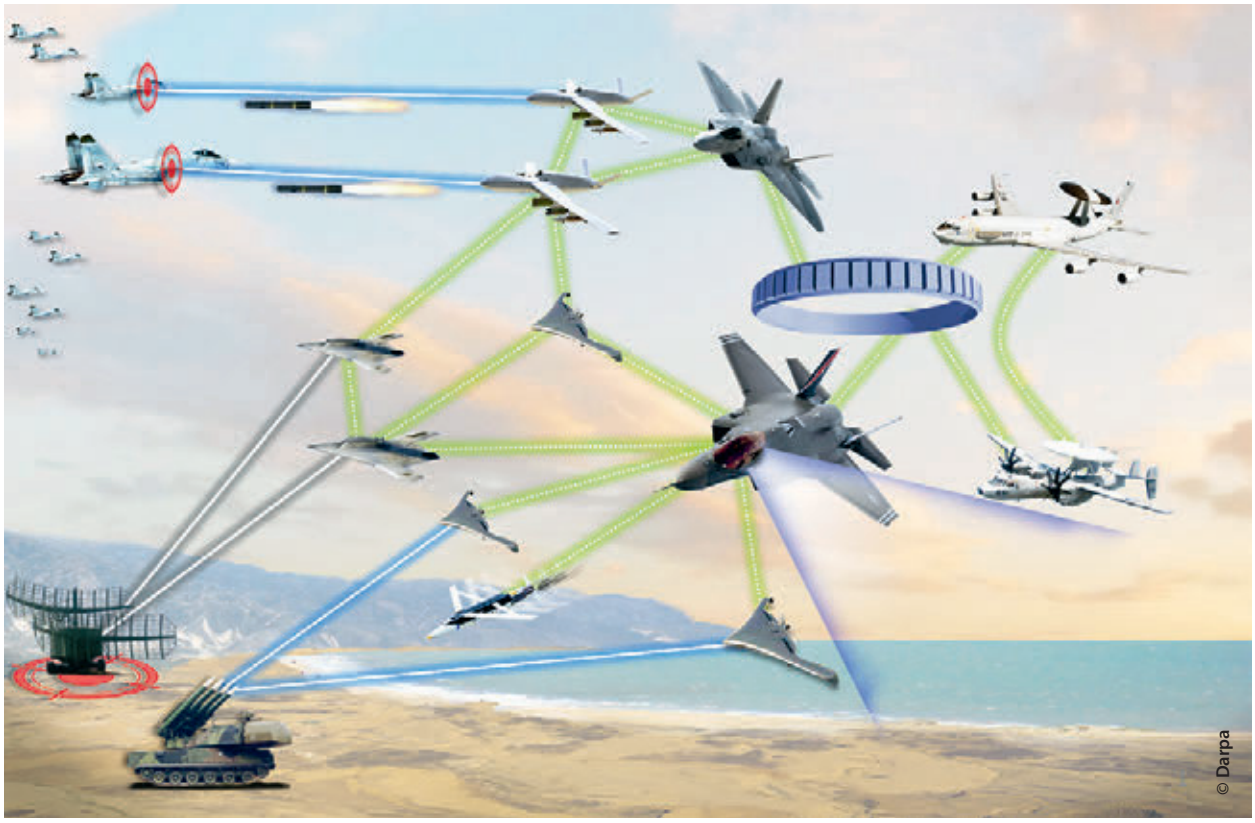
26. Carroll, Ward, 'Israel's Cyber Shot at Syria'. ***DEFENSE TECH,*** 26 Nov. 2007, https://www.defensetech.org/2007/11/26/israels-cyber-shot-at-syria/, accessed 30 Mar. 2017.
27. Adee, Sally, 'The Hunt for the Kill Switch', ***Spectrum Magazine,*** May 2008, http://online.qmags.com/IEEESM0508/, accessed 28 Mar. 2017.
28. United States Air Force, Office of the Chief Scientist, ***Cyber Vision 2025 – United States Air Force Cyberspace Science and Technology Vision 2012–2025, 13 Dec. 2012, p. 39.***
29. De Falco, Marco, Lt Col, 'Stuxnet Facts Report – A Technical and Strategic Analysis', CCD COE, 2012.
30. Lewis, p. 9.
31. Ibid., p. 7.
32. Ibid., p. 7.
33. Defence Cyber Command (Netherlands) Web Page, https://www.defensie.nl/english/topics/cyber-security/cyber-command, accessed 10 Aug. 2017.
34. Boutilier, Alex, 'Canada developing arsenal of cyber-weapons', The Star, 16 Mar. 2017, https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html, accessed 3 Apr. 2017.
35. Kalinyak, Rachael, 'New cyber command force launched in Germany', ***Fifth Domain,*** 4 Apr. 2017, http://fifthdomain.com/2017/04/04/new-cyber-command-force-launched-in-germany/, accessed 25 Apr. 2017.

