February 21-24, 2019

Carleton University, Ottawa

2019 MNATO

CIVILIAN INTELLIGENCE COMMITTEE BACKGROUND GUIDE

- Building Strategic Partnerships through the Cyber Defence Centre of Excellence
- Increasing Intelligence Sharing to Address Conflict in Grey Zones
- The Role of Intelligence in Preventing the Use of Chemical, Biological, Radiological, and Nuclear Weapons

Introduction to the Civilian Intelligence Committee

The Civilian Intelligence Committee (CIC) is the sole body that handles civilian intelligence issues at NATO. It reports directly to the North Atlantic Council and advises it on matters of espionage and terrorist or related threats, which may affect the Alliance.

Since September 11, 2001, NATO has sought to improve its intelligence gathering and intelligence sharing capabilities to support its strategic objectives. The CIC is integrated with NATO's new Joint Intelligence Security Division (JISD) and provides a forum for the intelligence agencies of the alliance to share intelligence and consider how the intelligence gathering services of NATO and its Member States can best support the alliance's objectives.

Representatives to the CIC must balance the need for the alliance to work with the best intelligence possible while ensuring that their own interests are protected when sharing intelligence. National sovereignty and the security of intelligence sources must be balanced against the need for allies to cooperate in the face of complex threats and challenges facing the alliance. The CIC must also carefully consider how to best leverage the alliance's intelligence assets to meet those challenges, working with priorities set by the NAC and NATO strategic command.

Topic A: Building Strategic Partnerships through the Cooperative Cyber Defence Centre of Excellence

Introduction

The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) was founded in Tallinn, Estonia, in 2008 a the mission to "enhance cooperative cyber defence capabilities of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber defence."[1] The center includes a diverse group of researchers, analysts, and teachers from 20 states that help support state and private sector actors address cyber defense.[2] CCD COE was originally established by seven NATO states (Estonia, Germany, Italy, Lithuania, Latvia, Slovak Republic, and Spain), but has since expanded to include a total of 18 NATO Sponsoring.[3] In addition to this core mission to the Alliance, CCD COE seeks to improve the capability and cooperation between NATO, Allies, and partners in cyber defense.[4] Non-NATO states can also join CCD COE as contributing participants, which currently includes Australia, Austria, Finland, Japan, and Sweden.[5]

CCD COE's vision is to become the primary point of reference for expertise on cyber defense, which requires partnerships.[6] Although CCD COE's core institutional partners and participants are states, NATO views partnerships with industry and academia as critical to effectively addressing challenges in cyberspace.[7] This view was underscored in the NATO Brussels Communique, which identified partnerships with international organizations, industry, and academia as critical to keeping up with technological advancements for cyber defense.[8] There is still significant room for CCD COE to grow its partnerships through both membership with NATO and non-NATO states as well as the private sector, to achieve CCD COE's vision of become an expert source on cyber defense.

NATO's Role

Since the creation of CCD COE in 2008, NATO has created a myriad of bodies to better understand cyberspace as a domain of conflict. Among these organizations, CCD COE is among the bodies that serve to improve cyber defenses as a research and training facility.[9] These efforts

[1] CCDCOE, 28 October 2008, "Centre Is the First International Military Organization Hosted by Estonia," https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html.
[2] CCDCOE, 20 May 2014, "About Cyber Defence Centre," https://ccdcoe.org/about-us.html.
[3] Ibid.
[4] Osula, A.-M. and H. Rõigas, 2016, *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO Cyber Defence Centre of Excellence, https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.
[5] NATO, 2018, "Allied Command Transformation: COE Catalogue," https://www.act.nato.int/images/stories/structure/coe_catalogue_2018a.pdf.
[6] Plantera, F., "NATOCCDCOE – Expertise and Cooperation Make Our Cyber Space Safer," *e-estonia*, https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/.
[7] NATO, 16 July 2018, "Cyber Defence," https://www.nato.int/cps/en/natohq/topics_78170.htm.
[8] NATO, 2018, "Brussels Summit Declaration," https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
[9] NATO, "Cyber Defence."

by CCD COE serve to bring policy and technical experts together and enhance understanding of this new domain of warfare. NATO's strategic partners, in some cases, improve upon the security of NATO and bring additional expertise to improve security in cyberspace.[10]

It was only in 2016 in the Warsaw Summit Communique that NATO recognized cyberspace as a domain of operations, despite the recognition of cyberspace security threats for more than a decade.[11] It is due to this lack of political, legal, and operational knowledge in addressing cyberspace that CCD COE was created and seeks to fill this gap. The pooling of expertise to be better prepared in the event an attack occurs remains critical, and partnerships play an important role.[12] As NATO continues to take steps to understand how to integrate operational capacities to address threats in cyberspace, CCD COE will help to learn how to best achieve cyber operation missions.[13]

