Capgemini

EUROPEAN VOICES

TRENDS IN PUBLIC SECURITY 2021-22: A PERSPECTIVE FROM THE NETHERLANDS

EUROPEAN VOICES

EUROPEAN VOICES

European Voices brings together viewpoints from our experts in Europe, working at regional, national and international organization level, on topics that will resonate with public sector leaders across the world.

Evolving legislation and data initiatives. The impact of new technologies on citizen service delivery. Governments' responsibility to enable business and sustainable economic growth in a fair society. Affirming European values in the digital domain. As Europe's digital decade unfolds, diverse points of view across the continent offer valuable insights that can build greater understanding and coherence, while providing a benchmark for the international community.

This series offers comparative perspectives to the global public sector community and a window into the latest thinking shaping local policy, technology choices, and citizen-centric innovation.

ABOUT THIS REPORT

The following executive summary gives European leaders insights into the safety and security trends affecting citizens in the Netherlands. More information can be found in the full Dutch report Trends in Security 2021-2022.

CONTENTS

TRENDS IN PUBLIC SECURITY 2021-22: A PERSPECTIVE FROM THE NETHERLANDS

How safe do citizens in the Netherlands feel today? What type of cybersecurity threats are they encountering? What are the security implications of the increase in remote working? And how have organizations in the security domain accommodated the new reality of life during and after a global pandemic? As digital technology drives unprecedented shifts in approaches to public security and safety, authorities need such insights to help them respond to the digitization of crime, new digital tools, and new forms of citizen interaction.

Now in its eleventh year, the *Trends in Security* report from Capgemini in the Netherlands offers new perspectives on the Dutch security domain that will also have implications for technology and security leaders across the global public sector. In particular, it offers insight into the adoption — and quality — of intelligence-led operations as data and information support greater efficiency and effectiveness, how the scope of cyber (security) is growing, and how the pandemic has accelerated digitalization efforts.

Tapping-in to the security zeitgeist

Trends in Security 2021-2022 draws on a survey of around 1,000 Dutch citizens aged 18 or older conducted from 1-5 February 2021. This found that citizens in the Netherlands expected the government to facilitate the fight against cybercrime through legislation, education, and other means at its disposal. Further, an overwhelming majority (95%) supported extra investment by government/police in technological resources, knowledge, and extra manpower to combat crime. For the key survey findings, go to Section 3 of this executive summary.

Trends in Security 2021-2022 brings together these findings with expert opinion on a diverse range of topics. These include the use of drones as enforcers, how AI-driven document control improves identification and why information-driven work ambitions are yet to take flight. Further perspectives look at intelligence-driven partnerships within agencies and across borders, how to exchange information without sharing or replicating sensitive data, what needs to be done to prepare the security domain for the 'quantum internet', and the mobile workplace enabling tomorrow's police officers to work safely anytime, anywhere.

Moving from risks to opportunities

This executive summary provides an overview of the key topics discussed, revealing new thinking among leaders in this field. We find that the focus is no longer on avoiding risks, but on grasping opportunities. This is epitomized in a comment by Ric de Rooij, deputy secretary-general at the Dutch Ministry of Justice and Security, who said: "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 step, start taking risks. Security as a driver to take risks. To do nothing is not an option."

Data presents safety and security agencies with new opportunities. Traditionally, the criminal justice system has been geared towards apprehending one or a few perpetrators, causing one or a few victims; now, with the exponential increase in cyber criminality, 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 to solve this problem.

A willingness to adapt

It is also clear that public security and safety teams must constantly adapt to new types of criminality and learn new ways of collaborating and engaging with citizens. For example, the increase in digitalized criminality and cyber criminality has seen its volume surpassing that of domestic burglaries; in security jargon, it has become Veel Voorkomende Criminaliteit, or "common criminality".

The *Trends in Public Security* survey found that public sector safety and security organizations in the Netherlands are, indeed, showing a significant ability to adapt. The adaptive security organization has been a response both to the ongoing coronavirus crisis, and more generally to a society that is digitalizing at an increasing rate. According to 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."

The implications of this faster pace of change and many other digital, social, and technological evolutions are discussed in depth in the full *Trends in Security 2021-2022 report*.

For an overview of the key topics for 2021 go to Section 2 of this executive summary.

KEY PUBLIC SECURITY TOPICS FOR 2021-22

Robocop: the flight of a drone as an enforcer — how to steer the technological and strategic development of drones in the right direction

The completion of legislation surrounding Unmanned Aerial Vehicles (AUV), popularly called drones, is a sign that the development of, and applications for drones are taking serious shape. With the number of human eyes and ears on the street decreasing as a result of an aging population, drones and sensors can help law enforcement entities fill the information shortage, provide a good situation overview, and aid in decision-making. An overarching Drone Expertise Center is needed in the Netherlands.

