2 November 2020

FOCUS ON

On 16 March 2020, the Dutch Prime Minister directly addressed the nation regarding the COVID-19 crisis. In the days before, many schools and universities, Restaurants, cafés and offices had closed their doors and working from home where possible had suddenly become the norm. Overnight, virtually all of the approximately 175,000 civil servants of the ministries and High Councils of State started working from home in so far as possible. Most of them rose to the challenge very successfully. While trains ran empty, roads were deserted, the work went on at home. Colleagues collaborated and communicated with each other by telephone, traditional network drives and email, and increasingly through video conferencing tools, messaging apps and online teamwork environments. Collaborative ICT tools are not new, but they were now being used en masse for a wide range of new purposes. This raised many questions among users: Was *Zoom* secure enough to discuss work-related information? Could work-related information be shared through a messaging app? How could I use my private laptop for work safely?

Between July and October 2020, we investigated what ICT tools were being used by the staff of ministries and High Councils of State, what they were being used for, what security risks they represented and how the organisations communicated their policies on digital home working.

We found that civil servants sometimes used collaborative ICT resources in a way that put information security at risk. Some rules were ignored and confidential work-related information, for instance, was shared via *WhatsApp*. Furthermore, not all civil servants

knew what the rules were or thought they were practical. Policy on collaborative ICT tools also differed from one organisation to another (figure 1). This created confusion among civil servants about what was permitted and what was not, and made communication between organisations more difficult (figure 2).

Collaborative ICT tools have proven to be unmissable during the corona pandemic. We want this investigation to contribute to the further development of digital collaboration within Dutch central government.

An organisation's choice of collaborative ICT tools in influenced by various factors