CCD COE hosts a multitude of events in order to act out in this role and provide advantages for partners including, but not limited to: law courses on the international law of cyber operations; executive cyber seminars for senior leaders new to addressing cyberspace; cyber defense monitoring courses for threat detection; cyber defense operations courses for operations planners; and technical courses such as on botnet mitigation.[14] It serves to increase understanding about the security and defense implications associated with the cyber domain and as a means to bring states, militaries, academia, and industry together.[15]

One of CCD COE's longest running events is Locked Shields, which is an annual "live-fire" cyber defense exercise, that included over 1000 experts from 30 states in 2018.[16] The event included government, military, and private-sector experts competing in a simulation of a large-scale cyber attack. While the exercise serves to improve the abilities and readiness of experts, the inclusion of decision-makers helps to practice chain of command response involving both civilian and military actors. During the 2018 exercise, participants found problems associated with dialogue between technical experts and decision-makers.

Conclusion

Despite NATO's efforts, cyber defense remains a broad and ill-defined field. The Brussels Communique highlights NATO's effort to enhance both NATO and allied state's abilities for cyber defense. To do so requires collaboration from NATO allies, non-NATO states, and private sector partners. Partnerships are still critical for building institutional knowledge and increasing

[10] NATO Review, "NATO's strategic partnerships," https://www.nato.int/docu/review/2003/NATO-Strategic-Partners/EN/index.htm.
[11] NATO, 2016, "Warsaw Summit Communiqué," https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[12] Pomerleau, M., 20 November 2017, "Here's How NATO Is Preparing for Cyber Operations," *Fifth Domain*, https://www.fifthdomain.com/international/2017/11/20/heres-how-nato-is-preparing-for-cyber-operations/.
[13] Ibid.
[14] CCDCOE, "Cyber Security Training Events," https://ccdcoe.org/events.html.
[15] NATO, "Cyber Defence."
[16] CCDCOE, 26 April 2018, "More than 1000 cyber experts from 30 nations took part in Locked Shields," https://ccdcoe.org/more-1000-cyber-experts-30-nations-took-part-locked-shields.html.

understanding between governments and the private sector. In the event of a cyber attack, full response requires the cooperation of the public and private sectors, underlining the importance of partnerships and the role of CCD COE in building them in NATO.

Guiding Questions:

- How can CCD COE encourage collaboration by non-NATO states and the private sector?
- Would CCD COE and its exercises benefit from greater transparency?
- Are there gaps in the current activities of CCD COE that can improve existing relationships with partners?
- What unique role can CCD COE play to build partnerships compared to other NATO cyber bodies such as the NATO Industry Cyber Partnership, NATO Cyber Range, or NATO Communications and Information Academy?

Further Reading:

CCDCOE. (n.d.). "About Cyber Defence Centre." https://ccdcoe.org/about-us.html.

CCDCOE. (n.d.). "Cyber Security Training Events." https://ccdcoe.org/events.html.

CCDCOE. (28 October 2008). "Centre Is the First International Military Organization Hosted by Estonia." https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html.

CCDCOE. (26 April 2018). "More than 1000 cyber experts from 30 nations took part in Locked Shields." https://ccdcoe.org/more-1000-cyber-experts-30-nations-took-part-locked-shields.html.

North Atlantic Treaty Organization. (2016). "Warsaw Summit Communiqué." https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

North Atlantic Treaty Organization. (2018). "Brussels Summit Declaration." https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

North Atlantic Treaty Organization. (16 July 2018). "Cyber Defence." https://www.nato.int/cps/en/natohq/topics_78170.htm.

Osule, A.-M. and Rõigas, H. (2016). *International Cyber Norms: Legal, Policy & Industry Perspectives*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

Plantera, F. (16 October 2018). "NATO CCDCOE – Expertise and cooperation make our cyber space safer." *e-estonia*. https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/.

Pomerleau, M. (2017). "Here's how NATO is preparing for cyber operations." *Fifth Domain*. https://www.fifthdomain.com/international/2017/11/20/heres-how-nato-is-preparing-for-cyber-operations/.

Topic B: Increasing Intelligence Sharing to Address Conflict in Grey Zones

Introduction

Since the 2000s, NATO's concern for grey zone conflicts has steadily grown in light of the ongoing conflict in Ukraine. Grey zone conflicts, often referred to as hybrid warfare or hybrid threats, attempt the blur the lines between civilian and military.[17] The central them to this form of conflict is the use of aggression and coercion without a state exposing itself to escalation, retribution, and often attribution.[18] These actions of political, economic, and military competition occurs just short of war, making a response difficult.

