# Sharing the Burden, Sharing the Secrets

## The future of European intelligence cooperation

Danny Pronk
Claire Korteweg

Clingendael Report
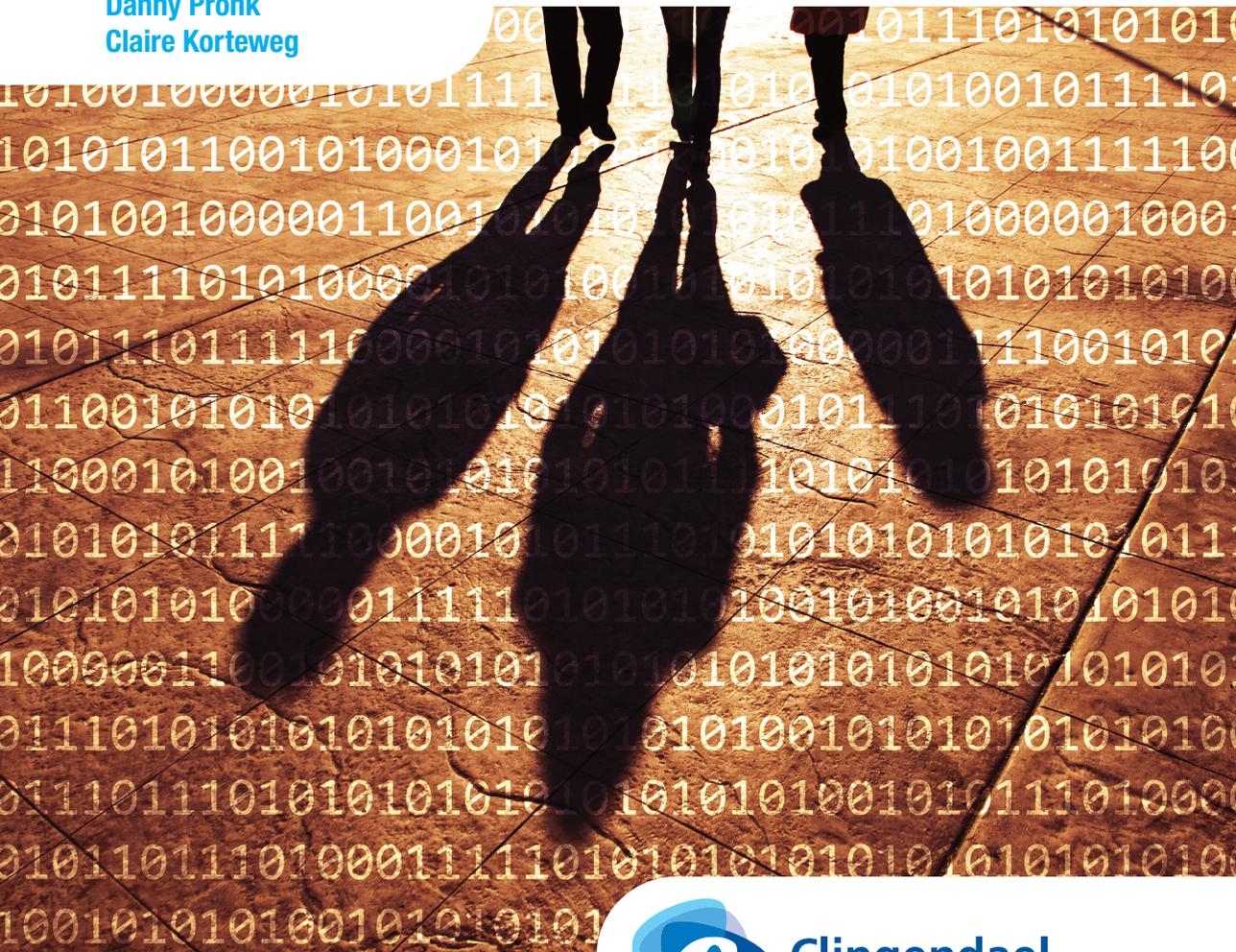
Clingendael
Netherlands Institute of International Relations

# Clingendael
Netherlands Institute of International Relations

# Sharing the Burden, Sharing the Secrets

## The future of European intelligence cooperation

Danny Pronk
Claire Korteweg

**September 2021**

**About the authors**

**Danny Pronk** is a Senior Research Fellow of the Security Unit at Clingendael. His research focuses on strategic foresight and on intelligence and national security issues, including intelligence support of military operations and international intelligence cooperation.

**Claire Korteweg** has been a research assistant (intern) at Clingendael, focusing on intelligence and national security issues and on strategic foresight.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media
 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute
 clingendael_institute
 Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

# Contents

# Summary

This report discusses the opportunities for enhanced European intelligence cooperation in light of the key challenges facing Europe over the next ten years, as identified in the Strategic Monitor 2020-2021, *Geopolitical Genesis: Dutch Foreign and Security Policy in a Post-COVID World*. In light of these challenges and the need to realise European strategic autonomy and deliver on the goals of the EU Strategic Compass for security and defence, closer intelligence and security cooperation by Europe is required. However, intelligence activities lie at the very heart of national sovereignty, and can perhaps be considered to be the hardest hurdle to cross. Nevertheless, over the years the EU has developed several institutions to facilitate intelligence sharing between its member states and agencies have been established that collect, analyse and operationalise intelligence in view of key security threats. Within this institutional context, there is scope to assess the opportunities for enhanced European intelligence cooperation.

This report starts by taking multilateral intelligence cooperation and its three main drivers – internal demand, external pressure and cooperative momentum – as its analytical framework. It subsequently focuses on the subjects of intelligence cooperation in the EU, intelligence culture in and cooperation with Asia, and intelligence cooperation in a Post-Brexit Europe. In doing so, this report addresses three specific questions:
- How can intelligence cooperation in the field of early warning help the EU better respond to external conflicts and crises, support the protection of the Union and its citizens and advance the development of a common European intelligence culture?
- How can useful entry points be identified for European intelligence cultural convergence with Asia that can enable EU intelligence cooperation with certain partners in that region?
- What are the opportunities for the continued engagement of British intelligence and security services in European cooperative arrangements for tackling the security challenges facing the EU?

On the topic of intelligence cooperation in the EU, this report concludes that the operationalisation of the EU Early Warning System could be strengthened by infusing it with elements from the NATO Intelligence Warning System. These elements are the inclusion of warning problems in the process, a system of institutionalised burden-sharing, and the combination of a long-term and short-term focus. Also, EU cooperation on enhancing resilience and countering hybrid threats needs to be guided by a regularly updated threat assessment and a comprehensive situational awareness. In order to do so, the EU's Hybrid Fusion Cell needs to strengthen and enhance its close cooperation with both NATO's Hybrid Analysis Branch and the Hybrid Centre of

Excellence. Finally, the platform of the Intelligence College Europe provides the ideal space and forum for organising panels, seminars and discussions to promote European intelligence cooperation in the field of early warning and the development of a common culture among European intelligence and security experts.

On the topic of intelligence culture in and cooperation with Asia, this report concludes that there are European commonalities with the intelligence culture of Japan, particularly in terms of that country's perceived security threats. The presence of a common perceived challenge in the shape of China will make Japan more inclined to seek intelligence gains through cooperation with the EU, and vice versa. Moreover, the EU and Japan seem to be natural cooperation partners: they share the same values and are both democratic entities. There is untapped potential for cooperation in the field of intelligence, for instance within the framework of the EU-Japan Strategic Partnership Agreement that explicitly references cooperation in areas which have hitherto achieved mostly low levels of cooperation, such as military and regional security issues.

On the topic of intelligence cooperation in a Post-Brexit Europe, this report concludes that there is an opportunity for the continued engagement of British intelligence and security services in an existing European cooperative arrangement for tackling the smuggling of drugs. The Maritime Analysis and Operations Centre (Narcotics) could build on the experiences in countering narcotics trafficking from the Caribbean in the Joint Interagency Task Force-South. The UK and the EU could benefit from exporting the best practices from their Caribbean collaboration to Europe and to investigate which particular elements can further strengthen European cooperation in the field of counternarcotics. A post-Brexit UK should remain involved as a key participant in the MAOC (N) even though it is no longer part of the Union funding it.

Based on these findings, this report argues that there is ample opportunity to increase both the scope and depth of European intelligence cooperation in the years to come. Moreover, the Netherlands can and indeed should play an active role in the development of enhanced intelligence cooperation in and of Europe by making effective use of the presence of important factors that can help drive European cooperation further. This report concludes with nine concrete policy recommendations for enhanced European intelligence cooperation in light of the key challenges facing Europe over the next ten years.

# 1   Introduction

The latest Strategic Monitor 2020-2021, *Geopolitical Genesis: Dutch Foreign and Security Policy in a Post-COVID World*, identified six key challenges facing Europe over the next ten years. For one, as the current incarnation of the multilateral order wanes, the interaction of the global powers – the United States, China, Russia and the European Union – will play a large role in defining the landscape of the international system. And in that landscape, it is the competition between the US and China that will be the most important aspect for the foreseeable future. In order to more effectively address this challenge a new menu of policy options is called for. Above all, the EU should prioritize policies and procedures that will facilitate its emergence as a global power in its own right. This is seen as an indispensable phase in its geopolitical genesis.[1]

Adopting a more assertive geopolitical stance is considered to be a key factor to safeguard European interests and values. This is why the emphasis should be placed on developing concrete policies and initiatives and on forming specific coalitions and partnerships to achieve the desired outcomes. As a medium-sized EU member state, the Netherlands lacks the influence of the biggest member states such as France and Germany. However, it can amplify its influence by partnering with these larger member states. In addition, by focusing on areas in which it has special expertise, the Netherlands can impact the overall direction of future EU policy. The recommendations in the Strategic Monitor 2020-2021 report all shared a common thread: each highlighted the need for the Netherlands and its European partners to develop new collaborations, relationships and partnerships in the emerging multipolar international system. Working out the specifics of these arrangements has been the focus of this year's research effort.[2]

For Europe to become a geopolitical actor in the context of a changing international order, with China, Russia and the United States as the main competing global powers, it is necessary to realise European strategic autonomy – also referred to as sovereignty, independence, self-sufficiency or responsibility.[3] European strategic autonomy embraces all elements of state power: political, economic, military and others. Europe's weakest element here is security and defence. And contrary to the field of trade and finance,

---

1   Jack Thompson, Danny Pronk and Hugo van Manen, *Strategic Monitor 2020-2021* (The Hague: The Clingendael Institute, 2021).
2   As announced in the *Strategic Monitor 2020-2021*, 139.
3   Daniel Fiott (ed.), *European Sovereignty: Strategy and interdependence* (Paris: European Union Institute for Security Studies, 2021).

for security and defence 'Europe' cannot be limited to merely the EU member states. In the post-Brexit era the United Kingdom – one of the key players in European security and defence – is no longer a member of the EU. Furthermore, If the EU truly wants to become a geopolitical actor, it can no longer stick to the Common Security and Defence Policy (CSDP) tasks defined in the 1990's. CSDP operations have to be adjusted, both in scope and spectrum. Moreover, it has to be taken beyond crisis management operations on land by extending the level of ambition to air and sea surveillance and maritime interdiction operations to protect the EU's wider interests.[4]