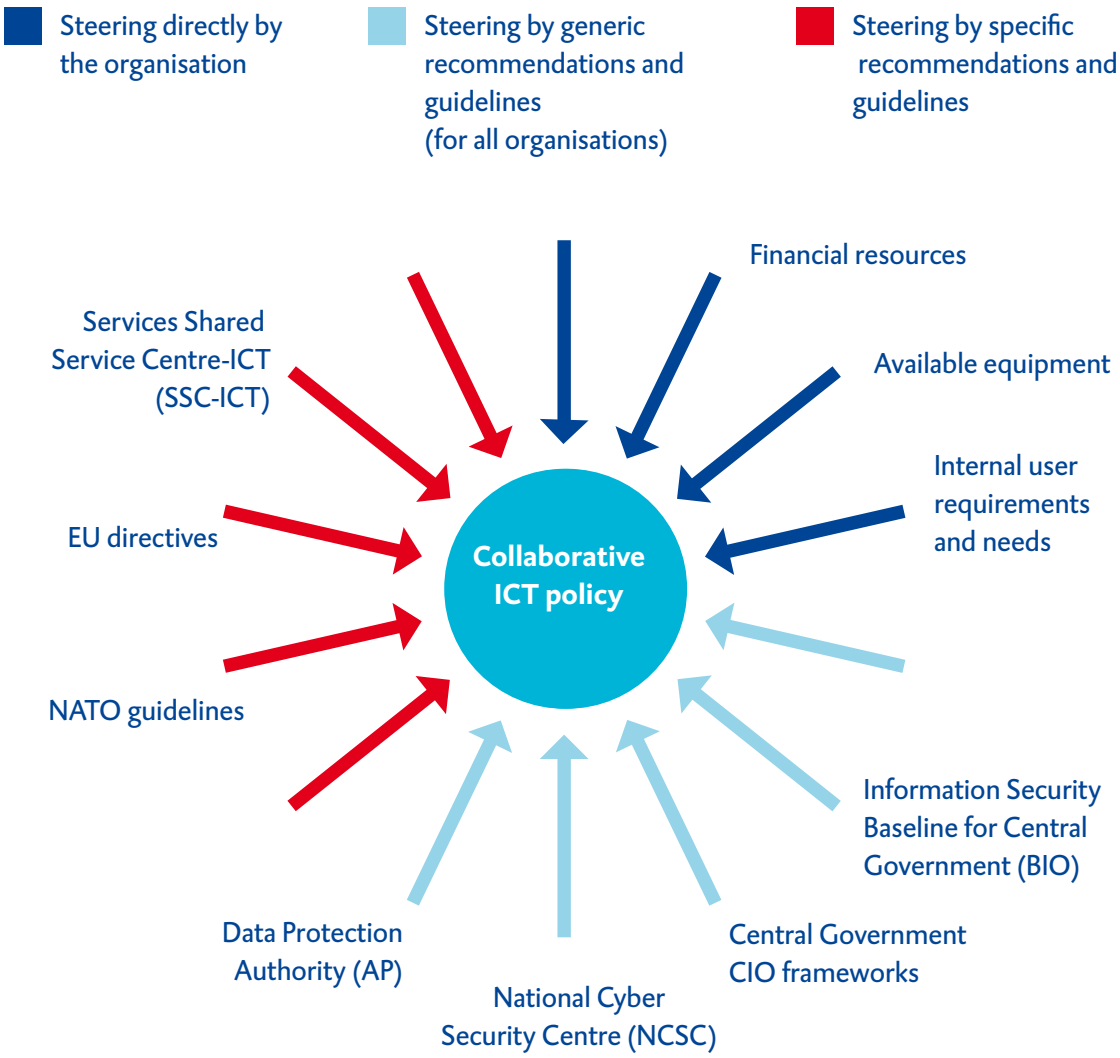

Figure 1 *Factors that influence policy on collaborative ICT*

Different working arrangements complicate collaboration between organisations

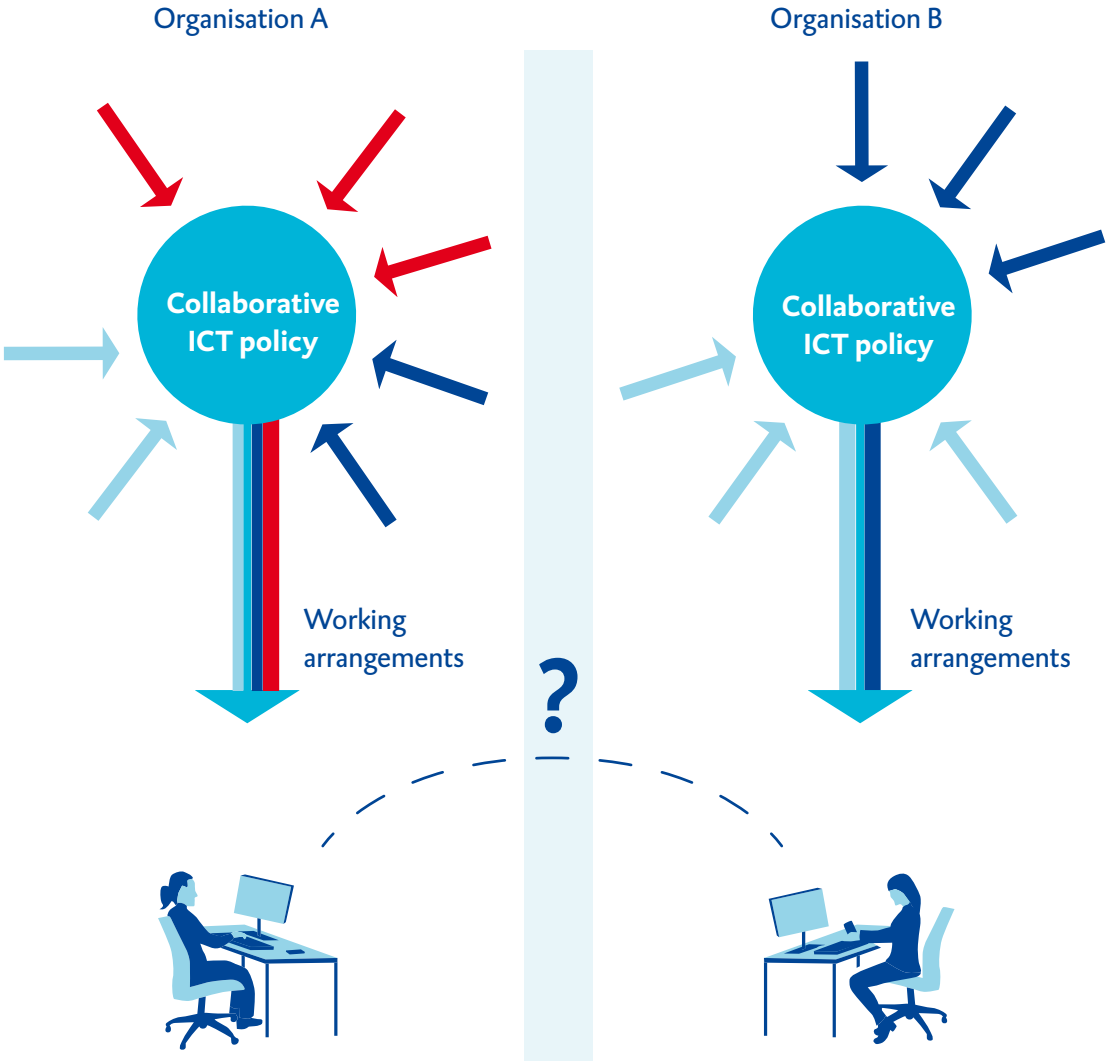

Figure 2 *Differences in policy and working arrangements*

A focus investigation differs from the Netherlands Court of Audit's customary audits in that it is performed over a considerably shorter period of time (about 14 weeks), responds to current affairs and addresses a strictly defined question. A focus investigation results in a clear, concise publication without conclusions or recommendations.

1 Use of collaborative ICT tools

In an online survey, we asked civil servants from ministries and High Councils of State about their use of collaborative ICT tools. Supplemented with interviews and documents, the survey results gave us a good insight into current situation. The current use of collaborative ICT tools is illustrated in this report by means of quotations from respondents.

1.1 Work-related video conferencing usually via the recommended apps

The civil servants who responded[1] to our questionnaire had used 42 different IT applications so far this year to hold video conference calls with their colleagues. 69% of them had used the *Webex* program for work-related conference calls. *Skype for Business and Microsoft Teams* were also often used. Most government organisations recommend that their staff use these applications. The respondents accordingly held video conference calls to share confidential work-related information using the recommended apps.

1.2 Confidential information shared via messaging apps

Messaging apps are used mainly for informal communication. Of the respondents who use *WhatsApp*, 7% said they had used it to share confidential work-related information, even though it was not permitted within ministries or High Councils of State. *MS Teams* and *Signal* were often used to send short messages containing both confidential and non-confidential work-related information. Some organisations recommend *Signal* for work-related communication.

> *"WhatsApp is not permitted for work-related communication but its functionality has too much added value not to use."*

1.3 Many collaborative platforms in use

The respondents used dozens of online collaborative platforms such as *MS Teams*, *SharePoint* and *Dropbox* in order to work with each other.[2] This category of applications is very wide. There are programs to collaborate on documents, to share large files and to manage planning. A second reason that so many different applications are used is that central government has few collaborative platforms on which organisations can work together securely.

It is striking that private email is regularly used to share confidential work-related information. This is not permitted under the guidelines.

