GLOBSEC
IDEAS SHAPING THE WORLD

NATO'S INTELLIGENCE ADAPTATION CHALLENGE

Artur Gruszczak

www.globsec.org

NATO'S INTELLIGENCE ADAPTATION CHALLENGE

Artur Gruszczak (Jagiellonian University, Krakow, Poland)

INTRODUCTION

NATO's adaptation to the contemporary security environment has been one of its most serious and toughest challenges. Its 29 member states continue to address the exceptionally demanding and complex task of transforming a transatlantic security organisation into a robust, effective and agile alliance capable of securing national interests through multilateral initiatives, readiness, joint operations and common financial efforts. Today, state and non-state actors as well as international organisations tend to acquire policy-relevant knowledge as a key factor in handling the most important and challenging security issues . The ability to build and develop a full strategic awareness through complete and multi-layered common situational pictures is considered as a basic requirement of the planning and conduct of military operations as well as gaining influenceon or control of the security environment.[1] Strategic awareness is required for effectivenes of decision making and chain of command where information and knowledge are placed and condensed in the form of intelligence.

For centuries, it has been widely acknowledged that intelligence is a specific type of state activity that seeks to prepare its institutions and forces for a large array of threats and hostile measures posed by enemies of the state. It also has been assumed that the building of an efficient intelligence apparatus is a difficult, responsible, long-term process requiring heavy investments in knowledge, technologies, equipment and human resources. The growing proliferation of threats and internationalisation of national security interests stimulated the emergence of international intelligence cooperation arrangements built on transverse connections between various stakeholders seeking to integrate scattered sources of information and knowledge on the basis of shared interests, values and objectives. NATO is no exception and its evolution as a transatlantic security community has illustrated the growing relevance of intelligence for its overall performance.

This analytical paper seeks to examine NATO's intelligence resources, assets and capabilities against the backdrop of its security environment, strategic concepts and international collaborative efforts. It assesses the Alliance's adaptability to the dynamic expansion of information production and diffusion in the context of strategic forecast, situational awareness and operational planning. It also looks at NATO's readiness to utilise potential synergetic intelligence opportunitiesin cooperation with the European Union. The last part contains conclusions and recommendations.

This study is based exclusively on non-classified resources: open sources of information, scholarly resources, analytical papers, the author's expertise and scholarship.

INTELLIGENCE IN THE CONTEMPORARY SECURITY ENVIRONMENT

Despite its broad application, the concept of intelligence contains a core element which is also present in NATO vocabulary. This is the collection, processing and analysis of data and information for the purposes of knowledge production and dissemination to relevant state authorities in order to improve or optimise decision-making processes. In the specific case of NATO, as well as other international security organisations, intelligence is bound with the state and its fundamental tasks of maintaining order, security and development. State institutions

[1] M. Guha, Reimagining War in the 21st Century. From Clausewitz to network-centric warfare, London – New York: Routledge, 2011, pp. 117-18; DJ Lonsdale, The nature of war in the information age: Clausewitzian future, London – New York: Frank Cass, 2004, pp. 41-43.

are authorised to acquire, gather, process and analyse information particularly relevant for the national interest and state objectives, including secret information acquired by way of clandestine operations. Since intelligence processes (cycles) involve a multitude of different actors (individuals, groups and organisations) acting as passive sources of data and information, an intelligence apparatus tends to consolidate in a community connecting its parts on the principles of accountability, loyalty, and – quite often – secrecy. Intelligence communities emerge both at national and international levels. Therefore, NATO can be seen as an international intelligence community because the national security interests of its members and international security cooperation arrangements have highlighted common risks and threats calling for concerted efforts in the areas of early warning, situational awareness, threat assessment and risk analysis.

