TO TELL THE STORY RIGHT

Major Liene Karale

JCSP 45	PCEMI 45
Exercise *Solo Flight*	**Exercice *Solo Flight***
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.
© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2019.	© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2019.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

TO TELL THE STORY RIGHT

Major Liene Karale

Word Count: 5062

Nombre de mots: 5062

TO TELL THE STORY RIGHT

INTRODUCTION

> *The role of information in our security has never been more important than now and the challenges to NATO [the North Atlantic Treaty Organization] and its values are crystal clear. We have a big job, but in the end, we will succeed because our story – the NATO story – is better. We just need to tell it right. We are all communicators now.[1]*

> - Mark Laity, *NATO and Strategic Communications: The Story So Far*

For more than a decade, the North Atlantic Treaty Organization (NATO) has been struggling to win hearts and minds due to the organization's traditional role as a hard power tool of Alliance member states where information played mostly a supplementary role to military attributes.[2] Rapidly evolving warfare has caused information to become a central domain for winning not only support of people, but also battles and eventually wars.[3] NATO is challenged to address these emerging components and layers of warfare.[4] NATO's struggle in Afghanistan to communicate with local populations and win support for NATO activities has raised the need to address the organization's communication shortfalls and initiate the development of a strategic communication (StratCom) concept within the Alliance.[5]

Nevertheless, the development process has been too slow. The weaknesses of NATO StratCom capabilities and insufficient efforts of the Alliance's member states to

---

[1] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, The Three Swords, Iss.33, Stavanger: Norway, March 2018), 73.

[2] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 1; Aigerim Raimzhanova, "Power in IR: Hard, Soft and Smart," (Institute for cultural Diplomacy and the University of Bucharest, Bucharest: Rumania, 2015), 6; Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, The Three Swords, Iss.33, Stavanger: Norway, March 2018), 73;David Loyn, "We Have Met the Enemy And He Is Us," (NATO Strategic Communications Centre of Excellence, Defence Strategic Communications, Volume 3, Riga: Latvia, 2017), 208.

[3] David Loyn, "We Have Met the Enemy And He Is Us," (NATO Strategic Communications Centre of Excellence, Defence Strategic Communications, Volume 3, Riga: Latvia, 2017), 208.

[4] *Ibid.*

[5] *Ibid.*

contribute to its development were exposed in 2014, when Russia launched a well-orchestrated hybrid warfare against Ukraine and illegally annexed Crimea.[6] Russia's capacity to use information to construct *a fog of war* by spreading disinformation, lies, false narratives and images highlighted the gaps NATO still had in StratCom capabilities.[7] NATO's failure in Afghanistan and Russia's effectiveness in information activities accelerated the development of NATO's StratCom capabilities.[8] However, the question remains whether these capabilities are sufficient to meet hybrid threats and whether NATO has enough StratCom expertise and skills to communicate strategically.[9]

This paper's supporting evidence will argue that dissonance amongst NATO member states in their understanding of the StratCom concept, insufficient contribution and alignment of member states to development of StratCom capabilities and StratCom narratives, pose a critical challenge to the achievement of joint NATO aims in effectively countering current threats. Firstly, this paper will demonstrate the main aspects of current hybrid threats to NATO and the importance of understanding the Information Environment (IE), understanding the critical challenges for NATO in IE, and key implications when dealing with hybrid threats. This paper will then analyze current NATO StratCom capabilities and its evolvement over time, as well as the main shortfalls

---

[6] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 1; Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 68.

[7] World Heritage Encyclopedia, Last access to the webpage 19 April 2019, http://self.gutenberg.org/articles/Fog_of_war; Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 68.

[8] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 1.

[9] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 73.

that limit NATO's ability to respond to current and future threats rapidly. Finally, it will analyse the importance of cohesion amongst NATO nations when conducting strategic communication.

HYBRID THREATS

Russia's activities in Ukraine facilitated the re-birth of the term *hybrid warfare*.[10] Experts emphasize that hybrid warfare as a term is nothing new and was observed during the second Lebanon War in 2006, when Israel encountered both hybrid and conventional warfare successfully executed by Hezbollah.[11] As a result, Hezbollah undermined Israel's ability to win the war despite Israel's conventional superiority.[12] However, Russia has elevated an understanding of hybrid warfare to a new level. As described by Mark Laity, Director of the Communications Division for Supreme Headquarters Allied Powers Europe (HQ SHAPE), Russia's ability to participate in modern conflicts was quite limited after the Soviet Union's disintegration.[13] Russia's actions in Ukraine has proven country's ability to synchronize its political, strategic and operational level assets as well as rhetoric's and lies told by President Putin himself.[14] Russia's ability to employ different realms of hybrid warfare proved to be sufficient to not only surprise the world, but also to have Russia emerge as the mastermind of hybrid war.[15]

---

[10] Thomas Michael Jopling, "Countering Russia's Hybrid Threats: An Update," (Draft Special Report, NATO Parliamentary Assembly, Committee on the Civil Dimension of Security, Brussels: Belgium, 27 March 2019), 1.

[11] Julio Miranda Calha, "Hybrid Warfare: NATO's New Strategic Challenge?" (General Report, NATO Parliamentary Assembly, Defence and Security Committee, Brussels: Belgium, 10 October 2015), 2 - 3.

[12] *Ibid.*

[13] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 68.

[14] *Ibid.*, 69.

[15] *Ibid*.

There is yet to be a universal agreement regarding the definition of the terms

hybrid warfare or *hybrid threat.*[16] However, the latest NATO definition of a hybrid threat

is "a type of threat that combines conventional, irregular and asymmetric activities in

time and space."[17] Nonetheless, in 2015 NATO agreed that hybrid warfare was an ability

to "exploit domestic weaknesses via non-military means (such as political, informational,

and economic intimidation and manipulation), but is backed by the threat of conventional

and unconventional military means."[18] Meanwhile, the NATO Strategic Communications

Centre of Excellence (NATO StratCom COE) highlighted that it was essential to focus on

the term hybrid rather than terms threat or warfare due to the fact that the term hybrid

essentially explains the changing nature of either threats or warfare.[19] In their report, the

term hybrid "…describes [usage of] a wide array of measures, means and techniques."[20]

Also, COE explains that some, but not all, of the hybrid attributes, are:

> …disinformation; cyber-attacks; facilitated migration; espionage;
> manipulation of international law; threats of force (by both irregular armed
> groups and conventional forces); political subversion; sabotage; terrorism;
> economic pressure and energy dependency.[21]

In addition, hybrid threats include the ability not only to influence political

leaders of targeted countries, but also to interact with vital Non-Governmental

Organizations (NGOs) within the state, i.e. Latvian Human Rights Committee, which "is

---

[16] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 8.