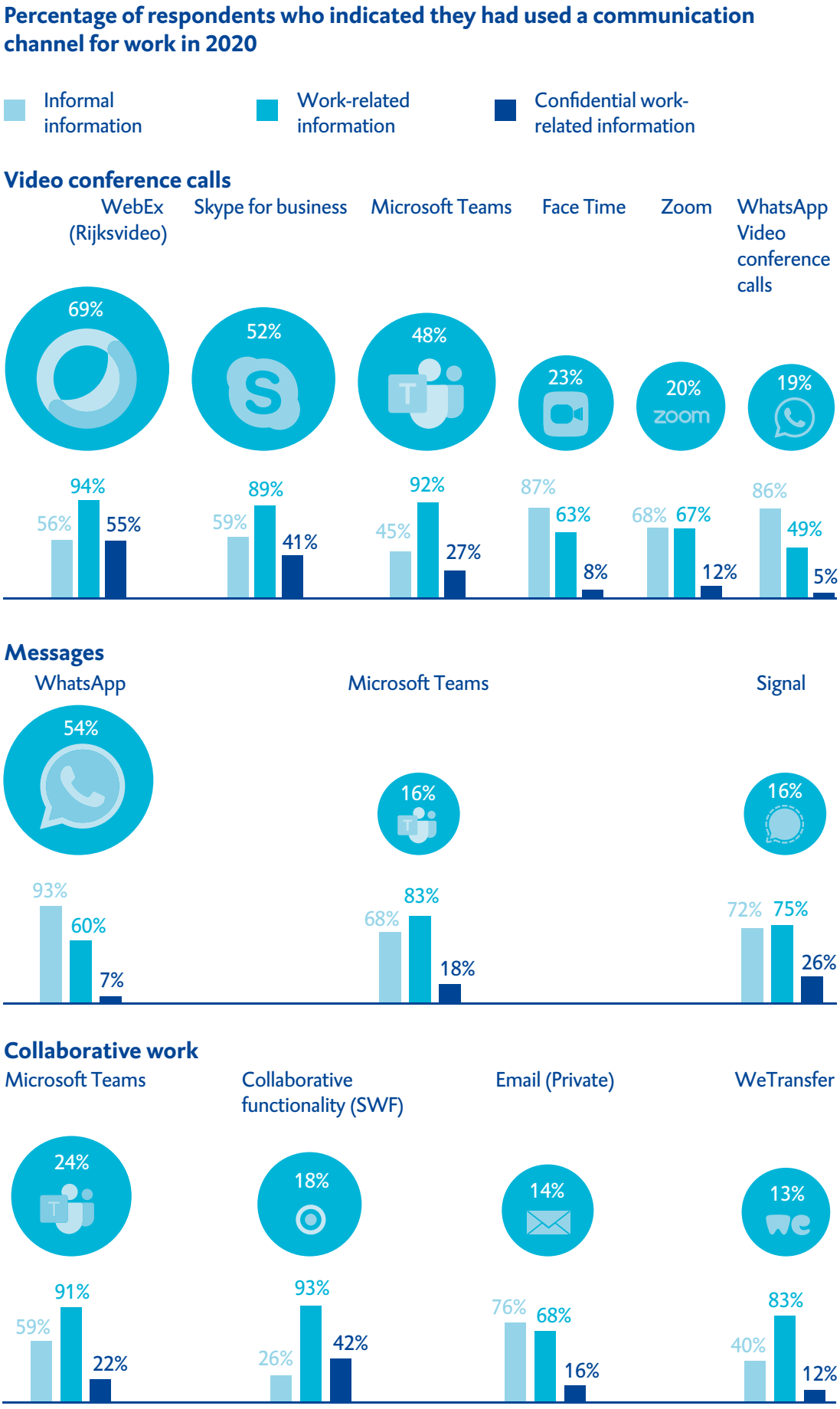

Figure 3 *Use of communication channels*

2 Working arrangements for the use of collaborative ICT tools

Ministries and High Councils of State are authorised to manage their operations as they see fit and are free to decide which ICT tools are used. We refer to all the staff regulations, arrangements and recommendations together as "working arrangements". We asked government civil servants about their experiences with the working arrangements for the use of collaborative ICT tools. In figures 4 to 7 below, the term "civil servants" refers to the respondents who completed our questionnaire.[3]

On average, 20% of the respondents indicated they were not aware of the working arrangements (figure 4); 22% said they were not satisfied with the way the working arrangements had been communicated (figure 5).

