Intelligence Sharing Practices in International Organizations: Developing a Theoretical Framework for Analysis - A Case Study of NATO

Language and International Studies, English
5th Semester Project
Aalborg University

Kathrine Schütz (20194321)

Kirsten Jæger

January 9th, 2023

Characters: 47 639

Abstract

This paper seeks to propose a new theoretical framework for analyzing intelligence sharing practices in international organizations. Based on presumptions from regime theory, three propositions that can be used for analysis will be presented, developed from a combination of theories on optimum intelligence reach (Svendsen, 2012), delegation in international organizations (IO) (Hawkins et al., 2006), and hierarchy in intelligence sharing (Walsch, 2010). The applicability of the framework is demonstrated by an analysis of intelligence sharing practices in NATO. This analysis shows a discrepancy between NATO's official ambitions for the organization's intelligence sharing practices and the actual intelligence sharing that takes place. Furthermore, the ill-defined benefits and the potentially high cost of delegating authority to the agent prevent the states from giving NATO autonomy in the intelligence area. Subsequently, the lack of trust toward NATO's intelligence sharing mechanisms, combined with the US-dominated power imbalance that exists within NATO makes it more desirable for states to engage in smaller hierarchical fora for intelligence sharing. The proposed framework for analysis presented here can hopefully inspire further development and expansion of the framework, as well as encourage future analyses of intelligence sharing practices in other IOs.

Contents

Introduction

"The biggest impediment to all-source analysis (...) is the human or systemic resistance to sharing information"

(National Commission on Terrorist Attacks Upon the United States, 2004, p. 416).

This was one of the primary conclusions from the final report in the evaluation of the intelligence failures that led to the 9/11 terrorist attacks on the United States. Since 9/11, efforts to improve intelligence[1] sharing practices in the Western world have increased dramatically, with a particular focus on strengthening intelligence cooperation within the North Atlantic Treaty Organization (NATO) as well as between NATO member states and countries outside the Alliance (Tuzuner, 2010, p. 56). While intelligence sharing has gained much attention in recent decades in the academic community, the focus has rarely been on intelligence sharing practices in international organizations (IO). This paper seeks to fill this gap in the literature by presenting a proposition for a theoretical framework for analyzing intelligence sharing practices in IOs. I aim to present a brief analysis of NATO's intelligence sharing practices, using the framework developed in this paper, in order to demonstrate its applicability. Lastly, I will present my findings from the analysis and discuss how the theoretical framework can be used in other contexts, with the hope of inspiring further research on this topic and in its development as a tool for analysis.

Data

Mainly three categories of literature have been used as data for this paper: existing theoretical literature on intelligence sharing and organization theory; academic papers and analyses of intelligence sharing, specifically for IOs and NATO; and a number of central papers that give insight to relevant NATO policies. In my review of the literature, I have mainly used large, well-known search engines and databases such as Google, Google Scholar, DuckDuckGo, Aalborg University's (AAU) online library Primo, in combination with AAU's library. For the online research and collection of literature, I have used keywords in relation to this paper's topic, such as "intelligence sharing practices", "intelligence and organization theory",

[1] One definition of intelligence, as presented by Walsch (2010) states that "(...) intelligence differs from raw information, or 'facts,' in that intelligence analyzes raw information, attempting to place it in a proper context and to use it to draw conclusions about those attributes of other actors or the state of the world that are not directly observable" (p. 11).

"intelligence sharing in international organizations", "NATO intelligence sharing" and combinations hereof. Furthermore, I have used search operators extensively to further narrow down the scope. In a later section I will provide a short literature review of the current (public) knowledge within this area, and subsequently argue for why the topic of this paper could contribute to filling a gap in the literature. However, the fields of intelligence and especially organization theory are vast and well-researched, and it can therefore not be ruled out that there have been other attempts at developing a framework for analyzing intelligence sharing processes in IOs, such as the one I aim to present here.

Analytical framework

In the following, I aim to develop a framework for analyzing intelligence sharing practices in IOs. Presumptions from regime theory will first be outlined, followed by a short literature review on existing academic research on intelligence sharing. Based on this, I present the theoretical background for developing the three propositions that I will argue to serve as a framework for analysis.

Regime Theory

In this paper, the overarching analytical approach will be based on presumptions from regime theory. Regime theory, often used synonymously with neoliberal institutionalism, is a state-centered theory that perceives states as rational actors who seek to maximize their self-interest through cooperation (Bradford, 2007, p. 3; Keohane, 1989). Regimes in this regard are to be understood as a set of "principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations" (Krasner, 1983). These emerge from state interests, and depending on which area of international politics, one can discuss the respective regimes[2] of relevance. The collective security regime, which will be the point of departure for this paper will be elaborated further in the analysis. As will be demonstrated in the following, this notion of states engaging in cooperation in order to maximize their self-interest is central to this paper and the theoretical framework built around it.

[2] As accounted for by Bradford (2007), well-known and well-studied regimes include, but are not limited to, economic regimes, environmental regimes, human rights regimes, and collective security regimes, of which this paper will center around the latter.

Literature Review on Intelligence Sharing Theory

Intelligence has long been a subject of research, and, along with globalization, so has the topic of intelligence sharing practices between nations. Due to the paradox between the secretive nature of the intelligence communities and the cooperative nature of globalization, there have been numerous attempts to theorize around the dynamics of international intelligence sharing practices. In the following, I aim to provide an overview of the most central theoretical developments in the literature in this area since 9/11.