[17] NATO Standardization Office (NSO), "NATO Glossary of Terms and Definitions," (APP-6, 2018 Edition, Brussels: Belgium, 2018), 62.

[18] Julio Miranda Calha, "Hybrid Warfare: NATO's New Strategic Challenge?" (General Report, NATO Parliamentary Assembly, Defence and Security Committee, Brussels: Belgium, 10 October 2015), 1.

[19] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 8.

[20] *Ibid.*

[21] *Ibid.*

one of more than 40 Russian-financed NGOs in the Baltic states,"[22] thus shifting and changing their behaviour and attitude towards the targeted country or organization.[23] Therefore, hybrid threat activities can be assumed "as information or influence activities."[24] Indeed, Russia is extensively using so-called web brigades and specifically hired people to comment and express opinions favourable to Russia on issues it is interested in.[25] For instance, in 2015 approximately 20,500 Twitter accounts were used to influence opinions.[26] A large number of the accounts were robotic accounts operated by troll-factories.[27] Moreover, "such activities are not limited to the "Information" instrument but involve the combination of different instruments of power, including Diplomatic, Economic and Military."[28] A Swedish Defence University experts also emphasized that building a definition of hybrid warfare based only on Russia's example regarding the Ukraine may limit our understanding of hybrid threats and hybrid warfare's adaptive nature.[29] Instead, experts suggest exploring the activities of hybrid threats, which are:

> …coordinated and synchronised across wide range of means,
> deliberately target democratic states' and institutions' systemic

---

[22] Alexandra Jolkina and Markian Ostaptschuk, "Activists or Kremlin agents - who protects Russian-speakers in the Baltics?" Last access to webpage 02 May 2019, https://www.dw.com/en/activists-or-kremlin-agents-who-protects-russian-speakers-in-the-baltics/a-18903695.

[23] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 9.

[24] *Ibid.*

[25] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 3; NATO Strategic communication Centre of Excellence, "Robottrolling," (Issue 1, Riga: Latvia, 2019), 1.

[26] *Ibid.*

[27] *Ibid.*

[28] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 9.

[29] Gregory F. Traverton *et al*, "Addressing Hybrid Threats," (Swedish Defence University, Center for Asymmetric Threats Studies, Hybrid CoE, 2018), 10.

vulnerabilities, use of wide range of means, exploit the threshold of detection and attribution as well as the border between war and peace, aim to influence different forms of decision-making at the local (regional), state, or institutional level, favour and/or gain the agent's strategic goals while undermining and/or hurting the target.[30]

In analysing hybrid threats or warfare from the NATO perspective, Russia defines NATO as a primary threat to its security. In 2000 Russia issued its National Security Concept where they emphasized that the national security threats to Russia were "…strengthening of military-political blocs and alliances [and] above all NATO's eastward expansion"[31] and the "…possible appearance of foreign military bases and large troop contingents in direct proximity to Russia's borders."[32] Therefore, understanding Russia's hybrid activities is crucial to analyse current NATO StratCom capabilities. Moreover, Russia may not have displayed all of its capabilities when invading Ukraine and Russia is continuously expanding its borders in terms of its ability to influence the global security arena.[33]

Dr. Damien Van Puyvelde argues that it is not necessary to single out hybrid warfare, but instead warfare as a whole should be addressed as "a complex set of

---

[30] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 8; Gregory F. Traverton *et al*, "Addressing Hybrid Threats," (Swedish Defence University, Center for Asymmetric Threats Studies, Hybrid CoE, 2018), 10.

[31] The Russian Federation, the Ministry of Foreign Affairs of the Russian Federation, "National Security Concept of the Russian Federation," Last access to the webpage 21 April 2019, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768, 7.

[32] *Ibid.*

[33] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 70-72.

interconnected threats and forceful means waged to further political motives."[34] Dr. Damien Van Puyvelde expands his opinion by explaining:

> …that, in practice, any threat can be hybrid as long as it is not limited to a single form and dimension of warfare. When any threat or use of force is defined as hybrid, the term loses its value and causes confusion instead of clarifying the "reality" of modern warfare.[35]

He suggests that the majority of conflicts, including ancient ones, were always utilizing asymmetric approaches to overcome opponents by exploiting weaknesses and vulnerabilities through the employment of conventional or unconventional ways and means.[36] Dr. Damien Van Puyvelde reinforces his statement with the idea that "warfare, whether it be ancient or modern, hybrid or not, is always complex and can hardly be subsumed into a single adjective."[37]

Valery Gerasimov, the General of the Russian Army, also argues that "using the phrase "hybrid warfare" as an established term is, at present, premature."[38] He explains that "the flip side of "hybrid operations" is a new perception of peacetime, when military or other overt violent measures are not used against some states, but its national security and sovereignty are threatened and may be violated."[39]

Despite the differences in opinions about hybrid warfare and what hybrid warfare means for modern warfare, it is clear that both terms highlight the difficulties and challenges of current threats. NATO StratCom CoE researchers highlighted "the effects

---

[34] Damien Van Puyvelde, "Hybrid War – does it even exist?" Last access to the webpage 21 April 2019, https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm.

[35] *Ibid.*

[36] *Ibid*.

[37] *Ibid.*

[38] Valery Gerasimov, "Contemporary Warfare and Current Issues for the Defense of the Country," Last access to the webpage 21 April 2019, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/Contemporary-Warfare-and-Current-Issues-for-the-Defense-of-the-Country/.

[39] *Ibid.*

the information can cause to the development of the conflict, as audience perception of the outcome of the conflict matters more than the actual facts on the ground"[40] as being what makes a huge difference in modern warfare.[41] Current social media networks and platforms provide the ability to transcend geographical borders and not only observe but also participate in the conflict in real time, thus elevating the importance of dominance in the ability to shape peoples' opinions and change their actions.[42] Also, Professor David Stupples argues that "information warfare combines electronic warfare, cyber warfare and psy-ops (psychological operations) into a single fighting organization and this will be central to all warfare in the future."[43] Notwithstanding other aspects of hybrid threats, this paper will continue to focus on the Information domain and more specifically on IE to analyze NATO StratCom capabilities.

INFORMATION ENVIRONMENT

Russia's hybrid activities examples emphasize the importance of the information domain in achieving tactical objectives. As a result, it is essential to understand what IE is and how influence in IE enables the ability to spread and communicate hybrid threats. The "NATO Strategic Communication Handbook" defines IE as "the virtual space and physical space, in which information is received, processed and conveyed; it consists of actors, the information itself and information systems."[44] NATO StratCom CoE provides a more specific explanation of IE where the "Information Environment is a model for

---

[40] NATO Strategic Communication Centre of Excellence, "Social Media as a Tool of Hybrid Warfare," (ISBN 978-9934-8582-6-0, Riga: Latvia, May 2016), 10.