"Too many rules in too many different places, you can search as much as you want for specific information but you'll be lucky to find it…"

A fifth of civil servants think working arrangements for ICT tools are not clear

"I am aware of the working arrangements in force"
Spread of answers (%)

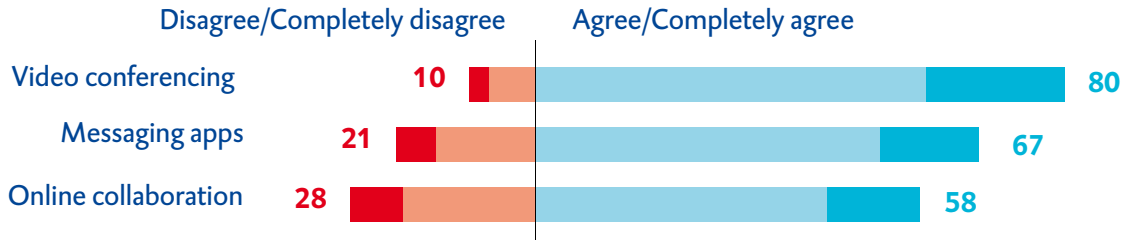

Figure 4 *Respondents' opinions on clarity of working arrangements*

A fifth of civil servants think working arrangements for collaborative ICT tools are not always workable

"I can always or nearly always adhere to the working arrangements in practice"
Spread of answers (%)

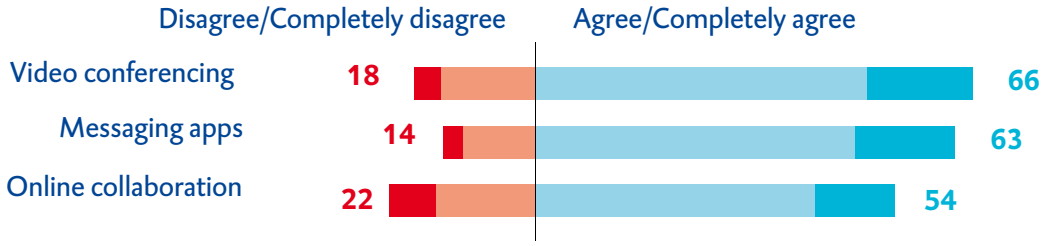

Figure 5 *Respondents' opinions on communication of working arrangements*

About 20% of the respondents indicated they could not always adhere to the working arrangements (figure 6). On the one hand, civil servants are required to use the secure home working environment (*Citrix*), but on the other, they are advised to use a private environment outside *Citrix* to make video calls. Risks attach to video calls in a private environment. As a matter of course, some video calling apps save chat messages in the device used. Information from these messages can therefore end up on a private device, over which the employer has no influence over the level of security.

"Security arrangements could be more consistent. Sometimes we are not allowed to link our name to the ministry and at other times we have to or it is linked automatically. You put a lot of effort into following one instruction and then it's all undone by another."

A quarter of civil servants are not satisfied with the collaborative options allowed by the working arrangements

"I am satisfied with the collaborative options allowed by the working arrangements"
Spread of answers (%)

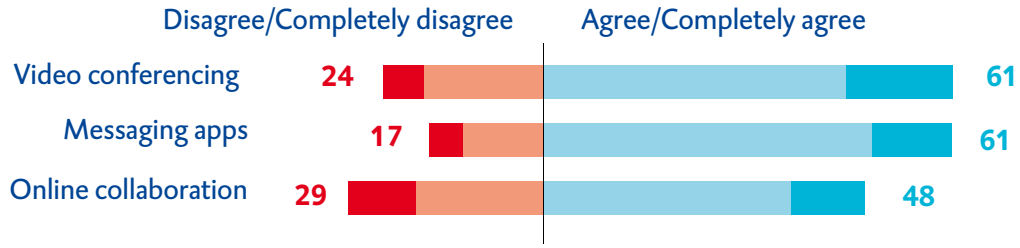

Figure 6 *Respondents' opinions on whether working arrangements are workable*

The recommended apps and advice for civil servants also differ from one organisation to another. As a result, civil servants do not know which apps they may or may not use. Central government's intranet (*Rijksportaal*), for instance, states that work-related use of *WhatsApp* is permitted under certain conditions. Several other organisations however, do not permit messaging apps such as *WhatsApp*.