Currently, the EU faces a wider set of challenges and threats than ever before.[5] First of all, 'Europe' runs the danger of becoming irrelevant and the object of great power attentions and actions, rather than being a global actor in its own right in the emerging global power competition between China, Russia and the United States. Furthermore, the so-called 'arc of instability' around Europe is unlikely to turn into an arc of stability any time soon. The security challenges posed have set the three strategic priorities for the EU's CSDP: to respond to external conflicts and crises, to support partners to provide security for their own population, and to protect the Union and its citizens. In order to do so, the EU is developing a Strategic Compass for security and defence, to be ready by March 2022. It is expected that the Strategic Compass will contribute to the development of a coherent and strategic approach to the existing initiatives and will bolster the EU's security and defence policy, taking into account the threats and challenges the EU is currently facing. The goal is that the Strategic Compass, building forth on a common European threat analysis completed in November 2020, will define the policy orientations and specific objectives in four dimensions, or so-called 'baskets': (1) crisis management, (2) resilience, (3) capability development and (4) partnerships. Additionally, the Strategic Compass aims to advance the development of a common European security and defence culture.[6]

As the global power competition between the major powers intensifies, it is grey zone operations, also known as hybrid conflict, that will be the mainstay of international relations over the next ten years. In the grey zone non-kinetic, non-military measures are used by actors to achieve the objectives of war without actually goading opponents into conventional war.[7] This zone is 'grey' because it straddles the line between war

---

4   Dick Zandee, Bob Deen, Kimberley Kruijver and Adája Stoetman, *European Strategic Autonomy in Security and Defence*, (The Hague: The Clingendael Institute, 2020).

5   Tania Lațici and Elena Lazarou, *Peace and Security in 2021: Overview of EU action and outlook for the future* (Brussels: European Parliamentary Research Service, 2021).

6   Dick Zandee, Adája Stoetman and Bob Deen, *The EU's Strategic Compass for security and defence* (The Hague: The Clingendael Institute, 2021).

7   Michael Mazarr, *Mastering the Grey Zone: Understanding a Changing Era of Conflict* (Carlisle Barracks: United States Army War College Press, 2015).

and peace. Tactics include cyber-attacks, economic and diplomatic coercion and information operations. One of the best-known examples is Russian election meddling. Because these tactics are not overt acts of war, it is difficult for victims to realize they are under attack or to figure out how, when, or even whether to respond.[8] Grey zone tactics have moved international aggression into a realm where conflict is shadowy and never-ending, and the enemy can be virtually impossible to detect, testing our ability to respond.[9] Though Russia dominates the grey zone arena, it is by no means alone.[10] These kinds of threats have become an ubiquitous feature of today's security environment and although the EU is much better placed to detect and combat them today than was the case several years ago, this form of conflict remains a major challenge for Europe.[11]

In light of the key challenges facing Europe over the next ten years, and the need to realise European strategic autonomy and develop an EU Strategic Compass for security and defence, closer intelligence and security cooperation by Europe is required. However, intelligence activities lie at the very heart of national sovereignty, and can perhaps be considered to be the hardest hurdle to cross. Nonetheless, over the years the EU has developed several institutions to facilitate intelligence sharing between its member states, and these institutions serve the function of creating mechanisms for the diffusion of intelligence between and among national authorities. Moreover, intelligence as a process and product has been strongly promoted by the EU as a useful tool in the fight against terrorism, radicalization, organised crime and public order problems. And a range of agencies has been established that collect, analyse and operationalise intelligence in view of these key security threats. Examples are INTCEN, Europol and Frontex.[12] Additionally, the Single Intelligence Analysis Capacity (SIAC) was created in 2007 as a means of combining analysis of intelligence from different sources into a refined product to support policymaking by the European External Action Service (EEAS).[13]

---

8    Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou (eds.), *The Landscape of Hybrid Threats: A Conceptual Model* (Luxembourg: Publications Office of the European Union, 2021).

9    Gregory F. Treverton et al., *Addressing Hybrid Threats* (Swedish Defence University, 2018).

10   Frans-Paul van der Putten, Minke Meijnders, Sico van der Meer and Tony van der Togt, *Hybrid Conflict: The Roles of Russia, North Korea and China*, (The Hague: The Clingendael Institute, 2018).

11   Daniel Fiott and Roderick Parkes, *Protecting Europe: The EU's response to hybrid threats* (Paris: European Union Institute for Security Studies, 2019).

12   Mai'a Davis Cross, "A European Trans-governmental Intelligence Network and the Role of IntCen," *Perspectives on European Politics and Society* 14, no. 3 (2013): 388-402; Monica Den Boer, "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis," *Intelligence and National Security* 30, no. 2-3 (2015): 402-419.

13   Simon Duke, "Intelligence and EU External Relations: Operational to Constitutive Politics," in *The Politics of Information: The Case of the European Union*, eds. Tannelie Blom and Sophie Vanhoonacker (Houndmills: Palgrave Macmillan, 2014), 242-259.

Within this institutional context, there is scope to assess the opportunities for enhanced European intelligence cooperation. This involves much more than cooperation within the Union, and includes cooperation in both the civilian and the military contexts. It also encompasses more than the multitude of existing cooperative activities between the EU members themselves, and between EU member states and EU institutions. Moreover, it concerns not just EU member states anymore, such as the United Kingdom post-Brexit specifically. Furthermore, there are now several countries outside of Europe, in particular in the Pacific region, that have a vested interest in cooperating with the EU in the field of intelligence and security. These considerations give rise to the general research question of what the prospects are for enhanced European intelligence cooperation in the future, and more specifically:

– How can intelligence cooperation in the field of early warning help the EU better respond to external conflicts and crises, support the protection of the Union and its citizens and advance the development of a common European intelligence culture?
– How can useful entry points be identified for European intelligence cultural convergence with Asia that can enable EU intelligence cooperation with certain partners in that region?
– What are the opportunities for the continued engagement of British intelligence and security services in European cooperative arrangements for tackling the security challenges facing the EU?

This report aims to contribute to the definition of a EU Strategic Compass, focusing specifically on the dimension of intelligence and security partnerships, but with a keen eye for complementary aspects with regards to the other 'baskets' of crisis management, resilience, and capability development. The next chapter provides a theoretical framework for analysing multilateral intelligence cooperation by describing its main drivers: internal demand, external pressure and cooperative momentum. These three drivers are then used to structure the following three chapters, which respectively focus on the subjects of intelligence cooperation in the EU, intelligence culture in and cooperation with Asia and intelligence cooperation in a Post-Brexit Europe. In the final chapter this report concludes with policy recommendations. The methodology applied to this report consists of an extensive desk review of academic and think-tank literature and interviews conducted with experts in the Netherlands and EU institutions.

# 2 Theorising multilateral intelligence cooperation

## Introduction

The notion of European intelligence cooperation may sound highly improbable to some. In fact, the phenomenon under scrutiny here – intelligence cooperation – is in itself somewhat of an oxymoronic concept. Intelligence activities are traditionally thought to be at the very heart of national security and prerequisites for a state's national sovereignty and the prospects for international cooperation or even integration in this particular field therefore seem to be modest.[14] The general difficulties with multilateral intelligence cooperation have been thoroughly covered in the intelligence literature.[15] While much cooperation takes place on a bilateral basis, this chapter therefore addresses the puzzle of the development of multilateral arrangements for cooperation. It specifically asks how we can explain multilateral intelligence cooperation in an area that is at the heart of national sovereignty. As a basis for analysing intelligence cooperation, the vast majority of state interests at play may be summarised as involving a simple trade-off: achieving intelligence and policy gains while minimising the costs in terms of loss of autonomy and increased vulnerability.[16]

Intelligence gains are the intelligence-related benefits of cooperation. They include things like access to currently unavailable sources, methods, technologies and information. Policy gains relate to the political motives for cooperation, such as the granting of legitimacy to an actor or organisation, the strengthening of political relationships, or the need to display commitment in the eyes of the public. In their aim to maximise any combination of these gains through intelligence cooperation, however, states are held back by issues of cost as well as risk. The main cost arises when states accept any development that curtails their authority, either in their internal or external

---

14  Pia Philippa Seyfried, *A European Intelligence Service? Potentials and Limits of Intelligence Cooperation at EU Level* (Berlin: Bundesakademie für Sicherheitspolitik, 2017).

15  See for instance Stefan Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and Counterintelligence* 16, no. 4 (2003): 527-542; Jennifer Sims, "Foreign Intelligence Liaison: Devils, Deals and Details," *International Journal of Intelligence and Counterintelligence* 19, no. 2 (2006): 195-217.

16  Björn Fägersten, "European Intelligence Cooperation," in *The Future of Intelligence: Challenges in the 21st Century*, eds. Isabelle Duyvesteyn, Ben de Jong and Joop van Reijn (London and New York: Routledge, 2014), 94-112.

affairs. This includes, for example, being dependent on external sources of information, or being drawn into operations by alliance commitments. The main risk is linked to the possible disclosure of knowledge level, methods and sources, or to the defection of a partner. This risk can be the product of incompetence, malign motives on the part of the other, or legal and other incompatibilities.[17]

There are also major obstacles which can stand between ambitions and actual outcomes and which can obstruct cooperation even in cases where governments favour it. In the case of Europe, the most potent barrier has been national intelligence staffers whose interests were challenged by suggested schemes for increasing intelligence cooperation, formalisation and centralisation. Perhaps the most striking example of this kind of 'bureaucratic resistance' is Europol and its role in counter-terrorism. European governments have called repeatedly for increased intelligence support for Europol from national security services, but these calls went largely unheeded. Even legal instruments to boost intelligence sharing were largely ineffective in this area.[18] Furthermore, existing institutions such as Europol may simply fail to overcome the common mistrust of the member states which can inhibit intelligence sharing.[19]

So, cost-benefit analyses explain the preference for cooperation in a specific instance, or at a specific point in time. However, if we want to explain dynamics in cooperation – as in the case of European intelligence cooperation – we must look at how and why the balance between these conflicting interests of costs and benefits can shift over time.[20] The remainder of this chapter discusses the main drivers that can shift the balance between the contending interests described above, thus affecting the prospects for intelligence cooperation in and of Europe in the future.[21] Three factors sway states towards cooperation, either by making them more inclined to seek cooperative gains, or by rendering them more willing to accept the costs and risks of cooperation: internal demand, external pressure and cooperative momentum.[22]

---

17    James Igoe Walsh, "Defection and Hierarchy in International Intelligence Sharing," *Journal of Public Policy* 27, no. 2 (2007): 151-181.

18    Björn Fägersten, "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol," *Intelligence and National Security* 25, no. 4 (2010): 500-520.

19    James Igoe Walsh, "Intelligence-Sharing in the European Union: Institutions Are Not Enough," *Journal of Common Market Studies* 44, no. 3 (2006): 625-643.