[41] *Ibid.*

[42] *Ibid.*

[43] David Stupples, "Are we prepared for information warfare?" (City, University of London, London: UK, 30 November 2015), 2; NATO Strategic Communication Centre of Excellence, "Social Media as a Tool of Hybrid Warfare," (ISBN 978-9934-8582-6-0, Riga: Latvia, May 2016), 10.

[44] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 4.

understanding how actors and audiences interact, how people see the world around them and consequently make decision based on the meaning they deduce from it."[45] In COE understanding, IE consists of three interconnected layers: "cognitive (where people think, understand and decide); physical (individuals, organizations and infrastructure) and informational (facts, knowledge and data)."[46] Experts of COE also believe that actors through the IE are specifically influencing the cognitive layer, where information as an "enabler to national power" and "the ability to influence audiences comes from the synergy of national instruments, including diplomatic, informational, military and economic measures."[47]

The "NATO Strategic Communication Handbook" mentions the same approach where "the IE itself is where humans and automated systems observe, orient, decide and act upon information and is, therefore, the principle environment of opinion building and decision-building."[48] Therefore, both sources emphasize the importance of not only understanding the information domain through detailed analysis, but also understanding that information itself has an enormous influence on the decision-making process of the target audience.[49]

A deep understanding of IE anatomy can inform how hybrid threats tend to identify and target vulnerabilities of target audiences exclusively.[50] Therefore belligerent

---

[45] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 9.

[46] *Ibid.*

[47] *Ibid.*

[48] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 4.

[49] *Ibid.*; NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 9.

[50] *Ibid.*

actors, through an array of hostile activities, conduct influence activities towards identified vulnerabilities of the target audience.[51] These hostile activities can be used based on the political, military, economic, social, information, and infrastructure (PMESII) realms.[52] For instance, in 2014 Russia flooded the internet with disinformation about their military activities in Ukraine and Crimea, affecting and to some extent paralyzing the decision-making process of the West and delaying its reaction towards Russia, until Russia had established full control over Crimea.[53] This example demonstrates that a detailed analysis and understanding of IE is paramount to success for all actors, whether hostile or friendly, in order to address hybrid threats properly. It is worth recognizing that the IE is not only complicated but that it also transcends borders, creating an opportunity to influence states across the globe. Besides, as identified in the "NATO Strategic Communication Handbook" an "understanding of IE is a fundamental component for operational planning, and is particularly important for effective StratCom."[54]

SLOW START

In 2001, the term "strategic communication" emerged in a research paper called the "Report of the Defence Science Board Task Force on Managed Information Dissemination."[55] In this particular paper, experts used the term to explain that

---

[51] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 9.

[52] *Ibid.*

[53] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 69.

[54] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 4.

[55] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?" (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 1; The

"sophisticated strategic communications can set the agenda and create a context that

enhances the achievement of political, economic, and military objectives."[56] However,

David Loyn argues that two main cornerstones of StratCom, i.e. Information Operations

(IO) and Public Affairs (PA), were known more than 150 years ago, when Sir Robert

Sandeman identified the importance of gaining the population of British India's support

by winning their *hearts and minds* rather than applying coercive methods to achieve its

goals.[57] The same concept of winning hearts and minds gained traction in the Vietnam

War and re-emerged in Iraq and Afghanistan wars that followed to 9/11 events.[58]

Despite the rapid development of the information domain, only lessons learned in

Afghanistan enabled the creation of the StratCom cell in HQ SHAPE in 2007.[59] NATO

also facilitated the agreement amongst its member nations to issue the NATO Strategic

Communication Strategy in 2009, thus starting the long and mostly steep road towards

creating a NATO-wide understanding of what StratCom is and what it can offer to the

Alliance.[60]

In 2009 NATO agreed to the following definition for NATO StratCom:

The coordinated and appropriate use of NATO communications activities
and capabilities – Public Diplomacy (PD), Public Affairs (PA), Military
Public Affairs [MPA], Information Operations (Info Ops) and
Psychological Operations (PSYOPS), as appropriate - in support of

---

Defence Science Board, "Report of the Defence Science Board Task Force on Managed Information Dissemination," (Washington, D.C.: USA, October 2001), 1.

[56] *Ibid.*

[57] David Loyn, "We Have Met the Enemy And He Is Us," (NATO Strategic Communications Centre of Excellence, Defence Strategic Communications, Volume 3, Riga: Latvia, 2017), 208.

[58] *Ibid.*

[59] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 2.

[60] *Ibid.*; David Loyn, "We Have Met the Enemy And He Is Us," (NATO Strategic Communications Centre of Excellence, Defence Strategic Communications, Volume 3, Riga: Latvia, 2017), 208.

Alliance policies, operations and activities, and in order to advance NATO's aims.[61]

The broad nature of the provided definition has caused critics to question its meaning. Steve Tatham provides a better definition in his work "Strategic Communications: A Primer."[62] According to Tatham, StratCom is "A systematic series of sustained and coherent activities, conducted across strategic, operational and tactical levels, that enables understanding of target audiences and, identifies effective conduits to promote and sustain particular types of behaviour."[63] Professors Julian Lyndley-French and Dr. Paul Cornish also refer to Tatham's definition, believing that it better describes the purpose of StratCom.[64]

The argument requesting a different formulation of StratCom lies in the fact that the NATO definition does not provide clear guidance as to whether StratCom belongs at the strategic or operational, thus creating confusion in its interpretation.[65] For instance, Steve Tatham and Rita Le Page highlight that "many members nations define Strategic Communication as a military function, whilst others talk about Strategic Communication as being part of the national instrument of power – and therefore a cross-government

---

[61] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 6; North Atlantic Treaty Organization, "NATO Strategic Communication Policy," (PO (2009) 0141, Brussels: Belgium, 29 September 2009), 1.

[62] Steve Tatham, "Strategic Communications: A Primer," (ARAG Special Series 8/28, Defence Academy of the United Kingdom, London: UK, December 2008), 3.

[63] Paul Cornish, Julian Lindley-French, and Claire Yorke, "Strategic Communications and National Strategy," (A Chatham House Report, The Royal Institute of International Affairs, London: UK, September, 2011), 4; Steve Tatham, "Strategic Communications: A Primer," (ARAG Special Series 8/28, Defence Academy of the United Kingdom, London: UK, December 2008), 3; Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?", (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 3.