Although many scholars treat intelligence sharing on an international level, few attempt to provide a perspective on intelligence sharing in international organizations. Scholars have highlighted the importance of gaining further insight into international intelligence cooperation, especially given the fact that a significant part of the cooperation is driven by informal alliances, informality, and individual cooperation (Svendsen, 2012, p. xix; Tuzuner, 2010, pp. 61 & 148). Many current perspectives provided on intelligence cooperation come from academics, former intelligence practitioners, and analysts who attempt to shed light on the importance of international intelligence cooperation, as well as providing suggestions to how this should be accomplished (see for instance Boatner, 2000, p. 91; Newton, 1991; Gordon, 2017; Svendsen, 2012, p. xix). Likewise, many scholars have adopted the perspective that secrecy and mutual trust play a decisive role in intelligence cooperation (see for instance Clough, 2004, p. 603; Hardin, 2002; Lander, 2004; Lefebvre, 2003, pp. 528-29; Reveron, p. 456; Walsch, 2010, p. 14). While this is an important aspect to consider, as will be elaborated in the next section, other scholars question this, and present alternative explanations for understanding intelligence cooperation dynamics, for instance by applying a lens of hierarchical relationships (Walsch, 2010, pp. 27 & 139). All these perspectives provide insight to the practical (dys-)functionalities of intelligence cooperation, but once again rarely relate it to the IO level.

Organization theory and intelligence sharing *have* been combined, although mostly adopting a national-level perspective. One such perspective is provided by Hastedt and Skelley (2008) who draw on a wide range of organization theories, such as classical bureaucratic theory, organizational economics, and environmental perspectives on organizational structure and behavior in order to gain insight into the effects of organization reform on preventing intelligence failures on a national level (p. 114). Drawing on principal-agent theory, they argue that the nature of intelligence organizations' work is in many ways paradoxical (Hastedt & Skelley, 2008, p. 126). These paradoxes include that:

> "[s]ecrecy is highly valued and argues for compartmentalization which, in turn, limits flexibility and information flow while increasing moral hazard and transaction costs. (...) Loosely structured arrangements provide for initiative but invite willful or inadvertent goal displacement"
>
> (Hastedt & Skelley, 2008, p. 127).

These paradoxes emerge from the fundamental secretive nature of intelligence and, while treated on the national level in the literature just presented, they should also be kept in mind when analyzing intelligence sharing practices in IOs.

The brief outline demonstrated here is a far-from-exhaustive list of perspectives taken on intelligence cooperation, and merely a selection of those I have deemed most relevant for this paper. Extensive studies exist on this topic providing insight into bilateral and multilateral intelligence cooperation; what should be done to improve intelligence cooperation in international organizations; and how the roles of secrecy and mutual trust are very often seen as a barrier to effective intelligence sharing. However, while many analyses build on cases from bilateral relationships as well as international organizations, there appears to be very little literature that combines research on intelligence sharing practices with organizational theory, let alone frameworks that can be used as tools for analysis on this matter. Thus, there is a gap in the research in the area of intelligence sharing practices in international organizations. The reason why this is important is that, while international intelligence sharing practices between nations are also very important topics, these alone rarely consider the shifting role and delegation of responsibilities that happen when a state becomes a part of an international organization. The value of such a framework will be elaborated on later, when I attempt to propose a model for analysis that builds on existing theoretical approaches to intelligence sharing practices in IOs.

Secrecy and Mutual Trust

As mentioned, mutual trust (or lack thereof) plays an important role in intelligence sharing. Secrecy and confidentiality are integral aspects of the intelligence community, primarily due to source-protection concerns (Aden, 2018). When secrecy is such a fundamental necessity in information sharing in this field, mutual trust often automatically becomes the logical foundation for cooperation (Hastedt & Skelley, 2008, p. 127; Maras, 2017). Therefore, as Walsch (2010) observes, "[t]his secrecy means that two common explanations of cooperation - mutual trust between participants, and the developments of institutions and practices

designed to provide information about the compliance - are unlikely to be very effective in the area of intelligence" (p. 5). Thus, the difficulty (arguably 'impossibility') of obtaining a level of complete mutual trust between intelligence agencies serves as a main barrier for intelligence sharing, because of the fear of defection[3]. In sum, the secretive nature of intelligence, the fear of defection, and the subsequent importance of mutual trust constitute significant barriers to intelligence sharing. As will be demonstrated later, this is not an insurmountable obstacle, but it is nonetheless central to consider when analyzing intelligence sharing practices.

Intelligence Sharing Practices in IOs: A New Framework for Analysis

The primary purpose of this theoretical framework is to develop a tool for analyzing and understanding intelligence sharing processes in IOs. As previously outlined, the fundamental presumption for this framework is centered around states as rational actors who seek to maximize their self-interest through cooperation. As such, when states engage in cooperation, they will seek to maximize the benefits as well as minimize the costs involved in the agreement. This notion is particularly relevant for the intelligence area, and subsequently when it comes to the question of intelligence sharing practices. Due to the secretive nature of intelligence and the severity of the costs of defection, states will strive to obtain an equilibrium between the costs and the benefits involved when engaging in intelligence sharing cooperation. There are several ways in which states can obtain this equilibrium, and understanding these dynamics for intelligence sharing may help us gain insight into the practices that take shape inside a given IO. In the following I aim to provide an understanding of how states may seek to obtain this cost-benefit equilibrium when engaging in intelligence sharing cooperation. Three perspectives are particularly relevant for this framework, being 1) Adam Svendsen's notion of optimized intelligence outreach, 2) principal-agent theory's perspective and the role of delegation, and 3) James Walsch's insights into the role of hierarchy in intelligence sharing. I will conclude this outline by developing a number of propositions that can be used as guidance for analyzing intelligence sharing practices in IOs.

[3] Defection is here to be understood as actors "violating their agreement to cooperate, for example, by manipulating shared intelligence to serve their own ends." (Walsch, 2010, p. 5)

Optimum Intelligence Outreach

Closely related to the notion of a state's wish to obtain a cost-benefit equilibrium when engaging in cooperation through an IO is Adam Svendsen's (2012) concept of optimum intelligence outreach. Svendsen (2012) presents a proposition for analyzing intelligence cooperation dynamics through the lens of the theory of optimized intelligence outreach. Although Svendsen's (2012) perspective does not concern itself specifically with the IO aspect of analyzing intelligence cooperation, it is central in understanding why and how states enter into intelligence cooperation with one another. Therefore, I will first present a brief overview of the most relevant aspects of Svendsen's (2012) framework and subsequently argue why I believe these to be relevant for my analysis.