20    Fägersten, "Bureaucratic Resistance," 102-103.

21    See Damien Van Puyvelde, "European Intelligence Agendas and the Way Forward," *International Journal of Intelligence and Counterintelligence* 33, no. 3 (2020): 506-513.

22    The theoretical framework constructed in this chapter is based on the work of Björn Fägersten, *Sharing Secrets: Explaining International Intelligence Cooperation* (Lund: Lund Political Studies, 2010).

## Internal demand

Internal demand implies that the reason for cooperation is to be found within the cooperating states. These demands can originate from the public or the political world. This driver implies that the establishment of European intelligence cooperation is the answer to one or many EU member states' perception that they face domestic problems they are unable or unwilling to address unilaterally. Such domestic needs can spring from a deteriorating security situation in the face of new challenges. Perceived national needs thus drives EU intelligence cooperation by increasing the intelligence and policy gains available.

Additionally, intelligence cooperation can cater for common needs that have become evident due to more general developments within the EU. This is essentially the neo-functional idea assuming that one political solution will lead to demands for another and that functional spill over will gear the integration process. In the case of intelligence it could be reasoned that common policies on internal and external security like the CSDP accentuate the need of 'common' intelligence to underpin these policies. Perceived functional needs hence drive intelligence cooperation because they raise the intelligence gains of cooperation.

Finally, there can be a need for an increased intelligence capacity but EU member states perceive that they can reach more cost-efficient solutions together. One example is when states pool intelligence resources and thus save costs at the national level. So, an economy of scale logic may sway member states to seek intelligence gains from cooperation since such gains enables the sates to save costs at the national level. Simply put, it's more efficient to have an analyst in Brussels watching Libya than to have one in every one of the capitals of the Union.

## External pressure

This perspective explains changes in states' preferences by looking at factors exogenous to the cooperating states. In traditional realism, external pressure is a vital explanatory factor when analysing state behaviour. External is then usually translated to systemic, i.e. states have a small freedom of manoeuvre within the international system. And change in the international system thus generates changes in state behaviour. However, the strength of systemic explanations is also their weakness. This report will therefore work with a more narrow focus where very specific, and not necessarily systemic, external processes provoke changes in state preferences. So, how do external events influence state interests concerning intelligence cooperation?

One example is when the intelligence power in the world changes. Intelligence power is simply the assortment of intelligence capabilities at the disposal for a specific actor.

Changes in the international intelligence power balance may put pressure on a specific state or a group of states to either rebalance an existing relationship to avoid a situation of intelligence dependency and reach a higher degree of intelligence autonomy, or to increase intelligence capabilities in order to balance against a common perceived threat. For example, the European countries could join forces with others in order to stand up against Russia, or China. Simply put, if external threats challenges states' intelligence power this may render these states more inclined to seek intelligence gains through cooperation.

## Cooperative momentum

The third and last driver to be included in this analytical framework is cooperative momentum. So far it has been implied that cooperation is generated by factors either outside of, or within, the involved states. Contrary to these views, cooperative momentum builds on the idea that cooperation originates from the cooperative process itself. As soon as a cooperative structure is established, there will be mechanisms that drive the cooperation further. This idea rests on concepts from the institutionalism literature.

First of all, it is hard to establish intelligence cooperation in the absence of trust. Therefore, trust building may be a forceful driver of increased cooperation. But what is it that generates trust building in a relationship? Trust building is a process with its own momentum where every successful act of risk taking on behalf of others generates trust. It follows that if the risk taking backfires, for example due to opportunistic behaviour by the trustee, the accumulated trust may vanish. So, trust is a volatile commodity. Another, although similar, way is that by cooperating one tends to get familiar with the preferences of others. Both processes thus generate trust over time. By taking common risks and getting familiar with the preferences of others trust accumulates.

The second factor relates to the effects of institutional design. Does the chosen form of a cooperative structure drive the states to cooperate more or less? A vital design question is how the institution is going to be controlled. This can be viewed as a continuum between two endpoints. One contains no centralization of control. Any state is a full and equal member of the institution, and rules are established and changed by traditional bargaining, deliberations, or by technical expertise of the represented states. A more centralized model is one that includes clear elements of hierarchy in the cooperation. Some members are thus more powerful than others. This is of course a sensitive point since it goes against one of the most prominent principles of international relations, the sovereignty of states. Some form of hierarchy may be a precondition for powerful states if they are to take part in intelligence cooperation.

## Conclusion

Thus far, this report has conceptualised the development of multilateral intelligence cooperation and how this can be explained by the configuration of some key state preferences. Furthermore, it has suggested reasons to why and how these preferences might change. Bringing these aspects together, the following three chapters employ the drivers that affect the dynamics in cooperation by altering key state interests as an instrument to structure the analysis into three constituent parts, focusing on the subjects of intelligence cooperation in the EU (driven by internal demand), intelligence culture in and cooperation with Asia (driven by external pressure), and intelligence cooperation in a Post-Brexit Europe (driven by cooperative momentum).

# 3  Intelligence cooperation in the European Union

## Introduction

In chapter two it was concluded that enhanced European intelligence cooperation can be the answer to the EU member states' perception that they face domestic problems they currently are unable or unwilling to address unilaterally. Specifically, common policies on internal and external security can accentuate the need of 'common' intelligence to underpin these policies. Moreover, there is a need for an increased intelligence capacity as EU member states perceive that they can reach more cost-efficient solutions together. This chapter on intelligence cooperation in the EU outlines how, driven by these internal demands, it is intelligence cooperation in the field of early warning that can help the EU better respond to external conflicts and crises, support the protection of the Union and its citizens, and advance the development of a common European intelligence culture. The latter encompasses things like shared

norms of behaviour, thinking collectively about future security challenges and threats and understanding each other's perceptions and outlook.[23]

Intelligence and security institutions have a more than average need to have foreknowledge of events. Therefore, one of their core functions is to provide early warning for both threats and opportunities. Furthermore, new types of threat, for instance climate change and pandemics resulting in security risks, or hybrid conflict, require new forms of international cooperation. Moreover, intelligence and security institutions are becoming increasingly involved with addressing complex issues, or 'wicked problems', for which no easy policy solutions present themselves. Also, the increasing number of transnational risks resulting from our increasingly interconnected societies demand an effective international collaboration. It is only by sharing information and resources, or by producing them collectively, that these complex security threats can be successfully analysed, forecast and managed. When seen from this perspective, European intelligence cooperation becomes a natural extension of the high level of interconnectedness that characterises Europe following decades of integration.[24]

When it comes to crisis management, the purpose of early warning is to alert decision-makers of the potential outbreak, escalation and resurgence of a crisis, and to promote an understanding among decisionmakers of the nature of the crisis and its possible impacts.[25] There is a consensus that in the context of crisis management, earlier equates with better: the earlier a potential crisis is detected, the easier it is to diminish its scope or prevent it altogether.[26] The increased complexity of the security environment underscores the need for policymakers and the intelligence community to start thinking about more sophisticated early warning systems.[27] Herein, the role for intelligence will be providing a more complex analysis, probing and trying to identify and make sense of the so-called 'unknown-unknowns'. It will have to change to a more open early warning system that probes and attempts to make sense of possible multiple scenarios. And analysts and policymakers will have to judge and assess together which are the

---

23   Damien Van Puyvelde, "European Intelligence Agendas and the Way Forward," *International Journal of Intelligence and Counterintelligence* 33, no. 3 (2020): 508; Yvan Lledo-Ferrer and Jan-Hendrik Dietrich, "Building a European Intelligence Community," *International Journal of Intelligence and Counterintelligence* 33, no. 3 (2020): 440-451.

24   Fägersten, "Bureaucratic Resistance," 94.

25   See Stefan Olsson (ed.), *Crisis Management in the European Union: Cooperation in the Face of Emergencies* (Berlin: Springer, 2009).

26   Florence Gaub, "Enhancing early warning and preparedness," in *Crisis Rooms: Towards a global network?*, eds. Patryk Pawlak and Andrea Ricci (Paris: European Union Institute for Security Studies, 2014), 78-82.

27   Sarah Bressan and Aurora Bergmaier, "From conflict early warning to fostering resilience? Chasing convergence in EU foreign policy," *Democratization* (2021).

more probable scenarios they should be responding to. It will require imagination to develop these scenarios.[28]

## Towards a hybrid early warning system

As one of today's global powers the EU continues to be confronted with situations of violent conflict all around the world. To step into its desired role of security actor, the EU needs to engage with early warning and crisis prevention, or it will risk playing catch-up too often. In order to strengthen the EU's predictive and preventive capabilities, the EEAS and European Commission rolled out the EU conflict Early Warning System (EWS) in 2014. In the context of intensified collaboration between the EU and NATO, it is important to look at areas where both organisations might learn from each other. This section therefore describes the process of this particular early warning system and compares it to the NATO Intelligence Warning System (NIWS) in order to assess how the EU can strengthen its EWS by infusing it with elements from the NIWS.

The EWS is a risk-management tool that has been set up to identify conflict prevention and peace building opportunities in conflict-prone regions. It aims to identify, prioritise and assess situations at risk of violent conflict in countries outside of the EU, thus contributing to the external security of the Union. The EWS obtains its input from the Global Conflict Risk Index (GCRI), which includes a list of structural indicators to forecast the probability and intensity of violent conflict over a timeline of four years.[29] The warning cycle itself takes 2,5 years and consists of four phases: global risk scanning, prioritisation of countries, in-country shared assessment and follow-up missions, and monitoring. The cycle is concluded with an overall monitoring report that is presented in the Political and Security Committee (PSC). While the global risk scanning step takes place yearly, the monitoring period for the implementation of identified actions in prioritised countries has recently been extended to 2,5 years.[30]

Intelligence is predominantly involved in the preparatory component of risk scanning. In this phase, input from the GCRI, open source analyses and internal assessments by the EEAS and the Commission are complemented with analyses provided by the SIAC.[31] This framework combines intelligence from the EU INTCEN (civil branch) and the EU Military Staff Intelligence Directorate (military branch) into all-source intelligence

---

28  Chong Guan Kwa, "Postmodern Intelligence: Strategic Warning and Crisis Management," in *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, eds. Floribert Baudet, Eleni Braat, Jeoffrey van Woensel and Aad Wever (The Hague: Asser, 2017), 97-118.

29  European Commission, *EU conflict Early Warning System: Objectives, Process and Guidance for Implementation - 2020*, SWD (2021) 59 final, March 10, 2021, 3.

30  EWS team members, interviewed by Claire Korteweg, online, July 27, 2021.

31  European Commission, *EU conflict Early Warning System*, 4.

assessments. The collaboration between the EWS and SIAC started in 2014 and has proven to be beneficial ever since.[32] In order to help inform the warning cycle, the SIAC is tasked to develop analyses specifically for the EWS. These analyses have a geographical approach, focusing on six regions of the world with a medium to long-term timeframe of up to 4 years. SIAC's analyses for the EWS focus on structural risk factors and resilience factors as well as the role of external actors and the risk of spill-over.[33] Additionally, as a customer of SIAC, the EWS team also has access to SIAC's other products and uses these to inform their warning cycle as well.