© Maximus256/shutterstock

operations' even for something 'as complicated as bringing down the enemy's Integrated Air Defense Systems'[36] and it is very possible the preferred method may turn out to be 'cyber means instead of conducting kinetic attacks'.[37] Adversaries' civilian Air Traffic Control and Airspace Management systems are also potential targets if employed even partially by the military.[38] Perhaps one of the most challenging of potential scenarios, and one currently confronting NATO, is an adversary's ability to establish Anti-Access/Area Denial (A2/AD) postures, weapons and methods to counter NATO Allied Forces projection of power and prevent them from accessing and achieving freedom of manoeuvre in key areas.[39] Hans Binnendijk explains that 'Russia, like China, is building formidable Anti-Access/Area-Denial capabilities that make gaining air superiority for US and NATO Air Forces more difficult'.[40] According to Binnendijk, 'NATO Joint Air Power would be the first responder to meet a Russian conventional challenge and could offset and deter a Russian strategy to "strike, pause, and win"',[41] a tactic they employed in the Ukraine. He adds that 'should deterrence fail, Russia may have critical advantages with regard to time, geography, and political will'.[42] In such a scenario, and where conventional forces of the traditional Maritime, Air and Land Domains are unable to overcome an A2/AD posture, it is not inconceivable, and may even be necessary, for a Joint Task force Commander (for example) to request cyberspace effects to exploit a vulnerability in the enemy's Air Defence or C2 System and create opportunities in time and space to, along with conventional forces as part of a joint effort, sufficiently degrade the adversary's A2/AD posture.

Impacting adversaries' systems in such a manner is not a trivial task and some will contend that it is implausible to impact adversaries' systems in order to sufficiently reduce the enemy's A2/AD posture. But, given the general understanding of cyberspace by those outside its own community, the same sentiment would have been expressed regarding the feasibility of attacking the highly isolated and protected systems controlling the gas centrifuges in Iran's nuclear facility before Stuxnet was exposed. Maren Leed writes 'the degree to which cyber capabilities can deliver on this promise is debated, but their potential to meet the substantial security challenges that lie ahead is sufficiently promising, especially in comparison to the available alternatives, that the possibility deserves, if not demands, further attention'.[43] It is to achieve this degree of effect that we should pursue the integration of OCO in the Joint Air Environment, into Joint Operational Planning and so provide options for the commander, just as we have invested significantly and for decades in traditional domains, such as for the

36. Schmitt, p. 2.
37. Ibid., p. 18.
38. Ibid., p. 11.
39. Hutchens, Michael E., Dries, William D., Perdew, Jason C., Bryant, Vincent D. and Moores, Kerry E., *Joint Concept for Access and Maneuver in the Global Commons – A New Joint Operational Concept,* Joint Force Quarterly 84, 26 Jan. 2017, p. 135.
40. Binnendijk, Hans, 'The Role of NATO Joint Air Power in Deterrence and Collective Defence', Joint Air Power Competence Centre, *Joint Air Power following the 2016 Warsaw Summit – Urgent Priorities,* Oct. 2017, p. 56.
41. Ibid., p. 2.
42. Ibid., p. 2.
43. Leed, Maren, *Offensive Cyber Capabilities at the Operational Level – The Way Ahead,* Sep. 2013, Center for Strategic and International Studies, page v.



Suppression of Enemy Air Defenses (SEAD) via kinetic means and the employment of EW measures. This may meet with general skepticism to those outside of the cyberspace community until a threshold of understanding and confidence is reached, generally, to factor OCO effects into operational level planning. Perhaps this is a natural part of the evolution as a new domain. However, the exhaustive process of development in the evolution of cyberspace as a domain beyond AJP 3.20 and ACO Road Map is only starting to be generated and requires a champion to drive the analytical assessments and apply the administrative rigour to determine the level of effort and implement these changes.