[64] Paul Cornish, Julian Lindley-French, and Claire Yorke, "Strategic Communications and National Strategy," (A Chatham House Report, The Royal Institute of International Affairs, London: UK, September, 2011), 4.

[65] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?", (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 2.

activity."[66] Such confusion in interpretation is mostly due to the lack of a NATO policy

and doctrine that would otherwise provide a more-in-depth explanation of the essence of

StratCom.[67] As a result, dissonance in understanding what is meant by StratCom has

impeded NATO's ability to implement StratCom policy more rapidly despite its efforts to

build its StratCom capabilities.[68]

In 2010 NATO issued its "Military Concept for NATO Strategic

Communications" wherein it identified that effects of StratCom would be gained over the

time as the mindsets of nations adapted to recognize what StratCom has to offer.[69]

Nevertheless, NATO understood that StratCom required the creation of:

> …a strong, professional force of information practitioners, able to
> deal with the challenges of the global communications environment, and
> to proactively tell and explain the NATO story to the widest possible
> audiences, building understanding and support for the Alliance.[70]

The invasion of Ukraine "forced NATO to swiftly respond to new reality."[71]

Besides other assurance measures included in the NATO Readiness Action Plan, NATO

welcomed the foundation of the NATO StratCom CoE in Latvia during the Wales

Summit and re-enforced the importance of enhancing StratCom capabilities to address

hybrid threats properly.[72] In July 2014 seven NATO Nations – Latvia, Lithuania, Estonia,

---

[66] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?" (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 2.

[67] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 66.

[68] *Ibid.*

[69] *Ibid.*; North Atlantic Treaty Organization, "Military Concept for NATO Strategic Communications," (MCM-0085-2010, Brussels: Belgium, Augusts 2010), 2.

[70] *Ibid.*

[71] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 2.

[72] North Atlantic Treaty Organization, "Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, issued in 5 September 2014," Last updated 30 August 2018, https://www.nato.int/cps/en/natohq/official_texts_112964.htm#rap.

Germany, Poland, Italy and United Kingdom (UK) –agreed to establish the NATO

StratCom COE and two months later received accreditation, and became a part of

NATO's Force Structure.[73] NATO agreed that "the Mission of the centre is to provide a

tangible contribution to the strategic communications capabilities of NATO, NATO allies

and NATO partners."[74] And that the purpose of the centre was "to contribute to improved

strategic communications capabilities within the Alliance and Allied nations."[75]

To achieve its contribution to the advancement of NATO StratCom capabilities,

the NATO StratCom CoE served "to improve NATO's communication process by

providing comprehensive analyses, timely advice and practical support to the Alliance."[76]

StratCom COE did not let NATO down and shortly after its establishment the first

products of NATO StratCom CoE were seen to provide insight to member countries of

NATO StratCom's actual status.[77]

In the first half of 2015, the COE conducted a study intending to understand "the

key characteristics of StratCom capacity and capability in the defence sectors of

NATO."[78] The design of the research included questionnaires and in-depth interviews.[79]

The results were alarming in several aspects. One of the aspects was participation, where

---

[73] NATO Strategic Communications Centre of Excellence, "About Us," Last access to the webpage in 23 April 2018, https://www.stratcomcoe.org/about-us.
[74] *Ibid.*
[75] *Ibid*.
[76] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 3.
[77] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 3; Gerry Osborne, NATO Strategic Communications Centre of Excellence, "Mapping of StratCom Practices in the NATO Countries," (Riga: Latvia, 2015), 5.
[78] *Ibid*.
[79] *Ibid*., 12.

only 11 of 28 nations responded.[80] Just one year after Russia's extensive use of

information operations, 17 nations did not use the chance to participate in the survey, thus

undermining not only the results of the study but also demonstrating the lack of

understanding of the importance of StratCom capabilities in NATO.[81]

Another discovery was how NATO member nations perceived and understood the

concept of StratCom. StratCom CoE experts emphasize that, to achieve effectiveness,

StratCom should be implemented as a baseline principle throughout different levels of

comprehensive approaches in order to create an understanding across the governmental

organizations and that StratCom is also a mindset "which is an appreciation that

everything – worlds, actions, images, policies –communicate."[82] Meanwhile, the NATO

definition to some extents contradicts the idea of a mindset defining StratCom as a

supporting discipline rather than an inherent part of NATO's activities. This statement is

re-enforced by the outcome of the study where "the majority of nations described

StratCom as a supporting rather than supported role at both political and military level."[83]

Nevertheless, some respondents acknowledged the need to change such an approach.[84]

Authors of the policy paper "NATO Strategic communications: More to be Done?"

support the opinion "that StratCom is not an adjunct function but integral to the planning

and conduct of all military operations and activities."[85] Furthermore, they considered

---

[80] Gerry Osborne, NATO Strategic Communications Centre of Excellence, "Mapping of StratCom Practices in the NATO Countries," (Riga: Latvia, 2015), 2.

[81] *Ibid.*

[82] NATO Strategic Communications Centre of Excellence, "Hybrid Threats: A Strategic Communication Perspective," Last access to the webpage 20 April 2019, https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective, 10.

[83] Gerry Osborne, NATO Strategic Communications Centre of Excellence, "Mapping of StratCom Practices in the NATO Countries," (Riga: Latvia, 2015), 20.

[84] *Ibid*.

[85] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?", (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 5.

examples of the UK's activities in Sierra Leone in 2000 and Afghanistan in 2007 where UK military forces mostly used "soft power assets – PsyOps, Media Ops, and Deception – with Hard Power very much a secondary, supporting pillar."[86]Another point was exposed when states were asked to describe their contribution in each of the key StratCom disciplines in their political and military structures. The results showed that states mostly contributed to the realms of PD and PA, including MPA, leaving other disciplines behind.[87] Results thus raise concern that states perceive StratCom as part of information management rather than as a strategy.[88]

Experts of COE also argue that there is a huge tendency to tie StratCom to PA rather than to operations and that the current NATO StratCom structure is contributing to that fact.[89] As defined in the "NATO Strategic Communication Handbook," the Assistant Secretary-General for Public Diplomacy Department (ASG PDD) holds overarching "responsibility for StratCom on behalf of [the] Secretary General" and "oversees the coordination of all StratCom activities across all NATO."[90] Meanwhile, authors of "NATO Strategic Communication: More to Be Done?" suggest that NATO should follow the UK example where StratCom planning, as part of the UK's Ministry of Defence Operations Directorate, is embedded at the operational side of the house within the

---

[86] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?", (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 5.

[87] Gerry Osborne, NATO Strategic Communications Centre of Excellence, "Mapping of StratCom Practices in the NATO Countries," (Riga: Latvia, 2015), 22 -23.

[88] *Ibid.*, 28.

[89] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?", (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 4; Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 4.

[90] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 12.

International Military Staff where strategy should belong.[91] Moreover, some StratCom practitioners think that attempts to associate StratCom with PA and the wrongful placement of StratCom within NATO's structure demonstrates that NATO "has failed to grasp the importance of this instrument and explains why military commanders in most NATO nations remain unaware of its power to affect the operational environment."[92]

Another interesting conclusion of the COE study "Mapping of StratCom Practices in the NATO Countries," was related to the various training activities each state attends during the calendar year.[93] Although NATO countries mostly contribute to PD and PA domains of StratCom, Figure 1 below demonstrates that PD and PA are the least trained domains. COE explains these results by comparing the differences between military and civilian training, where militaries tend to have more formalized training processes.[94] Nevertheless, COE could not find any evidence of PD training for military personnel, thus raising questions as to whether there exists a sufficient understanding of StratCom within the military and PD as its discipline in accordance with NATO definition.[95]

---

[91] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?", (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 4.

[92] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 4.

[93] Gerry Osborne, NATO Strategic Communications Centre of Excellence, "Mapping of StratCom Practices in the NATO Countries," (Riga: Latvia, 2015), 24.

[94] *Ibid*., 24-25.

[95] *Ibid*.

Discipline	Total Training Activity (Courses delivered / year)
MPA	33
Info Ops	17
PSYOPS	11
StratCom (General)	8
PD	0
PA	0

Figure 1 – Number of Training Courses Nation's attend in Calendar Year

Source: Osborne, *Mapping of StratCom Practices in the NATO Countries*, 24

Indeed, lack of training was and still is a big issue among StratCom practitioners. Mark Laity, a StratCom expert, explains that NATO often suffers from staff rotations that impede the effectiveness of the organization due to the differences in training or understanding between member states, as well as an overall eagerness of member states to interact within communications disciplines.[96] Moreover, often on the job training was the only training people in key positions received.[97] Unfortunately, this situation has yet to be properly addressed. For instance, "Food for Thought: Paper on NATO Public Affairs Training" issued in 2018 as a result of the NATO Public Affairs Working Group identified the same problem, stating that "in many cases, nations risk sending personnel into high-profile, high-pressure PAO staff positions with limited or even no training and/or experience."[98]

Despite criticisms of StratCom that outline its slow development in terms of policy, doctrine and training, there are several significant improvements within NATO regarding the organization. First and foremost is the establishment of NATO StratCom

---

[96] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 66 - 67.

[97] *Ibid*.

[98] North Atlantic Treaty Organization, "Food for Thought: Paper on NATO Military Public Affairs Training," (1710/TSC-GSU-0300/TT-0161/Ser: 469, Brussels: Belgium, 30 August 2018), A-1.

COE, which since its beginning has supported the development of policy and doctrine, conducted extensive research on the information campaigns of potential adversaries and identified the gaps within the StratCom capabilities of NATO.[99] Also, the "NATO Strategic Communication Handbook" identified that countries should recognize and implement the need to incorporate "communication into operational planning"[100] and "increase volume, pace, capacity, and coherence in NATO communication process."[101] The author of "The Continuing Evolution of Strategic Communications within NATO" also emphasized that the issuance of the "NATO Strategic Communication Handbook," which provides a better insight into the relevance of StratCom, and the establishment of NATO StratCom CoE were the right measures taken to continue the development of NATO's StratCom capabilities.[102] The author of "Strategic Communications: A Caution to Military Commanders" suggests that, in terms of StratCom capabilities, NATO is currently "building a roof without the underlying walls and foundation."[103] He referred that statement to the fact that NATO needs to step up and take a serious position when it comes to developing and maintaining a "robust information capacity."[104] Indeed, incoherent perceptions of StratCom as a concept, slow development of its capability, and an absence of doctrine and proper training leaves NATO's approach wanting in terms of

---

[99] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 3.

[100] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 5.

[101] *Ibid*.

[102] Daniel Gage, "The Continuing Evolution of Strategic Communications within NATO," ((The Magazine of Joint Warfare Centre, the Three Swords, Iss.27, Stavanger: Norway, 2014), 53.

[103] J.D. Scanlon, "Strategic Communications: A Caution to Military Commanders," (Army University Press, Military Review, Fort Leavenworth, Kansas: USA, 3 November 2017), 2.

[104] *Ibid*.

robustness, particularly when comparing NATO's abilities to the on-going information warfare waged by Russia.

NARRATIVE

In 2017, General Gerasimov pointed out that "achieving information dominance is an indispensable pre-requisite of combat actions."[105] Russia has been using such an approach to information since 2012, when they recognized its importance and placed it amongst the pre-existing tools, for example political, economic and military, pivotal for the defence of Russia.[106] The importance of information dominance has not diminished over the years. Instead, its importance has grown and examples of Russia's counter-NATO and EU propaganda activities in Sweden or Russia's alleged interference with Catalonian independence in 2017 have proven that information will continue to be an integral part of future warfare as well.[107] Both examples indicate that Russia is adept at utilizing "the psychological aspect of information confrontation [which] targets the very foundation of a society, both its domestic and military populations."[108] Russia utilizes information operations by focusing "on undermining the targeted state's institutions and belief systems"[109] thus influencing "a targeted country's domestic opinions on particular subjects [to] increase that country's societal divisions."[110] Russia has used such an approach against NATO.

---

[105] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 70.

[106] Jeff Edmonds and Samuel Bendett, "Russian Battlefield Awareness and Information Dominance: Improved Capabilities and Future Challenges," Last access to the webpage 27 April 2019, https://www.realcleardefense.com/articles/2019/02/26/russian_battlefield_awareness_and_information_do minance_improved_capabilities_and_future_challenges_114218.html.

[107] *Ibid*.

[108] *Ibid*.

[109] *Ibid.*

[110] Jeff Edmonds and Samuel Bendett, "Russian Battlefield Awareness and Information Dominance: Improved Capabilities and Future Challenges," Last access to the webpage 27 April 2019,

NATO's internal consistency and cohesion are core principles for StratCom as well, therefore "NATO operations and communication need to be perceived as one voice."[111] NATO defines strategic narrative as:

> A concise but comprehensive written statement of an organization's situation and purpose, which can stand on its own as the principle context to strategic planning directives or be used to support the creation of individual culturally attuned stories that will resonate with particular audiences and foster cohesion within the organization.[112]

NATO doctrine also emphasizes that "the NATO strategic Narrative should drive the overall NATO Strategy [and] Narratives provide a tool to align words and deeds."[113] Besides, J.D. Scanlon, the author of the article "Strategic Communication: A Caution to Military Commanders" points out that "ideally, an SC [StratCom] narrative would be at once truthful and influential, and would build support amongst NATO publics and other audiences for Alliance missions."[114] Meanwhile, member states would develop their country's narratives "from the agreed NATO metanarrative, ensuring repetition and coherence across the Alliance."[115] Unfortunately, this is often not the case for NATO as, due to the internal political situations of various alliance members, some nations might not support the overarching NATO narrative as agreed within the NAC. Moreover, some

https://www.realcleardefense.com/articles/2019/02/26/russian_battlefield_awareness_and_information_dominance_improved_capabilities_and_future_challenges_114218.html.

[111] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 10.

[112] *Ibid.*, 9.

[113] *Ibid.,* 28.

[114] J.D. Scanlon, "Strategic Communications: A Caution to Military Commanders," (Army University Press, Military Review, Fort Leavenworth, Kansas: USA, 3 November 2017), 5.

[115] *Ibid.*

national narratives contradict the NATO narrative, to some extent undermining NATO's credibility.[116]

NATO's Operation *Unified Protector* in Libya demonstrated the challenge NATO faced in ensuring that the messages of member states are aligned with the organization.[117] In 2011, United Nations Security Council Resolution (UNSCR) 1973 (2011) enabled NATO "…to protect civilians and civilian populated areas under threat of attack in the Libyan Arab Jamahiriya, including Benghazi, while excluding a foreign occupation force of any form on any part of Libyan territory."[118] Despite NATO's approved narrative that aligned with the UN resolution, some nations admitted to deploying a small number of troops to Libya and others publicly expressed their willingness to facilitate regime change in Libya.[119] Neither of these were ever officially part of NATO's agenda, which generated suspicion regarding the actual purpose of NATO's operation and caused other participating nations to question its credibility as an organization.[120]

In a 2018 statement to the Senate of the United States of America (USA), USA Army general Curtis M. Scaparrotti, Commander of European Command and Supreme Allied Commander Europe (SACEUR), highlighted that "throughout Europe, Russia exercises malign influence to disrupt and attempt to fracture NATO, undermine trans-

---

[116] J.D. Scanlon, "Strategic Communications: A Caution to Military Commanders," (Army University Press, Military Review, Fort Leavenworth, Kansas: USA, 3 November 2017), 5.

[117] North Atlantic Treaty Organization, "Operation Unified Protector," Last updated 27 March 2012, https://www.nato.int/cps/en/natolive/71679.htm.

[118] United Nations Security Council, "Resolution 1973 (2011), adopted by the Security Council at its 6498th meeting, on 17 March 2011," (S/RES/1973 (2011), New York: USA, 2011), 3; J.D. Scanlon, "Strategic Communications: A Caution to Military Commanders," (Army University Press, Military Review, Fort Leavenworth, Kansas: USA, 3 November 2017), 5.

[119] *Ibid*.

[120] *Ibid*.

Atlantic cohesion, and erode democratic foundations."[121] He emphasized the fact that Russia exploits the disputes either among NATO member countries, with particular reference to Turkey, or internally within the country itself to contribute to its narrative and "undermine trust and unity"[122] of NATO.[123] In addition to political disputes between Turkey, USA, and NATO regarding involvement in Syria, Turkey also purchased the S-400 missile system from Russia.[124] This spurned discussions between the US and NATO internally as it ignored the agreement signed by all member states that NATO defence systems should be comparable.[125]

In another example of differing narratives between NATO and one of its member states, Hungary's Prime Minister Orbān is considered to be the biggest supporter of Russia's leadership politics.[126] Prime Minister Orbān not only openly supports Russia's activities but also welcomes Russia's propaganda against the EU, USA and NATO. Additionally, Russia's propaganda channels *Sputnik* and *Russia Today* both freely disseminate their content in the information space of Hungary and are also widely used as a primary source of information for pro-government media outlets.[127] Current political

---

[121] Curtis M. Scaparrotti, "Statement of General Curtis M. Scaparrotti, United States Army Commander and United States European Command," (United States Senate, Committee on Armed Services, Washington D.C.: USA, 8 March 2018), 3; North Atlantic Treaty Organization, Supreme Headquarters Allied Power Europe, "Command Group," Last access to the webpage 27 April 2018, https://shape.nato.int/about/leadership-staff/command-group.

[122] *Ibid.,*13.

[123] *Ibid*.

[124] Jonatham Katz and Torrey Taussing, "An inconvenient truth: Addressing Democratic Backsliding within NATO," (The Brookings Institution, Washington. D.C.:USA, 10 July 2018), https://www.brookings.edu/blog/order-from-chaos/2018/07/10/an-inconvenient-truth-addressing-democratic-backsliding-within-nato/.

[125] *Ibid*.

[126] *Ibid*.; United States Senate, Committee on Foreign Relations, "Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security," (U.S. Government Publishing Office, Washington. D.C: USA, 2018), 94 - 95.

[127] *Ibid*.

activities of both NATO member countries Turkey and Hungary are dissonant to a

NATO issued statement:

> All practical civilian and military cooperation under the NRC [NATO –
> Russia Council] with Russia has been suspended since April 2014, in
> response to Russia's military intervention and aggressive actions in
> Ukraine, and its illegal occupation and annexation of Crimea, which Allies
> condemn in the strongest terms.[128]

D. J. Scanlon and other experts acknowledge that "examples of dissonance will be

found in almost any NATO or coalition operation as member nations confront their own

national politics, making the sustainment of a coherent allied narrative highly

challenging."[129] Additionally, Mark Laity emphasizes that "…it appears the West is

losing the StratCom struggle. It is not tactics, techniques and procedures that are the

problem, but a lack of certainty about what we want or lack of unity about our aims."[130]

Despite the struggle for internal cohesion, NATO is successfully improving its

cohesion in the realm of strategic communications with other governmental and non-

governmental organizations in the region. For instance, since 2015 the EU's East

StratCom Task Force has developed partnership with NATO key StratCom agencies

including StratCom COE to share situational awareness between both organizations.[131]

Furthermore, in 2016 the EU and NATO signed a joint declaration "which set out a

"common set of proposals" with 74 concrete actions, many of which focus on hybrid

---

[128] North Atlantic Treaty Organization, "Relations with Russia," Last updated 4 February 2019, https://www.nato.int/cps/en/natolive/topics_50090.htm.

[129] J.D. Scanlon, "Strategic Communications: A Caution to Military Commanders," (Army University Press, Military Review, Fort Leavenworth, Kansas: USA, 3 November 2017), 7.

[130] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 73.

[131] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 4.

threats, building resilience in cyber security, and strategic communications."[132] In the

same year NATO and the EU boosted their partnership in "the establishment of a Hybrid

Fusion Cell as part of the EU Intelligence and Situation Centre, and a European Centre of

Excellence for Countering Hybrid Threats in Helsinki."[133] Nevertheless, experts of the

German Marshall Fund of the United States highlight that even though COEs are

providing valuable research and analysis of different issues across organizations, "these

centers are also removed from policy discussions and meaningful decision-making

structures in Brussels and in individual member states."[134]

      Mark Laity highlights that "Without a clear story and strategy, we are vulnerable

and will find it hard to set, let alone achieve, desired communication effects and

outcomes."[135] In the political circumstances dictated by different national agendas, which

often are not adjusted to those of NATO, the challenge to develop a consistent and

coherent strategy and narrative will always be present. Inconsistencies in the

organization's common strategy and aims create confusion and impede its ability to

achieve strategic effects. This in turn often affects NATO's credibility and enables

---

[132] Ministry of Foreign Affairs of Finland, Mission of Finland to NATO, "Cooperating to Counter Hybrid Threats," Last updated 17 December 2018, http://www.finlandnato.org/public/default.aspx?contentid=380118&contentlan=2&culture=en-US; North Atlantic Treaty Organization, "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," Last updated 05 December 2017, https://www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en.

[133] Ministry of Foreign Affairs of Finland, Mission of Finland to NATO, "Cooperating to Counter Hybrid Threats," Last updated 17 December 2018, http://www.finlandnato.org/public/default.aspx?contentid=380118&contentlan=2&culture=en-US.

[134] Brittany Beaulieu and David Salvo, "NATO and Asymmetric Threats: A Blueprint for Defence and Deterrence," (Alliance for Security Democracy, German Marshall Fund, Policy Brief, No 031, Washington. D.C.: USA, 2018), 4.

[135] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 73.

adversaries to exploit its weaknesses, diminishing its capability to counter current threats.[136]

CONCLUSION

The examples provided in this paper re-assert that Russia and insurgent groups such as ISIS will continue to use asymmetric activities, for example through the usage of social media platforms, to achieve their aims. Hybrid threats will remain an integral part of current and future threats to NATO where information warfare will have a fundamental role in shaping opinions and influencing behaviour of NATO as organization and its individual member states.[137]

NATO needs to enhance its understanding of IE, as IE is paramount to successfully countering hybrid threats and preventing undesired external influence on the decision making process of NATO, at the same time enabling the execution of NATO operations such as StratCom.[138] Dissonance in the understanding of StratCom amongst member states, along with the lack of a policy and doctrine that would properly explain StratCom, has impeded the implementation of StratCom policy. To fix this problem, NATO need to provide additional clarification regarding the definition of StratCom and to present it as being more of an information management process than a strategy that has a supporting function to the operations rather than a central role.[139]

---

[136] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 73.

[137] NATO Strategic Communication Centre of Excellence, "Social Media as a Tool of Hybrid Warfare," (ISBN 978-9934-8582-6-0, Riga: Latvia, May 2016), 10.

[138] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 69; North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 4.

[139] Steve Tatham and Rita Le Page, "NATO Strategic Communication: More to Be Done?" (National Defence Academy of Latvia, Center for Security and Strategic Research, Riga: Latvia, 2014), 2; Mark

One of the key achievements in the StratCom realm is the establishment of NATO StratCom COE, which since its beginning has supported the development of policy, the conduct of extensive research on the information campaigns of potential adversaries, and has identified the gaps within the StratCom capabilities of NATO.[140] Nevertheless, COEs should be involved in discussions related to NATO policy and decision-making structures. Furthermore, the results of the studies that the centre delivers should be immediately incorporated into NATO's policy documents and doctrine.[141]

Despite current hybrid threats and the continuously changing information environment, NATO's member states incoherent perceptions of StratCom as a concept, the slow development of national and organizational StratCom capabilities, and the absence of proper training leaves NATO requiring a more robust NATO's approach to StratCom.[142]

In the political circumstances dictated by different national agendas, which are not properly coordinated with NATO one, the challenge to develop a consistent and coherent NATO strategy and narrative will always be present. Inconsistencies between the common strategy and the organization's aims frequently create confusion and impede NATO's ability to achieve strategic effects. This in turn affects its credibility and enables

---

Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 66.

[140] Naja Bentzen, "NATO Strategic Communications: An Evolving Battle of Narratives," Last access to the webpage 19 April 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600, 3.

[141] Brittany Beaulieu and David Salvo, "NATO and Asymmetric Threats: A Blueprint for Defence and Deterrence," (Alliance for Security Democracy, German Marshall Fund, Policy Brief, No 031, Washington. D.C.: USA, 2018), 4.

[142] J.D. Scanlon, "Strategic Communications: A Caution to Military Commanders," (Army University Press, Military Review, Fort Leavenworth, Kansas: USA, 3 November 2017), 2.

adversaries to exploit its weaknesses, diminishing NATO's capability to counter current threats.[143]

Dissonance in the understanding of the concept of StratCom, insufficient contributions to developing its capabilities, and a lack of cohesion regarding the narratives of member states and NATO StratCom, pose the main challenges to the achievement of joint NATO aims in countering current threats. NATO continues to face a challenge in synchronizing its words, as reflected in the contrast between its standing policy documents and its member states deeds. Undoubtedly, these factors combine to impede NATO's ability to tell the story right.[144]

---

[143] Mark Laity, "NATO and Strategic Communications: The Story So Far," (The Magazine of Joint Warfare Centre, the Three Swords, Iss.33, Stavanger: Norway, March 2018), 73.

[144] North Atlantic Treaty Organization, "NATO Strategic Communications Handbook (Draft for Use)," (HQ, SACT, Ver.9.1.21, Norfolk: Virginia, USA, 31 March 2015), 28.

BIBLIOGRAPHY

Beaulieu, Brittany and David Salvo. "NATO and Asymmetric Threats: A Blueprint for Defence and Deterrence." Alliance for Security Democracy. German Marshall Fund. Policy Brief. No 031. Washington. D.C.: USA, 2018.

Bentzen, Naja. "NATO Strategic Communications: An Evolving Battle of Narratives." Last access to the webpage 19 April 2019. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)586600.

Cornish, Paul, Julian Lindley-French, and Claire Yorke. "Strategic Communications andNational Strategy." A Chatham House Report. The Royal Institute of International Affairs, London: UK, September, 2011.

Edmonds, Jeff and Samuel Bendett. "Russian Battlefield Awareness and Information Dominance: Improved Capabilities and Future Challenges." Last access to the webpage 27 April 2019. https://www.realcleardefense.com/articles/2019/02/26/russian_battlefield_awareness_and_information_dominance_improved_capabilities_and_future_challenges_114218.html.

Gage, Daniel. "The Continuing Evolution of Strategic Communications within NATO." The Magazine of Joint Warfare Centre, the Three Swords. Iss.27. Stavanger: Norway, 2014.

Gerasimov, Valery. "Contemporary Warfare and Current Issues for the Defense of the Country." Last access to the webpage 21 April 2019. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/Contemporary-Warfare-and-Current-Issues-for-the-Defense-of-the-Country/.

Jolkina, Alexandra and Markian Ostaptschuk. "Activists or Kremlin agents - who protects Russian-speakers in the Baltics?" Last access to webpage 02 May 2019. https://www.dw.com/en/activists-or-kremlin-agents-who-protects-russian-speakers-in-the-baltics/a-18903695.

Jopling, Thomas Michael. "Countering Russia's Hybrid Threats: An Update." Draft Special Report. NATO Parliamentary Assembly. Committee On The Civil Dimension of Security. Brussels: Belgium, 27 March 2019.

Laity, Mark. "NATO and Strategic Communications: The Story So Far." The Magazine of Joint Warfare Centre. The Three Swords. Iss.33. Stavanger: Norway, March 2018.

Loyn, David. "We Have Met the Enemy And He Is Us." NATO Strategic Communications Centre of Excellence. Defence Strategic Communications. Volume 3. Riga: Latvia, 2017.

Ministry of Foreign Affairs of Finland. Mission of Finland to NATO. "Cooperating to Counter Hybrid Threats." Last updated 17 December 2018. http://www.finlandnato.org/public/default.aspx?contentid=380118&contentlan=2&culture=en-US.

NATO Standardization Office (NSO). "NATO Glossary of Terms and Definitions." APP-6. 2018 Edition. Brussels: Belgium, 2018.

NATO Strategic communication Centre of Excellence. "Robottrolling." Issue 1. Riga: Latvia, 2019.

NATO Strategic Communication Centre of Excellence. "Social Media as a Tool of Hybrid Warfare." ISBN 978-9934-8582-6-0. Riga: Latvia, May 2016.

NATO Strategic Communications Centre of Excellence. "About Us." Last access to the webpage in 23 April 2018. https://www.stratcomcoe.org/about-us.

NATO Strategic Communications Centre of Excellence. "Hybrid Threats: A Strategic Communication Perspective." Last access to the webpage 20 April 2019. https://www.stratcomcoe.org/hybrid-threats-strategic-communications-perspective.

North Atlantic Treaty Organization. "Food for Thought: Paper on NATO Military Public Affairs Training." 1710/TSC-GSU-0300/TT-0161/Ser: 469. Brussels: Belgium, 30 August 2018.

North Atlantic Treaty Organization. "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." Last updated 05 December 2017. https://www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en.

North Atlantic Treaty Organization. "Military Concept for NATO Strategic Communications." MCM-0085-2010. Brussels: Belgium, Augusts 2010.

North Atlantic Treaty Organization. "NATO Strategic Communications Handbook (Draft for Use)." HQ, SACT.Ver.9.1.21. Norfolk: Virginia, USA, 31 March 2015.

North Atlantic Treaty Organization. "NATO Strategic Communication Policy." PO (2009) 0141. Brussels: Belgium, 29 September 2009.

North Atlantic Treaty Organization. "Operation Unified Protector." Last updated 27 March 2012. https://www.nato.int/cps/en/natolive/71679.htm.

North Atlantic Treaty Organization. "Relations with Russia." Last updated 4 February 2019. https://www.nato.int/cps/en/natolive/topics_50090.htm.

North Atlantic Treaty Organization. "Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, issued in 5 September 2014." Last updated 30 August 2018. https://www.nato.int/cps/en/natohq/official_texts_112964.htm#rap.

North Atlantic Treaty Organization. Supreme Headquarters Allied Power Europe. "Command Group." Last access to the webpage 27 April 2018. https://shape.nato.int/about/leadership-staff/command-group.

Osborne, Gerry. NATO Strategic Communications Centre of Excellence. "Mapping of StratCom Practices in the NATO Countries." Riga: Latvia, 2015.

Raimzhanova, Aigerim."Power in IR: Hard, Soft and Smart." Institute for cultural Diplomacy and the University of Bucharest. Bucharest: Rumania, 2015.

Scanlon, J.D. "Strategic Communications: A Caution to Military Commanders." Army University Press. Military Review. Fort Leavenworth, Kansas: USA, 3 November 2017.

Scaparrotti, Curtis M. "Statement of General Curtis M. Scaparrotti, United States Army Commander and United States European Command." United States Senate. Committee on Armed Services. Washington D.C.: USA, 8 March 2018.

Stupples, Davis. "Are we prepared for information warfare." City. University of London. London: UK, 30 November 2015.

Tatham, Steve and Rita Le Page. "NATO Strategic Communication: More to Be Done." National Defence Academy of Latvia. Center for Security and Strategic Research. Riga: Latvia, 2014.

Tatham, Steve. "Strategic Communications: A Primer." ARAG Special Series 8/28. Defence Academy of the United Kingdom. London: UK, December 2008.

The Defence Science Board. "Report of the Defence Science Board Task Force on Managed Information Dissemination." Washington, D.C.: USA, October 2001.

The Russian Federation. The Ministry of Foreign Affairs of the Russian Federation. "National Security Concept of the Russian Federation." Last access to the webpage 21 April 2019. http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768.

Traverton, Gregory F., Anrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." Swedish Defence University. Center for Asymmetric Threats Studies. Hybrid CoE, 2018.

United Nations Security Council. "Resolution 1973 (2011), adopted by the Security Council at its 6498th meeting, on 17 March 2011." S/RES/1973 (2011. New York: USA, 2011.

United States Senate. Committee on Foreign Relations. "Putin's Asymetric Assault on Democrasy in Russia and Europe: Implications for U.S. National Security." U.S. Government Publishing Office. Washington. D..C.: USA, 2018.

Van Puyvelde, Damien. "Hybrid War – dies it even exist." Last access to the webpage 21 April 2019. https://www.nato.int/DOCU/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm.

World Heritage Encyclopedia. Last access to the webpage 19 April 2019. http://self.gutenberg.org/articles/Fog_of_war.