In terms of a further operationalisation of the EWS warning cycle, NATO may provide a constructive example. NATO redesigned its NIWS in 2002 to serve as a format to share knowledge and information in a simple and understandable manner. Central to the NIWS methodology is the formulation of a 'Warning Problem': a clear, concise statement describing the warning issue of interest to the Alliance (not any particular member state) and the so-called end-state that must be deterred. A distinction is made between conventional (country) and transnational warning problems. NATO's warning cycle is divided into five stages: (1) Define the threat, (2) Develop scenarios, (3) Develop critical indicators, (4) Collect and collate intelligence, and (5) Issue warning (see figure).

**Figure 1      The five stages of NATO's intelligence warning cycle**



---
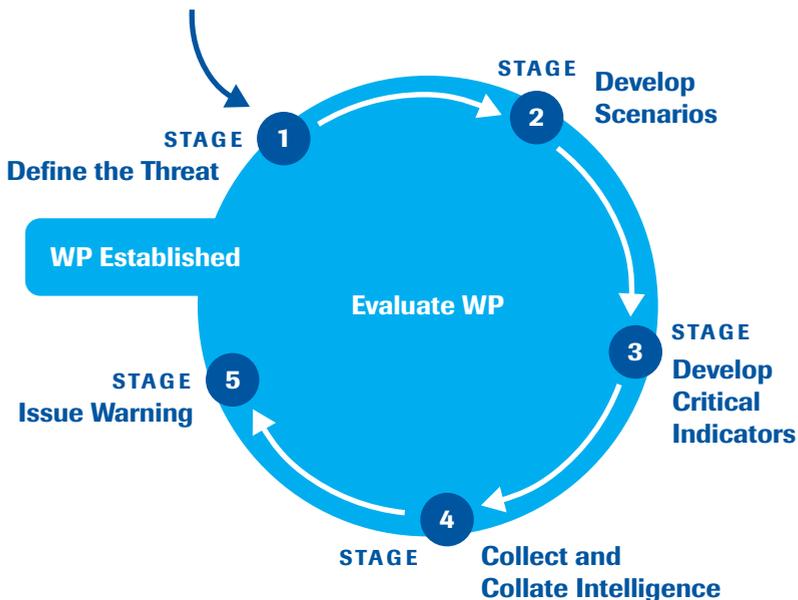
32   EWS team members, interviewed by Claire Korteweg, online, July 27, 2021.

33   EWS team members, interviewed by Claire Korteweg, online, July 27, 2021.

Each warning problem is sponsored by a member state, which produces a warning report every thirty days consisting of three analytical tiers. The first tier contains a short and concise overview and trend assessment aimed at decision-makers. The second tier consists of a warning matrix assessing different aspects of a threatening situation. The third and last tier consists of a list of critical indicators that represent crucial turning points in the evolution of a situation and their assessed status. Critical indicators can cover a broad range of aspects and may be political, military, economic, social or technical. The NIWS method is intended to feed into crisis management at NATO. If a warning is significant enough, it will trigger the NATO Crisis Response System (NCRS) and the North Atlantic Committee (NAC) will then need to issue a response accordingly.[34]

Looking at the designs of both warning cycles, the processes of the EU and NATO seem similar, yet their content differs greatly. Firstly, while NATO works with specific warning problems as described above, the EU EWS produces broader country assessments instead of specific scenarios, although the focus of these assessments will be shifting to a more geographical approach, as the GCRI is framed in 6 regions. The reason for this difference can be found in the character of both organisations. Influencing structural risk drivers is a better fit for the EU's broader conflict prevention toolbox, of which the EWS is one part. It sets out to compare which countries are most at risk of conflict with the help of multiple global, open-source datasets. Scenario analysis may happen if this is deemed necessary for prioritised countries, although this is not usually within the EWS process itself, but rather happens as part of the broader toolbox. NATO on the other hand, as a military organisation, will logically focus more on very specific outbreaks of conflict and look less into the economic and socio-political opportunities to prevent them.

Secondly, NATO member states supply the NIWS with intelligence from their national agencies. Meanwhile, the EWS obtains its intelligence input from SIAC, which does not have its own collection capabilities and thus depends solely on voluntary contributions from the EU member states. While the relationship between the EWS team and SIAC is a strong one, this is not necessarily the case at the input side as it has been reported that member states are reluctant to share operational or single source data with INTCEN.[35] Compared to the more direct link between NATO member states and their points of contact, this particular relationship might undermine the efficiency of sharing crucial information with the EWS. Member states must be adequately incentivised to share their national intelligence with each other through EU institutions. Building trust is

---

34    NATO School, "Introduction to NIWS," NATO Intelligence Warning Systems Course N2-47-C-10.

35    Simon Duke, "Intelligence and EU External Relations: Operational to Constitutive Politics," in *The Politics of Information - The Case of the European Union*, eds. Tannelie Blom and Sophie Vanhoonacker (Palgrave Macmillan, 2014), 251.

crucial to this end and will be discussed later in this chapter. More effective intelligence-sharing will lead to better results, consequentially leading to more trust and even more willingness to cooperate.

Thirdly, the warning cycle of each organisation differs in duration. The EWS cycle currently takes 2,5 years to complete. The process consists of two in-country missions and three reports culminating in the final monitoring report presented in the PSC.[36] The NIWS warning reports, by contrast, look 90 days ahead and are updated every 30 days by the sponsor state. These are backed up by NATO's annual strategic intelligence estimates covering all regions and transnational issues, providing a very effective combination of both short-term and long-term analyses.

## Towards joint sensemaking in crises

Over the past two decades, the EU has put considerable effort into protecting external security and has been actively engaged in regions far from its borders. The next decades of the 21st century, however, ask for additional and different types of action much closer to home and within our borders. One of the most pressing security issues of our time is the emergence of hybrid conflict, also known as grey zone operations.[37] In this section the need for a clear definition and common understanding of the term 'hybrid' is discussed, as well as the importance of sensemaking in this field and the potential contribution of both EU and NATO collaborative frameworks. Furthermore, the possibility of applying early warning methods to these new kind of threats is assessed.

As is the case with all issues that are subject to cooperation, a clear definition contributes to a common understanding of the problem and is crucial for an efficient approach. This is particularly important for hybrid threats, as the term 'hybrid' has been used to cover a rather broad range of subjects and measures. The European Commission's Joint Framework on countering hybrid threats describes these as "the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological) […] while remaining below the threshold of formally declared warfare."[38] This includes a very diverse range of activities to protect against, thus making it imperative that all organisations involved be on the same page. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki has been of great value in solidifying the conceptual basis of the threats we are facing and has published numerous analyses on the subject in cooperation

---

36   European Commission, *EU conflict Early Warning System*, 8.

37   Frank Bekkers, Rick Meessen and Deborah Lassche, *Hybrid Conflicts: The New Normal?* (The Hague: TNO & The Hague Centre for Strategic Studies, 2019).

38   European Commission, Joint Framework on countering hybrid threats, April 6, 2016, 2.

with academic and policy institutions across Europe.[39] The concept of hybrid warfare is certainly not a new phenomenon. However, with digital technologies being developed at a rapid pace, its possibilities now seem endless and it is becoming increasingly harder to anticipate and protect against. Unsurprisingly, Russia and China are currently the most threatening actors using hybrid methods in an attempt to destabilise Europe, thereby further undermining a global order already under pressure.[40]

When working with complex issues such as hybrid threats, it is perhaps helpful to consider the existing concept of sensemaking in crisis applied to so-called 'wicked problems'.[41] Wicked problems are gaining importance because of their transnational character, "in a world where nation-states are no longer the principal actors."[42] As opposed to the traditional puzzles (questions to which we can find a definitive answer) and mysteries (questions to which no one truly knows the answer), wicked problems are not only essentially unsolvable, but possible solutions may change the problem altogether.[43] What is crucial in sensemaking, especially so with wicked problems, is to consider all factors possibly involved, even the ones that may seem irrelevant at first and to continuously question existing assumptions.[44] Moreover, Moore reminds us that "sense-makers can never know if they have determined all the solutions to a wicked problem."[45] Early warning in this field can be hindered by the lack of consensus on the different meanings and interpretations of the term hybrid. The concept as formulated by the European Commission is insufficiently delimited and the development of a more specific definition is still ongoing. Moreover, non-state actors and non-military instruments make it increasingly difficult to identify future attacks, let alone warn for them.[46] To reach a greater degree of situational awareness and common understanding within the EU of hybrid threats as wicked problems, contribution of the Hybrid CoE as well as SIAC remains indispensable.

---

39   See for example European Union and Hybrid CoE, *The Landscape of Hybrid Threats: A Conceptual Model* (Luxembourg: Publications Office of the European Union, 2021).

40   Danny Pronk, *Hybrid Conflict and the Future European Security Environment* (The Hague: The Clingendael Institute, 2018); Treverton et al., *Addressing Hybrid Threats*.

41   Arjen Boin, Magnus Ekengren and Mark Rhinard, "Sensemaking in crises: what role for the EU?" in *Crisis Rooms: Towards a global network?*, eds. Patryk Pawlak and Andrea Ricci (Paris: European Union Institute for Security Studies, 2014), 118-125.

42   David Moore and Robert Hoffman, "Sensemaking: A Transformative Paradigm," *American Intelligence Journal* 29, no. 1 (2011): 29.

43   David Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Defence Intelligence College, 2011), 19.

44   David Moore, Elizabeth Moore, Seth Cantey and Robert Hoffman, "Sensemaking for 21st century intelligence," *Journal of Intelligence History* 20, no. 1 (2021): 45-59.

45   Moore, *Sensemaking*, 24.

46   Patrick Cullen, *Hybrid threats as a new 'wicked problem' for early warning*, Strategic Analysis 8 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, May 2018), 4.

Although hybrid conflict has mostly stayed under the threshold of violence needed to trigger Article 5, actions in the grey zone also effect NATO and its member states, as well as the EU. As a direct response NATO has set up its own Hybrid Analysis Branch. It has produced parallel and coordinated assessments in collaboration with the EU INTCEN Hybrid Fusion Cell, thereby illustrating the value of close cooperation and complementarity between EU and NATO.[47] But while extensive efforts have been made on describing and defining hybrid, now is the time to take it further and identify concrete ways to be better prepared for modern challenges such as hybrid threats. One option may be to investigate whether the EWS or NIWS could be applied to hybrid threats, or whether it is possible to develop an entirely new early warning system for these specific threats.[48] The Hybrid CoE has already stated that "there is still a lot to do in the context of determining the indicators of hybrid threats, and their prioritisation, tracking, detection and attribution."[49] Taking the ambiguous character of hybrid threats into account, the Hybrid CoE observes that "warning intelligence must look for indications of activity that can turn into hybrid threats beyond the traditional realm of military activity."[50] Moreover, hybrid threats are constantly changing and evolving, which means that our response to them also needs to be constantly evolving in order to keep up.[51]

## Towards a common intelligence culture

Interacting regularly, getting to know each other and learning from each other are crucial steps in order to build trust within the broader intelligence community. While many intelligence and security services in Europe often work well together already, a common European intelligence culture is still lacking.[52] In 2017, during a speech about the future of Europe, French president Emmanuel Macron advocated for a common culture in Europe and suggested the idea of a European intelligence academy. This idea was further developed into the Intelligence College Europe (ICE), launched in 2019 in

47   Gustav Lindstrom and Thierry Tardy (eds.), *The EU and NATO: The essential partners* (Paris: European Union Institute for Security Studies, 2019); Council of the European Union, *Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils*, Brussels, June 3, 2021; Council of the European Union, *Fifth progress report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, Brussels, July 22, 2021.