'Intelligence liaison' - a concept that is essential for understanding what Svendsen (2012) builds his argumentation on – is defined as "relevant communication, cooperation and linkage between a range of actors (...) on intelligence matters - essentially exchanging or sharing information (...)" (p. 13). As he points out himself, the term 'intelligence liaison' is therefore also coterminous with 'intelligence sharing' (p. 12). While his definition reaches wider than the sole aspect of intelligence sharing, this will be the focus of this paper. Moreover, he argues that international intelligence liaison and the preservation of confidentiality (i.e., secrecy) are paradoxical entities, and while there have been numerous attempts to set up mechanisms to facilitate intelligence sharing and simultaneously ensure that confidentiality measures are upheld, their effectiveness is debatable (Svendsen, 2012, p. 14). Rather, the ineffectiveness of the mechanisms and the distrust towards these are often illustrated by the many informal intelligence sharing arrangements that are made outside the officially established mechanisms (Svendsen, 2012, p. 14). Thus, one must also consider the informal arrangements that exist parallel to the officially established mechanisms in order to gain a thorough understanding of the dynamics at play.

Closely related to the concept of intelligence liaison, and central to understanding Svendsen's (2012) theory of optimized intelligence outreach, is the concept of 'reach dynamics' (p. 13). In short, 'outreach' in reach dynamics can be understood as "reach further than (...) the extent of reaching out (...) an organization's involvement with the community" (Svendsen, 2012, p. 13; Oxford English Dictionary). Based on this, Svendsen (2012) argues that intelligence liaison can be understood as "a covert form of 'outreach'" (p. 13). By association, the phenomena of 'overreach' and 'underreach' relate to the level of reach exercised in the intelligence community in relation to information sharing. In presenting the terms of

‘overreach’ and ‘underreach,’ there is an implication of levels of reach that become problematic for the intelligence sharing processes, namely if sharing becomes overextended and thereby uncontrolled (overreach) or if sharing becomes too limited, thereby hampering effective intelligence operation (underreach) (Svendsen, 2012, p. 13).

Svendsen (2012) presents his primary argument, being that the theory of optimized intelligence outreach is the theory that provides the best explanation for intelligence sharing dynamics (p. 154). Furthermore, both ‘overreach’ and ‘underreach’ are undesired by intelligence practitioners, as these have the potential to inflict disastrous damage in both instances (Svendsen, 2012, p. 110; Sims, 2005, p. 17). Following this argument, Svendsen (2012) asserts that intelligence practitioners will always seek a “(…) ‘holy grail’ of intelligence liaison, namely: *optimum intelligence and security outreach*” (p. 153). In other words, the desired goal for the actors is therefore to obtain a form of intelligence equilibrium, i.e., ‘optimum outreach’, when it comes to intelligence sharing and cooperation; not sharing too much or building too open intelligence liaisons (overreach), while at the same time ensuring a fruitful cooperation and mutually beneficial intelligence sharing practices (avoiding underreach) (Svendsen, 2012, p. 110). Translating this into the terms already introduced at the beginning of the theoretical framework, the ‘optimum outreach’ explained here thus stems from the same presumption of actors striving for a cost-benefit equilibrium in a given intelligence cooperation case, thereby maximizing their self-interests by means of cooperation.

By uncovering the reach dynamics at play in an IO, we thus gain an understanding of the intelligence sharing practices in the organization which in turn helps us understand why and how states enter into intelligence cooperation with one another.

Principal-Agent Theory: Combining Intelligence and Organization Theory

In order to be able to analyze the dynamics of intelligence sharing practices in IOs, it is necessary for us to understand the authority that has been given to the IO by its members. A widely used and well-known framework for analysis is principal-agent (PA) theory. In the following, PA theory in relation to IOs will be briefly outlined with the purpose of demonstrating how states seek to obtain a cost-benefit equilibrium when delegating authority to an IO.

Following the definition by Hawkins et al. (2006), PA theory is useful for understanding “the strategic interaction between these actors [principals and agents] and to

help make sense of the outcomes we observe" (p. 7). The concepts of *principals* and *agents* are here to be understood as an actor, i.e., the *principal*, delegating authority to an *agent*, thereby giving the agent permission to act on behalf of the principal (Hawkins et al., 2006, p. 7). Thus, when putting this in the perspective of IOs, the member (state) constitutes the principal, who has delegated authority to the agent, i.e., the IO.

In relation to the benefits of the principals delegating to IOs as agents, the authors state that "the larger these benefits, the greater the likelihood that states will choose to delegate to an IO" (Hawkins et al., 2006, p. 23). This aspect is particularly important to specify in relation to establishing a framework for investigating intelligence sharing processes. As Hawkins et al. (2006) state, the authority granted to the IO is conditional. While their logic is based on the notion of 'the greater the benefit, the greater the likelihood of delegation', one can also presume that the inverse applies, i.e., 'the greater the cost, the lower the likelihood of delegation'. As mentioned, this paper's primary focus is centered around the topic of intelligence sharing practices and when researching this, secrecy and mutual trust are crucial aspects to consider. Therefore, when considering the delegation of authority to an IO in relation to intelligence sharing, trust becomes central to the evaluation of the level of delegation being dependent on the extent of the benefits gained through the cooperation.