When it comes to a transregional security alliance, as NATO is, intelligence cooperation is substantiallypoliticised and often subject to strategic guidelines reflecting vital national security interests. Quite often heterogeneitymay hinder an efficient and flexibleresponse to emerging threats, problems and challenges. This is particularly significant in the context of the dynamic development of intelligence technologies and extension of intelligence fields. Non-traditional intelligence collection disciplines (such as: social media intelligence; research-originating intelligence; cyber intelligence; situational intelligence; and crowdsourcing intelligence) have been expanding rapidly, making it problematic for intelligence communities and their services to adjust to the dynamically changing social, technological and cultural determinants of contemporary intelligence security. A complete adaptation to new intelligence requirements by a transregional security organisation, such as NATO, is extremely difficult, if not impossible, in a short span of time.

A functional differentiation of NATO intelligence assets and capabilities results from the Alliance's strategy (strategic concept), organisation and institutional structure (civilian and military branches; two strategic commands), decision-making rules and procedures, the nature of the security environment (in its regional and global dimensions), as well as forms and types of active engagement in security problem-solving. From a general perspective, NATO's intelligence capabilities should correspond with four principal objectives:

- Contributing to global peace and regional stability;
- Ensuring and enhancing national security of member states;
- Consolidating NATO's position as a security provider and peacemaker;
- Supporting operational activities in the framework of military missions and operations.

Respectively, these capabilities should include:

- Strategic analyses, threat assessments and global estimates built on all-source analysis based on open-source information and data;
- Tailored analyses and reports on national security of member states (individual countries or regional groups) containing elements of warning, crisis management and threat assessment, built on open sources as well as civil and military intelligence deliveries from the Allies and NATO partners;
- Strategic awareness and situational assessments taking advantage of NATO intelligence fusion capabilities, geospatial surveillance, airborne reconnaissance (UAVs) and intelligence sharing with NATO partners (esp. the European Union);
- Operational and tactical intelligence in support of planned and/or ongoing operations, exploiting available intelligence, surveillance and reconnaissance (ISR) capabilities, real-time intelligence deliveries and all-source analyses of scattered data originating in the realm of missions and/or operations.

NATO'S INTELLIGENCE ASSETS

NATO as a multinational alliance has to develop adequate intelligence capabilities on the basis of the member states' contributions as well as its own assets. The heterogeneous architecture and complex multi-layered structure of the Alliance is particularly challenging when it comes to data acquisition, information gathering and intelligence production and sharing. Scattered sources of information, diversified tools of gathering, processing and analysis and different national inteligence cultures have posed a considerable restraint for coordinating international cooperation within NATO and developing autonomous intelligence capabilities. Moreover, the essential division of intelligence into non-operational (strategic and situational intelligence) and operational (tactical) areasbrought about a deep imbalance. The Alliance attributed the fundamental importance to intelligence, surveillance and reconnaissance (ISR) as elements of preparedness and planning of its operations and missions . At the strategic level, intelligence production and sharing sought to enhance defence and security capacity building in the face of common threats.

Strategic intelligence supports NATO's main bodies, such as the North Atlantic Council, Secretary General and Military Committee, in building strategic awareness and facilitating decision-making processes. This was initially provided by the Situation Centre, which was created in 1968 as a unit answerable to the Secretary General and connecting civilian International Staff and the International Military Staff (IMS). The latter's Intelligence Division occupied the central position in NATO Headquarters, coordinating through the Current Intelligence and Warning Branchthe production and dissemination of NATO strategic intelligence products, operating intelligence information services, facilitating intelligence reporting by the Alliance's member states and giving strategic warning.