As conflicts in grey zones do not necessitate an automatic kinetic military response, NATO must use other forms of defense to respond, including intelligence. Due to the blurred lines between civilians and military in hybrid conflicts, it also makes it necessary to integrate civilian and military intelligence for NATO to understand the conflict in its entirety.[19] This comes as part of a recognition of its level of complexity, requiring knowledge in such areas as social movement theory, regional, language and cultural studies, negotiation and mediation, social network analysis, influence operations, cyber tools and methods, subversion and political warfare, and more. Due to the complexity of the threats and responses, cooperation and intelligence sharing is of the utmost importance.[20]

NATO's Role

Clandestine and intelligence operations are used in hybrid conflicts in order to avoid attribution and retribution, making it difficult for NATO to intervene to stop the aggressive acts. In addition, these methods make it difficult for NATO members to agree on intervention to stop such acts in the first place. Successful intervention requires more than military power, instead requiring cooperation among both NATO allies and non-NATO partners, including the European Union.[21]

The Brussels Communique notes NATO's concern for hybrid threats, which includes specific concern for disinformation campaigns and malicious cyber activities as part of the hybrid challenges.[22] In particular, the communique refers to Russia's use of hybrid actions to challenge Euro-Atlantic security and stability.[23] Noteworthy is that the Brussels Summit Declaration

[17] von Loringhoven, A. F., 9 August 2017, "Adapting NATO intelligence in support of 'One NATO'," *NATO Review Magazine*, https://www.nato.int/docu/review/2017/also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/en/index.htm.

[18] The Economist, 25 January 2018, "Neither war nor peace," https://www.nato.int/docu/review/2017/also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/en/index.htm.

[19] von Loringhoven, "Adapting NATO intelligence in support of 'One NATO'."

[20] Pindják, P., 2014, "Deterring hybrid warfare: a chance for NATO and the EU to work together?," *NATO Review Magazine*, https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm.

[21] Ibid.

[22] NATO, 2018, "Brussels Summit Declaration," https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[23] Ibid.

specifically cites intelligence sharing as a critical support mechanism to assist against hybrid threats.[24]

In 2017, NATO created the Joint Intelligence Security Division (JISD) as a response to an increasing amount of global challenges including an assertive Russia, the rise of terrorism, and more.[25] Among the specific threats the JISD addresses includes conventional military, cyber attacks, terrorism, and hybrid warfare.[26] In noting the threat associated with hybrid warfare, JISD created a hybrid analysis branch in July 2017 to analyze the "full spectrum of hybrid actions, drawing from military and civilian, classified and open sources."[27]

To increase sharing with NATO partners, NATO created the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki, Finland.[28] The purpose of the center is to encourage dialogue, research, conduct training, investigate, and engage on hybrid threats. The Hybrid CoE serves as one way to increase cooperation and intelligence sharing between NATO and the European Union and increase the capacity to engage on the myriad of threats in grey zone conflicts.

Conclusion

As highlighted in the Brussels Communique, NATO recognizes that grey zone conflicts represent a significant challenge to the security of the Alliance. As a response, NATO has sought to improve upon existing methods which acknowledge the diffuse nature of hybrid conflicts.

Guiding Questions:

- How does each Member State cooperate with NATO in intelligence sharing?
- Which Member States have policies to address hybrid conflicts?
- Are there gaps in how intelligence sharing is conducted in NATO that diminishes NATO's capacity to respond to hybrid threats?
- How can civilian and military intelligence apparatuses be integrated to address grey zone conflicts without diminishing their capacities to support their individual mandates?

Further Reading:

CCDCOE. (n.d.). "About Cyber Defence Centre." https://ccdcoe.org/about-us.html.

CCDCOE. (n.d.). "Cyber Security Training Events." https://ccdcoe.org/events.html.

CCDCOE. (28 October 2008). "Centre Is the First International Military Organization Hosted by Estonia." https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html.

[24] NATO, 2018, "Brussels Summit Declaration," https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
[25] von Loringhoven, "Adapting NATO intelligence in support of 'One NATO'."
[26] Ibid.
[27] Ibid.
[28] Hybrid CoE, 2018, "About Us," https://www.hybridcoe.fi/about-us/.

CCDCOE. (26 April 2018). “More than 1000 cyber experts from 30 nations took part in Locked Shields.” https://ccdcoe.org/more-1000-cyber-experts-30-nations-took-part-locked-shields.html.