Hawkins et al. (2006) attempt to generalize this notion of delegation, arguing that one predominant aspect is whether this delegated authority allows the agent, i.e., the IO, to act autonomously (Hawkins et al., 2006, p. 258). This point is especially relevant for the analysis of intelligence sharing practices, due to the secretive, resource-centered, and often time-sensitive nature of the intelligence work. For these reasons, the barriers for delegation in intelligence are arguably even higher than for other areas of delegation in IOs. As such, for the principals to delegate authority to the agent, i.e., increase their level of autonomy in the intelligence area, the principals require relatively larger benefits in order to minimize the cost of the agent engaging in behavior that is undesired by the principal. Similarly, the principal's sensitivity toward the costs is arguably higher in the intelligence area, and the principal's overall incentive to delegate to IOs is therefore low to begin with. Expanding slightly on this, one could consider it as such: The larger the benefits and the lower the cost involved in engaging in an intelligence cooperation in an IO, the greater the likelihood that states will choose to delegate to an IO, and by extension: The more capable the IO is of fulfilling its mandate.

Policy Externalities

Complementary to the points above, Hawkins et al. (2006) also touch upon the role of policy externalities as an encouragement for states to engage in cooperation in an IO. They argue that principals are more likely to engage in cooperation and thus delegate to an IO if there are large policy externalities involved (Hawkins et al., 2006, p. 15; Milner, 1997, p. 44; Lake, 1999, p. 44-52). Policy externalities are here to be understood as unintended consequences of a cooperation that may bring effects – positively and/or negatively – outside of the intended cooperation agreement. This concept similarly applies to intelligence sharing in the sense that states may choose to delegate authority to an IO if they estimate that they can minimize policy externalities and thereby maximize its self-interest through cooperation.

Thus, by using PA theory in an analysis of intelligence sharing practices in IOs, we become able to establish the sphere of the delegated authority and responsibility to the IO in the intelligence area. Additionally, the policy externalities that derive from delegating to the IO are central in states' evaluation of the costs and benefits involved with delegation. In other words, states may choose to delegate to an IO if they can obtain an equilibrium between the costs and the benefits in intelligence sharing.

Hierarchy and Intelligence Sharing Practices

The third and last pillar in this theoretical framework will be based on James Walsch' (2010) framework for understanding intelligence sharing in international politics. Overall, he suggests that hierarchical relationships are crucial to understanding the dynamics of intelligence sharing practices between states, and that relational contracting is a promising tool for analyzing these dynamics (Walsch, 2010, p. 27). As Svendsen, Walsch does not present this framework for analysis in relation to IOs but gives a valuable insight into intelligence sharing dynamics - insight that arguably can also be applied to IOs.

As argued in a previous section, secrecy and mutual trust play an important role in intelligence sharing. However, as Walsch (2010) asserts, intelligence sharing may occur even when there is very little trust between the practitioners, and they will in this case most often replace trust with a hierarchical relationship in their intelligence sharing agreement (pp. 14 & 140). Thus, when analyzing intelligence sharing dynamics, for instance in an IO, one should not only consider agreements between the states based on the notion of trust, but also

consider the hierarchical relationships - formal as well as informal - as important for mapping the intelligence sharing practices in the given context.

In order to understand the role that hierarchy plays in intelligence sharing, Walsch (2010) draws on relational contracting theory, a theory initially developed by legal scholar Ian MacNeil (1974) for regarding contracts as being relations rather than transactions (pp. 720-724). Walsch subsequently argues that this theory "draws attention to how states can incorporate hierarchical control, oversight, and monitoring mechanisms in their cooperative agreements in order to minimize defection by participants" (p. 5). In other words, the fear of defection, as well as challenges in obtaining mutual trust, can be overcome by instituting a hierarchical relationship as a part of the relational contract between the parties that wish to share intelligence.

Based on relational contracting theory, Walsch (2010) argues that "if at least one state estimates that the other's incentives to defect are high, it will construct a hierarchical relationship to govern intelligence sharing when the benefits from sharing are thought to be greater than the costs of creating and maintaining the hierarchy plus the cost of defection" (p. 134). Building on this, he states that in order to be able to establish a hierarchical relationship, "power imbalances between dominant and subordinate states are a necessary (...) condition for creating a hierarchy (...)" (Walsch, 2010, p. 137). Hence, a prerequisite for the establishment of a hierarchical relationship is power imbalance between states. If this condition is in place, and if one or more states believe that there is a high risk of defection, i.e., a potentially high cost, a hierarchical relationship will be established. However, the benefits for engaging in this hierarchically based intelligence cooperation must outweigh both the costs of defection and the cost of upholding the hierarchy.

Relating this framework to an IO context, understanding the hierarchical dynamics between states - formal as well as informal - can thus provide valuable insight into intelligence sharing practices in an IO. This aspect is particularly valuable in identifying the informal power balances and consequently what these mean for the correlation between the non-institutionalized intelligence sharing processes between member states on the one hand, and the official mechanisms established within the IO on the other. This, in turn, can give an indication of the functionality of the IO's official authorities and mechanisms established to facilitate intelligence sharing within the organization.

Analytical Framework in Practice

Taking an overall point of departure in the presumptions from Regime Theory, and developed from the theoretical walk-through above, I suggest the following three propositions as a framework for analyzing intelligence sharing practices in international organizations:

1. *States' engagement in intelligence liaisons in IOs is guided by their wish to obtain optimum reach.*
2. *Delegation from states to the IO in the intelligence area is contingent on relatively higher benefits and lower costs, compared to other areas of delegation.*
3. *In cases with low or no levels of trust, states will engage in a hierarchical relationship in their intelligence sharing cooperation.*

The first proposition helps us understand why and how states enter into intelligence cooperation with one another. The second proposition seeks to provide insight into the intended level of delegation by the states to the IO and thus to determine to what extent the IO is capable of fulfilling its mandate in the intelligence area. Finally, the third proposition considers the role of hierarchical relationships in the context of an IO, through which we can gain a deeper understanding of the intelligence sharing dynamics that take place in the organization. Using these three propositions – optimum reach, delegation, and hierarchy – as a guideline for analyzing intelligence sharing practices in an IO can help the researcher gain a deep and nuanced understanding of both the formally established intelligence sharing mechanisms and the intelligence sharing practices that take place informally, as well as why these have emerged.