In the wake of the 11 September 2001 attacks on the United States, the fight against terrorism was placed at the top of NATO's agenda. A transformation and adaption of intelligence structures and capabilities took place within NATO, seeking to develop analytical tradecraft and improve intelligence sharing, with particular reference to threats from terrorism, WMD and local conflicts. NATO put forward the concept of an integrated platform for intelligence cooperation, including The Terrorist Threat Intelligence Unit (for analysis of terrorist threats), Network-Enabled Capabilities (a communication and information infrastructure for networked information exchange for the sake of better situational awareness and faster decision making),an Intelligence Fusion Centre (a unit providing warning supporting the planning and execution of NATO operations) and a new NATO Intelligence and Warning System (NIWS) based on military and non-military risk indicators and early warning of potential sources of instability, crises or risks jeopardising NATO strategic security interests.[2]

Despite numerous post-9/11 efforts and achievements, some factors still hindered the scope and substance intelligence cooperation and hampered genuine progress in this area of NATO's performance. NATO Heads of State and Government gathered at the Lisbon Summit in 2010 highlighted the importance of enhanced information and intelligence sharing within the Alliance to better predict and prevent crises, terrorist threats, transnational criminal activities and cyber threats. A comprehensive reform of the NATO intelligence sector was put in place in 2010-2011 and brought about considerable improvements in the quantity and quality of interinstitutional coordination, information analysis and intelligence sharing. The Intelligence Steering Board (ISB) was tasked with overseeing and developing strategic intelligence requirements. The Intelligence Unit (IU) was created at NATO headquarters as a joint civilian and military body supporting decision makers with intelligence-based analyses and assessments, produced in close cooperation with IMS Intelligence Division. The Intelligence Liaison Unit improved the mechanism of civilian and military intelligence sharing with partners.

In the operational dimension, Allied Command Transformation (ACT) increased and improved strategic analyses of and forecasts regarding intelligence concepts and capabilities. Allied Command Operations (ACO) bolstered intelligence support for operational planning and execution, uprading communications and information systems for the purposes of information exchange and intelligence sharing. In this regard, the development of Joint Intelligence, Surveillance and Reconnaissance (JISR) was recognised as one of the vital elements of military operations, including pre-operational capabilities and enhanced situational awareness. In February 2016, an Initial Operational Capability for JISR was declared, comprising enhanced interconnectivity across NATO

[2] S. Santamato with M.-Th. Beumler, The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions, INSS Strategic Perspectives, No. 13, Washington, D.C.: National Defense University Press, 2013, p. 20.

communication and information systems, training and expertise among personnel, and updated procedures for automated information management and sharing.

At the 2016 Warsaw Summit, Heads of State and Government, fully aware of the complexity of the information environment and indispensability of new solutions to intelligence deficits, agreed to set up a new Joint Intelligence and Security Division (JISD) led by a newly established Assistant Secretary General for Intelligence and Security. This position is empowered to provide broad strategic guidance to the North Atlantic Council and Military Committee on intelligence and security matters as well as streamline and coordinate the Alliance's analysis and assessment capabilities. An Intelligence Production Unit within JISD was tasked with strategic all-source intelligence support for key civilian and military decision makers in NATO HQ as well as the production of intelligence available for member states.

NATO-EU INTELLIGENCE COOPERATIVE FRAMEWORK

Despite close relations between both organisations, double membership and functional bonds (NATO has provided the foundation of the collective defence of EU member states), intelligence cooperation was long absent from Euro-Atlantic relations. Permanent underdevelopment of EU military capabilities and limited scope of activities (crisis management, peace operations, humanitarian missions) created a wide gap between the EU and NATO under strong US leadership. It was only in the early 2000s that both organisations began regular consultations in working groups, including matters of information security and exchange of classfied documents. An interim security arrangement on access to and exchange of classified information and related material was concluded in May 2000. Following 9/11 EU countries started to provide US authorities with valuable counterterrorism information and expertise, including intelligence products. The EU's plans to launch first missions and operations under the European Security and Defense Policy (ESDP) were backed by the US and resulted in the so-called 'Berlin Plus' comprehensive EU–NATO framework for permanent military cooperation.

As the first planned EU mission in the Balkans implied a takeover from the NATO-led forces, in March 2003 NATO and the EU signed an agreement on information security, complementedby provisions on common standards for the protection of classified information.This agreement established common safeguards and institutional responsibility for managing the delivery ofclassified information, set standards for security clearance, registry systems, encryption of electronic transmissions and control over the EU–NATO classified information exchange system.

