ABOUT THE CIVILIAN INTELLIGENCE COMMITTEE (CIC)

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. Such matters may include information sharing, the integration of intelligence agencies with NATO, and intelligence-gathering strategies. Each NATO member country is represented on the Committee by its security and intelligence services. It is chaired on an annual rotational basis by members of the Alliance.

Delegates are recommended to come prepared with an understanding of their domestic agencies and their relationship/jurisdiction to each other. A knowledge of current affairs, especially in relation to security and intelligence, is also recommended.

TOPIC A: Creation of a modern Standard Operating Procedure for terrorist-related intelligence

Background (courtesy of the NATO Multimedia Library):
After the events of 11 September 2001, NATO has sought to increase consultations on terrorism and terrorism-related issues among its members, as well as with non-member countries. Information-sharing and, more specifically, intelligence-sharing, are key aspects of this exchange.

At the 2002 Prague Summit, improved intelligence-sharing was identified as a key aspect of cooperation among Allies. A Terrorist Threat Intelligence Unit (TTIU) was set up under the NATO Office of Security at the end of 2003, replacing a temporary cell established immediately after the 11 September 2001 attacks. The TTIU functioned for the following seven years as a

joint NATO body composed of officers from civilian and military intelligence agencies, having as its main task the assessment of the terrorist challenges, risks and threats to NATO and its member nations. To that end, the TTIU developed an efficient liaison mechanism with Allied intelligence services and national terrorism coordination centres. In addition, the TTIU shared terrorism-related information with partner nations.

Based on the decision taken at the 2004 Istanbul Summit to review the intelligence structures at NATO Headquarters, connections with partner nations have been improved. In that regard, a new intelligence liaison cell was created at SHAPE in Mons, Belgium, and an Intelligence Liaison Unit (ILU) at NATO Headquarters in Brussels.

Within the framework of the comprehensive intelligence reform at NATO Headquarters that took place in 2010-2011, the TTIU's functions were taken over by a newly-created Intelligence Unit. That transformation further enhanced the analytical approaches on terrorism and its links with other transnational threats. The current mechanism has also enhanced cooperation among the NATO civilian and military intelligence components, and preserved the previously developed mechanisms that ensure coherent intelligence-sharing with partners.

Contemporary Considerations:
The current security environment has proven that effective intelligence sharing between Allies, particularly in relation to terrorism, is more critical than ever. Key terrorism-related issues include intelligence sharing related to lone actor terrorists, foreign terrorist fighters, and imminent attacks.

Terrorist organizations, such as the Islamic State, have taken advantage of modern technology by using social media to recruit and radicalize individuals around the world. The phenomenon of self-radicalized individuals, or those who conduct terrorist attacks with only limited connection to a terrorist group, represent a concern as these individuals have a different intelligence footprint than those who connect with and possibly travel to join to fight with a terrorist organization.

Those individuals, called foreign terrorist fighters, (defined by United Nations Security Council Resolution 2178 as "individuals who travel to a state other than their states of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training…") represent a threat to NATO members both in their actions away and when they return home. Many foreign terrorist fighters die in theatre; however, those who do not represent a unique security concern, as they may have gained the skills necessary to conduct a successful attack upon their return. Tracking the movements and associations of foreign fighters represents a key issue for NATO in the near term.

Questions for consideration:

Should NATO members adapt the current Intelligence Unit framework to facilitate the rapid sharing of terrorist-related information between member states?

In light of terrorist events in Paris, what obligations should member states have to share information regarding individuals with known terrorist ties with Allies?

Should there be a standard for the quality and source of intelligence that is shared between members? If intelligence is proven incorrect, what consequences (if any,) should be placed on the state that provided the intelligence?

Should NATO consider an intelligence-sharing regime specifically targeted at tracking foreign terrorist fighters? What privacy concerns might come into play in this regime and how could NATO respond to them?