Solution Models Exist

It is not necessary for NATO to acquire a large number of additional forces to start bridging this gap. In fact, NATO has few of what can be termed its own forces. One such example is the NATO Airborne Warning and Control System (AWACS) force located at the airbase in Geilenkirchen, Germany. NATO's military forces are comprised primarily from contributions from member nations and together they form the integrated military structure of the Alliance. These assets remain under national C2 until such time as required by NATO for a particular mission or operation. The military assets required for operations are identified during the Combined Operational Planning Process (COPP) and for which there are established processes for requesting specific forces and/or effects. In the Autumn of 2016, it was the understanding of those involved in the planning and execution of a major NATO exercise that participants (other than opposing forces) were not authorized to plan, carry out or even request offensive cyber effects from member nations. This remains the situation in accordance with NATO Policy and will be the case until guidance to the contrary is promulgated. However, in a positive development during a session of a joint panel of cyberspace Subject Matter Experts (SMEs) from NATO HQ, the Cooperative Cyber Defence COE and ACT at the NATO School in

Oberammergau, Germany, on 21 March 17[44] it was stated that while NATO does not have OCO capabilities, a commander is not restrained from requesting offensive cyber effects. In fact, the panel suggested that exercise participants initiate requests for offensive cyber effects during NATO exercises, qualifying that there is currently no official mechanism for NATO to do this. A request was attempted in at least one large NATO exercise without success due to lack of approved policies and procedures. Still, this is a significant declaration that encourages development of OCO policy, doctrine and procedures. The lack of official direction and guidance supports what James A. Lewis observed, that 'procedures for integrating offensive cyber operations into NATO's defensive actions are not at all obvious, if they exist'.[45] This further demonstrates that the gap is not necessarily that NATO lacks the authority to exploit offensive cyberspace effects, rather it lacks the processes and/or procedures to obtain these effects from its member nations that it requires as part of its mission. It is important, therefore, to determine what NATO must do next, in this evolution, to be able to obtain these effects.

Most, if not all, nations regard their capabilities in OCO as highly classified and would restrict whether and how information about their capabilities is shared with NATO. However, this is not unique to offensive cyberspace capabilities; the answer may already be found in existing NATO processes and procedures. Procedures are already established, for example, for integrating nuclear weapons in NATO operations. Yet, 'the well-developed procedures for release and integration into NATO planning created for nuclear weapons do not exist for cyber'.[46] Nations tend to protect the capabilities of their Special Operations Forces (SOF) as well. The special capabilities of NATO's SOF remain classified and well protected, yet they can be called upon to provide highly specialized effects either to complete a mission independently or to support another operational domain in a joint/combined effort. Perhaps a solution may be found in some of the structures and processes employed by the intelligence community, through and within which is passed and filtered highly classified information among specialized, multinational personnel with requisite security clearances. It should be possible to establish a centre within which a similar function is performed for OCO. Regarding established processes for identifying and requesting resources from member nations at the strategic level, Step 7 of the NATO Operational Planning Process (OPP) calls for the preparation of Combined Joint Statement of Requirement (CJSOR) within which will include the 'capabilities required for the conduct and sustainment of joint actions'.[47] Once approved by the Joint Force Commander (JFC) they are forwarded to the Supreme Allied Commander Europe (SACEUR) for approval. When approved, the SACEUR will forward the CONOPs to the Military Committee (MC) and the provisional CSJOR to the nations through their National Military Representatives (NMR) at Supreme Headquarters Allied Powers Europe (SHAPE). This process allows nations to consider the CONOPS and the capabilities required for its implementation.[48] Similar solutions for obtaining cyber effects could be established in order to safeguard the classified capabilities of each nation while providing the offensive cyber assessment and/or capability required. With respect to incorporating OCO at the operational level, a solution may be found in options proposed for integrating cyberspace into the USAF Air Operations Centers (AOC).[49] In this model 'the AOC provides operational-level C2 of air, space and cyberspace operations, and is the focal point for planning, directing, and assessing air space and cyberspace operations to meet JFACC (Joint Force Air Component Commander)

44. Joint Panel of Cyber Subject Matter Experts (SMEs) from NATO HQ, CCD COE and Allied Command Transformation at the NATO Consultation Command and Control Course in the NATO School in Oberamergau, 21 Mar. 17.
45. Lewis, p. 2.
46. Ibid., p. 7.
47. NATO AJP-5 Allied Joint Doctrine for Operational Level Planning, p. 3–42.
48. Ibid., p. 3–46.
49. Rueter, Maj Bradley A. (USAF), ***Cyber Integration Within The Air Operations Center,*** May 2013, Graduate Research Project, Graduate School of Engineering and Management, Air Force Institute of Technology.