Although the EU was lagging behind NATO's military assets and capabilities, its achievements in intelligence cooperation were unjustly underestimated by the US and its non-EU allies. European countries started common efforts at the beginning of the 1990s, focusing on geospatial intelligence and strategic awareness. They established an intelligence division and an early warning unit in military structures, and later set up a situation centre (SITCEN) responsible for monitoring the security landscape and preparing situational assessments, especially in the field of ESDP and during crisis-management operations. In 2007 a Single Intelligence Analysis Capacity was created with the aim of pooling civilian intelligence obtained by SITCEN with early warning and situational assessment provided by military intelligence services. Following the Lisbon treaty reform, in 2012 SITCEN was transformed into the EU Intelligence Analysis Centre (INTCEN)[3] and tasked with situation and risk assessments as well as special reports and in-depth analyses based on available open-source material, as well as military and non-military intelligence from member states and diplomatic reports.

Despite the steady development of intelligence capabilities of NATO and EU, exchanges of information and intelligence between both organisations have been difficult and annoying. Deficiencies and shortcomings of intelligence sharing at the strategic level, as well as certain problems in operating communication and information systems, effectively hampered interinstitutional intelligence cooperation. One of the impeding factors was US scepticism about sharing sensitive NATO information and intelligence with EU bodies. Given that the United States is the main originator of the Alliance's strategic as well as operational/tactical intelligence, any substantial exchange of sensitive information or intelligence sharing between NATO and EU is subject to US consent. The

[3] In July 2015 INTCEN was renamed EU Intelligence and Situation Centre.

cases of maritime operations conducted 'jointly but separately' by NATO and EU forces render a pessimistic account. The counter-piracy operations around the Horn of Africa conducted by both organisations (NATO's 'Ocean Shield' and EUNAVFOR's 'Atalanta') have experienced serious limitations, red lines and practical barriers to information exchange and intelligence sharing.[4]

In this context, the NATO-EU Joint Declaration adopted in 2016 in Warsaw[5] is a promising step towards an intensified collaborative approach to the dynamic complex security environment determined by non-traditional threats, terrorism and extremism, hybrid warfare and offensive cyber operations. The new institutional setup in NATO, as well as guidelines adopted in Warsaw, open up new opportunities for wider information sharing for the purpose of better situational awareness, more accurate threat assessments and stronger resilience to non-military threats, such as terrorism and organised crime. In addition, hitherto informal EU-NATO intelligence sharing could at least be partially redirected towards the established institutional framework.

CONCLUSIONS AND RECOMMENDATIONS

The 360-degree security and defence environment in which NATO has been operating for years determines the Alliance's adaptability and capacity to respond to common threats and other challenges. In their statements of 25 June 2015 NATO Defence Ministers acknowledged that „... a substantial, far-reaching adaptation of NATO's military strategic posture is/was required to respond to the changed security situation."[6]

An appropriate strategic awareness is the crucial factor in setting in motion decision-making processes which bring about a firm and adequate response to emerging security dilemmas. In all five dimensions of the contemporary security environment (land, air, sea, space, cyber) intelligence activities, including surveillance and reconnaissance, are essential for conducting military operations and building strategic situational awareness of threats and opportunities.

Recent decisions and undertakings have augmented the need for comprehensive and accurate intelligence. The deployment of Very High Readiness Joint Task Force brigades on NATO's eastern flank requires enhanced situational awareness capabilities in order to monitor military and political developments beyond the borders of its eastern members and work out an effective response to hybrid threats in advance, given the conventional vulnerabilities of the Baltic theatre and other regional tensions. NATO also has to adapt to the growing challenges and threats emerging from the south, namely the Mediterranean and Balkans.

