Trends in Security 2021:

Adaptive organizations are keeping the Netherlands safe

As we write this, we are still in the midst of our struggle with COVID-19. Words fail to describe how grateful we are for everyone's contribution to efforts to contain it and deal with it, not least the co-workers in the security domain. Because organizations in the security domain, too, have had to accommodate the new reality and its repercussions for society as a whole, and the organizations themselves – including their ways of working.

One of the most interesting aspects of this shift is the role of technology. More than ever before, technology has brought people together, facilitating collaboration and the sharing of creativity and information. It has even translated the urgency felt into actual acceleration of developments that heretofore had been progressing slowly. And thanks to that urgency, the focus is not on avoiding risks, but on grasping opportunities. In the security domain, too, this was tangible, as Ric de Rooij, deputy secretary-general at the Ministry of Justice and Security told us in a recent conversation:

"Corona has reinforced the realization that we have to invest more into information security. Not to shore up the walls, but rather to, step by steps, start taking risks. Security as a driver to take risks, then. To do nothing is not an option. The sense of urgency has, for instance, helped us to accelerate the definition of a Cloud strategy and a Cloud assessment framework. This will support organizations in the domain in promoting continued development."

In this trend report, there are numerous examples of the security domain's significant adaptation abilities. In response to the crisis, on the one hand, but also in response to a society that is digitalizing at an increasing rate.

Ric de Rooij: "A number of practical developments are being realized faster, such as the implementation of 'tele-hearing'. More broadly speaking, we are allocating more resources to data use, and the smart and secure organization of data availability. A prosecutor needs to be able to be convinced that she or he can rely on information supplied by the police, and not have to worry about possible data corruption. The criminal justice system plays an important role in safeguarding such guarantees." In several articles, this aspect of information-driven working and data and information sharing will be addressed. Smart technology can help us to enable information sharing, without having to share the underlying data.

It is clear that the adoption – and quality – of information-driven working in the domain is increasing. Efforts are ongoing to assess the uses of Artificial Intelligence (AI) in prioritizing criminal cases. Intake of cyber cases and digital criminality is being improved, in order to generate intelligence that can be used to counter this phenomenon through innovative interventions. Due to the increase in digitalized criminality and cyber criminality, its volume has surpassed that of domestic burglaries; in security jargon, it has become 'Veel Voorkomende Criminaliteit', or 'common criminality'. Traditionally, the criminal justice system has been geared towards apprehending one or a few perpetrators, causing one or a few victims; now, it has to deal with one single perpetrator causing hundreds of victims, nationwide, and within a matter of hours. Use of technology in general – and data in particular – will help us to solve this problem. One of the articles in the report explains how.

Information-drive working and use of data are top priorities right now, especially in the security domain. This should always go hand in hand with a focus on transparency, safety and ethics. Again, there are risks, but most of all there are opportunities.

We see innovative developments that enable organizations to create new social value. Take, for instance, the CJIB, that most of us in The Netherlands will be familiar with because of its role in processing and collecting traffic violation fines. With smart data analyses in the Security and Justice data lab, the CJIB aims to identify citizens with outstanding fines and provide support, instead of just letting the amount of debt grow uncontrolled. In this way, CJIB hopes to prevent people from getting into more trouble.

Another example has to do with identity fraud, a type of criminality that, in the last 6 years, has grown with more than 500%.[1] And due to the COVID-19 crisis, the rate of growth has accelerated further. In order to tackle one of the main causes of this growing problem, data and AI can support us by increasing our ability to quickly and accurately check the authenticity of identity documents. In this report, you can read all about it.

The pandemic has once more reinforced the notion that not only will organizations in the security domain have to adapt to a changing society, they also need to look inward. The pandemic has seen a shift in where we work, and how. Working from a distance is the most obvious aspect but is only the tip of the iceberg. The new way of working has fundamental consequences for talent retention in organization, its processes, its real estate, sustainability, and technology. Organizations in the security domain will have to create a new social contract with co-workers and with society; the autonomy and flexibility that co-workers have gotten used to, will permanently re-define expectations. By embracing these developments, the domain will be able to profit from an (even more) committed and loyal workforce, lower costs, and a smaller ecological footprint.

However, the acceleration in the application of AI and robotization – and the significant consequences for the workforce and the work itself - dates back to pre-pandemic times. In order to maximize the return on investments in AI and automation, managers and board members in the domain need to fully grasp the implications for the roles, skills and talents needed to keep on thriving, and create a culture of continuous learning and continuous adaptation. As every organization starts to realize that we have to make haste in finding and binding new skills and talents, the fire and hire-method just won't cut it anymore. The talent pool is too small, and soon there will be too many fishermen. We have to start anticipating on these developments now, by taking a long, hard look at reskilling our workforce, and at making full use of the possibilities new technology has to offer. We call this 'reinventing work'. This report addresses this in several ways, for instance by detailing the new strategic personnel planning that the Defense Ministry has adopted to anticipate upon this development.

Ric de Rooij, too, stresses the importance of this: "We are fully aware that we need to invest more into what we call the 'public officer's craftsmanship'. We don't need to be able to do everything ourselves, but we do need to be able to assess the threats and opportunities of digitalization, for instance in the field of information security. We don't need to have all of the state-of-the-art knowledge, that's what we can hire you for, but we do need to be able to judge where we can add value and increase the impact on security."

This trend report offers several perspectives on how data and information can support the domain in becoming more effective and efficient, how the scope of cyber (security) is growing and how our own organizations and innovation processes are anticipating upon the future. Once again, it was a pleasure to compile this report. We hope you'll enjoy reading it.

Erik Staffeleu
Senior Director Public Sector, Capgemini Invent

erik.staffeleu@capgemini.com

Martijn van de Ridder
Insights & Data Lead, Public Sector, Capgemini

martijn.vande.ridder@capgemini.com