Neighborhood officer — assistance wanted! How can community police officers avoid drowning in the increasing amount of available information?

The stream of information from social media, sensors, and statistics is changing the work of community police officers. But too much information and "infobesity" threatens their effectiveness. An Intelligent Virtual Assistant (IVA) offers a solution. An IVA can filter information by relevance and monitor behavior and stress in order to provide only the most pertinent information for a given officer or situation.

How semantics can contribute to a safer Netherlands

Is "knowledge-conscious operation" the next step after "data-driven work" and "information-driven action"? Security professionals are empowered to deal more effectively with their data and information through the use of RDF-based semantic models that ensure the data exchanged between digital systems has a shared meaning. RDF (Resource Description Framework) helps train and keep artificial intelligence (AI) explainable. AI can use semantic models in digital form to become smarter and more efficient in identifying meaningful relationships, for instance in a policing scenario.

Staying agile and in control in the risk society: the application of AI in a risk management system

How can an Information Security Management System (ISMS) and artificial intelligence (AI) contribute to an organization's cyber risk management? Risk management is essential for putting organizations in control of key strategic, preventive, cyber, and external risks. The exponential increase in cyber risks each year forms a separate risk category that needs a different way of managing. An ISMS offers a way for organizations to mitigate cyber risks without losing sight of the business goals. The addition of AI further strengthens defenses, for example AI could automate the risk analysis process and play a role in predicting events.

The Netherlands' national digital security — from compliance to risk management

Society is increasingly dependent on digital systems and infrastructure. The Security of Network and Information Systems Act (known in the Netherlands as the WBNI) is designed to trigger a move from a cyclical compliance approach to cybersecurity to one that fosters a risk management culture at all layers. It mandates organizations providing vital services, such as at the country's ports, and central government to report serious digital security incidents to the public authorities and integrate cybersecurity into their risk culture. It is a unique opportunity for cybersecurity to receive attention at board level and will demand public-private partnerships going forward.

Chain collaboration without having to share data — new technology makes it happen

Data sharing is essential for public order and security. At the same time, data privacy regulation (GDPR) and different classifications (e.g. from NATO and the EU) make this difficult. Sharing data is also risky without appropriate controls. New technology, such as cryptography, can make the difference. Zero-Knowledge Proof cryptography is a special type of cryptography that is now maturing due to the rise of blockchain technology. This allows data sharing to take place without the need to provide protected information — and much more.

Giving the police a new weapon — a mobile workplace

By 2025, every officer in the Dutch police will have a new weapon in the fight against crime — a mobile workplace. The ability to work together safely anytime, anywhere will become possible as the workplace meets the expectations of a new generation of officers. Information is only valuable in the right context, in the right place and at the right time. So, equipping officers with a mobile workplace — whether that's on a mobile, or augmented reality glasses, or even a smartwatch — with which they are in contact with their colleagues, the citizen, and the information systems necessary to carry out their tasks directly, is essentially giving them a new weapon against crime.

Improved identification through AI-driven document control — how AI and privacy-sensitive data can work together

Everyone in the Netherlands over the age of 14 is required to have at least one identity document. These documents contain basic personal information used during official actions or activities such as travel, opening a bank account, taking out insurance, a police check, etc., and present a fraud risk. The year-on-year increase in reported identity fraud is an increasing risk to both national security and systems. While the sensitivity of personal data stops the implementation of complete AI solutions, control bodies need to switch to specialized AI components to keep up with technological advances and use the power of AI to prevent fraud in the future.

Want, must, can: the road to information-driven working

How do you strengthen willingness to change in the pursuit of intelligence-led operations (IGW)? IGW has been a priority in public security for years. Police, inspections, defense, municipalities and implementing bodies all have firm ambitions in the field of IGW. But these ambitions are lagging behind reality. A focus on willingness to change is a promising strategy for closing this gap. The proven DINAMO method (want, must, can) provides tools for measuring and improving willingness to change.

Digital security and quantum internet — do they go together?

What questions should the security domain ask itself in preparation for the quantum internet? The choices we are currently making about the quantum internet will determine our future security. With the advent of computers easily cracking contemporary encryption, we must think about the laws and rules in the world of tomorrow, right now. Quantum technology must not fall into the wrong hands, so how can governments prevent this? A broad-based framework is needed that steers towards responsible use, while choices must be made about openness and sovereignty.

Steering intelligence in partnerships to make a real impact on undermining crime

Intelligence is often seen as a technical or privacy issue, but targeted intelligence stands or falls with a management strategy based on collaboration. In the Netherlands, a Multidisciplinary Intervention Team comprised of six government organizations (Police, Public Prosecutor's Office, Borders, Customs, Tax Authorities and FIOD) aims to create intelligence on subversive crime. Such partnerships need a common language and scope that's continuously developed, as well as a dynamic intelligence process and priorities based on a strategic and objective view of the security domain.

Cybercrime forces the police organization to change

With cybercrime on the rise, as well as being a relatively new form of criminality, the police face a major task in effectively combating it. Cybercrime is dynamic, unnoticed, and unlimited. Further, it has increased since the start of the Covid-19 pandemic. It forces a different policing approach from detection and prosecution to prevention and disruption. In turn, this demands the building of a better intelligence position, with data-driven work now a core aspect of facilitating the move towards prevention and disruption.

Innovation and ethics in forensic care — getting the right balance

The government in the Netherlands strives for a gradual and responsible return of perpetrators to society by continuously optimizing the quality and effectiveness of forensic care (where professionals provide care, mental health treatment and security for patients who have been convicted of crimes). However, with social trust in technological innovation crucial, organizations are cautious about taking steps towards technological innovations because they do not sufficiently understand the social impact. Defining ethical values in advance and the purpose of the innovation process help to make both the social value and possible impact transparent, defining the trade-offs and conclusions.

Security is human work — how the Ministry of Defense uses "Intelligent HR" to win the battle for talent

Disruptive change in the security arena is ongoing and the cyber and information domains are under fire every day. The defense of the nation demands appropriate skills but in the world of IT the "battle for talent" makes this no mean feat. What's needed is a strong battle plan — one that considers: the technological developments that lie ahead and when; the current and new roles that will be needed in the future; how to organize the organization for new technological developments; and whether the hierarchical command-and-control line still works, or should the focus be on more flexible forms of collaboration such as Agile or DevOps?

Innovating with impact — successfully scaling up of innovations

Millions are being invested in innovation by organizations and governments in response to the changing needs of citizens and the new possibilities of technology. But

innovations are only valuable when scaled up and achieving this scale is a challenge. The best approach is to treat scaling up as a separate area of focus in the overall innovation process and to recognize that collaboration across departments is often necessary.

Organizational innovation — fighting crime the Cruijffian way

Dutch soccer legend Johan Cruyff once said: "Football is a simple game: you just score one goal more than your opponent and then you basically won". The same applies in the fight against crime. But how should the safety chain organize itself to win in daily practice? It requires organizational innovation with the implementation of new ways of thinking and organizing. This is the foundation for making the Netherlands safer. It requires the wisdom of the crowd: the opponent has new technologies, so you cannot win the match alone. And the safety chain — or network — must accelerate to (continue to) win.

Safety at the time of a pandemic

The measures taken by the government in the Netherlands to prevent the spread of the coronavirus have had a major social impact. In general, people appear to have started to feel safer at home and on the street. However, worries about online security have grown, with certain offences, notably involving phishing and hacking, being a growing cause for concern. The perceived threat from digital, rather than physical causes extends to national security, with 74% of respondents thinking a digital attack could shut down the entire country. The advice of citizens in the Netherlands to their government is to deploy more skilled people and to come up with creative technical solutions, in which cooperation with the citizen should not be shunned.

TRENDS IN SECURITY 2021-22: KEY SURVEY FINDINGS

The *Trends in Security 2021-2022* survey involved 1,000 citizens in the Netherlands aged 18 years and above. It was conducted from 1-5 February 2021 via the online quantitative research Ipsos MORI Online Interview Panel. The data captured was subsequently weighted to be representative by gender, age, region, and education.

Overall, the survey found that respondents rated their overall security higher than last year, while their sense of online security declined. The report authors are not surprised by this, citing the global pandemic as the primary cause. The accelerated increase in digital crime as a result of the pandemic has forced people to pay more attention to combating cybercrime.

Key findings

The following uses a scale of 1 (lowest) – to 10 (highest), along with percentages of the responses.

1. Digital versus physical threats

Women and young people are more likely to feel unsafe.

39% of respondents indicate they sometimes or often feel unsafe. That's similar to 2019 (3% often, 42% sometimes unsafe). Women (49%) and young people aged 18 to 29 (53%) report feeling unsafe relatively often.

People feel safest at home, followed by on the street. Online safety is rated with a 6 or 7 (out of 10) and less often with an 8 or higher. Men and over-65s give relatively high marks for their sense of security at home, on the street and online.

A digital attack on the Netherlands is considered more probable than a physical one.

58% of respondents consider a digital attack in the Netherlands (very) likely.

A physical attack is considered a lot less likely (23%).

2. How should the Netherlands be protected? Expectations of the government, which resources should be utilized, and what investments are needed

Citizens expect the government to have a facilitating role in the fight against cybercrime.

A majority of respondents see a facilitating role for the government to increase digital safety by increasing authorization, imposing extra legislation, heavier penalization and by providing better awareness education.

There is support for the use of technology by the government/police for the fight against crime.

A majority has no objection to the use of technology by the government and police to combat crime.

There is support for extra technology and knowledge investment by the government and police.

An overwhelming majority (95%) supports extra investments by government/police to keep the Netherlands safe. Investments can be in terms of technological resources, knowledge and thirdly in terms of extra manpower.

Of the respondents that think extra investments in knowledge should be made, 72% think it is a good idea to involve IT savvy citizens with online searches.

3. Trust in organizations

Not everyone trusts the government to handle citizens' personal information safely.

38% of the respondents trust the government to handle personal information safely. The government scores worse than hospitals, police, and banking/insurance companies in this respect. Trust in the government is relatively high among youths aged 18-29 years (48%) and the higher educated (42%).

62% of the respondents trust that once collected and saved, citizen information is well protected against malicious persons and organizations by the government. And 51% trust the government to utilize the information lawfully, and sufficiently protect citizens' privacy.

There is support for exchange of personal information by intelligence agencies to combat terrorism and fraud.

60% approve of intelligence agencies exchanging personal information to combat crime. In particular, men (69%) and the higher educated (66%).

78% expect the police to have access to the historical police records of someone who seeks contact with them.

4. How safe do you feel?

The majority of respondents have at some point encountered internet criminality, and a quarter have been a victim of cybercrime.

39% of respondents had an experience with cybercrime. Of these, 52% of the cases were an attempted crime and in 48% of cases an actual cybercrime took place.

Actual cybercrimes are reported more often to the police (50%) than attempts of cybercrime (24%).

Spam and phishing are the most commonly occurring forms of internet crime. Most victims are targeted through spam, viruses, and fraud with fake websites.

In general respondents who had experience of, or were victimized by cybercrime estimated the likelihood of being victimized in the next two years as relatively high.

Respondents found it hard to recognize phishing mails.

67% indicate that phishing mails have become harder to recognize in recent years. Of these, 68% expect it will not be possible to distinguish phishing mails from real mails in five years' time.

Dutch citizens see their digital safety as their own responsibility.

At 69% of the respondents, the Dutch predominantly hold themselves responsible for their own digital safety. This is followed by internet providers (44%), website/app owners and developers (29%) and politics (14%).

The most common measures to protect privacy are regular software and app updates and avoiding suspicious websites.

Regular software updates (69%), avoiding suspicious websites (62%) and app updates (58%) were cited as the top three measures. This is followed by regularly erasing cookies (50%) and frequently changing passwords and usernames, turning off devices when not in use, and not publishing private information online at 44%.

5. Current themes

Coronavirus

All information sources are subject to perceptions of doubt regarding the reliability of news surrounding the coronavirus. Information from the government and TV-news is perceived as most reliable.

For all information sources except social media, trust is higher among those with higher levels of education. Conversely for social media, the higher educated are the most sceptical group.

Respondents perceive that during the pandemic, criminal activity shifted from offline to online. 75% of respondents indicate that online crime has increased since the pandemic.

Six out of 10 respondents hope that increased surveillance will remain after the crisis, but many expect otherwise.

Dutch parliamentary (Tweede Kamer) elections 2021

When determining their voting choice during the Dutch national election of 2021, respondents indicate the use of the Stemwijzer/Kieskompas tool, TV news and news websites as information sources and these are perceived as reliable.

A majority of respondents expect attempts by foreign countries/ governments to influence the elections. A large portion (30%) indicated this to be (very) likely.

Traditionally voting occurs with pencil and paper. Due to the pandemic, voting by post was made possible. There are supporters and opponents of digital voting. Distance voting is seen as more prone to fraud (53%) and among respondents aged 70+ this was 43%. Digital voting at a polling station is perceived as less sensitive to fraud when compared to voting digitally at home.

Fake news

A majority of respondents identify the existence of fake news and attribute that to criminal groups and hackers. Only 5% of respondents deny this.

Half of the respondents doubt whether they could recognize fake news. 67% indicate it is increasingly difficult to distinguish between real and fake news compared to three years ago.

For the identification of fake news, respondents most frequently check source/sender, other sources, styling and language. 45% of the respondents indicate that they actively check the messages they read.

A majority of respondents (85%) are familiar with the social media trap, in which users of social media increasingly receive messages that fit their profile. Knowledge of this makes them less vulnerable to being influenced by fake news.

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 300,000 team members in nearly 50 countries. With its strong 50-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion.

Get The Future You Want

www.capgemini.com

For more details contact:

Pablo Derksen
Vice President and Segment Head,
Public Sector
pablo.derksen@capgemini.com

Thomas de Klerk
Marketing Manager,
Public Sector
thomas.de.klerk@capgemini.com

GET THE FUTURE YOU WANT

MACS 3691_10-2021