48   NATO Advanced Research Workshop, *Pooling Expertise to Develop the Early Warning System to Counter Hybrid Threats*, 25-26 April 2019; Sebastiaan Rietjens, *A warning system for hybrid threats - is it possible?* Strategic Analysis 22 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2020).

49   Treverton et al., *Addressing Hybrid Threats*, 67.

50   Cullen, *Hybrid threats as a new 'wicked problem' for early warning*, 4.

51   Eitvydas Bajarūnas, "*Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond*," *European View* 19, no. 1 (2020).

52   Lledo-Ferrer and Dietrich, "Building a European Intelligence Community".

Paris. In reality it is neither an academy nor a college. The Letter of Intent, signed by 23 European countries in February 2020, states the College's function as "a platform for reflection, engagement and outreach."[53] Bulgaria, Greece, Ireland, Luxemburg, Poland, Slovakia and Switzerland have either joined in a more flexible partner status, or are expected to become full members later.[54] The goal of the ICE is to facilitate dialogue at a non-operational level between the different member states' intelligence communities, as well as between practitioners, academics and decision-makers. By creating such a platform to share knowledge and experiences, the ICE "enriches national cultures with an additional European layer, which is not imposed from above but is actually shaped by the individual intelligence officers themselves through regular interaction with their peers."[55]

The strength of the ICE lies in the fact that participation is not limited to intelligence officers, but includes a larger network of intelligence and security experts, academics and decision-makers at both national and European levels. Collaboration happens through "community webinars, seminars and research on key security and intelligence issues," according to Beth Sizeland, who has taken on the year-long presidency of the College as of February 2021. The theme of the activities to be organized this year is 'fusing policy and intelligence to build resilience in the 21st century.'[56] While the ICE will not facilitate discussions about operational issues, it does provide a space to discuss all kinds of surrounding, non-operational topics – e.g. issues such as accountability – that all European agencies might encounter in a more informal manner through personal interaction. This also provides a great opportunity for reaching out to a larger public. To promote security in the 21st century it is ever more important to create understanding across society for the work of intelligence and security agencies. While secrecy is an inherent part of their activities, agencies should strive to be more open about their perceptions and have public discussions about the difficulties they deal with on a day-to-day basis in order to cultivate more understanding and support for their work.

The ICE is a place where EU and national practitioners can meet and discuss, making it the perfect venue to discuss how national agencies can contribute more to EU efforts in the fields of intelligence and security. As already stated, smooth cooperation is crucial for effective early warning, thereby protecting European external security. Moreover, solid links between practitioners in Europe are also imperative to improve joint situational awareness and reach a common understanding of issues threatening

---

53  "*Letter of Intent*," Intelligence College in Europe, published in February 2020

54  "*European Spies Dare to Share*," Politico, published February 26, 2020.

55  Lledo-Ferrer and Dietrich, "Building a European Intelligence Community," 447; Rubén Arcos and José-Miguel Palacios, "EU INTCEN: a transnational European culture of intelligence analysis?", *Intelligence and National Security* 35, no. 1 (2020): 72-94.

56  "*Declaration of Mrs. Beth Sizeland*," Intelligence College in Europe, published in March 2021.

our internal security, particularly hybrid threats. These threats can only be addressed through an approach that integrates intelligence and security as well as mobilises the whole of society.[57] To this end, a common paradigm and conceptual framework are essential and this can be reached inter alia by regular interaction and open discussions which the ICE can enable.

## Conclusion

This chapter has outlined how, driven by internal demand, intelligence cooperation in the field of (hybrid) early warning can help the EU better respond to external conflicts and crises, support the protection of the Union and its citizens, and advance the development of a common European intelligence culture. The EU and NATO are obviously organisations with clearly different characters and toolboxes. Nevertheless, there are opportunities to learn from each other. The operationalisation of the EWS could be strengthened by infusing it with elements from the NIWS. First, including warning problems in the process would allow the EEAS to better prepare for specific threatening situations in a more targeted manner. This method also allows for a more detailed and focused list of critical indicators. Second, one of NATO's success factors is the division of labour between member states and NATO institutions with regards to the warning cycle as well as the follow-up actions. One member state takes responsibility for one particular crisis area or issue for which they formulate scenarios, which they monitor and report on to NATO. With this system of institutionalised burden-sharing, resources can be focused on one problem at a time while the findings can be shared with all member states and institutions.[58] Finally, NATO combines its annual long-term estimates with regular reports looking back and forward 90 days. These reports serve as direct input for the NCRS, thereby directly influencing decision-making at the highest political level. This combination of a long-term and short-term focus may provide an even more comprehensive approach for the EU's early warning strategy, allowing it not only to look at the structural risks and opportunities but also to be on higher alert for when to step into its role of global security actor.

Lack of trust, but also lack of experience has often been an obstacle for deeper cooperation between EU member states on sensitive topics involving national security, thus touching upon national sovereignty. Nonetheless, the EU has shown that it is willing and increasingly capable of dealing with complex, transnational issues, both on its own and in cooperation with NATO. It is now crucial to press ahead with concrete actions for the EU to continue to show its added value. If it succeeds to do so, more cooperation will

---

57    Treverton et al., *Addressing Hybrid Threats*, 80.

58    See Tania Latici, *How the Strategic Compass can incubate a European prototype for burden sharing* (Brussels: Egmont Royal Institute for International Relations, 2021).

follow, as member states will deem they have more to gain and less to lose from getting involved. EU cooperation on enhancing resilience and countering hybrid threats needs to be guided by a regularly updated threat assessment and a comprehensive situational awareness. The work of the EU Hybrid Fusion Cell should be further enhanced, taking into account an appropriate level of resources including professional expertise, in order to achieve a common, inter-institutional, EU-wide approach on hybrid threats and a comprehensive situational awareness. Within existing limitations of classified information sharing, the Hybrid Fusion Cell needs to strengthen and enhance its close cooperation with both NATO's Hybrid Analysis Branch and the Hybrid CoE, with the aim of strengthening joint situational awareness and a mutual understanding of respective activities.

Finally, the Netherlands could use the platform of ICE to take the lead in organising discussions on all of the issues mentioned in this chapter. The Netherlands Defence Intelligence and Security Service (MIVD) has demonstrated its expertise before when it hosted the annual NATO Warning Intelligence Working Group and Symposium together with NATO's Joint Intelligence and Security Division in 2019. The Dutch government also hosts the EU Early Warning/Early Action (EWEA) Forum twice a year in cooperation with Germany, during which practitioners from the EEAS and member states exchange views and knowledge about current threats and preventive actions.[59] The ICE therefore provides the ideal space and framework for the Netherlands to take on a leading role in organising relevant panels, seminars and discussions to promote European intelligence cooperation in the field of early warning and the development of a common culture among European intelligence and security experts.

---

59    Melle Brinkman, *EU samenwerking op Early Warning Early Action*, *De Veiligheidsdiplomaat*, May 18, 2021.

# 4 Intelligence culture in and cooperation with Asia

## Introduction

In chapter two it was concluded that external developments can influence state interests concerning intelligence cooperation. Changes in the international intelligence power balance may put pressure on a group of states to either rebalance an existing relationship to avoid a situation of intelligence dependency and reach a higher degree of autonomy, or to increase intelligence capabilities in order to balance against a common perceived threat. This external pressure is why the first step in the EU's Strategic Compass process for security and defence was producing a common threat analysis to identify the nature and severity of the threats facing the EU over the short to medium term (2025 to 2030).[60] Differences in the assessments of internal and external threats

---

[60] Daniel Fiott, *Uncharted territory? Towards a common threat analysis and a Strategic Compass for EU security and defence* (Paris: European Union Institute for Security Studies, 2020).

and challenges is one among many reasons why it is so difficult to form a common strategic culture in Europe. In order for a common European strategic culture to emerge, to be able to set common strategic goals and to better cooperate together, some degree of convergence of the different national strategic cultures is deemed necessary.[61] The same reasoning can be applied to the more narrow concept of intelligence culture.

Just as in the case of strategic cultures, one of the dividing lines between national intelligence cultures worldwide is their perceptions of past, current and future security threats. Another is for whom or what the national intelligence and security organisations are actually working. Is it for the state, the government, the constitution, or the people? Another are differences regarding the limitations of what constitutes intelligence. And finally, there can be differences in to what extent these organisations come under public scrutiny. Hence, a comparative analysis is needed to facilitate awareness of the extent of similarities and differences between national intelligence communities and cultures, and to allow for the identification of opportunities to increase both the scope and depth of cooperation. In order to do so, this report uses a framework that was suggested by Mark Phythian as a basis for the comparative analysis of European and Asian cultures of intelligence. This framework is based on four levels of analysis: strategic environment, regime type, organisation and society (see figure).[62]

**Figure 2  Levels of analysis for the comparison of intelligence cultures**

**Level 1:** Strategic environment

↕

**Level 2:** Regime type

↕

**Level 3:** Organisational

↕

**Level 4:** Societal

---

61 See Dick Zandee and Kimberley Kruijver, *The European Intervention Initiative* (The Hague: The Clingendael Institute, 2019); Dick Zandee and Kimberley Kruijver, *The European Intervention Initiative: a 'new kid on the block'*, (The Hague: The Clingendael Institute, 2019) for a discussion on the topic of a common strategic culture in Europe.

62 Mark Phythian, "Cultures of National Intelligence," in *Routledge Companion to Intelligence Studies*, eds. Robert Dover, Michael Goodman and Claudia Hillebrand (London and New York: Routledge, 2014), 33-41.

Using this framework, this chapter assesses whether useful entry points for European intelligence cultural convergence with Asia can be identified that enable EU intelligence cooperation with certain partners in that region. In order to do so, it analyses European commonalities with the intelligence culture of Japan in terms of that country's current and future security threats (level 1: strategic environment), the structure of its intelligence and security community and mission (level 3: organisation), and the way accountability is organised in terms of internal control and external oversight (level 4: society). At first sight there is no such thing as an Asian intelligence culture, with each intelligence organization having its own peculiarities, protocols, and structures. However, Asia's intelligence communities do have several common characteristics compared to European countries.[63] The selection of Japan as a case study here was made primarily based upon consideration of its similarities in regime type (level 2) with the EU member states, with Japan being one of three Asian countries, together with South Korea and Taiwan, that is consistently rated as a "full democracy" in the Democracy Index.[64] Japan is also one of the EU's closest, like-minded partners. The EU-Japan partnership is based on longstanding cooperation, shared values and principles such as democracy, the rule of law, human rights, good governance, multilateralism and open market economies.[65] Furthermore, EU-Japan relations have undergone a major uplift over the past years. Bound by the Economic and Strategic Partnership Agreements, as well as a Partnership on Sustainable Connectivity, the two once-distant players have been stepping up efforts to address the many shared security concerns in the Indo-Pacific and beyond.[66] Therefore, it is Japan's intelligence culture that is treated on the three levels of analysis in the three subsequent sections of this chapter.[67] To explore the potential of convergence in intelligence culture between Europe and Japan, these sections respectively analyse the level of overlap in the strategic environment, intelligence organisations and accountability.[68]

---

63 Bob de Graaff, "Elements of an Asian Intelligence Culture," in *Intelligence Communities & Cultures in Asia & the Middle East: A Comprehensive Reference*, ed. Bob de Graaff (Boulder and London: Lynne Rienner, 2020), 461-470.