"Working arrangements should be stated clearly on Rijksportaal. There are currently several interpretations depending on which part of the government you are holding a meeting with."

Some 23% of the respondents indicated the working arrangements and recommended tools lacked the necessary functionalities for collaboration (figure 7). The literature we studied showed that dissatisfaction with functionality was an important motive to seek alternatives to permitted IT applications or to completely ignore the working arrangements.[4] The Interministerial Collaboration Platform (ISWF), for instance, enables civil servants to work with each other across several ministries, but it is not user friendly.

It is then just a short step to an alternative that does not meet the ministries' security standards, such as *Dropbox*.

A fifth of civil servants are not satisfied with how working arrangements are communicated

"I am happy with the way working arrangements are communicated"
Spread of answers (%)

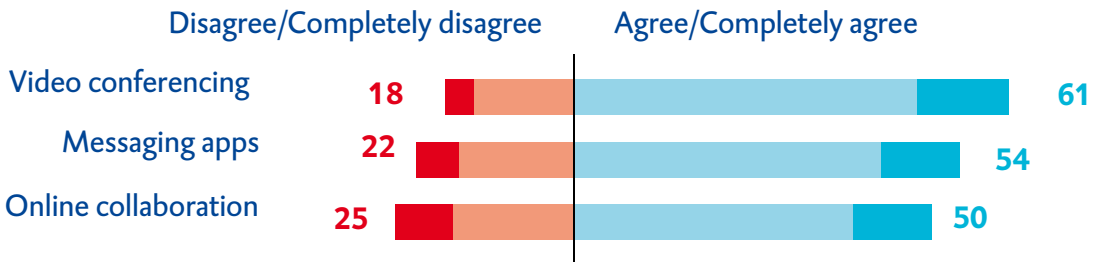

Figure 7 *Respondents' opinions on options allowed by working arrangements*

"There were no approved mobile chat options suitable for the ministry's confidential information for many years. So users sought their own solutions, with inevitable consequences."

3 Opportunities and risks of collaborative ICT

The most important risks of remote collaboration tools relate to information security, privacy and adequate record-keeping. If the ministries worked together more closely there would be more opportunity to arrive at a shared secure collaborative ICT tools and clear working arrangements. Further technological advances would also help.

3.1 Information security and privacy

The main risks attaching to use of collaborative ICT tools relate to information security and privacy. Information can slip into unauthorised hands if insecure tools are used or recommended tools are used incorrectly. Commercial parties can also obtain personal information on the users. Messaging apps on mobile phones are thought to represent the biggest risk. To give a concrete example, staff who leave an organisation can stay in an app group and continue to have access to confidential work-related information.

We also learned from our interviews that senior civil servants, ministers and state secretaries often do not use the prescribed IT tools either. Yet they have a duty to set an example so that the rest of the organisation uses secure IT apps. The chief information officer (CIO) at one ministry indicated that a lot of time, money and effort had been invested in secure (secret) communication tools such as the Sectra Tiger telephone but little use was made of them because they were not user friendly. Senior civil servants, ministers and state secretaries often preferred popular messaging apps, tablets and smartphones to the highly secured tools because they were easier, faster and more user-friendly.

After the start of the coronavirus pandemic, the media reported that ministers and state secretaries were using *Zoom* and *WhatsApp*.[5] Use of these applications to share confidential information in central government is not recommended. Slightly longer ago, it was revealed that a minister was saving confidential documents in *Gmail*.[6] In one of our interviews for this investigation it transpired that in spring 2020 one of the ministries had set up an extra-secure environment for video meetings at the request of the central government Chief Information Officer (CIO). The ministry allowed the political heads of other ministries to use the environment to share confidential information with the ministry and among themselves. Members of the government, however, had no interest in such a system. In practice ministers and state secretaries do not follow the guidelines on ICT tools. This is problematic because they are not formally civil servants and are not answerable to the Secretary-General or the Chief Information Security Officer.

We found that civil servants at ministries and High Councils of State also used alternative collaborative ICT tools as well as the recommended ones. Their organisations are aware that adequate information security and privacy levels cannot be guaranteed. It is virtually impossible to check precisely what collaborative ICT tools civil servants are using. The use of a tool that is not permitted is sometimes unavoidable. Government civil servants do not always decide which tool are used to interact with others. *Zoom*, for instance is the standard video conferencing app for many international organisations. Ministries and High Councils

of State cannot always avoid using it, even though it is not recommended. Without using *Zoom*, the Netherlands would not be able to take part in some international conferences.

Aware that the rules cannot cover every eventuality, civil servants rely on their common sense and conscience and work according to principles instead of hard rules.

"It would help if users were more aware of the risks of sharing information through certain tools. We should exercise our professional judgement instead of following rules."

3.2 Poor records kept of collaborative ICT

The absence of orderly records of the information shared across collaborative ICT tools is not without risk. If records are not kept, insight into what has been agreed and the associated decision-making process will also be poor. This will lead to problems in establishing the audit trail and it will no longer be possible for a ministry to be fully accountable to inspectorates, auditors, the media and parliament. It cannot be assumed that relatively new forms of collaborative ICT will keep records as well as more established ones such as email.

"Everyone is going to work with Dropbox/Google Drive. No one will know what happens if records are not being kept centrally."

3.3 Opportunities for common collaborative ICT

Our investigation revealed a need for common collaborative ICT that enabled civil servants at ministries and High Councils of State to work securely with each other. What is important is not standardised use (everyone using the same apps) but interoperability (using the same standards so that different apps can communicate with each other). The *Webex* and *Jabber* video conferencing apps, for example, use the same technology and can communicate with each other. Users of these two apps can therefore collaborate using their own applications.

Standardisation is not always possible within central government owing to the specific requirements and needs of individual organisations. Some ministries, for instance, must satisfy NATO or EU requirements that are stricter than the Netherlands' own requirements. The technical security requirements of both NATO and the EU, for instance, prevented the Ministry of Foreign Affairs from taking part in a common document printing solution and holding video conference calls.

Epilogue

The outbreak of the COVID-19 pandemic in March 2020 accelerated digital home working in central government and its associated organisations. It has demanded a great deal of flexibility from tens of thousands of people and dozens of support services. Civil servants had to set up permanent workplaces at home, often in the same room that their children were receiving remote schooling, and at the same time often care for vulnerable people. The support services pulled out all the stops to ensure the ICT infrastructure continued meeting the demands of the huge number of home workers and deal with their requests for help. Ministries, the central government CIO, individual civil servants and service providers such as SSC-ICT must be complimented for their response to the crisis.

Working processes that were largely exceptional at the beginning of the year were commonplace by April. For many, video conferencing has become a daily routine and – after years of government reluctance – the advance of digital signatures now seems unstoppable. Remote working has taken off and is here to stay.[7] Our investigation found that civil servants need unambiguous and more user-friendly information on collaborative ICT tools and the conditions under which they can be used.

"Why is there one government for the public but not for the civil servants?"

Working from home is making inroads into all areas of society and the government, and will probably have consequences for many organisations' office spaces and buildings. The government has presented concrete plans for the future of the civil service in the Civil Service 2022 programme. It has also drawn up an investment plan that provides funding to, for instance, prepare meeting rooms for hybrid meetings.