Analysis: NATO's Intelligence Sharing Practices

Having proposed a theoretical framework for analyzing intelligence sharing practices in IOs, I will now attempt to demonstrate how it can be used in practice, using NATO as my object of analysis. Due to the limited time and space allowed for the production of this paper, the following analysis will not be an in-depth analysis of NATO based on each of the propositions. Rather, it will serve as a surface-level analysis of intelligence sharing practices in the organization with the purpose of demonstrating the applicability of the theoretical framework outlined above, hopefully laying the groundwork for further analysis in the future,

as well as serving as an inspiration for further development and expansion of the theoretical framework presented here.

The Collective Security Regime: NATO

As mentioned in the analytical framework, this paper revolves around the collective security regime. As listed by Bradford (2007), the collective security regime is based on norms and principles from the UN, including guidelines for the use of force. NATO as an international organization is founded on the very same principles as the ones outlined in the UN charter, as explicitly stated in the North Atlantic Treaty introduction (the North Atlantic Treaty, 1949). While international organizations should not be considered as an embodiment of international regimes, the two are often closely related (Bradford, 2007). Concerning the collective security regime, the principles and norms set out by the UN thus constitute the regime, although the regime itself reaches farther than the confinements of the organization (Bradford, 2007). As the NATO treaty demonstrates, NATO is founded directly on the principles of the UN, although the organization stands independently from the UN. By this logic, NATO as a product of the collective security regime seeks to safeguard and enforce peace, security, and freedom in all its endeavors (the North Atlantic Treaty, 1949). This, in turn, also pertains to the established intelligence sharing practices within NATO, as will be elaborated in the following.

NATO's Intelligence Sharing Practices since 9/11

NATO's history of intelligence sharing has, as much else, been largely driven and shaped by global developments, especially since 9/11. In the following, the most significant official developments in the intelligence sharing area within NATO will be outlined in order to provide a basic understanding hereof, prior to diving deeper into the analysis of NATO's intelligence sharing practices.

The desire for a truly increased focus on intelligence cooperation in NATO became apparent following the Prague summit in 2002, in the wake of 9/11 (Gordon, 2017, p. 16). Improvements of NATO intelligence in support of missions became one of the initiatives for NATO transformation that was agreed upon at the summit, leading to the establishment of the sole strategic command, Supreme Headquarter Allied Powers Europe (SHAPE), which later became the Allied Command Operations (ACO)(Gordon, 2017, p. 17; NATO, 2002, pt. 4.d.). Consequently, the leadership began paving the way to what eventually became the NATO

Intelligence Fusion Centre (NIFC) whose purpose was to give NATO a well-functioning intelligence organization, with a particular focus on its ability to facilitate intelligence sharing, mutual trust, and cooperation (Mitchell, 2006). In the years to come, the organization saw rapid development and expansion, and made progress in improving intelligence sharing between NATO member states and NATO's allies. Jumping ahead to the second significant development in NATO intelligence sharing practices since 9/11 was the appointment of the first Assistant Secretary General for Intelligence and Security (ASG-I&S) as well as the establishment of the Joint Intelligence and Security Division (JISD) under his command following the 2016 NATO summit in Warsaw (NATO, 2016, pt. 79). These were similarly results of a (still increasing) desire to strengthen intelligence cooperation within NATO (Ballast, 2017; Cerulus, 2022; Horrell, 2022).

NATO and the Intelligence Reach Equilibrium

As demonstrated in the theoretical framework, states seek to obtain an equilibrium between the costs and the benefits of engaging in intelligence cooperation. This attempt to obtain a cost-benefit equilibrium is manifested by the effort to achieve an optimum level of reach in intelligence liaisons. In order to analyze the intelligence sharing practices that take place in NATO, we must therefore establish the different ways in which NATO and its member states seek to obtain this equilibrium. In the following, using the propositions from the framework above as a guideline, I aim to provide an analysis of the intelligence sharing dynamics that take place within NATO. Using the concept of reach as a reference for explaining the dynamics, I will investigate both the sphere of delegation that has taken place from the member states to NATO as an IO, as well as the hierarchical structures that can be seen. The analysis here will to a certain degree rest on other scholarly analyses of the intelligence sharing dynamics in NATO and subsequently be related to how the theoretical framework developed here can be useful in explaining why these dynamics occur.

Delegation of Authority: NATO Intelligence Sharing

When considering the question of delegation, we must take a look at the official NATO policies on intelligence sharing in order to establish how NATO as an organization envisions these practices.

Before diving into the details of NATO's intelligence sharing practices, it is worth taking a step back and establishing the sphere of delegated authority from the member states,

i.e., the principals, to NATO, i.e., the agent. Drawing on Hawkins et al.'s (2006) analysis of delegation issues in NATO, they state that "NATO's administrative element does not decide when force will be employed; states do. (...) [C]ertainly, NATO's administrative element may influence principals' preferences and behavior, but it has limited autonomy" (p. 259). In other words, states have only delegated very limited authority to NATO, meaning that NATO enjoys a very low level of autonomy in decision matters. Therefore, there appears to be a discrepancy between NATO's ambitions for intelligence sharing within the alliance and the (lack of) delegated authority from the member states in reaching these ambitions.

To elaborate, NATO has since 9/11 expressed an increasing wish to strengthen intelligence sharing within the alliance, as outlined in a previous section. This wish is visible in a number of different ways. While not explicitly stated in the NATO charter, NATO policies on intelligence sharing within the alliance can be drawn from it. The NATO Treaty's article 4 states that "The Parties will consult together whenever (...) the territorial integrity, political independence or security of any of the Parties is threatened" (The North Atlantic Treaty, 1949). Resting on the principle of this article, NATO stated in its 2010 strategic concept that information sharing also falls under this article (NATO, 2010, p. 9). Furthermore, when the NIFC was established, while the ambition was to strengthen NATO intelligence sharing capabilities, it is officially recognized as a 'Memorandum of Understanding' (MoU) rather than a legally binding initiative (Gordon, 2017, p. 16; Department of Education, 2022).

