Cybergeddon Paves the Way for New Deal on Cybersecurity

John Hermans

It's very tough to make predictions, especially about the future. Nonetheless, there is hardly any doubt that the very nature of cybersecurity will radically evolve in the next decades. Fueled by the fact that we will witness an exponential growth of connections, devices and networks. This will lead to an interconnected world so complex that it is hardly possible to be in control. And fueled by the growing awareness that our current paradigm on cybersecurity no longer works. Below, I will not elaborate on what *will* happen. Rather, I will take a look at what *could* happen.

December 2020. Time Magazine choses Mija Rahandra to be the person of the year. The headline: "This woman keeps you safe". In the past decade, this business woman has built Trace, a company that now tops the Fortune 500 list and is widely recognized as the market and opinion leader in the domain of cybersecurity. The company successfully deploys machine learning, artificial intelligence and smart algorithms to service the ever growing need for security in a complex world with an estimated 130 billion connected devices and (human) sensors. The security industry as a whole has tripled in 5 years' time and is now the largest industry in terms of turnover. Bringing more intelligence has been the name of the game in this domain. It's no longer about building thicker and higher walls to protect systems and networks, it's predominantly about real-time smart analysis of variations in behavior that indicates and predicts unauthorized and malicious activities. The company was also a pioneer in the use of DNA profiles in identity management techniques.

June 2025. Business magazine The Economist looks back at two weeks of total world chaos. The website depicts a meltdown of our globe accompanied by the headline "Security professionals must have been smoking something really bad". The magazine offers an in-depth analysis of what has been dubbed "cybergeddon": the series of tragic events that took place after a coordinated series of terrorist cyberattacks, leaving the world in despair after a lengthy outage of power networks, vital infrastructures and public transport that caused chaos and anarchy throughout the whole world. Mija Rahandra is quoted making public excuses: "We really thought we were in control. But the truth is that we were wrong, so wrong. We thought we were smart. But all we really did is offer a false feeling of secureness. And the truth is that with our current paradigm on cybersecurity, we will never be in control. Do we have an alternative? Honestly, I'm not so sure."

July 2025. World leaders meet in Zurich for a summit on how to rebuild trust and security in the digital world. They challenge experts from both the business and the scientific world to come up with a new paradigm for cybersecurity. After three days of intense debate, these leaders agree on a new deal on cybersecurity. The sense of urgency has never been so deeply felt and has inspired the industry to rapidly adopt new thinking that has in fact been around for years but was never taken very seriously. The quintessential change in the approach is that cybersecurity will no longer focus on building walls and bringing intelligence around systems and networks, but will rather focus on securing the data itself by giving the owners of the data control over their data.

Around 2015, organizations found new ways to share their experiences and real-time insights regarding cyber defense

Adding a protection layer around data – a layer that defines the criteria for getting rights to use or alter the data and that is dynamically managed by the owner of the data – enables this so-called context-based security. In a joint statement, the leaders declare that civilians worldwide have to prepare for more cyber accidents to happen in the next years, but also assure that the new deal will lead to tangible improvements in the near future.

April 2029. Satoshi Nakomoto receives the Nobel Prize for peace. The inventor of the blockchain who has been living an anonymous life for decades, has now become a public figure at the end of his life. Back at the start of this century, hardly anyone could have imagined that the blockchain, that became well-known for its application for cryptocurrency Bitcoin, would bring such a fundamental societal change as it introduced a whole new concept for generating trust. Over time, people started to realize that the blockchain is more than a fundamentally new architecture for a global financial services infrastructure. The concept is based on a distributed, consensus-driven ledger that enables and records encrypted digital asset transfers without the need of a confirming third party. This offers many opportunities in basically all areas where people do transactions and it also offered a whole new way of looking at security. In the blockchain approach, security comes from within the network, not from a third party.

June 2031. My retirement from an active consulting career. Looking back on the past decades, it is good to see that the foundation for better cybersecurity started around 2015 with the belief that we needed a stronger focus on cooperation. Before 2015, organizations acted somewhat isolated in their cyber defense. Around 2015, they found new ways to share their experiences and real-time insights. Cybergeddon further contributed to this belief. In business, organizations will always compete. In cybersecurity, they don't have to. I am proud to have been part of this development. Very proud.

John Hermans is the Cyber Security lead partner at KPMG Advisory and heads the cyber security team of KPMG in the Netherlands. He is also a member of KPMG's Global Cyber Security leadership team. John has assisted many national and international organizations in defining cyber security strategies and transforming into cyber-resilient organizations.