64 See for the latest scores The Economist Intelligence Unit, *Democracy Index 2020: In sickness and in health?* (London: The Economist Intelligence Unit, January 2021).

65 See the factsheet on *EU-Japan relations - European External Action Service (europa.eu)*.

66 Céline Pajon and Eva Pejsova, *EU-Japan Relations: Moving Forward*, CSDS Policy Brief (Brussels: Brussels School of Governance, 2021).

67 The rest of this chapter is, unless stated otherwise, based on Yoshiki Kobayashi, "Japan," in *Intelligence Communities & Cultures in Asia & the Middle East: A Comprehensive Reference*, ed. Bob de Graaff (Boulder and London: Lynne Rienner, 2020), 149-162. Kobayashi's work is based on the analysis of publicly available data as well as interviews with former and current government officials in Japan.

68 Michito Tsuruoka and Daniel Fiott, *EU-Japan cooperation on defence capabilities: possibilities?* (Madrid: Elcano Royal Institute, 2020), similarly look at the rationale for closer European-Japanese cooperation on defence capabilities.

## The strategic environment of Japan

Europe and Japan have a common interest in developing cooperation in the area of intelligence that is conditioned by the shifting geopolitical landscape. As a middle power in Asia, Japan finds itself in a key arena of accelerating great power competition. Perhaps nowhere are the economic dominance and political-military ambitions of a rising China more evident and nowhere is the potential for military escalation between China and the US greater than in Asia. Much sooner than in other regions of the world, such as in Europe, it is the countries in Asia that have had to position themselves in the growing US-China rivalry that is expected to dominate the foreseeable future.[69]

What is notable about the strategic environment of Japan is that, first of all, while interdependency among countries is further expanding and deepening, thanks to growth of the national power of such countries as China, changes in the balance of power are accelerating and becoming more complex.[70] In addition, uncertainty over the existing order is increasing. Against this backdrop, competition on a continuous basis is emerging across the political, economic and military realms, in which states seek to shape global and regional orders to their advantage as well as to increase their influence. In this competition, hybrid tactics are adopted, forcing affected actors to take complex measures not limited to pure military ones. So-called grey zone situations are becoming persistent over a long period of time, playing out as part of this competition, and they might increase and expand in the future.

Secondly, technological progress is about to change fundamentally how security should be managed. Against the backdrop of the advance of military technology due to rapid technological innovation, contemporary warfare increasingly features capabilities combined across all domains: not only land, sea and air, but also new domains, such as space and cyberspace. States are seeking to gain superiority in the technologies that undergird capabilities in these new domains, and they endeavour to develop weapons that leverage potentially game-changing technologies that could drastically change the conduct of future warfare. It is believed that the development and international transfer of civilian technologies will have a major impact on improvements in the military capabilities of each country, and that technological innovations are expected to make it difficult to foresee future warfare.

---

69    Linda Maduz, "*Chapter 5: Japan and South Korea: Adapting to Asia's Changing Regional Order*," in *Strategic Trends 2021: Key Developments in Global Affairs*, eds. Brian Carlson and Oliver Thränert (Zurich: Centre for Security Studies, 2021).

70    This summation is derived from Ministry of Defence, "Chapter 1: 'Security Environment Surrounding Japan," *Defence of Japan 2021* (Annual White Paper).

Thirdly, security challenges which cannot be dealt with by a single country alone are emerging. First of all, securing the stable use of and promoting the rule of law in new domains such as space and cyberspace has become an important challenge. In the maritime domain, there have been cases where a country unilaterally claims its entitlement and takes actions based on its own assertions that are incompatible with the existing international order, thereby unduly infringing upon the freedom of navigation on the high seas and of overflight. The proliferation of weapons of mass destruction and of ballistic missiles that serve as their means of delivery and international terrorism are also viewed as significant threats, and there is a clear need to continue to monitor such issues. In order to counter these challenges in Japan's security environment, it is deemed essential not only to strengthen Japan's own capabilities, but also to closely cooperate with countries that share the same fundamental values.

## The Japanese intelligence community

Currently, the intelligence community in Japan consists of five organisations: the Cabinet Intelligence and Research Office (CIRO), the Defence Intelligence Headquarters (DIH) of the Ministry of Defence, the Intelligence and Analysis Service (IAS) of the Ministry of Foreign Affairs, the Public Security Intelligence Agency (PSIA), and the National Police Agency (NPA).[71]

– *Cabinet Intelligence and Research Office.* The CIRO's roles and functions are somewhat similar to those of the Cabinet Office in the United Kingdom. Since the CIRO is a part of the cabinet secretariat, it is directly connected to the prime minister and responsible for coordinating the entire intelligence community. The director meets with the prime minister on a regular basis (usually at least once or twice a week) to provide updated intelligence briefings, and also attends National Security Council (NSC) meetings. The NSC is chaired by the prime minister, and its other core members include the chief cabinet secretary, foreign minister, and defence minister. The CIRO does not have much intelligence collection capabilities of its own, except for the Cabinet Satellite Intelligence Centre (CSIC) and the International Counterterrorism Intelligence Collection Unit (CTU), both of which are affiliated with the CIRO. The CSIC is in charge of running the reconnaissance satellite program which operates synthetic-aperture radar satellites as well as electro-optical satellites. The CTU is responsible for collecting terrorism-related intelligence abroad, the political momentum for which accelerated after the it was decided to hold the Olympic Games in Tokyo. The CIRO has fairly intensive analytical capabilities and is responsible for producing estimative intelligence reports, which are "all-source" products representing the official views of the entire intelligence community.

---

71 See for an overview Cabinet Secretariat of Japan, *Japan's Intelligence Functions* (Tokyo: Cabinet Secretariat, 2013).

All of these functions of the CIRO have been enhanced as a result of recent reforms to the Japanese intelligence community.[72]

– *Defence Intelligence Headquarters.* Resorting under Japan's Ministry of Defence, the DIH deals with military intelligence, including signals intelligence (SIGINT) and imagery intelligence (IMINT). The DIH's roles and functions are thus somewhat similar to those of the Netherlands Defence Intelligence and Security Service (MIVD).

– *Intelligence and Analysis Service.* Located within the Ministry of Foreign Affairs, the IAS provides general analyses of the international situation for diplomatic purposes. The main sources of the IAS's analyses are the diplomatic cables sent from Japan's diplomatic missions overseas.

– *Public Security Intelligence Agency.* The PSIA is an affiliated agency of Japan's Ministry of Justice. Its mission is to investigate organizations that engage in violent activities against the public. For example, Aum Shinrikyo, the cult which carried out the sarin gas attack on the subway system in Tokyo in 1995, has been under the PSIA's surveillance. This is somewhat similar to the Dutch National Counter-Terrorism and Security Coordinator (NCTV).

– *National Police Agency.* Within the NPA, the Security Bureau is in charge of counter-terrorism, counter-intelligence, counter-proliferation, and the investigation of national security-related criminal cases. The NPA does not have its own investigative powers or jurisdiction. Instead, it is responsible for coordinating all prefectural police forces in the country. This is similar to the internal security roles and functions of the Netherlands General Intelligence and Security Service (AIVD).

In 2008 four organizations joined the intelligence community as associate member organizations: the Financial Services Agency; the Ministry of Finance; the Ministry of Economics, Trade, and Industry; and the Coast Guard. These associate members participate in intelligence community activities on an ad hoc basis. For instance, the Coast Guard may be involved in the assessment of maritime territorial disputes between Japan and neighbouring countries.

## Intelligence accountability in Japan

According to the intelligence cycle theory, the primary mission of any intelligence community is to support decision-making by policymakers, and intelligence activities should thus be initiated by the delivery of policymakers' intelligence requirements to the intelligence community. Therefore, there should be a mechanism within the government that effectively connects the policymakers with the intelligence community. Otherwise,

---

72   Yoshiki Kobayashi, "Assessing Reform of the Japanese Intelligence Community," *International Journal of Intelligence and Counterintelligence* 28, no. 4 (2015): 717–733.

policymakers' intelligence requirements cannot be properly delivered to the community and, as a consequence, the community cannot function adequately.[73]

Within the government of Japan, the Cabinet Intelligence Council (CIC) is regarded as the primary hub connecting policymakers and the intelligence community. Within the cabinet secretariat, the CIC is chaired by the chief cabinet secretary, and its members include senior officials (i.e. vice-ministerial–level officials) of major policy departments as well as the heads of the member organizations of the intelligence community, with the CIRO performing secretarial functions. The CIC is responsible for assembling and deciding the intelligence requirements of the entire Japanese government as well as for delivering these requirements to the intelligence community. The community, in turn, is supposed to produce intelligence products such as the estimative reports based on the given requirements and to report these products back to the CIC. The director of cabinet intelligence is almost always invited to attend NSC meetings, representing Japan's intelligence community as a whole.

In Japan, neither policymakers nor the general public appear to have paid much attention to the issue of oversight. Japan has had a functioning parliamentary system since its political modernization in the late nineteenth century, so in theory all governmental activities, including those of the intelligence community, are accountable to the national parliament (the Diet). Cabinet ministers related to the intelligence community, such as chief cabinet secretary, foreign minister, defence minister, and justice minister, answer to the Diet's inquiries regarding the intelligence community's activities. However, beyond that Japan currently has no major mechanism specialized in the oversight of the intelligence community equivalent to the Dutch parliamentary Intelligence and Security Committee (CIVD), nor to the Dutch Review Committee on the Intelligence and Security Services (CTIVD).

## Conclusion

According to the latest guidelines for strengthening Dutch and EU cooperation with partners in Asia, the EU should step up its security efforts in Asia, exploring opportunities in the realm of defence and security.[74] In this context, this chapter has identified useful entry points for European intelligence cultural convergence with Asia that can enable more EU intelligence cooperation with that particular region. It has done so by analysing European commonalities with the intelligence culture of Japan in terms of that country's perceived security threats, the structure of its intelligence community

---

73   Yoshiki Kobayashi, *Fundamentals of Intelligence*, 2nd ed. (Tokyo: Tachibana Shobo, 2014), 58–59.

74   Government of the Netherlands, *Indo-Pacific: Guidelines for strengthening Dutch and EU cooperation with partners in Asia*, 13 November 2020.

and mission, and the way its accountability is organised both in terms of internal control and external oversight.