Thus, while there are attempts at establishing official mechanisms and institutions to facilitate intelligence sharing, little delegation of authority has taken place. It is clear to see NATO's ambitions for strengthening intelligence sharing through its policy development, the establishment of the NIFC and the JISD, and the appointment of NATO's first 'Intelligence Chief', the ASG-I&S. However, the actual delegated authority from the member states to NATO leaves very little room for autonomous action for NATO, in line with the conclusions drawn from the analysis by Hawkins et al. (2006). Other analyses concur with this point, arguing that the question of delegation of authority to an agent such as NATO is to a larger degree determined on a case-by-case basis, depending on the suitability of NATO as an agent to react to the given situation (Fahron-Hussey, 2019, p. 241). Similarly, NATO member states show reluctance toward institutional change, such as reform within the intelligence area, as demonstrated by Hylke Dijkstra (2015). He argues that the reason for this is that principals "may fear the inevitable uncertainty that institutional reform brings in terms of future payoffs and control over NATO" (Dijkstra, 2015). Recalling the proposition that

delegation from states to the IO in the intelligence area is contingent on relatively higher benefits and lower costs, compared to other areas of delegation, these points suggest that the member states do not deem the benefits high enough and/or the costs low enough to decisively engage in an intelligence sharing cooperation under the authority of NATO. The concept of reach can help explain this development. Given the uncertainty of these mechanisms, as well as its associated policy externalities, the reach equilibrium for each of the member states will vary greatly, depending on the different resources that the state is able to present. Hence, if member states were to engage in intelligence sharing under NATO leadership, there would be an imbalance in the risks of overreach for each of the states, potentially imposing a high cost on some states more than others. Additionally, the benefits of engaging in this intelligence cooperation for the individual member state are ill-defined, further weakening the incentive to delegate authority to the agent.

NATO's Formal and Informal Hierarchies

As outlined in the theoretical framework, hierarchy can play an important role in states' effort to obtain an optimum level of reach in intelligence liaisons. Recalling the third proposition, *in cases with low or no levels of trust, states will engage in a hierarchical relationship in their intelligence sharing cooperation*, and it is therefore necessary to investigate the hierarchical dynamics – formal as well as informal – at play in NATO.

Officially, NATO states have the right to veto, and all decisions must be made by consensus, placing the member states in an equal relationship with one another (NATO, 2022). However, a number of analyses and factors assert an American leadership in NATO, as well as to the fact that this has been the case since the Alliance's establishment in 1949 up until today (Haar, 2020; Layne, 2000; Seagle, 2015; Streeck, 2022). Furthermore, US dominance in NATO can also be seen in several places in the treaty: New states' accession to the Treaty must be deposited to the US (article 10); treaty ratifications must be deposited to the US (article 11); parties' denunciation from the Treaty must be given to the US (article 13); and the official Treaty texts are stored in US archives (article 14) (The North Atlantic Treaty, 1949). Moreover, this can also be seen in NATO's intelligence sharing policies, in the sense that in official NATO terminology, the NIFC is under US sponsorship and regarded as the 'framework nation', and the US holds the commander's position of the Center (Gordon, 2017, pp. 16-17).

In the intelligence area, informal arrangements often evolve parallel to the officially established mechanisms for governing intelligence sharing (Svendsen, 2010; 2012, p. 14). This is also the case for NATO, where numerous informal bilateral and multilateral intelligence sharing agreements exist, both NATO members in between, as well as between NATO member states and third parties. Perhaps the most widely known intelligence cooperation is the Five Eyes (FVEY), an agreement between UK, the United States, Canada, Australia, and New Zealand (Aldrich, 1998, pp. 331-351; Walsch, 2009, pp. 31-44; Svendsen, 2010; Tossini, 2020; Office of the Director of National Intelligence). The FVEY intelligence cooperation is arguably one of the most extensive, exclusive, and robust alliances for intelligence sharing, and scholars have contended that its effectiveness overtakes that of NATO intelligence sharing (O'Neil, 2017; Ballast, 2017). Additionally, the FVEY agreement has since been extended to related fora of select third party states, including the 'nine-eyes' (FVEY plus Denmark, France, Norway, and the Netherlands) and 'fourteen-eyes' (nine-eyes plus Belgium, Germany, Italy, Spain, and Sweden) agreements (Tossini, 2020; Cremer, 2013). Another example is the US and Poland's bilateral agreement, under American leadership - both nations members of NATO (Seagle, 2015). Several other similar agreements exist within the Alliance (see Lefebvre, 2003), all of which demonstrate intelligence sharing establishments that exist outside of the authority of NATO's official ambitions for a collective intelligence sharing policy. Furthermore, in accordance with Walsch' notion of the conditions required for a hierarchical relationship to be established, there is an apparent power imbalance in favor of the US (albeit arguably with a smaller imbalance between the US and the UK, for instance, compared to other, smaller states).

Drawing on the third proposition and based on the fact that there are hierarchical establishments within NATO – namely US dominance in several aspects as well as the parallel formal, informal, and overlapping intelligence arrangements within NATO member states and third-party states – it can be concluded that states exhibit low or no levels of trust towards NATO's official intelligence sharing mechanisms. While there are suggestions that US leadership in NATO's intelligence sharing policies have produced positive outcomes (see for instance Gordon, 2017, p. 17), this dynamic has also been argued to seriously impede intelligence sharing within NATO (Seagle, 2015). In other words, in their efforts to obtain an optimum level of intelligence reach, and thereby finding the equilibrium between the costs and the benefits of engaging in the intelligence liaisons, states have established both formal and informal hierarchical relationships to replace an intelligence cooperation based on mutual trust.