TOPIC B: Intelligence sharing with non-state actors

The global intelligence regime is still primarily an *international* model, which means that activities such as intelligence sharing are focused primarily on state-to-state cooperation. This model was influenced by the Cold War, when the primary threat came from other states. However, national security threats are more diverse since the collapse of the Soviet Union. International terrorism, insurgencies and civil wars are dominated by non-state actors who are either directly or indirectly involved in hostilities. Further than that, non-state actors such as NGOs, corporations and international organizations are increasingly becoming important global actors that can influence events. States are no longer the only relevant actors in intelligence, but there are only limited signs that intelligence practices are keeping pace.

Some areas have seen increasing recognition and cooperation with non-state actors. A notable example is the fight against terrorism financing. The intelligence regime is a combination of state actors, such as a Ministry of Finance or a Financial Intelligence Units, and corporations such as banks and other financial institutions. Most countries such as Canada have domestic laws that force financial institutions to comply with state intelligence requirements with mandatory record-keeping and reporting requirements. The banks carry the burden of absorbing the costs of compliance. The international anti-terrorism financing regime is also largely coordinated and managed through international institutions due to the international nature of financial flows, which move expeditiously from one national jurisdiction to another.

Non-state actors have also become important allies in certain conflict zones. Western militaries are increasingly using on-the-ground proxies in conflicts, which include non-state actors such as the People's Protection Units of Syrian Kurdistan (known as the YPG). Although training and military support is accepted, it is unclear whether and how far combatant non-state actors should be integrated in intelligence sharing regimes.

A key feature of *all* intelligence sharing regimes is the 'need to know' model and the 'originator control' principle. The 'need to know' model has dominated intelligence sharing and is focused on only providing information to those who, as the name suggests, need to know. The issue with this model is that the controller of the information may not be in the best position to judge what the receiver *actually* needs to know. Information siloing and an inability to connect to proverbial dots are common in this model. However, it also maintains secrecy. Alternative models have been provided such as the 'need to share' model or 'whole of government' approach to information sharing. It is unclear what degree of sharing would best facilitate cooperation between state and non-state actors.

The 'originator control' principle is another key element in intelligence sharing regimes, and it is essentially an honour system that allows the original sharer of information to stipulate how a particular piece of intelligence should be used. This honor principle works well between organizations that have an ongoing relationship and which are mutually dependent on each other. However, there is no ability to effectively enforce the originator control principle especially in relationships that are not continual or in which the receiver of information has no interested in honouring the relationship.

Question for consideration:

What national security goals could be improved by increased collaboration with non-state actors?

What should the role do non-state actors involved in hostilities have in an intelligence regime?

What responsibilities should states have if information they shared with non-state actors is used in human rights abuses?

Who should bear the cost of cooperation in intelligence sharing arrangements between states and non-state actors?

Topic C: Creation of a centralized open-source intelligence system for NATO members

Open-source intelligence (OSINT) is the use of freely available information as sources of intelligence. OSINT is usually used as a starting point before other intelligence is gathered since its freely available and therefore cost effective. Some intelligence services, such as the Dutch are legally required to canvas publically available information before engaging in any other form of intelligence gathering.

OSINT traditionally encompassed foreign newspapers, trade magazines and other sources of intelligence that could be used to enhance situational awareness. With the advent of Web 2.0, and in particular social media, the amount of data publically available for consumption has increased exponentially. Social media in particular is a rich source of intelligence – everyday over 200 million tweets are sent out on Twitter, 4 billion video views are recorded on YouTube and 250 million photos are added to Facebook. Not only is social media an abundant source of

information, it also allows unprecedented insight into citizens' lives. People share minute details about their daily routine, political views and opinions on social media site.

