Author:
Erik Staffeleu

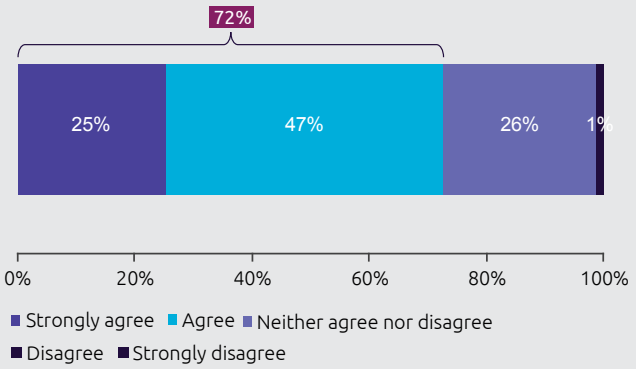
Management summary

The attack on the Utrecht tram on March 18, 2019 once again pointed out the vulnerability of security. Even though the investigation was still running at the time of publication of this report, we can already conclude that the attack was a symptom of an increasingly complex society. A society that poses new challenges and questions to security organizations. The attack also showed that security organizations are developing innovative answers to these challenges and questions. The speed of escalation, the use of drones for imaging, the facial recognition of the perpetrator in the tram, innovative big data analyses, real time analysis based upon online banking – these are just a few examples of innovative measures reported by the media. Innovation clearly is more than just a buzz word in the security domain; many actors are looking for new ways to approach their primary tasks. In this report, we discuss the new challenges before us, celebrate recent breakthroughs and offer concrete strategies to accelerate innovation.

Are criminals more innovative than the government?

73% of the Dutch people feel that criminals are more innovative than the government (Figure 1). This is one of the conclusions of the survey, conducted by Ipsos on behalf of Capgemini. It implicates that the government has work to do; in the public eye, but also in daily practice. Just staying the course will, for many partners, turn out to be the quickest way to lose the battle against breaches of security. The security domain is replete with valuable innovation, as is pointed out by the articles in this report. This does not automatically mean, however that good ideas will always be put to practice in any meaningful way. Questions need to be addressed about the practical viability, ethical repercussions and organizations' ability to change. The potential of new technologies and related innovations is enormous. The security domain can make a big difference, by going all-in on innovation – in the right way.

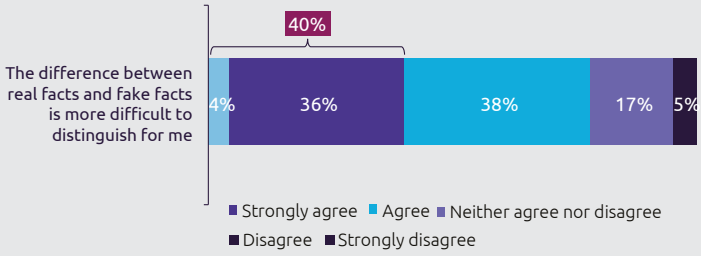
Figure 1: 72% thinks criminals are more innovative than the government; only 1% believes the opposite.



Technological development

Existing technologies are getting better and better and new technologies and applications are steadily emerging. The Ministry of Justice and Security and its service organizations are actively identifying the opportunities and threats that technical innovations represent[1]. The report touches upon a number of them. Quantum computing, for instance, is rapidly evolving. The computing power of these computers is unparalleled. This offers a great deal of potential, but also poses new challenges. How to keep encryptions safe from such computing power and, beyond that, protect our security? Deep fake is another example of a technology that represents a threat to security. This technology is able to generate fake video material that is hard to distinguish from real material. We are nearing the point where we can no longer believe our eyes. The results of our survey illustrate this (Figure 2). In a domain that relies upon the sharing of information, the verity of data and information should never be in doubt. Another development is blockchain. This can play a valuable part in promoting trust and security, by validating the origin of and actions around information. A good example is the Whiteflag project, developed in conjunction with the Ministry of Defence.

Figure 2: Fake news: for 40% of the Dutch citizens it is harder to see differences between fake and real facts, compared to 5 years ago.