Findings from Analysis

In conclusion, NATO member states' engagement in the different intelligence sharing constellations - formal as well as informal - is guided by their wish to obtain optimum reach, i.e., in accordance with the first proposition from the framework. Drawing on the second proposition regarding the level of delegation, there is an indication that the member states do not deem the benefits high enough and/or the costs low enough to decisively engage in an intelligence sharing cooperation under the authority of NATO, subsequently delegating very little authority to NATO to act autonomously. This can likely be explained by the fact that the costs and benefits for each state vary greatly, begging the question of how a common intelligence sharing cooperation between states of such various gravities might look. Lastly, with the third proposition concerning the role of hierarchy in mind, the (mostly) US-dominated hierarchical dynamics present in NATO intelligence sharing, both formally and informally, indicate that there is a low level of trust present between the member states and NATO.

As the theoretical framework dictates, presuming that states will always seek to obtain a cost-benefit equilibrium, i.e., optimum reach helps explain the apparent discrepancy between NATO's official ambitions for the organization's intelligence sharing practices and the reality of the smaller bilateral and multilateral (formal and informal) fora that emerge. The unclear benefits and the potentially high cost of delegating authority to the agent prevent the states from giving NATO autonomy in administering intelligence sharing within the organization. Subsequently, the lack of trust toward NATO's intelligence sharing, combined with the existing US-dominated power imbalance that exists within NATO members, makes it more desirable for states to engage in smaller hierarchical fora for intelligence sharing, thus minimizing the risk of overreach.

Concluding Remarks and the Way Ahead

The primary aim of this paper has been to introduce a suggestion for a theoretical framework for analyzing intelligence sharing practices in international organizations. While extensive research exists on the topic of intelligence sharing, this paper seeks to fill the apparent gap in the literature that analyzes intelligence sharing practices in an IO context. The three propositions presented, based on Svendsen's (2012) concept of optimum intelligence reach, on Hawkins et al.'s (2006) notion of delegation in IOs, and on Walsch' (2010) approach to

using hierarchy to understand intelligence sharing dynamics, should be used as a guideline for analyzing intelligence sharing in a given IO. I have attempted to demonstrate an application of the framework in practice, by using NATO as my object of analysis. The analysis showed a discrepancy between NATO's official established mechanisms for intelligence sharing and the actual intelligence sharing practices that are taking place beyond these mechanisms. Thus, the conclusions from the analysis could be used as a point of departure for optimizing intelligence sharing within NATO, on the basis of understanding the reasons behind the current dynamics.

Although the theoretical framework presented here can be used as a starting point for understanding intelligence sharing practices in IOs, further development is required. Rather, the basis here should be considered an inspiration for further research into intelligence sharing practices in IOs, one that could develop in a number of different directions. Further research should investigate the applicability of the framework for other IOs, as well as a more in-depth analysis of NATO than the surface-level analysis that has been presented here, limited by the space and time allowed for the production of this paper. Other developments of the framework could for instance take the shape of certain criteria for successful intelligence sharing in IOs that could (with time) be extracted from the three propositions presented here, based on analyses of other IOs. Another direction worth exploring is the use of this framework for understanding how intelligence sharing practices for IOs affect individual member states.

In sum, the framework should be able to help uncover both the formally established processes and ambitions for the IO in intelligence sharing, as well as provide insight into the parallel interactions and cooperations that exist beyond the established mechanisms. This, in turn, may help the researcher understand why these dynamics occur and subsequently identify how these processes could be optimized, depending on the desired outcome for the organization. Hopefully, the proposed framework for analysis presented here can lay the groundwork for future analyses of intelligence sharing practices in IOs, while at the same time serve as an inspiration for further development and expansion of the theoretical framework in this research area.

Bibliography

Aden, H. (2018) Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union, *West European Politics*, 41:4, 981-1002, DOI: 10.1080/01402382.2018.1475613

Aldrich, R. J. (1998). British Intelligence and the Anglo-American 'Special Relationship' during the Cold War. *Review of International Studies, Vol. 24,* No. 1.

Ballast, J. (2017). *Trust (in) NATO: The future of intelligence sharing within the Alliance*. NATO Defense College. http://www.jstor.org/stable/resrep10248

Boatner. (2000). Sharing and Using Intelligence in International Organizations: Some Guidelines. *National Security and the Future*, *1*(1.), 81.

Bradford, A. (2007). Regime Theory. *Max Planck Encyclopedia of Public International Law.* Available at SSRN: https://ssrn.com/abstract=2770647

Cerulus, L. (2022, March 24). NATO steps up intelligence-sharing 'in preparation' for Russian cyberattacks. *Politico.* Retrieved from https://www.politico.eu/article/nato-steps-up-intelligence-sharing-in-preparation-of-russian-cyberattacks/

Clough, C. (2004). Quid pro quo: The challenges of international strategic intelligence cooperation. *International Journal of Intelligence and Counterintelligence 17:601-13*

Cremer, J. (2013, November 4). Denmark is one of the NSA's '9-Eyes'. *The Copenhagen Post.* Retrieved from https://web.archive.org/web/20131219010450/http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html

Department of Education. (2022, October 19). *Guide to writing a memorandum of understanding (MOU).* Retrieved from https://www.gov.uk/government/publications/setting-up-school-partnerships/guide-to-writing-a-memorandum-of-understanding-mou

Dijkstra, H. (2015). Functionalism, multiple principals and the reform of the NATO secretariat after the Cold War. *Cooperation and Conflict*, *50*(1), 128–145. https://doi.org/10.1177/0010836714532919

Fahron-Hussey, C. (2019). Conclusion. In: Military Crisis Management Operations by NATO and the EU. Springer VS, Wiesbaden. https://doi-org.zorac.aub.aau.dk/10.1007/978-3-658-23518-5_7

Gordon, J. S. (2017). Intelligence sharing in NATO. *Atlantisch Perspectief*, *41*(6), 15–19. https://www.jstor.org/stable/48581386

Haar, R. N. (2020). Why America should continue to lead NATO: Why Europe should embrace U.S. leadership. *Atlantisch Perspectief*, *44*(2), 31–37. https://www.jstor.org/stable/48600530

Hardin, R. (2002). *Trust and Trustworthiness.* Russel Sage. New York.