Hybrid CoE. (2018). “About Us.” https://www.hybridcoe.fi/about-us/.

NATO Review. (n.d.). “NATO’s strategic partnerships.” https://www.nato.int/docu/review/2003/NATO-Strategic-Partners/EN/index.htm.

North Atlantic Treaty Organization. (2016). “Warsaw Summit Communiqué.” https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

North Atlantic Treaty Organization. (2018). “Allied Command Transformation: COE Catalogue.” https://www.act.nato.int/images/stories/structure/coe_catalogue_2018a.pdf.

North Atlantic Treaty Organization. (2018). “Brussels Summit Declaration.” https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

North Atlantic Treaty Organization. (16 July 2018). “Cyber Defence.” https://www.nato.int/cps/en/natohq/topics_78170.htm.

Pindják, P. (2014). “Deterring hybrid warfare: a chance for NATO and the EU to work together?.” *NATO Review Magazine*. https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm.

The Economist. (25 January 2018). “Neither war nor peace.” https://www.economist.com/special-report/2018/01/25/neither-war-nor-peace.

Von Loringhoven, A. F. (9 August 2017). “Adapting NATO intelligence in support of ‘One NATO’.” *NATO Review Magazine*. https://www.nato.int/docu/review/2017/also-in-2017/adapting-nato-intelligence-in-support-of-one-nato-security-military-terrorism/en/index.htm.

Topic C: The Role of Intelligence to Preventing the Use of Chemical, Biological, Radiological, and Nuclear Weapons

Introduction

Chemical, Biological, Radiological, and Nuclear (CBRN) Weapons, or weapons of mass destruction, pose a threat to civilian populations. Proliferation of CBRN weapons, not only among states, but also among non-state actors, is a major international security risk. The development, production and use of chemical and biological weapons is banned under two international treaties, the Chemical Weapons Convention and the Biological Weapons Convention. These treaties have been ratified by most countries in the world including the US and Russia.[29]

While production and stockpiling these weapons is banned by the CWC and BWC, the gas attacks in Syria illustrate the difficulties in enforcing them. Having acceded to the Chemical Weapons Convention in 2013, the Syrian government proceeded to launch multiple chemical strikes on its own population.[30] Not only was a state party to the treaty willing to use these weapons, but the attacks indicate that stockpiles have evidently not been destroyed. These stockpiles could potentially be seized by non-state actors like ISIL, and indeed there have been multiple confirmed gas attacks originating from ISIL, including one instance of a mustard gas shell being fired at American troops in Iraq.[31]

The European Union in particular has been highly concerned with the potential for groups like ISIL to launch a CBRN attack on a domestic taget. The Eurpoean Parliament reported in 2015 ISIL's access to key materials in Iraq, Syria, and Libya as well as the seizure of an ISIL laptop containing detailed instructions on prodcing a bioweapon to point to the potential capacity of the group to launch an attack.[32] The difficulty in finding and seizing stockpiles of chemical and biological weapons, as well as the relative ease with which they can be created, means that NATO must remain well-guarded against the threat posed by these weapons of mass destruction, both at home in NATO member countries, and abroad on NATO missions.

NATO's Role

NATO founded its Weapons of Mass Destruction Non-Proliferation Centre (WMDC) in 1999, which acted to limit proliferation, including through facilitating information sharing According to Ted Whiteside, the first head of the WMDC: "central to very extensive information-

[29] OPCW, "The Chemical Weapons Convention," https://www.opcw.org/chemical-weapons-convention.; UN Office at Geneva, "The Biological Weapons Convention," https://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument.

[30] Chasse, K., 2016, "Is NATO Prepared in Case of a Chemical, Biological, Nuclear, or Radiological Attack?," *NATO Association of Canada*, http://natoassociation.ca/is-nato-prepared-in-case-of-a-chemical-biological-nuclear-or-radiological-attack-the-ongoing-cbrn-threat-and-canadas-role-in-protection-and-defence/.

[31] Ibid.

[32] European Parliament, December 2015, "ISIL/Da'esh and 'non-conventional' weapons of terror," http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/572806/EPRS_BRI%282015%29572806_EN.pdf.

sharing that took place with Russia in the context of the NATO Russia Council."[33] Information sharing has been crucial to NATO's capability to combat CBRN weapon threats from the beginning. The WMDC was merged with the Arms Control and Coordination Section into the Arms Control, Disarmament, and WMD Non-proliferation Centre (ACDC) in 2017[34].