operational objectives and guidance'.[50] The AOC would be organized, trained and equipped to 'provide cyber planning and operation expertise in order to coordinate and synchronize cyberspace operations activities with other domains' and would 'ensure all cyber taskings are deconflicted, integrated and coordinated into the Air Tasking Order (ATO)'.[51] The Intelligence Section would work closely with the Strategy and Combat Plans Divisions to 'assess threats and enemy capabilities and process cyber-related targets'[52] and 'for targeting effects and master attack planning'.[53] To support the targeting cycle 'the goal would be to develop sets of weapons for preplanned types of operations, much the same as we currently understand and use for kinetic weapons … to derive effects-oriented, weapons-target pairings'.[54]

50. Rueter, Maj Bradley A.(USAF), ***Cyber Integration Within The Air Operations Center,*** May 2013, Graduate Research Project, Graduate School of Engineering and Management, Air Force Institute of Technology., p. 6.
51. Ibid., p. 14.
52. Ibid., p. 15.
53. Ibid., p. 30.
54. Leed, p. 5.

© Titima Ongkantong/shutterstock

NATO planners are very familiar with contributing member nations' capabilities and available resources in the traditional domains of maritime, land and air. This is presently not the case for offensive cyber capabilities. There is a general lack of knowledge of how offensive capabilities might benefit NATO during operations. NATO requires increased cyberspace SME participation (including Cyber Intelligence personnel for example) with the planners in traditional domains and to have the opportunity to explain how cyberspace can assist in achieving operational mission objectives. To successfully implement a mechanism to request cyber effects, NATO planners must have at least a general understanding of the offensive cyber capabilities of contributing nations. As Schmitt explains, it is 'prudent for those who plan, approve and execute military operations to have ready access to cyber expertise that apprise them of cyber options'.[55] Equally, the nation(s) contributing personnel skilled in OCO must be familiar with NATO doctrine, operational planning and ideally, the specific mission. Again, since the cyber capabilities are highly classified, it may mean that both the requests for effects and the corresponding responses must be filtered through an interface to ensure highly classified information is safeguarded.

What Next?

NATO must focus energies on bridging the gap in the cyberspace domain in order to be able to request the offensive cyber effects necessary to complete its mission, if not increase the number of personnel

55. Schmitt, p. 18.

trained in OCO as part of its organization. It is generally believed by those within the cyberspace field that there is a requirement to improve overall awareness of cyberspace among all personnel working outside the cyberspace domain. We need to determine the changes necessary in the organization and in the mission planning and execution processes and procedures. Allied Command Operations (ACO) Cyberspace Workshop has outlined a 'Roadmap' which includes laying out the initial steps required.[56] Initiating change in a large organization can be a challenge, particularly if consensus must be achieved among 29 nations. Until formal processes on how the incorporation of OCO effects into NATO missions are determined and published, further progress will be slow and NATO will continue to be disadvantaged compared to its opponents who are conducting OCO on a daily basis. It does not necessarily mean a significant increase in the number of cyberspace experts in the NATO establishment, but a modest increase is the minimum required to provide commanders with a sufficient number of SMEs for planning, to prevent the few existing SMEs from filling multiple roles during Exercises (e.g. as Opposing Forces and Exercise Control) and to ensure adequate representation at key cyberspace planning meetings and working groups. Furthermore, since nations tend to closely guard OCO capabilities, NATO Allies should explore providing Liaison Officers (LNOs) from OCO-capable nations who are able to plan, exercise and operate alongside NATO personnel in order to establish and refine the process of contributing offensive cyber effects to operations.