We do not express an opinion on the use of collaborative ICT or the regularity of related expenditure in this report. We will not express such opinions until we publish our 2020 Accountability Audit report in May 2021.

Response of the State Secretary for the Interior and Kingdom Relations

The State Secretary for the Interior and Kingdom Relations responded to this report on 30 October 2020 given his responsibility for coordinating ICT within the civil service.

The State Secretary thanked us for the report and agreed that the situation created by COVID-19 had demanded a great deal of flexibility from central government both as an employer and as a service provider. He also thanked us for the compliment we gave for the way in which home working had been facilitated for so many civil servants in such a short period of time.

The State Secretary indicated that a range of measures had been taken in the initial phase of the crisis. Whether and how they should be continued, tightened up or scaled down would be determined in the medium term. According to the State Secretary, permanent attention is devoted to risk management in the fields of information security, privacy and appropriate archiving within central government. He referred to the 'Awareness of Secure Work' campaign launched on 21 October 2020 and additional measures to improve the way in which government information relating to COVID-19 is archived.

The State Secretary further noted that central government was developing a medium-term vision of hybrid working practices (any time, any place) as part of the Civil Service 2022 programme. He therefore appreciates the insights provided by our report into the current use of video conferencing applications, messaging apps and collaborative ICT platforms, and the points for attention it highlights. The picture drawn of the working arrangements within central government will also contribute to the further development of digital c ollaboration and underlines the importance of a government-wide integrated approach.

Finally, the State Secretary expects the inclusion of digital home working in the government-wide 2020 accountability audit to increase insight into the occurrence of the risks and opportunities we identified in our focus investigation. The findings of the focus investigation will be used to strengthen awareness of the secure use of collaborative ICT tools within central government.

The full text of the State Secretary's response (in Dutch) is available on our website at www.rekenkamer.nl.

Endnotes

1. "Who responded to our questionnaire" was added by way of clarification after the text of the report had been adopted by the Netherlands Court of Audit. See also the methodology (in Dutch) at www.rekenkamer.nl.
2. We could not determine the exact number because we suspect that some respondents use different names for the same platforms.
3. This sentences was added by way of clarification after the text of the report had been adopted by the Netherlands Court of Audit. See also the methodology (in Dutch) at www.rekenkamer.nl.
4. Kopper and Westner (2016); *Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature*.
5. See, for instance: Het Parool (4 June 2020) *Halsema en Grapperhaus ruzieden via de app over demonstratie dam* (Femke Halsema [the mayor of Amsterdam] and Ferd Grapperhaus [the Minister of Justice and Security] argued by app about the demonstration on Dam Square) and de Volkskrant (18 July 2020) *Minister Koolmees van Sociale Zaken: "Dit is geen gezonde baan"* (Social Affairs Minister Wouter Koolmees: "This is not a healthy job").
6. NRC (17 November 2016) *Staatsgeheim in privé-mail minister Kamp (State secret in minister Kamp's private mail*).
7. See, for instance, the study by the Netherlands Institute for Transport Analysis, *Thuiswerken en de coronacrisis - Een overzicht van studies naar de omvang, beleving en toekomstverwachting van thuiswerken in coronatijd* (Home working and the COVID-19 Crisis – An overview of the extent and experience of home working in corona time and expectations for the future).

Department Communication
P.O. Box 20015
2500 EA The Hague
phone +31 70 342 44 00
voorlichting@rekenkamer.nl
www.courtofaudit.nl

Original title
Focus op Digitaal thuiswerken (Algemene Rekenkamer)

The Netherlands Court of Audit adopted the text of the publication Focus on digital home working on 30 October 2020 and submitted it to the president of the House of Representatives on 2 November 2020. An annexe to account for the methodology used in the investigation formed part of the publication. The methodology annexe and the anonymised survey results (in Dutch) are available as open data on our website at www.rekenkamer.nl.