Cyber Risks requires modeling of risks and their parameters. That is already a challenge for insurers and those dealing with the various aspects of cyber attacks via cyber crime and cyber war.

Anything that is connected to data bears the risk of cyber and its variations. Programs and data structures that have been built and developed by people can be corrupted by other people, in various ways, whether by accident or by deliberate criminal behavior.

Is there a cyber risk for Artificial Intelligence?

Artificial Intelligence (AI), or the earlier form of Machine Learning (ML), differs from the construction of programs or coding with specific step-by-step instrutions. AI and ML are forms of technologies that learn and adapt through experience, just as humans do. “Deep learning” machines can build models and recognize patterns. This leads to the representation of knowledge through the use of logical principles in order to automate various kinds of reasoning, i.e. developing models by learning from behavior and experience that has been recorded in the memory of the machine. A phenomenon that began in the world of high-tech toys is now increasingly being used in the fields of medicine, psychology, acquisition of language skills and various other areas to help people live better.

Although knowledge-based programming started many years ago, is has only been during the past five years that the risks from AI/ML have started to become visible for enterprises involved with big data and cloud computing. This has been a hot topic of discussion for all such firms, not just specifically technology-oriented ones. Early commercial applications of ML were the Google search engine, Amazon product recommendations and Facebook news feeds.

In today’s world, machines are increasingly taking over service areas, both for work and entertainment. Voice-powered assistants (such as Siri and Alexa) and self-driving vehicles are only two examples of artificial intelligence already in daily use. However, even these are not yet truly self-learning artificially-intelligent systems which can learn on their own. When such systems become prevalent, we will see a new level of major societal change.

Organizations began using Artificial Intelligence to enhance cybersecurity and improve data protection against sophisticated hackers by automating complex processes for detecting attacks and reacting to breaches. AI will certainly continue to play an important role in cybersecurity. Yet, paradoxically, the use of Artificial Intelligence will also create vulnerabilities, in particular when data users depend on interfaces across organizations. We can certainly expect attackers to use AI as well, to help them hack into systems through the use of machine learning. Automated hacking attacks are certain to come.

The impact of Artificial Intelligence on cybersecurity is already real and already there. We are only beginning to learn what this technology is capable of doing.