Hastedt, G., P. & B. Skelley, D. B. (2008). Intelligence in a turbulent world: Insights from organization theory. In Gill, P., Marrin, S., & Phythian, M. (Eds.). (2008). *Intelligence Theory: Key Questions and Debates* (1st ed.). Routledge. https://doi.org/10.4324/9780203892992

Hawkins, D. G., Lake, D. A., Nielsen, D. L., Tierney, M. J. (2006). *Delegation and agency in international organizations.* Cambridge University Press.

Horrell, S. (2022, July 1). NATO's Joint ISR and the Madrid Summit. *CEPA.* Retrieved from https://cepa.org/article/natos-joint-isr-and-the-madrid-summit/

Keohane, R. (1989). *International Institutions And State Power: Essays In International Relations Theory.* Routledge. Retrieved from https://www.taylorfrancis.com/books/mono/10.4324/9780429032967/international-institutions-state-power-robert-keohane?refId=e24dc385-643f-4528-87f0-6410f71fd770&context=ubx

Krasner, S. D. (1983). *International Regimes*. Cornell University Press. Retrieved from https://books.google.dk/books/about/International_Regimes.html?id=WIYKBNM5zagC&redir_esc=y

Lake, D. & Powell, P. (1999). *Strategic choice and international relations.* Princeton, NJ: Princeton University Press.

Lander, S. (2004). International intelligence cooperation: An inside perspective. *Cambridge Review of International Affairs 17, no. 3: 481-93.*

Layne, C. (2000). US hegemony and the perpetuation of NATO. *Journal of Strategic Studies*, 23:3, 59-91, DOI: 10.1080/01402390008437800

Lefebvre, S. (2003). The difficulties and dilemmas of international intelligence liaison. *SAIS Review 24, no. 1.* https://www.tandfonline.com/doi/abs/10.1080/716100467

MacNeil, I. R. (1974). The many futures of contracts. *Southern California Law Review,* 47(3), 691-816. Retrieved from https://heinonline-org.zorac.aub.aau.dk/HOL/Page?collection=journals&handle=hein.journals/scal47&id=728&men_tab=srchresults

Maras, M-H. (2017). Overcoming the intelligence-sharing paradox: Improving information sharing through change in organizational culture. *Comparative Strategy*, 36:3, 187-197, DOI: 10.1080/01495933.2017.1338477

Milner, H. (1997). *Interests, institutions and information: Domestic and international relations.* Princeton, NJ: Princeton University Press.

Mitchell, B. (2006, October 17). NATO Intelligence Fusion Center opens in England. *Stars and Stripes.* Retrieved from https://www.stripes.com/news/nato-intelligence-fusion-center-opens-in-england-1.55546

National Commission on Terrorist Attacks Upon the United States. (2004). *THE 9/11 COMMISSION REPORT: Final Report of the National Commission on Terrorist Attacks Upon the United States.* Retrieved from https://9-11commission.gov/report/

NATO. (2002, November 21). *Prague Summit Declaration [press release]*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_19552.htm

NATO. (2010, November 19-20). *Strategic Concept: for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO. (2016, July 09). *Warsaw Summit Communiqué [press release]*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2022, June 14). *Consensus decision-making at NATO.* https://www.nato.int/cps/en/natohq/topics_49178.htm

Newton, V. (1991). *Cambridge Spies - The Untold Story of McLean, Philby, and Burgess.* University Press Of America.

OECD. (2002). Externalities. *Glossary of Statistical Terms.* Retrieved from https://stats.oecd.org/glossary/detail.asp?ID=3215

Office of the Director of National Intelligence. (2022). *Five Eyes Intelligence Oversight and Review Council (FIORC).* Retrieved from https://www.dni.gov/index.php/who-we-are/organizations/enterprise-capacity/chco/chco-related-menus/chco-related-links/recruitment-and-outreach/217-about/organization/icig-pages/2660-icig-fiorc

O'Neil, A. (2017). Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs,* 71:5, 529-543, DOI: 10.1080/10357718.2017.1342763

Oxford English Dictionary. (2012). Oxford Dictionaries. Retrieved from https://books.google.dk/books?id=mYicAQAAQBAJ&lpg=PA509&ots=fBwTM3Qh0R&dq=definition%20outreach%20%22an%20organization's%20involvement%20with%20the%20community%22&hl=da&pg=PA509#v=onepage&q=definition%20outreach%20%22an%20organization's%20involvement%20with%20the%20community%22&f=false

Seagle, A. N. (2015). Intelligence Sharing Practices Within NATO: An English School Perspective. *International Journal of Intelligence and CounterIntelligence,* 28:3, 557-577, DOI: 10.1080/08850607.2015.1022468

Sims, J. (2005). Understanding Friends and Enemies. In Sims, J. and Gerber, B. *Transforming U.S. Intelligence.* Georgetown University Press.

Streeck, W. (2022, May 20). The EU after Ukraine. *American Affairs Journal.* https://americanaffairsjournal.org/2022/05/the-eu-after-ukraine/

Svendsen, A. D. M. (2010). Intelligence Cooperation and the War on Terror. *Anglo-American Security Relations After 9/11.* London and New York, Routledge.

Svendsen, A. D. M. (2012). *Understanding the Globalization of Intelligence.* Palgrave Macmillan.

The North Atlantic Treaty. (1949, April 4). *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Tossini, J. V. (2020, April 14). The Five Eyes – The Intelligence Alliance of the Anglosphere. *UK Defence Journal.* Retrieved from https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/

Tuzuner, M. (2010). *Intelligence Cooperation Practices in the 21st Century: Towards a Culture of Sharing*. IOS Press. Retrieved from http://ebookcentral.proquest.com/lib/aalborguniv-ebooks/detail.action?docID=593777.

Walsh, J. I. (2009). The International Politics of Intelligence Sharing. *New York: Columbia University Press.*

Walsch, J. I. (2010). *The international politics of intelligence sharing*. Columbia University Press.