Knowledge security: insights for NATO

Snetselaar, D.; Frerks, G.; Gould, L.; Rietjens, S.J.H.; Sweijs, T.

Knowledge security: insights for NATO

D. Snetselaar, G. Frerks, L. Gould, S. Rietjens, T. Sweijs

30 September 2022

Listen to this article

0:00/15:41

Knowledge security entails mitigating the risks of espionage, unwanted knowledge transfers, intellectual property theft, data leakage and the misuse of dual-use technology (technology that is primarily "focused on commercial markets but may also have defence and security applications").

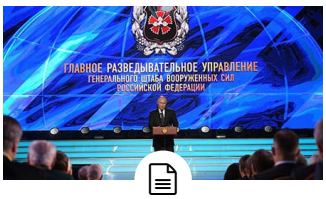
In the context of research on and the development of high-end technology, knowledge security is vital to NATO's ability to deter and defend against adversaries and protect the prosperity of its members. Countering hybrid threats that target critical national security technologies requires a whole-of-society approach that comprises the public sector, private companies, civil society and individuals aligning their principles and standards to engage meaningfully on an issue. The development of such an approach is hindered by diverging threat perceptions, interests and levels of awareness of the stakeholders (civilian and military; private and public) involved. To develop calibrated whole-of-society responses, NATO needs to understand what the opposing imperatives are for different stakeholders and how they can be bridged.

SHARE THIS ARTICLE

RELATED ARTICLES

The consequences of Russia's invasion of Ukraine for international security – NATO and beyond

Inside-out: what changing Russian domestic politics mean for NATO



Russian intelligence operations shifting tactics not goals

In the context of research on and the development of high-end technology, knowledge security is vital to NATO's ability to deter and defend against adversaries and protect the prosperity of its members. © NCIA

This article examines the contrasting perspectives on a Sino-Dutch research project on Artificial Intelligence (AI) called DREAMS Lab and offers an innovative analytical framework to identify and understand those different perspectives and interests, referred to as the assemblage approach. Assemblage is a concept that has come into usage in international social theory as an alternative to more traditional concepts like 'state', 'alliance' or 'network' to study the emerging and fluid social-material formations in contemporary societies. The assemblage approach is used here to analyse how a group of heterogeneous actors came together and responded to the DREAMS Lab project despite their different perceptions and, at times, conflicting interests. Similarly, the assemblage approach can help NATO and its Allies recognise and respond to hybrid threats in and beyond the knowledge domain.

Hybrid warfare: the context for knowledge security at NATO

Though 'hybrid warfare' is still a contested subject of academic and policy debates, effectively responding to hybrid threats has nonetheless become a top priority for NATO and its members. Opponent states increasingly deploy combinations of hybrid tactics to pursue their strategic interests, often in order to remain below the threshold of armed conflict. As such, hybrid threats are considered a pressing, cross-domain challenge that inhabits a 'grey zone' between war and peace. Examples of hybrid threats include disinformation, political meddling, cyber warfare and the theft of technologies.

In the economic domain, hybrid threats pose challenges in relation to energy security, critical infrastructures, foreign direct investments and research on high-end technologies. Such challenges may not have immediate military implications, but are still of vital importance to the resilience of the Alliance and its members. The 2022 Madrid Summit Declaration explicitly mentioned energy security and resilience to cyber

and hybrid threats, while Article 2 of the North Atlantic Treaty calls for “economic cooperation” in national security matters such as the abovementioned challenges.

The subject is also pertinent in view of the Artificial Intelligence Strategy for NATO, adopted by Allied Defence Ministers in October 2021, which highlighted the international security risks implied in the field of artificial intelligence. Understanding what knowledge security entails and how it can contribute to achieving resilience against hybrid threats is therefore of particular relevance to NATO.

At issue: Sino-European research collaborations on high-end technology

To illustrate the challenges of responding to hybrid threats in the knowledge domain, we draw on empirical fieldwork conducted in 2021 on a Sino-Dutch research project on AI called DREAMS Lab.DREAMS Lab is a collaborative project run by the University of Amsterdam (UvA) and the Free University of Amsterdam (VU). The project is funded by the Chinese telecommunication company Huawei, which will invest a total of EUR 3.5 million over four years. The aim of the project is to study the use of AI to optimise search engine functionality. Huawei has an interest in optimising its search engine technology as it is banned from using apps like Google Search.