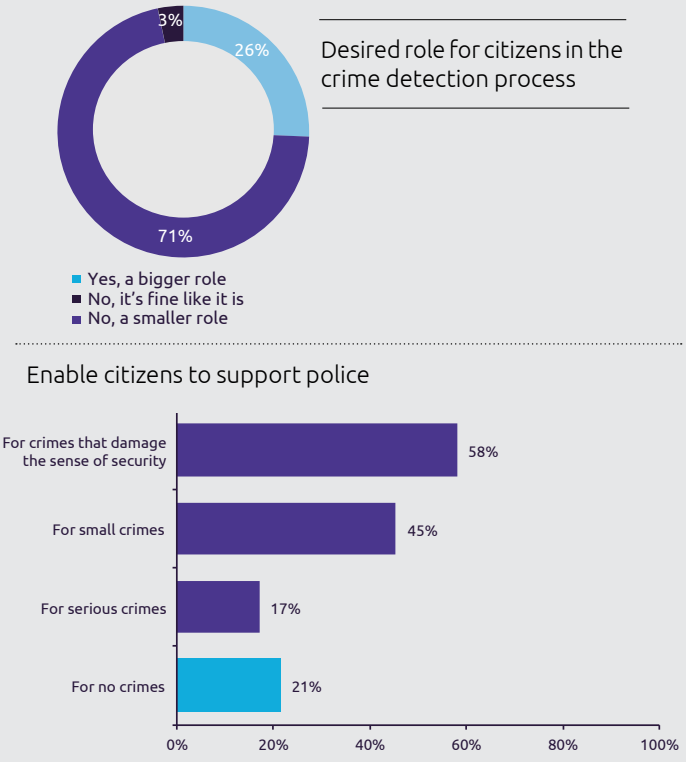
Data is everywhere

Data gathering efforts in the security domain are intensifying. The introduction of 5G enables real time communication between sensors on a much larger scale. The resulting explosion of data represents a challenge for data analysis. Artificial Intelligence helps security agencies to glean patterns and insights from large data sets. The enormous amount of information and insights that is gathered in this way can be deployed to make the Netherlands more secure. An example is sensing technology that harnesses licence plate recognition to uncover the movement patterns of criminals at large. By predicting the behaviour of criminals, the police operation becomes pro-active instead of reactive.

Technology as accelerator for innovation

Technologies are inherently innovative, but their potential goes beyond that: technology is an enabler for process innovation. Whole business models are changing as a result of the possibilities of new technologies. The advent of digital signatures for documents, for instance, is more than just a means to speed up an isolated action; e-signing makes the collaboration between police and Public Prosecution Service as a whole more efficient. E-signing, as such, helps to transform the criminal justice chain. The use of digital channels can also benefit the relationship between security organizations and citizens. Apps, for instance, enable citizens to contribute to the crime detection process. Civic participation through apps opens up many possibilities, but should always be approached with care. Citizens themselves are positive about working together with the security domain in fighting cyber crime. A quarter of the Dutch people even wants to play a bigger role (Figure 3).

Figure 3: A quarter of respondents demand a bigger role for citizens in the crime detection process



Technical challenges

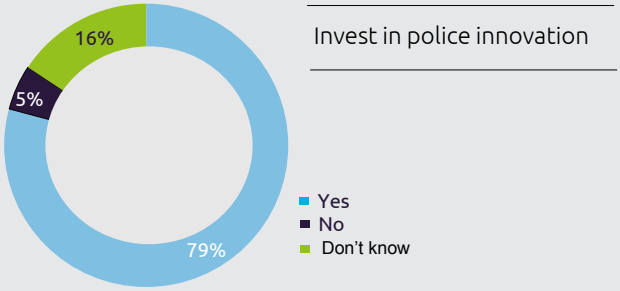
The uses of technology seem endless. Still, not everything that is technically viable is desirable. In this day and age, it is very important to be careful about the amount of influence technology is allowed to have on security and quality of life. The deployment of technologies also brings about more practical risks and challenges. Digital and physical threats, for instance, are increasingly connected. As a result, signalling and mitigating these threats is increasingly challenging and critical, as is explaining to the public why certain measures may be necessary. This also requires another communication strategy with regards to the measures taken by security organizations and the way technology is deployed. TechnoVision, as discussed in one of the articles, provides building blocks to create such a narrative. Based upon described trends, a clearer and more appealing innovation story can be built, easing people into the change without ignoring the negative aspects.

The innovative technology is there; will the organisation follow?

Research by Capgemini Invent points out that 93% of CEOs regard innovation as the most important factor for future success2. Still, the same deciders in organizations find it hard to manage innovation, motivate people and reward innovation. A common strategy, for instance, is to adopt a sequential approach towards improvement and innovation; in other words, to first make sure that the organizations is properly geared up, and to then start innovating. Organizations that choose this strategy, run the risk of being left behind by competitors or criminals that aren't content just sitting on their hands. On top of that, management choices are constantly involving, whether or not dictated by cost cutting measures; as a result, room for innovation is constantly visible on the horizon, as a future target, but never attainable in the here and now.

Moreover, we often see that innovations get stuck in the experimental phase. This also applies to the security domain. Technically, a great deal proves to be possible, but innovation gets hindered by the organization and the people in it. Internal politics, internal bureaucracy, resistance to change and a lack of continuity due to too much dependence on a small group of the willing, are often-heard obstacles for innovation. It is important not to get discouraged by these obstacles, but to keep on investing in innovation. 80% of citizens agrees with this.

Figure 4:



In short, it isn't easy to innovate and bring together the right skills, technologies, people, processes and deciders, and to also learn from successes and failures. But there is hope. Through the years, especially the many failures of organizations have taught us that innovation is about more than just starting a few experiments, implementing an innovation hub or taking over promising start ups. It helps to have a clear innovation strategy, coupled with a clearly defined purpose. Formulating an approach with a clear scope, governance, organization structure and process is also helpful. Innovation flourishes within well-defined boundaries. Finally, it is advisable to introduce innovative methods of working that stimulate sustainable innovation by supporting the ability to innovate. Good examples are Agile methods, new platforms for collaboration and sharing, new learning methods in communities and more effect-oriented, purposive ways of measuring and accounting for performance.

That the security domain will accelerate innovation is beyond question. Rather, the question is: how is the domain going to accelerate innovation? It will at least require a more focused deployment of innovation. What contribution will innovation have to make? How to organize different activities in a way that support the type of innovation you seek? And how to create an environment where the ability to innovate grows while innovation is commencing? This report offers inspiration, vision and trains of thought to help you harness the potential of innovation and to latch onto opportunities that present themselves. We especially hope you will enjoy yourself in your journey of discovery!

Erik Staffeleu
Head of People & Organization at Capgemini Invent

erik.staffeleu@capgemini.com

[1]For more information: https://www.innoveermeemetjenv.nl/