6-14-2024

A Framework for Digital Open Strategic Autonomy: Perspectives from the NL and the Uk

Pauline Weritz
Industrial Engineering and Business Information Systems, p.weritz@utwente.nl

A FRAMEWORK FOR DIGITAL OPEN STRATEGIC AUTONOMY: PERSPECTIVES FROM THE NL AND THE UK

TREO Paper

Pauline Weritz, University of Twente, Enschede, Netherlands, p.weritz@utwente.nl

Abstract

Open Strategic Autonomy encompasses a strategic EU framework with policy initiatives to promote public interest and protect economic resilience. To mitigate risks specifically in the digital domain, initiatives include regulations on big tech, secure telecommunications, and efforts to diversify suppliers for key enabling technologies such as quantum, photonics, or semiconductors. Considering challenges such as lower technology investments compared to the US and China, the Netherlands promotes an agenda on Digital Open Strategic Autonomy that aims to boost independence across various digital layers. To promote such initiatives, this research addresses issues on the conceptualization and mapping mechanisms for high-risk dependencies. The study contributes to the bigger discourse on the topic by comparing the approaches in and outside the EU. Besides these theoretical contributions, the practical implications have societal relevance and offer lessons learned for ministries on collaborating to promote economic resilience, mitigate risks, and enhance strategic autonomy in the digital economy.

Keywords: Digital Open Strategic Autonomy, Economic Resilience, European Union, Information Systems.

1 Introduction

Digital Open Strategic Autonomy (DOSA) is a new umbrella term for policy initiatives and tools to enhance resilience and security in the digital economy (Pannier, 2023). For instance, measures have been taken in the EU to prevent big tech companies from becoming too powerful (Digital Markets Act, Digital Services Act), to make telecommunications more secure and to diversify suppliers (Telecoms Security Act), first regulations on artificial intelligence (AI Act), along with other initiatives on knowledge security, investment screening, and export controls (European Council, 2023; Okano-Heijmans, 2023). Although countries like the Netherlands (NL) offer a solid economic foundation for the EU (Agenda Digitale Open Strategische Autonomie, 2023), global digital threats must be continuously addressed. For example, investments in new technology in the EU are lower than in the US and China, and the digital innovation market share is decreasing compared to other countries (Agenda Digitale Open Strategische Autonomie, 2023). With DOSA, the EU could strengthen its independence from other countries for different Information Systems (IS), as displayed in various layers of the digital stack, such as hardware (e.g., photonics, semiconductors, quantum technology), physical infrastructure, soft infrastructure (e.g., cloud), data (e.g., AI), and applications and services (e.g., cybersecurity). Hence, the need to make independent choices on a geopolitical level has gained high relevance in the disruptive global environment, but several issues and challenges remain regarding how to address a DOSA framework. This leads to the problem formulation for the researchers in the IS field.

First, as highlighted in the Letter to Parliament (2023), the need to address high-risk dependencies to ensure knowledge security in the EU is critical. However, there is a lack of knowledge on the risk that the supply chain could be disrupted (e.g., the possibility of substitution and relationship with the country)

(European Centre for International Political Economy, 2023). Though some research institutes have aimed to address this issue (Digitale Open Strategische Autonomie, 2023), the high-risk dependencies to respond to a contested and volatile world have not yet been fully explored. Second, there is no precise mechanism to map these dependencies for the different layers of the stack (Letter to Parliament, 2023). Some earlier research on assessments, frameworks for guidance, making use of trigger diagrams and management theories exist (European Liberal Forum, 2022; Timmers & Dezeure, 2021), but the dependencies are not well reflected and mostly only quantitatively explored (Letter to Parliament, 2023). Third, although DOSA is an increasingly important topic to explore on the geopolitical level, there are different ways to approach it within and outside the EU. Other terms and approaches like sovereignty (Broeders et al., 2023; Gstrein, 2023; Sheikh, 2022) might help to understand strategic information and help in bilateral discussions with and between measures. Whereas the NL addresses the DOSA issue in an EU context, the United Kingdom (UK) seeks tailor-made international partnerships (Okano-Heijmans, 2023).

Due to the similar stages of policy development in the UK and NL, a comparative analysis could help to understand the UK's position as a non-EU country with different trade-offs than the NL (Okano-Heijmans, 2023). Fourth, after understanding the high-risk dependencies and exploring the framework of DOSA, there are no implications for mitigating the risk required for economic resilience. Deriving implications from the framework that offers guidelines for practice is required to advance strategic independence and enhance measures to promote, protect, and partner within the EU. Based on these identified practical problems, we aim to solve the following research question: *How do governments approach digital open strategic autonomy to mitigate high-risk dependencies in the digital economy?*

We follow a qualitative approach to address the research question as the topic is still exploratory (Diaz Andrade et al., 2023; Sarker et al., 2013). We chose a multi-method design with longitudinal field research from September 2023 to April 2024. First, the data collection included interviews with both authors to get an overview of the different policy initiatives in the NL, to identify where the UK diverges, and how the UK defines DOSA. Second, we conducted a document analysis with official information, such as policy briefs, public speeches, or documents. Third, we conducted field observations as the researchers were involved in the Embassy.

2 Findings and Discussion

The preliminary results show a common approach to addressing the risk assessment yet considering different vulnerabilities. When exploring policy initiatives, the UK mainly focuses on promoting public interest rather than including how to protect it, which is detailed and elaborated in the framework from the NL. Different policy frameworks are being discussed because of the interdependencies and many technologies having a value chain across borders. In DOSA, different independence from other countries is identified, as displayed in various layers of the digital stack, such as hardware (e.g., photonics, semiconductors, quantum technology), physical infrastructure, soft infrastructure, data (e.g., AI), and applications and services (Agenda Digitale Open Strategische Autonomie, 2023).

To respond to the previously laid out challenges, the outcomes of this research aim to investigate how governments are approaching digital open strategic autonomy to mitigate high-risk dependencies in the digital economy. We contribute to practice by exploring the framework of DOSA, mapping the dependencies, comparing them with non-EU measures, and deriving policy-focused recommendations. First, we identify the dependencies between the different layers of the stack in the NL. Second, we develop a conceptual framework for how to visualize the layers of the stack and their relations. Third, we offer a comparative analysis between NL and the UK to identify similarities, differences, and potential best practices. Fourth, based on the findings, we derive lessons learned with policy-focused recommendations that explain how to mitigate risk and dependencies. The guidelines aim to transform into concrete implications supporting future policy advice.

References

Agenda Digitale Open Strategische Autonomie (2023). *Minister of Economic Affairs and Climate*. URL: https://open.overheid.nl/documenten/5cb9749c-7efa-40db-9328-5da7fa5fcb7c/file

Broeders, D., Cristiano, F., and Kaminska, M. (2023). "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," *Journal of Common Market Studies*.

Diaz Andrade, A., Tarafdar, M., Davison, R. M., Hardin, A., Techatassanasoontorn, A. A., Lowry, P. B., Chatterjee, S., and Schwabe, G. (2023). "The Importance of theory at the Information Systems Journal," *Information Systems Journal,* 33(4), 693–702.

European Centre for International Political Economy (2023). *A Forward-Thinking Approach to Open Strategic Autonomy.* Policy Brief. 13/2023.

European Council (2023). *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world.* URL: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial- intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/

European Liberal Forum (2022). *Decoding EU Digital Strategic Autonomy Sectors, Issues, and Partners.* URL: https://liberalforum.eu/wp-content/uploads/2022/06/Decoding-EU-Digital-Strategic- Autonomy_ELF-Study_Techno-Politics_vol.1-2.pdf

Gstrein, O. J. (2023). "Data autonomy: Recalibrating strategic autonomy and digital sovereignty," *European Foreign Affairs Review,* 28(4).

Pannier, A. (2023). *Technological vulnerabilities that threaten the European Union's 'Open Strategic Autonomy' and the EU's response.* URL: https://sciencemediahub.eu/2023/03/06/technological-

Letter to Parliament (2023). Letter from the Minister of Economic Affairs and Climate Policy, the Minister of Foreign Affairs, and the Minister for Foreign Trade and Development Cooperation to the President of the House of Representatives on the government's policy on strategic dependencies.

Okano-Heijmans. (2023). *Open strategic autonomy: The digital dimension. Clingendael Report*. URL: https://www.clingendael.org/sites/default/files/2023-01/Open_strategic_autonomy_.pdf

Sarker, S., Xiao, X., and Beaulieu, T. (2013). "Guest editorial: Qualitative studies in information systems: A critical review and some guiding principles," *MIS Quarterly* (37:4).

Sheikh, H. (2022). "European Digital Sovereignty: A Layered Approach," *Digital Society,* 1(3), 25.

Timmers, P. and Dezeure. F. (2021). Strategic Autonomy and Cybersecurity in the Netherlands.