It is in particular the presence of a common perceived challenge in the shape of China that will make Japan more inclined to seek intelligence gains through cooperation with the EU, and vice versa. The rise of China opens clear opportunities for the EU and its member states for more cooperation with Japan on security issues. And the EU and Japan seem to be natural cooperation partners: they share the same values and are both democratic entities. As the flag bearer of universal values in the Indo-Pacific region, such as freedom, democracy, the rule of law, and respect for fundamental human rights, Japan is keen to join hands with like-minded partners. Moreover, although located in different parts of the world, the EU and Japan have many similarities, including a more comprehensive view of security and the challenges posed by the increasing strategic competition between states.[75]

Both the EU and Japan face an increasingly insecure environment and there is convergence across a growing number of policy dimensions. There is therefore an untapped potential for cooperation. The Strategic Partnership Agreement between the EU and Japan which entered into force in 2019 makes explicit references to more cooperation, specifically in areas such as military and regional security, which have hitherto achieved mostly low levels of cooperation. It allows the EU and Japan to develop an agenda for future cooperation, and has set a useful framework to establish collaboration that promises to directly enhance the security of both.[76] According to the EU Strategy for Cooperation in the Indo-Pacific launched in April 2021, the EU will strengthen cooperation with certain partners in Asia on counter-terrorism, cyber-security, maritime security and crisis management.[77] Therefore, possible agenda items could be the sharing of intelligence on existing and potential threats and security risks to space systems, on China's military affairs, maritime policy and the modernisation of the People's Liberation Army (PLA), on nuclear and ballistic missile developments in North Korea, and on terrorism.

75   Jeffrey Hornung, *Allies Growing Closer: Japan–Europe Security Ties in the Age of Strategic Competition (Santa Monica: The RAND Corporation*, 2020).

76   Emil Kirchner and Han Dorussen, "New horizons in EU–Japan security cooperation," *Asia Europe Journal* 19, no. 1 (2021): 27–41.

77   Council of the European Union, *Indo-Pacific: Council adopts conclusions on EU strategy for cooperation - Consilium (europa.eu)*, Brussels, 16 April 2021.

# 5   Intelligence cooperation in a post-Brexit Europe

## Introduction

While the British political decision to leave the EU generated much debate and concern about Britain's future in Europe, Brexit so far hasn't really impacted the intelligence and security ties between Britain and Europe. Especially in matters of counter-terrorism, Britain is firmly bound to Europe. It is every day, 'bread-and-butter' intelligence cooperation that indicates the effective participation of Britain in the European space of counter-terrorism cooperation.[78] This has been aided by the fact that over the years, the EU has developed into an international counter-terrorism actor in its own right,

---

78   Hager Ben Jaffel, *Anglo-European Intelligence Cooperation: Britain in Europe, Europe in Britain* (London and New York: Routledge, 2020).

a role that is increasingly accepted by third countries.[79] However, if the EU and the United Kingdom do not manage to create a strategic partnership in the field of intelligence – a 'special relationship', as it were – both sides will lose. The UK remains a potentially valuable partner for the EU in military and political terms. In the security and defence domains, Brussels will therefore surely benefit from collaborating with London, and vice versa.[80]

A comparative study of collaborative security regimes post-Brexit based on the overlap in national strategic documents found that there is potential for future convergence between EU and the UK at the industrial level, in internal security matters and in military missions.[81] So, while there are good reasons to maintain practical cooperation between the UK and the EU after Brexit in many areas, cooperation between intelligence services is another obvious example given the security challenges currently facing Europe. Moreover, there is no point in debating who needs the other more. Both Brussels and London stand to gain from a partnership. First of all, this will send a strong signal to the other global powers, such as Russia and China, that in intelligence matters even after Brexit there still is one Europe, which is in the interest of all European states. Secondly, the UK will also benefit, because it retains an important asset in its own trans-Atlantic 'special relationship' with the US. And thirdly, the EU member states will benefit because if the UK remains fully involved in the CSDP, they need not fear the emergence of new parallel circuits that would bypass the EU.[82]

In chapter two it was concluded that intelligence cooperation can originate from the cooperative process itself. As soon as a cooperative structure is established, there will be mechanisms that will drive the cooperation further. Trust building may in particular be a forceful driver of increased cooperation. In light of the presence of this important driver – cooperative momentum – this chapter identifies a clear opportunity for the continued engagement of British intelligence and security services in an existing European cooperative arrangement for tackling one of the most complex security challenges facing the EU over the next ten years, namely the smuggling of drugs. In today's interconnected world, this phenomenon is increasingly global. Moreover, organised crime groups, of which more than one-third are directly involved in the drug markets, are also very adaptive. After cannabis, the cocaine market is the second largest

79  Jörg Monar, "The EU as an International Counter-terrorism Actor: Progress and Constraints," *Intelligence and National Security* 30, no. 2-3 (2015), 333-356.

80  Paolo D'Alesio, *EU-UK Defence Cooperation After Brexit* (Brussels: Finabel, 2021).

81  Cornelia Baciu, "Collaborative security regimes post-Brexit – estimating the potential for convergence based on the overlap in national strategic documents. A comparative study of EU27+1 and the US," *Comparative Strategy* 39, no. 6 (2020): 549-564.

82  Cornelia Baciu and John Doyle (eds.), *Peace, Security and Defence Cooperation in Post-Brexit Europe: Risks and Opportunities* (Cham: Springer, 2019).

illicit drug market in the EU. Seizures of large volumes of the drug at European ports are now common and the cocaine seized in Europe is of high purity. The Caribbean in particular is a major transit point for shipments of Latin American cocaine destined for the European markets (see figure).[83]

**Figure 3    Cocaine trafficking routes to and reception in Europe**



Source: InSight Crime investigations
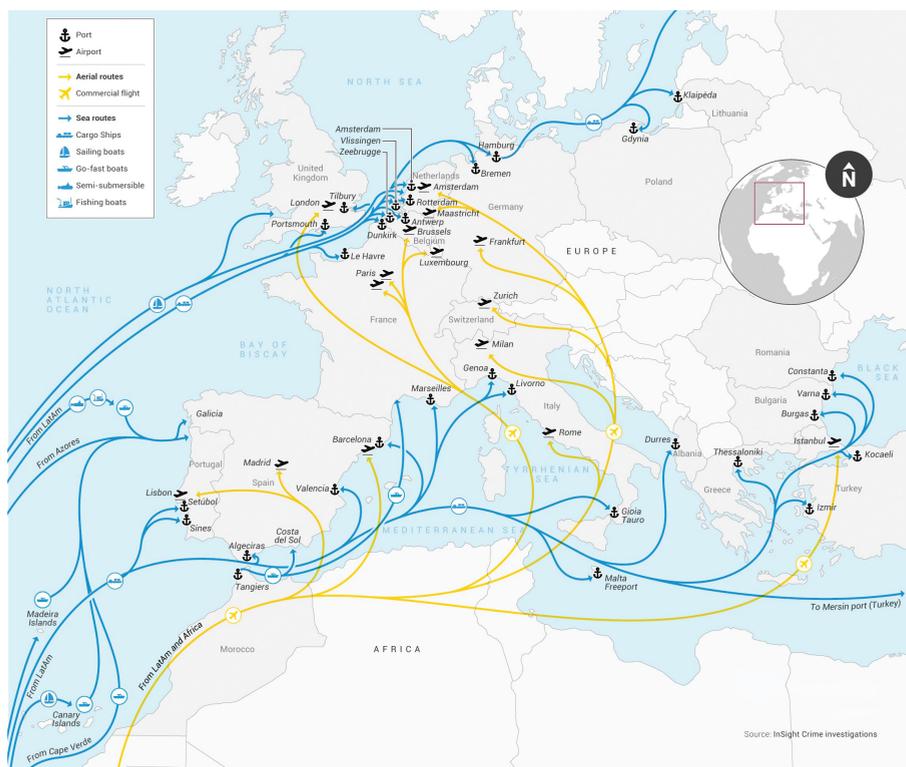
The relationship between transnational organised crime and the smuggling of narcotics poses a serious threat to European stability and security and calls for enhanced intelligence and security cooperation between the states concerned. In line with its Security Strategy for 2020-2024, the European Commission has therefore significantly stepped up action on tackling illicit drugs through a new EU Agenda and Action Plan on Drugs.[84] Effective international partnerships are essential to the success of the

---

83   Jeremy McDermott, James Bargent, Douwe den Held and Maria Fernanda Ramírez, *The Cocaine Pipeline to Europe* (Geneva: The Global Initiative Against Transnational Organized Crime, February 2021).

84   European Commission, *EU Agenda and Action Plan on Drugs 2021-2025 COM(2020)* 606 final, July 24, 2020.

counter-narcotics mission, as it depends on cooperation among the concerned nations. Sharing information with partners has been proven over and over again to be absolutely critical to success in combating any transnational threat. No one country or organisation can do it all, due to the complexity involved and the resources required. And as there are clear parallels between counter-narcotics operations and counter-terrorism operations, it is possible to apply the lessons from the latter to the former.[85] The following sections of this chapter focus on the kind of organisation that seems especially suited for dealing with the complex challenge of counternarcotics operations: the interagency task force.[86] More specifically, it assesses the usability of a specific Caribbean business model in the European maritime arena.

## Counternarcotics in the Caribbean

The Joint Interagency Task Force-South (JIATFS) in the Caribbean is known as the "gold standard" for interagency cooperation and intelligence fusion in the field of counternarcotics.[87] Indeed, it is often cited as a model for 'whole-of-government' problem solving in the academic literature on interagency collaboration. The JIATFS is tasked with countering drug trafficking from Latin America to the United States. Its origins can be traced back to the 1980's, when powerful Colombian drug cartels brought large quantities of drugs and the associated crime to the US. The US government realised that these drug cartels could not be countered with traditional means. It therefore decided to establish an interagency task force in which law enforcement agencies work together with the military, partner nations and their intelligence agencies. The JIATFS was created in 1994 and focused particularly on improving the intelligence fusion process, resulting in actionable intelligence products that operators could use to great effect. These products are based on multiple intelligence sources, ranging from imagery intelligence provided by the US Coast Guard, signals intelligence provided by the National Security Agency (NSA), human intelligence provided by the Drug Enforcement Agency (DEA) and by agents and sources of foreign partner countries.

JIATFS receives operational resources from partner countries, with France, the Netherlands, and the United Kingdom in particular providing maritime interdiction assistance. Continuing improvements in its intelligence networks and operational

---

85    Aaron Davenport, *Lessons from Maritime Narcotics Interdiction: Interdiction in the Maritime Source, Transit, and Arrival Zones of the Western Hemisphere* (Santa Monica: The RAND Corporation, 2020).

86    Robert Pope, "Interagency Task Forces: The Right Tools for the Job," *Strategic Studies Quarterly* 5, no 2 (2011): 114-152.

87    Unless indicated otherwise, this treatment of JIATFS is based on Evan Munsing and Christopher Lamb, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success* (Washington, DC: National Defence University Press, 2011).

practices over the years allowed the JIATFS to increase its success in interdiction and arrests. The latter indicates that organisational processes such as trust building and creating momentum are of paramount importance regarding interagency cooperation. Over more than 25 years the JIATFS has maintained its record of success, even though its 'enemy' has proven to be elusive and adaptable, typical characteristics of a hybrid opponent. But its success is completely dependent on its partnerships. Its intelligence-driven operations would not be possible without partners delivering the intelligence, the platforms and the authority while using the JIATFS' organisational backbone as its fundament. The next section will indicate which performance variables enabled the JIATFS to become and remain so successful.

## JIATFS: a measure of success

The success of the JIATFS has been examined using ten variables originating from the organization and management literature on cross-functional teams. All of these ten variables are attributes of the team, but they can be grouped on three levels of scope: the organization as a whole, the team itself and the individual. The organizational-level variables are team purpose, empowerment and support. The team-level variables are team structure, decision-making, culture and learning. The individual-level variables are team composition, rewards and leadership.[88] The effort that the JIATFS has put into interagency cooperation at the organizational, team and individual levels is the foundation for its success and provides valuable lessons for similar efforts.[89]

*Organizational-level.* Within the JIATFS it is completely clear to all participants what the purpose of the task force is and this unifies the team and provides direction to all the participants. For the success of the JIATFS it is also essential that the teams are empowered, meaning that they have control over the resources they need to succeed. Therefore, it has been arranged between the JIATFS and its partners that it gains tactical control over the participating units, including the related funds and personnel, while the operational control over the units remains with the partnering agency. Finally, on the organizational level the JIATFS is supported by the various organisations and political actors in the national security systems, in order to gain the necessary authority, funds and direction.

---

88   For a further discussion of these performance variables, see James Orton and Christopher Lamb, *Interagency National Security Teams: Can Social Science Contribute?* (Washington, DC: National Defence University Press, 2011).

89   This examination was done by Minne Boelens, "The Revolution in Intelligence Affairs: Problem Solved?" in *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, eds. Floribert Baudet, Eleni Braat, Jeoffrey van Woensel and Aad Wever (The Hague: Asser, 2017), 119-144.

*Team-level.* For the JIATFS the complexity of the subject requires several functional competencies in its teams, and therefore also several partnering organisations. It also requires a focus on intelligence collection and fusion so that actionable intelligence drives operations. Within the JIATFS the tenure of personnel is also an important issue because it is relevant that team members stay long enough to really get to know their job and reach higher performance levels. The JIATFS balances the turnover of interagency personnel with a core of long-term civilians. Concerning decision-making, it focuses on collaborative decisions, based on consensus, in order to benefit from the often-diverging viewpoints that exist as a result of the interagency composition. Collaborative decision-making takes longer than an authoritative model, but it produces better solutions and maintains the support of interagency and international partners. Creating a positive team culture, which means having shared values, norms and beliefs, requires time in an interagency context because members must overcome their personal and agency's views in order to work as an integrated team. In order to remain effective the teams must also be able to adapt and learn quickly. Therefore, a lot of emphasis is placed on passing existing knowledge to new members. This is done informally by more experienced members acting as mentors for newcomers and formally through training programs and standard operating procedures.

*Individual-level.* The JIATFS consists of temporary personnel from the various participating agencies supplemented by permanent civilians and contractors. The civilians provide stability and institutional knowledge while the rotating military and other agency personnel provide new ideas and a periodic review of how business is done. The JIATFS supports the idea that individuals need to be rewarded for their responsibilities as team members but also that teams should receive joint awards. Therefore it provides a range of recognitions to its members and it also communicates these appraisals with the parent organisations. It is the shared leadership model that has proven to be the most beneficiary for the JIATFS. In this model authority is pushed down to a low level so team members can make decisions rapidly without having to consult their superiors, hereby enabling the teams to quickly adapt and act on developing situations.

## Counternarcotics across the Atlantic

Across the Atlantic, the EU has already accrued much useful experience in deploying naval operations, undertaking border control and coastguard functions, and performing maritime security tasks such as countering piracy and conducting maritime surveillance.[90] The increase in illicit drug trafficking by sea and air from Latin America

---

90    Daniel Fiott, *Naval Gazing? The Strategic Compass and the EU's Maritime Presence* (Paris: European Union Institute for Security Studies, 2021).

and the Caribbean across the Northern Atlantic to Europe raises the question of whether the successful JIATFS business model can be transposed into the European maritime arena. There is an organisation, the Maritime Analysis and Operations Centre (Narcotics), MAOC (N), that could be considered to be the Union's answer to this question.[91]

The MAOC (N), based in Lisbon, is an initiative by seven European countries: France, Ireland, Italy, Spain, the Netherlands, Portugal and the UK, and is co-financed by the European Commission. It provides a forum for multilateral cooperation to suppress illicit drug trafficking by sea and air. The MAOC (N) officially opened in 2007 and is a European law enforcement unit with military support that, like the JIATFS, coordinates maritime and aerial intelligence, resources and trained personnel in order to respond to the threat posed by illicit drug trafficking. Its headquarters is staffed by liaison officers representing the police, customs, military and other authorities of the participating European nations, as well as by a permanent observer from the US through the DEA. The European Commission, Europol, the EEAS, the European Defence Agency (EDA), and Frontex are all observers. The mission of MAOC (N) is to enhance intelligence cooperation and coordinate law enforcement action on the high seas, with a view to intercepting vessels carrying cocaine and cannabis.[92]

Intensifying the fight against illicit drug trafficking requires closer cooperation in counternarcotics operations with EU-partners such as the UK post-Brexit and the US. The classic deployment of naval vessels, submarines, aircraft and helicopters remains important, but more is needed to increase the pressure on transnational criminal organisations. This primarily concerns sharing of operational intelligence between partners in order to map international criminal networks and financial flows. This effort can be supported by the EU's Copernicus satellite maritime surveillance capabilities. Earth observation data can be used to detect and identify unlawful activities, which often occur in locations on the high seas that are difficult to monitor and involve either small vessels which do not send position alerts, or larger vessels which have switched off their position reporting systems.[93] In 2017, the MAOC (N) requested Copernicus' support to provide imagery, allowing for the seizure of around 2.4 tonnes of cocaine – worth an estimated €100 million wholesale.[94]

---

91   Carsten Weerth, *What is the Maritime Analysis and Operations Center of the EU? EU's Answer in the War on Drugs*!, 11 September 2020.

92   See the official website of *MAOC (N)*.

93   European Maritime Safety Agency, *Copernicus Infosheet Law Enforcement - Overview*, 17 August 2020.

94   European Maritime Safety Agency, *Copernicus Infosheet Law Enforcement - Use Case: Anti-Drug Trafficking Operations in the Mediterranean*, 17 August 2020.

## Conclusion

Based on the presence of an important driver of intelligence cooperation – cooperative momentum – this chapter has identified a clear opportunity for the continued engagement of British intelligence and security services in an existing European cooperative arrangement for tackling one of the most complex security challenges facing the EU over the next ten years, namely the smuggling of drugs. Experience with interagency teams in counternarcotics operations shows that the fusing of all-source intelligence with operational capabilities creates results. Existing European organisations, like the MAOC (N), can build on the experiences in countering illegal narcotics trafficking from the Caribbean in the JIATFS. They should consist of personnel from various organisations and partners that are all stakeholders in countering the illegal drugs trade, and all personnel should be organised into small, empowered and diverse teams. This adaptability and flexibility has made the JIATFS an important and successful asset in countering the illegal drugs trade.

Its participation in the JIATFS not only provides the Netherlands with a wealth of special and valuable operational experiences, but – more importantly – has also proven to be an effective framework for regional cooperation with partner countries, the US and European partners in the Caribbean. In the years that the Netherlands has participated in the JIATFS, its intelligence position in the Caribbean has greatly improved and its participation has been an incubator for the kind of information-driven operations directed by the recent Defence Vision 2035. The Netherlands and Europe would therefore benefit from exporting these best practices from the Caribbean to Europe and to investigate which particular elements can further strengthen European cooperation within the MAOC (N).

Activities such as those already conducted by the MAOC (N) should be strengthened and expanded, e.g. monitoring of vessels and aircraft of interest carrying illicit drugs on the high seas and in airspace surrounding the Europe's maritime borders and airspace with the goal to intercept them before or when they reach their first European port of entry. Moreover, a post-Brexit UK should remain involved as a key participant in the MAOC (N) even though it is no longer part of the EU. International cooperation in the area of maritime and air surveillance and intelligence sharing is key to improving the intelligence and real-time action capabilities of EU member states and partner nations tasked with border security and counternarcotics in the present time.

# 6 Recommendations

Based on this research, there is ample opportunity to increase both the scope and depth of European intelligence cooperation in the years to come. Moreover, the Netherlands can and indeed should play an active role in the development of enhanced intelligence cooperation in and of Europe by making effective use of the presence of important factors that can help drive European cooperation further. In light of the arguments put forward in the preceding chapters, the following nine recommendations are made:

1. **Strengthen the EU Early Warning System by infusing it with three distinct elements from the NATO Intelligence Warning System**: the inclusion of warning problems in the process, a system of institutionalised burden-sharing, and the combination of a long-term and short-term focus.

2. **Guide EU cooperation on enhancing resilience and countering hybrid threats by a regularly updated threat assessment and a comprehensive situational awareness** by strengthening and enhancing the EU's Hybrid Fusion Cell's close cooperation with both NATO's Hybrid Analysis Branch and the Hybrid Centre of Excellence.

3. **Use the platform of the Intelligence College Europe** as the forum for organising panels, seminars and discussions **to promote intelligence cooperation in the field of early warning and the development of a common culture** among European intelligence and security experts.

4. **Make use of the presence of a common perceived challenge in the shape of China** to make Japan more inclined to seek intelligence gains through cooperation with the EU and **to step up collaborative efforts with Japan in the realm of military and security issues**.

5. **Use the commonalities with Japan in values** and regime type, **and the similarities in the view of security** and of the challenges posed by the increasing strategic competition between states **to jointly tackle the challenges of the emerging multipolar world order**.

6. **Use the framework of the EU–Japan Strategic Partnership Agreement to** develop an agenda for further cooperation and **tap into the potential for collaboration in the field of intelligence** in areas such as threats to space systems, China's military affairs, nuclear and ballistic missile developments and international terrorism.

7. **Build on the common experiences from the Caribbean in countering illegal narcotics trafficking within the framework of the Joint Interagency Task Force-South** by infusing the Maritime Analysis and Operations Centre (Narcotics) with its best practices.

8. **Use the demonstrated adaptability and flexibility** that has made the Joint Interagency Task Force-South a successful asset in countering the illegal drugs trade **as a model for further development of the Maritime Analysis and Operations Centre (Narcotics)** by incorporating all stakeholders and organising its personnel into small, empowered and diverse teams.

9. **Keep a post-Brexit UK involved as a key participant in the Maritime Analysis and Operations Centre (Narcotics)** even though it is no longer part of the Union that is funding it.