NATO's intelligence adaptation should take into account the following observations:

1. NATO will continue to operate in an increasingly complex security environment saturated with gigantic amounts of data and information. Irrespective of the fact that IT technologies are becoming increasingly efficient and artificial intelligence solutions are entering the analytical stage, any intelligence cycle can be closed solely by human resources, i.e. skilled analysts with considerable experience and appropriate expertise.

2. New security challenges, such as terrorism, cyber operations or illegal migration, require a holistic yet differentiated approach on the part of NATO institutions as well as member states' relevant authorities and services. NATO's role in countering threats and responding to challenges is multifaceted and draws on experience gained in its every-day activities as well as military operations, including mechanisms for sharing intelligence and developing analytical capabilities.

---

[4] C. Gebhard and S.J. Smith, 'The two faces of EU–NATO cooperation: Counter-piracy operations off the Somali coast', Cooperation and Conflict, 2015, 50 (1), p. 115.

[5] 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, Warsaw, 8 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133163.htm.

[6] Statement by NATO Defence Ministers, 25 June 2015, http://www.nato.int/cps/en/natohq/news_121133.htm?selectedLocale=en.

3. Intelligence capabilities, resources and assets are relatively big in total, but they are kept within member states' national intelligence communities. Optimisation of their use requires a deep mutual confidence based on accountability, reliability and proportionality.

4. The United States has been a 'natural' leader predestined to shape and determine NATO intelligence capabilities because of its resources, capacities, assets and global reach.Some intelligence capacities (global signals intelligence, satellite-based sensors) are almost exclusively owned by the US. Therefore, NATO's adaptation is subject to US policy towards the Alliance as well as willingness to share and pool assets in cooperation with other Allies.

5. OSINT (open-source intelligence) deliverables barely fill the gaps left by national intelligenceservices. 'Hard' intelligence has been relatively limited and reduced to operational ISR requirements.

6. Secure communication systems enabling transfer of classified information and sharing of intelligence products have been largely underdeveloped. Despite interoperability between Secure Communications Interoperability Protocol (SCIP) protocols and Active Network Infrastructure at NATO HQ, distinct Communities of Interests within NATO may experience deficits of intelligence workflow.

In response to the abovementioned considerations, the following recommendations are offered:

1. Enhanced intelligence efforts taken individually by the Allies as well as made collectively on the NATO level should occupy a prominent place on the Alliance's agenda.

2. NATO should develop a specific intelligence tradecraft adequate for civil and military structures. For this purpose, it should implement appropriate technical and technological solutions to improve the flow of data and information and secure their transmission and storage.

3. NATO should help overcome national reservations and encourage member states to share an even greater amount of intelligence assets and resources, particularly when it comes to prioritised intelligence needs and operational requirements.

4. Civil-military intelligence cooperation, inter-agency connections,fusion mechanisms and all-source analytical solutions should be regardedas structural and functional components of NATO's intelligence network architecture. Fusion capabilities should be developed and consolidated in the Fusion Centre. EU experience of sharing not only civil and military intelligence but also criminal intelligence should be taken more into account, especially with regards to terrorism and transnational organised crime (WMD materials and precursors, migrant smuggling, illegal arms trade).

5. Military intelligence should underpin all-source analysis, being a core part of situational awareness building as well as operational planning and execution. Open sources of data and information should support intelligence production with regards to mass communication and social media, where large-scale data mining and processing is required. Knowledge created by academia and expertise built by analytical institutions may enrich analytical input and enhance the quality of intelligence outcomes.

6. NATO should develop and strengthen its institutional framework for intelligence capabilities, especially around the new Joint Intelligence and Security Division (JISD) and Assistant Secretary General for Intelligence and Security.

7. Cooperation between JISD and the Civilian Intelligence Committee (formerly the Special Committee) representing national civilian security and intelligence services should be fundamental for managing effectively such issues as counter-terrorism, counter-intelligence and prevention of non-traditional threats.

Polus Tower II
Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 321 37810
info@globsec.org

www.globsec.org