OSINT in general has several benefits. It is usually substantially cheaper than Human Intelligence (HUMINT) or Signals Intelligences (SIGINT) since it is less resource intensive. OSINT, due to its inherently open nature, is considered to have a lower threshold for sharing among agencies as well. Increased information sharing can lead to better cooperation and ultimately better intelligence results. OSINT can also be used to provide context or to corroborate clandestine information. Especially in the digital age, OSINT is usually the first type of information available on breaking events such as a terrorist attack.

The downsides, like the benefits, stem from the very nature of OSINT. OSINT is often incomplete and can be inaccurate. Furthermore, the volume of data poses its own challenges. Traditional methods of detecting trends or intelligence are not practical. Consequently, automated data processes need to be used to mine the information for useful intelligence. Although OSINT is "openly available" and therefore does not have any inherent privacy implications, activists are concerned about the privacy implications of compiling and mining mass quantities of data especially from social media. The issues becomes even trickier when OSINT is combined with more clandestine sources of information.

Since OSINT is freely available, a cost effective intelligence solution could be the creating of a collective NATO database that each member can access. There are several significant benefits including cost reduction and improved cooperation. However, there are also critical obstacles including the concern of where it should be located, who contributes what technology and what the security/privacy implications are for such a large database.

Questions for consideration:

What role should OSINT play in NATO intelligence operations?

What are the privacy implications of creating a centralized database of open source information that each country can contribute, access and mine?

What are the security implication?

Who should carry the cost of development and maintenance?

Who is contributing the relevant technology?

What impact would this have on non-NATO military relations? Would other partners and allies be able to access this information? For example, what are the access or sharing rights for countries such as New Zealand and Australia who are part of the Five Eye Alliance with USA. UK and Canada?

FURTHER READING

NATO Pages related to Committee Topics

Countering Terrorism

This page is a key starting resource in understanding NATO's role in relation to terrorism.

http://www.nato.int/cps/en/natolive/topics_77646.htm?selectedLocale=en

NATO Policy Guidelines on Countering Terrorism

http://www.nato.int/cps/en/natohq/official_texts_87905.htm?

NATO Partnerships

http://www.nato.int/cps/en/natohq/topics_84336.htm

Security-related resources

Jihadology

The first stop on the web for up-to-date primary source material related to radical Islamic terrorism. Analysis on material is frequently included, and the blog also runs a weekly podcast on current issues.

http://jihadology.net/

Small Wars Journal

A blog and news service focused on so-called "small wars" or non-traditional wars such as insurgencies and founded by former Marine Corps members. Maintains a fairly even global focus, with special attention paid to hotspots such as the current conflict in Syria and international terrorism.

http://smallwarsjournal.com/

Intelligence Practice

Intelligence Information: Need-to-Know vs Need-to-Share (Congressional Research Service)

https://www.fas.org/sgp/crs/intel/R41848.pdf

State of the Art: Social Media Intelligence Capabilities for Counterterrorism (Demos)

http://www.demos.co.uk/project/state-of-the-art-2015/

Intelligence Law Related Resources

National Security Law: Canadian Practice in International Perspective
A blog centered on national security law by Craig Forcese, an associate professor at the Faculty of Law (Common Law Section) at the University of Ottawa. The blog also discusses relevant international law concepts related to security and intelligence.
http://craigforcese.squarespace.com/national-security-law-blog/

Lawfare: Hard National Security Choices

A blog centered on security and defense issues published in cooperation with Brookings Institute and mostly run by Harvard Law faculty. The focus is primarily American intelligence and defense law, however it does occasionally cover other countries including Britain and France.

https://www.lawfareblog.com/

Just Security

A blog and news bulletin related to security law and policy that is run out of the Center for Human Rights and Global Justice at New York University School of Law. The focus is primarily American national security, but it frequently covers international security issues. The blog places a strong emphasis on human rights law. It provides a daily newsletter with a curated list of security news.

https://www.justsecurity.org/

EJIL Talk!

The official blog of the European Journal of International Law. The blog takes a European perspective on several international law issues, including surveillance and terrorism law and policy.

http://www.ejiltalk.org/