NATO's Joint CBRN Defence Task Force was established in 2003 to provide the alliance with CBRN defence capabilities, operating within the NATO Response Force.[35] The Defence Task Force's CBRN Defence Battalion is equipped with the capabilities to identify CBRN substances and weapons, perform decontamination operations, and advise NATO command.[36] It has also been assigned to assist civilian operations in large-scale events.[37]

The Joint Centre of Excellence on CBRN Defence was launched in 2007 in the Czech Republic. The COE, according to NATO:

> …provides opportunities to improve interoperability and capabilities by enhancing multinational education, training and exercises; assisting in concept, doctrine, procedures and standards development; and testing and validating concepts through experimentation[38].

The COE is NATO's best asset for facilitating knowledge transfer, training, and expertise to Member States. It stands ready to "provide scientific and operational advice in the event of an attack on military forces and to help protect civilian populations against the consequences of a terrorist attack."[39]

The NATO Intelligence Fusion Centre (NIFC) provides key information and intelligence sharing support to NATO members. It provides information for analysis by ACDC allowing for careful analysis of critical threats. Located in the United Kingdom, NIFC was specifically created to foster intelligence sharing among the allies, and to facilitate the fusion of its intelligence gathering in critical areas.[40] NIFC's mission is critical to NATO's sharing intelligence capabilities in combatting CBRN threats.

Conclusion

NATO has recognized the threat posed by chemical and biological weapons, especially given its potential in the hands of terrorist organizations. NATO has several bodies that work in

[33] NATO, 4 September 2015, "Fighting weapons of terror," https://www.nato.int/cps/en/natohq/news_122272.htm.
[34] NATO, 8 December 2017, "Weapons of mass destruction," https://www.nato.int/cps/en/natohq/topics_50325.htm.
[35] Ibid.
[36] NATO Review, 2005, "Boosting NATO's CBRN capabilities," https://www.nato.int/docu/review/2005/combating-terrorism/NATO-CBRN-Capabilities/EN/index.htm.
[37] Ibid.
[38] NATO, "Weapons of mass destruction."
[39] NATO, "Fighting weapons of terror."
[40] NATO Intelligence Fusion Centre, "What is the NIFC?," http://web.ifc.bices.org/about.htm.

cooperation to study, analyze, protect against, and contain potential CBRN attacks. The CIC is responsible for setting NATO policy regarding intelligence sharing and its relation to CBRN weapons, as well as providing a forum for representatives of intelligence agencies from Member States to discuss the issue and reach a consensus.

The CIC will need to consider whether NATO's current intelligence sharing capabilities through the NIFC, the Joint Command structure, and relationships among Member States are adequate. Even though ISIL's capabilities have been greatly reduced in the last few years, the potential for a terrorist strike using CBRN weapons remains a potential, devastating threat, especially to civilian populations.

Guiding Questions

- How can NATO improve its intelligence sharing in this area? In what areas should it seek to improve its intelligence sharing?
- How should NATO best make use of its bodies and agencies tasked with handling the CBRN threat? Should their roles be expanded or modified?
- What sort of intelligence sharing arrangements should NATO and Member States pursue with outside partners?

Further Reading

Chasse, K. (2016). "Is NATO prepared in Case of a Chemical, Biological, Nuclear, or Radiological Attack? The ongoing CBRN Threat and Canada's Role in Protection and Defence." *NATO Association of Canada*. http://natoassociation.ca/is-nato-prepared-in-case-of-a-chemical-biological-nuclear-or-radiological-attack-the-ongoing-cbrn-threat-and-canadas-role-in-protection-and-defence/.

European Parliament. (December 2015). "ISIL/Da'esh and 'non-conventional' weapons of terror." http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/572806/EPRS_BRI%282015%29572806_EN.pdf.

NATO Intelligence Fusion Centre. (n.d.). "What is the NIFC?." http://web.ifc.bices.org/about.htm.

NATO Review. (2005). "Boosting NATO's CBRN capabilities." https://www.nato.int/docu/review/2005/combating-terrorism/NATO-CBRN-Capabilities/EN/index.htm.

North Atlantic Assembly. (1996). "Chemical and Biological Weapons: The Poor Man's Bomb." https://fas.org/irp/threat/an253stc.htm.

North Atlantic Treaty Organization. (4 September 2015). "Fighting weapons of terror." https://www.nato.int/cps/en/natohq/news_122272.htm.

North Atlantic Treaty Organization. (8 December 2017). “Weapons of mass destruction.” https://www.nato.int/cps/en/natohq/topics_50325.htm.

Organization on the Prohibition of Chemical Weapons. (n.d.). “The Chemical Weapons Convention.” https://www.opcw.org/chemical-weapons-convention.

United Nations Office at Geneva. (n.d.). “The Biological Weapons Convention.” https://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument.