Impact of Artificial Intelligence on Data and Information Security

Prof. Dr. Joachim Hasebrook

Dr. Patrick Lohmann

March 2019

Abstract

We computationally analyzed the public discourse on Artificial Intelligence (AI) in the German trade press to understand opportunities, challenges, and risks for the financial services industry and society from the growing deployment of AI-related technologies in organizations. We applied AI-methods to extract common topical themes from the articles. We classified them as influencing factors or risk domains and asked experts to provide their judgement on the relationships between them. Experts' judgements were fed into another AI-method that estimated strengths of causal loops and overall effect sizes on the risk domains. We found that in publications about AI and financial services risks do not play a significant role whereas regulation-related publications mainly discuss requirements imposed on companies for the safe and transparent use of AI as a pre-requisite for high customer acceptance. Human experts' judgements revealed increasing standardisation of data and customer behavior as the two hotspots and decreasing costs and systemic risks as two cold spots of the interrelationship of all automatically extracted topics. A short-term prognosis based on these judgements identified a lack of quality data and perceived shortage of regulation as a major driver of operational risks. In the long run, new and improved AI methods will become a major driver for reduction of operational as well as systemic risks, if new and improved algorithms become more sophisticated by learning based on less data.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute focussed on research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which offers both major opportunities and risks, decision-makers in the economic and political arena depend more than ever on the advice of highly qualified thematic experts.

ISPSW therefore offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, security and defence. ISPSW network experts have held, in some cases for decades, executive positions covering a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

AI reading the press on AI

It has been argued that the ever-increasing deployment of artificial intelligence (AI)-related technologies will increase strategic and systemic risk exposures for enterprises, undermine data security standards and customer protection, and may even lead to loss of significance of governmental organizations, as the legislation is lagging behind the technological development. Over the past two years, an overwhelming 1,500 articles were published in the German trade press on these issues: Too much to be read and grasped by human experts, but just a few seconds of computational processing time for AI-based linguistic text analyses. This technology helps to process natural language texts and is already in use with large international law firms and a growing part of the public administration in the United States of America in order to create summaries and reviews of large bodies of documents such as administrative and legislative texts.

We deployed this technology in order to seek answers to some major questions concerning security issues and risks related with the use of AI:

- What are major AI-related issues discussed in the trade press?
- What risks are discussed in the public debate? Is there a dominating view on risks?
- What are commonalities and differences in the AI-risk views of businesses and regulators?

Natural language processing can provide answers to these questions, but it also requires human expertise and judgement to answer questions like:

- What are relationships between issues and risks?
- Are there any 'causal loops' reinforcing or inhibiting each other?

Once such a causal relationship model is established, new important questions arise:

- What happens to causal loops that experts have identified, over time: How will the development and relevance of issues look like in the short-, mid- and long-term?
- What kind of risks and security issues are mostly influenced by AI? Does this pattern differ in a short-, mid- and long-term perspective?

Again, we employed AI-technologies in order to model reinforcing and inhibiting causal loops and to generate short-, mid-, and long-term prognoses based on these models.

AI in the press: An eye on risks

We examined all 1,500 articles published in the German trade press about AI risks and security threats between 2017 and the beginning of 2019 with AI-based linguistic text analyses. These analyses resulted in so-called topic maps. Topic maps show the relevance and relationship of dominating words used in the articles. We compared a general topic map covering all articles with a domain-specific topic map covering 105 articles discussing regulatory issues (e.g., EU Data Protection, EUDATAP, and the German DSGVO).

To generate the topic maps, we had AI read the articles and cluster them into topics that were latent in their structures. A topic is a mixture of words. Words that dominate within a topic tend to co-occur across articles. The relative positioning on the topic map indicates the proximity with which topics are discussed together

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

within an article: A closer proximity implies that topics are discussed together more often and share a similar context.

The general discussion of AI revolves largely around access to customer and complementary data and as well as transparency requirements of the use of AI in business organizations. There is no specific debate about the role of AI in society. Instead the discussion is characterized by technical systems development issues and future customer-business interactions enabled by AI. A debate about risks doesn't play a predominant role in the public discussion. The only risk, which is discussed to some extent, is the risk of losing jobs due to automation enabled by AI.

A comparison of the general discussion with the discussion prevalent in the supervision and regulation-related articles reveals interesting insights. Here, the topics are more closely connected. In particular, a differentiated discussion of AI with regard to the regulatory framework and impact on the workplace becomes visible. Risks are an important topic and are viewed from the point of view of the requirements imposed on companies. Access, transparency, and the way in which data is analyzed are closely related to customers and how they view the use of data.

Human experts: In search for the causal loop

Using the topics generated by the linguistics text analyses, we classified 32 topics as factors and the remaining 12 topics as risk domains. Example factors range from societal aspects, such as the view of citizens on AI or the general accessibility of AI technology, to organizational aspects, such as efficiency gains through advanced automation and the substitution of human labor by AI, to technical aspects such as IT-investments and enterprise data management. Risk domains include reputational and legal risks, operational risks, data security risks, and systemic risks.

We asked 50 experts from inside and outside of zeb what positive, negative, and neutral relationships they see between the 32 factors and between each factor and the 12 risk domains. The result was a heatmap visualizing inhibiting influences („cold spots") and reinforcing influences („hot spots") reflecting overall expert opinions – the stronger the agreement, the more intensive the influence.

Four spots were particularly intense, two hot spots of amplifying risk influences and two cold spots of inhibiting risk influences. The hotspots are the increased use of data and standardization of customer behavior as well as increasing automation and productivity through AI. Cold spots related to the falling costs and operational risks as well as fewer reputation and system risks.

Neural prognosis: setting the loops in motion

But these expert judgements are based on the fact that one factor is assessed after another without considering interdependencies between them. Such a network of relationships – in this case consisting of more than 1.400 connections – cannot be evaluated by human experts. Hence, we transferred the expert assessments into a self-learning, artificial neural network that simulates all influences in form of boundary conditions. On this basis, forecasts of future developments can be calculated. If many inhibiting influences act on a factor, the factor will not advance and lose its significance. In contrast, intensifying influences lead to further development and growing relevance.

The factors having an impact on the systemic and strategic risks of financial services providers can be grouped according to whether their developments are positively or negatively affecting the risk domains and whether

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

they will increase or reduce in their relevance. At the moment, the most important driver of systemic and strategic risks is a lack of quality data and perceived shortage of regulation clarifying the decisions that can be made by algorithms or require human involvement. Laws and regulation use a language that cannot be directly translated into the inner workings of algorithms, and these language barriers induce uncertainty combined with a shortage of proper governance inside financial services organizations. In line with this argumentation, short-term factors reducing risk are the deployment of AI to support rather than replace human for decision-making.

While societal factors – seen through the lens of the experts' combined judgements – play little to no role for the further development of AI-based systemic risks, new and improved AI methods will become a major driver for their reduction. As algorithms become more sophisticated, the experts unanimously said that AI will help on average to reduce systemic risks but in the case of a risk event, shocks will become more radical rippling through the financial services industry because algorithms are not trained on extremes where hardly any of no data exist.

These developments run in part against the need to have sufficient data for the training of AI-methods. Transparency of the use of AI and the interpretability of their inner workings are critical for their further development. New and improved algorithms will need to become more sophisticated by learning based on less data: „Small data" and "one shot learning" were terms resonating well among the experts. While the role of policy-makers was considered as a factor further developing information and data security risks, the role of supervisory authorities such as the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) was seen as a factor losing relevance for the further development.

AI will not replace people, but job and training profiles

AI-based innovations do not replace human beings: Typical human abilities will play an even more decisive role, but they must be adapted to the new challenges. Human Factors consider different system levels such as individual, team, organization, but also workplace, task, tools, technology, processes, framework conditions and environment with their respective interactions. In order to sustainably optimize the human-technology and human-human interaction in the agile socio-technical/human-machine system, it is necessary to redefine the roles in all management and work processes and to integrate lifelong learning into everyday working life. Twenty years ago there were no data scientists or software developers. Today there is not enough of them on the labor market. Thus, completely new job profiles will also establish: The spectrum ranges from the „User Experience Designers" who optimizes human-machine interactions to the „VA – Virtual Assistant" who no longer provides on-site support but „remotely" via online tools.

The training for the safe and intuitive application of new technologies. Above all, processes that must function automatically even under extreme conditions should be practiced continuously until they can be reliably called up even under stress or fatigue. Simulators also offer the opportunity to acquire these skills with a sufficient stress level but without real danger. Standardized procedures are one way of achieving the greatest possible uniformity of action across people and situations. This serves the safety, if and because proven problem solutions are given, so that the individual person does not have to develop the solution way. Work processes are particularly at risk of error at interfaces due to increased communication requirements and different assumptions and knowledge of the participants. Therefore, particular care must be taken when designing interfaces. In reality, however, it is precisely these processes that fall „between" the responsibilities. A further challenge lies in overcoming the classic boundaries and hierarchies and working together in an interdisciplinary manner.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

The management of such organizations must be enabled to initiate and control a process that favors the development of characteristics that characterize HROs.

Conclusion: AI-technology reduces risks, if it becomes user-centric

The most important development driver for AI is access to quality data. At the moment, data available in organizations is yet often not sufficient to train existing AI-models. Legacy application systems infrastructures lead to „data stains" in many financial service providers, which make a holistic view of the data treasure difficult. Even if an integrated data view exists, it is often technically-driven and does not optimally allow to automate business processes and operational decisions. In the future, as forecast simulation shows, the comprehensibility and transparency of AI methods will no longer be sufficient to learn from the available data.

While AI methods may today be a factor of competitive advantage, they will arguably become general purpose. Financial supervision and public administration can create clarity about the conditions of use and become an example for the use of AI in order to reduce uncertainty in the market and increase acceptance in business and society. It is above all a question of promoting not only short-sighted technology and infrastructure, but also business ideas and their implementation. Clarity about the use of data and comprehensibility of AI results will determine the further success of dissemination and market access.

Looking ahead the current trajectory of AI developments, it becomes obvious that improving data and information security risks and systemic risks may not go hand in hand. Possible solutions to escape from this trap, the financial industry learn from other industries that successfully master the balance: High-Reliability Organizations and high security teams, such as emergency rooms and plane cockpits, introduce new processes and technologies in a way that avoids new risks and reduces existing ones. New contents of human-technology interaction must be taken into account in addition to specialist knowledge and skills. AI-based technology will not increase but reduce risks if – and only if – organizations and their use of technology becomes effectively user-, that is human-, centric.

***

Remarks: Opinions expressed in this contribution are those of the authors.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Authors of this Issue

Joachim Hasebrook, Ph.D., studied cognitive psychology and computer science. He is professor for human resources and innovation management at Steinbeis University Berlin and academic director of zeb's business school at the Steinbeis University. He was academic director of the 'International School of New Media' (ISNM) at the University Luebeck, founding director of efiport Inc., e-learning hub of Frankfurt's major banks, and Knowbotic Systems, an AI company. He was awarded several pedagogical and IT prizes including Comenius Award and ASP ecoAward and was winner of the Startup Prize of the City of Frankfurt. Currently, he leads several publicly funded research projects and consulting projects for the digital transformation of financial and health service providers.

Prof. Dr. Joachim Hasebrook

Patrick Lohmann, Ph.D., is a consultant with zeb, a leading European strategy and management consultancy for financial services, where he co-leads the firm's natural language processing initiative. He partners with banks to support them digitally-transform their business and decision-making capabilities, blending robotics, machine learning, and artificial intelligence into their processes and operations. Mr. Lohmann serves as a panelist on industry forums, where he speaks about the disintegration of financial services value-chains due to ongoing industry digitization trends, and organizational implications on processes, technology, governance, and skills.

Dr. Patrick Lohmann

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de