Projects like DREAMS Lab offer several benefits for European research institutions, including access to talent, funding and expertise in key technological areas. Despite these benefits, however, European governments, politicians, think tanks and journalists increasingly perceive collaborations with Chinese research partners as risky in the context of ongoing geopolitical tensions and rivalry.

The Artificial Intelligence Strategy for NATO, adopted by Allied Defence Ministers in October 2021, highlighted the international security risks implied in the field of artificial intelligence. Understanding what knowledge security entails and how it can contribute to achieving resilience against hybrid threats is therefore of particular relevance to NATO. © European Union

The development and use of high-end technologies like AI is expected to have a large impact in both economic and military domains. Having access to AI is therefore considered crucial for a country's economic prosperity and national security. Driven by the ambition to become a world leader in key technological areas including AI, China is often suspected of using international research collaborations to access and acquire the knowledge it needs. Because of this, think tanks warn undesired knowledge transfers, intellectual property theft, data leakage, encroachment on academic freedom and ethical dilemmas (see for example the reports published by the Leiden Asia Centre and the Hague Centre for Strategic Studies).

These concerns have led the Netherlands, but also countries like the United Kingdom, Germany and Sweden, to take preventive measures. Such measures include raising awareness among staff, conducting due diligence, ensuring compliance to dual-use regulations and investing in information security. As will become clear, the DREAMS Lab case offers insights relevant to NATO regarding the nature of hybrid threats in the knowledge domain and could help encourage member countries to take appropriate knowledge security measures.

Case study: the DREAMS LAB project

When a journalist from the Dutch Financial Daily began reporting about the DREAMS Lab project, a fierce debate started to unfold amongst policy makers and academics. The articles questioned the UvA and VU's decision to work with Huawei in light of concerns over state espionage and data theft facilitated by Huawei as a 5G supplier. Though the DREAMS Lab project had nothing to do with 5G, politicians wanted to know why the Dutch government had given approval for the project. The government made clear that the Ministries of Economic Affairs and of Education and the Security Services had only informed the UvA and the VU about the possible risks and that it had not given its formal approval as it has no mandate to do so.

Amongst scholars, the debate focused on the ethics of working with Huawei. The Chinese telecommunication company has been accused of being complicit in the oppression of the Uyghurs (a Muslim ethnic minority living in Xinjiang) by the Chinese government. In October 2020, an assemblage of Dutch scientists and scholars sent an open letter calling on the UvA and the VU to reconsider the project on ethical grounds, as working with Huawei could be construed as symbolically justifying the company's actions and ethics.

The debate in politics and in academia did not result in the termination of the DREAMS Lab project, but it put 'knowledge security' high on the Dutch political agenda. Knowledge security is a term used by the Dutch government (and increasingly by universities) to refer to the risks of working with research partners from countries such as China but also Iran and Russia. After the DREAMS Lab incident, an assemblage of government ministries, universities and national research organisations started working (collaboratively and separately) on practical guidelines to help research institutions assess the security risks and ethical implications of international research collaborations. One of the primary objectives of

these knowledge security measures is to ensure a reciprocal exchange of knowledge and expertise and prevent the undesired transfer of sensitive knowledge or technologies.
On 21 July 2021 the resulting Framework Knowledge Security Universities was published by the Association of Dutch Universities (VSNU). The Framework not only encompassed a risk analysis and guidelines, but also offered six concrete instruments to promote knowledge security and prevent abuse, such as a national network of advisory teams, a checklist for international collaboration, a risk and incident register, training sessions and awareness campaigns.

Key insights

Using the assemblage approach, three key insights were drawn from the response to the DREAMS Lab project.
First, the threat representation of DREAMS Lab as both a security and human rights risk helped align the interests of the parties to the assemblage. While the security reading resonated with the government agencies concerned with national security, academics were more concerned with Huawei's complicity in human rights violations. However, the two threat perceptions were not mutually exclusive, but reinforced one another. Concerns about the implication of undesired knowledge transfer for the Dutch innovation and research community resonated with the Ministries of Economic Affairs and of Education as well as sector organisations like the aforementioned VSNU.

Complex challenges like hybrid threats in the knowledge domain, and the economic domain more broadly, require an in-depth understanding of their multi-layered and multi-vectored nature. Specifically, NATO needs to invest more in social science research to understand the nature of the challenge and to formulate effective responses.

Second, the policy and practice of knowledge security helped to bring the concerns of different actors together and make the threat actionable. Following the debate on DREAMS Lab, the Minister of Education, the State Secretary of Economic Affairs and the Minister of Justice and Security sent a letter to parliament in which they addressed the different risks involved in international research collaborations with countries of concern and explained how these risks pose a threat to knowledge security. The Ministers and State Secretary identified a number of countermeasures, including the development and implementation of the guidelines that resulted in the above mentioned Framework.

Third, the DREAMS Lab project confronted government ministries and universities with questions of responsibility, autonomy, ideological dilemmas and external dependencies. Determining who is responsible for knowledge security and how international research should be regulated not only raised practical issues of capacity and awareness, but also ideological questions on the extent of government involvement while safeguarding academic freedom. In addition, both government and academic institutions were limited in their responses by external dependencies. The competitive position of Dutch scientific research, for example, depends on international collaboration and not least with China, which represents a crucial research partner for the Netherlands outside of Europe (see the following report for the scope of Sino-Dutch collaboration). Rather than a ban on all collaboration with China, therefore, a tailored and case-by-case approach was favoured by the assemblage.

Responding to cases like DREAMS Lab requires a careful analysis and consideration of the different perceptions, interests and dependencies of the actors involved, and close collaboration across government and society at large. It also inherently entails weighing security interests against economic and scientific interests and against democratic values like academic freedom.

Recommendations

Though we do not argue that NATO should become directly involved in responding to projects like DREAMS Lab, three recommendations for the Alliance flow naturally from this case study.

First, complex challenges like hybrid threats in the knowledge domain, and the economic domain more broadly, require an in-depth understanding of their multi-layered and multi-vectored nature. Specifically, NATO needs to invest more in social science research to understand the nature of the challenge and to formulate effective responses. It does not suffice to recognise these challenges from a purely technical or military-strategic perspective; a broader perspective needs to be adopted. The assemblage approach used to study the DREAMS Lab case can be applied to study similar perceived security threats to help unravel the different actors, technologies, interests and perspectives involved for more tailor-made responses.

Second, based on this research, NATO should invest in raising awareness on how knowledge and technologies can travel across borders and to what effect. In doing so, it should encourage members to take a nuanced and tailored approach and bolster collaboration between military and civilian actors, in and outside governments to address collective challenges. Articles 2 and 3 of NATO's founding treaty create a basis and framework for the Alliance to do so. However, because this requires a whole-of-society approach, NATO needs to understand and consider the perspectives and interests of all stakeholders. In these forms of collaboration, the Alliance can take on the roles of facilitator and enabler of crucial policy and implementation guidelines, while national implementation is the responsibility of individual member countries.

Third and finally, in order to effectively respond to hybrid threats in civilian domains, not just in the knowledge domain, stakeholders must weigh conflicting interests and address inherently political questions. NATO must transparently consider not just security and economic interests, but also the fundamental freedoms that define what the Alliance stands for. For example, such considerations also apply to policies aimed at countering disinformation.

Applying the assemblage approach to the DREAMS Lab case has offered an empirical example of what such a response to hybrid threats in the civilian domain might look like. It has also shown the necessity to deal diligently with the multidimensional dynamics of working with the heterogeneous actors that converge in international academic collaborations.

This is the second article in a mini-series on "the grey zone" which focuses on hybrid threats, knowledge security and defence.

- Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote

ABOUT THE AUTHOR

David Snetselaar MA is PhD candidate at Utrecht University (UU) and the Netherlands Defense Academy (NLDA). Prof. Georg Frerks (UU and NLDA), Dr. Lauren Gould (UU), Prof. Sebastiaan Rietjens (NLDA and Leiden University) and Dr. Tim Sweijs (NLDA and Hague Centre for Strategic Studies) are David's supervising team. This article is based on research carried out in the UU/NLDA PhD-project 'The re-footing of early warning in a new era'.

RELATED TAGS

NATO-Russia Council | Russia | Russia-NATO relations | Emerging security threats | International security | Military | Armed Forces