Conclusion

Cyber has become 'an indelible facet of contemporary warfare'.[57] Although NATO has made great strides in recent years adapting to the rapid change in cyberspace overall (particularly with respect to exploiting it), in protecting its own IT/CIS against cyber-attack and recognizing its influence in grand strategy, more work needs to be done to fully capitalize on cyberspace capabilities even for NATO to continue its role as a defensive Alliance. Experience and research have both demonstrated that the synergy of both offensive and defensive capabilities combined are, at the very least, more efficient and, more likely, critical to mission success. Offensive cyber capabilities can be extremely precise and, as long as the effects conform to the LOAC, there are no regulations prohibiting NATO commanders from integrating OCO into its operations through requesting cyber effects from member nations. The field of Joint Air Power is a particular benefactor where the effects of OCO can be applied to opponents' air mission systems, either independently or to provide an advantage in time and space in joint collaboration with the other domains. The challenge is to agree upon and exercise the processes and/or procedures required to link member nations' offensive cyber capabilities with NATO's operational planning and execution processes. 'NATO should be more explicit in how offensive cyber operations fit into its defensive and deterrent strategy' including 'how NATO members with offensive cyber capabilities would retain national control but make these capabilities available to NATO'.[58] The NATO CJSOR, the procedures under which the SOF and Intelligence communities operate and the proposal for integrating cyberspace into USAF Air Operations Centers offer some suggestions on how this can be accomplished. Furthermore, the process must include negotiations with those member nations possessing and developing offensive cyber capabilities, since a critical factor for success is the nations' willingness to share their capabilities with Alliance partners. The incorporation of OCO effects in NATO operations is imperative and, ultimately, inevitable and as cyberspace as a domain will continue to evolve rapidly it is, and will be, critical for NATO and its member nations to proceed promptly, particularly with respect to the projection of Joint Air Power.

56. The ACO Cyberspace Workshop has prepared a Roadmap outlining some initial steps.
57. Schmitt, p. 2.
58. Lewis, p. 12.

ANNEX A

References

1. Adee, Sally, 'The Hunt for the Kill Switch', *Spectrum Magazine,* May 2008. *http://online.qmags.com/IEEESM0508/,* accessed 28 Mar. 2017.

2. Boutilier, Alex, 'Canada developing arsenal of cyber-weapons' The Star, 16 Mar. 2017, https://www.thestar.com/news/canada/2017/03/16/canada-developing-arsenal-of-cyber-weapons.html, accessed 25 Apr. 2017.

3. Concept for the Joint Air Power Competence Centre (JAPCC) MOD Bonn, 31 Jul. 2003.

4. Defence Cyber Command (Netherlands) Web Page, https://www.defensie.nl/english/topics/cyber-security/cyber-command, accessed 10 Aug. 2017.

5. Defense Science Board, Department of Defense, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan. 2013.

6. Grindal, Karl, 'Operation BUCKSHOT YANKEE', from Healy, Jason, Editor, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Cyber Conflict Studies Association publication, 2013.

7. Harvey, Shaun, Group Captain RAF, 'Unglamorous Awakenings: How the UK Developed Its Approach to Cyber', from Healy, Jason, Editor, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Cyber Conflict Studies Association publication, 2013.

8. Joint Panel of Cyber Subject Matter Experts (SMEs) from NATO HQ, CCD COE and ACT at the NSO NATO Consultation Command and Control Course, 21 Mar. 17.

9. Binnendijk, Hans, 'The Role of NATO Joint Air Power in Deterrence and Collective Defence', Joint Air Power Competence Centre, *Joint Air Power Following the 2016 Warsaw Summit – Urgent Priorities,* Oct. 2017.

10. Hutchens, Michael E., Dries, William D., Perdew, Jason C., Bryant, Vincent D. and Moores, Kerry E., *Joint Concept for Access and Maneuver in the Global Commons – A New Joint Operational Concept,* Joint Force Quarterly, 84, 26 Jan. 2017.

11. Kalinyak, Rachael, 'New cyber command force launched in Germany', *Fifth Domain,* 4 Apr. 2017, http://fifthdomain.com/2017/04/04/new-cyber-command-force-launched-in-germany/, accessed 25 Apr. 2017.

12. Leed, Maren, *Offensive Cyber Capabilities at the Operational Level – The Way Ahead,* Sep. 2013, Center for Strategic and International Studies.

13. Lewis, James A. 'The Role of Offensive Cyber Operations in NATO's Collective Defence', Tallinn paper no. 8, 2015, *The Tallinn Papers.*

14. North Atlantic Treaty Organization, *AJP 3.20 Allied Joint Doctrine for Cyberspace Operations* (DRAFT), 15 Jan. 2017.

15. North Atlantic Treaty Organization, *AJP 5.0 Allied Joint Doctrine for Operational Level Planning,* 26 Jun. 2013.

16. North Atlantic Treaty Organization 'Cyber Defence' http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 20 Mar. 2017.

17. North Atlantic Treaty Organization, 'Warsaw Summit Communiqué' http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 15 Mar. 2017.

18. NATO Communications and Information Agency (NCIA), North Atlantic Treaty Organization http://www.nato.int/cps/en/natolive/topics_69332.htm, accessed 28 Mar. 2017.

19. NATO Standardization Office, Military Committee Joint Standardization Board, 'Doctrine Task (DT) for Allied Joint Doctrine for Cyberspace Operations – Allocation of Study Number and Detailed Tasking' (14 Jul. 2016).

20. Prague Summit Declaration, North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/official_texts_19552.htm, accessed 20 Mar. 2017.

21. Rueter, Maj Bradley A.(USAF), *Cyber Integration Within The Air Operations Center,* May 2013, Graduate Research Project, Graduate School of Engineering and Management, Air Force Institute of Technology.

22. Schmitt, Michael N. 'The Law of Cyber Targeting' Tallinn paper no. 7, 2015, *The Tallinn Papers.*

23. United States Air Force, Office of the Chief Scientist, *Cyber Vision 2025 – United States Air Force Cyberspace Science and Technology Vision,* 2012–2025, 13 Dec. 2012.

24. Ward, Carol, 'Israel's Cyber Shot at Syria' DefenseTech, 26 Nov. 2007, https://www.defensetech.org/2007/11/26/israels-cyber-shot-at-syria/, accessed 27 Mar. 2017.

ANNEX B

Acronyms and Abbreviations

ACCS	Air Command and Control System
ACO	Allied Command Operations
AJOD WG	Allied Joint Operational Doctrine Working Group
AJP	Allied Joint Publication
AOC	Air Operations Centre
ATO	Air Tasking Order
AWACS	Airborne Warning and Control System
A2/AD	Anti-Access/Area Denial
BMD	Ballistic Missile Defence
CCD	Cooperative Cyber Defence
CERT-EU	Computer Emergency Response Team of the European Union
CIS	Communication and Information Systems
CJSOR	Combined Joint Statement of Requirement
COE	Centre of Excellence
COPP	Combined Operational Planning Process
C2	Command and Control
DCO	Defensive Cyberspace Operations
DoD	Department of Defense (USA)
EW	Electronic Warfare
FMN	Federated Mission Network
HOSG	Heads of State and Government
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology
JAPCC	Joint Air Power Competence Centre
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JWICS	Joint Worldwide Intelligence Communications System
LNO	Liaison Officer
LOAC	Law of Armed Conflict
MCJSB	Military Committee Joint Standardization Board
NACMA	NATO ACCS Management Agency
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCSA	NATO CIS Services Agency

NC3A	NATO Consultation, Command and Control Agency
NDPP	NATO Defence Planning Process
NMR	National Military Representative
NSA	National Security Agency (USA)
OCO	Offensive Cyberspace Operations
OPP	Operational Planning Process
RAF	Royal Air Force (UK)
SACEUR	Supreme Allied Commander Europe
SEAD	Suppression of Enemy Air Defence
SHAPE	Supreme Headquarters Allied Powers Europe
SME	Subject Matter Expert
SOF	Special Operations Force
UK	United Kingdom
US	United States (of America)
USAF	United States Air Force

Paul J. MacKenzie
Lieutenant Colonel (RCAF), NATO OF-4
C4ISR & Space Branch
Cyber Subject Matter Expert

ANNEX C

About the Author

Lieutenant Colonel (RCAF)
Paul J. MacKenzie CD, MSM (US)

A Communications and Electronics Engineering (Air) Officer in the Royal Canadian Air Force, he is the Cyberspace SME at the NATO Joint Air Power Competence Centre. He holds a Master's of Science degree in Computer and Information Systems (System Engineering) and has over 28 years of experience in the provision of IT/CIS support to operations, primarily in the air environment and from the tactical through to strategic levels. A graduate of the CF Joint Command and Staff Program his senior appointments include Director of Operational Support (CIS) – Canadian Operational Support Command (Ottawa), Chief of the A6 Staff – NATO Airborne Warning and Control Airbase (Geilenkirchen), Commanding Officer, Canadian Contingent (Technical Element) NATO Airborne Early Warning and Control Force (Geilenkirchen) and Director of the A6 Staff – 1 Canadian Air Division (Winnipeg). His Cyberspace specific studies include Cyber Warrior, Network Enabled Operations and Cyber at the Operational Level and he recently served as the Deputy Chair of the RCAF Cyber Functional Integration Team and Chief OPFOR (Cyberspace) for Exercise Trident Javelin 2017.

Notes

Joint Air Power Competence Centre

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