2 november 2020

FOCUS OP

Op 16 maart 2020 sprak de minister-president alle Nederlanders rechtstreeks toe omdat er sprake was van een ernstige crisis. In de dagen daarvoor sloten vele onderwijsinstellingen, horecagelegenheden en kantoren hun deuren. Thuiswerken werd, indien mogelijk, plotseling de norm. Ook vrijwel alle circa 175.000 ambtenaren van ministeries en hoge colleges van staat moesten van de ene op de andere dag hun werk zoveel mogelijk vanuit huis doen. Dat lukte vaak heel goed. Terwijl de treinen leeg waren en de wegen verlaten, ging het werk door vanuit huis. De samenwerking en communicatie verliep via de telefoon, de traditionele netwerkschijf en e-mail, maar ook steeds meer via videovergaderingen, berichtenapps en online samenwerkingsomgevingen. Samenwerkings-ICT bestond uiteraard al langer, maar werd nu ineens grootschalig en voor diverse nieuwe doeleinden gebruikt. Dat riep bij gebruikers veel vragen op: is videobellen via Zoom nu wel of niet veilig? Welke informatie mag ik delen in een appje? Hoe kan ik mijn privélaptop veilig gebruiken voor werk?

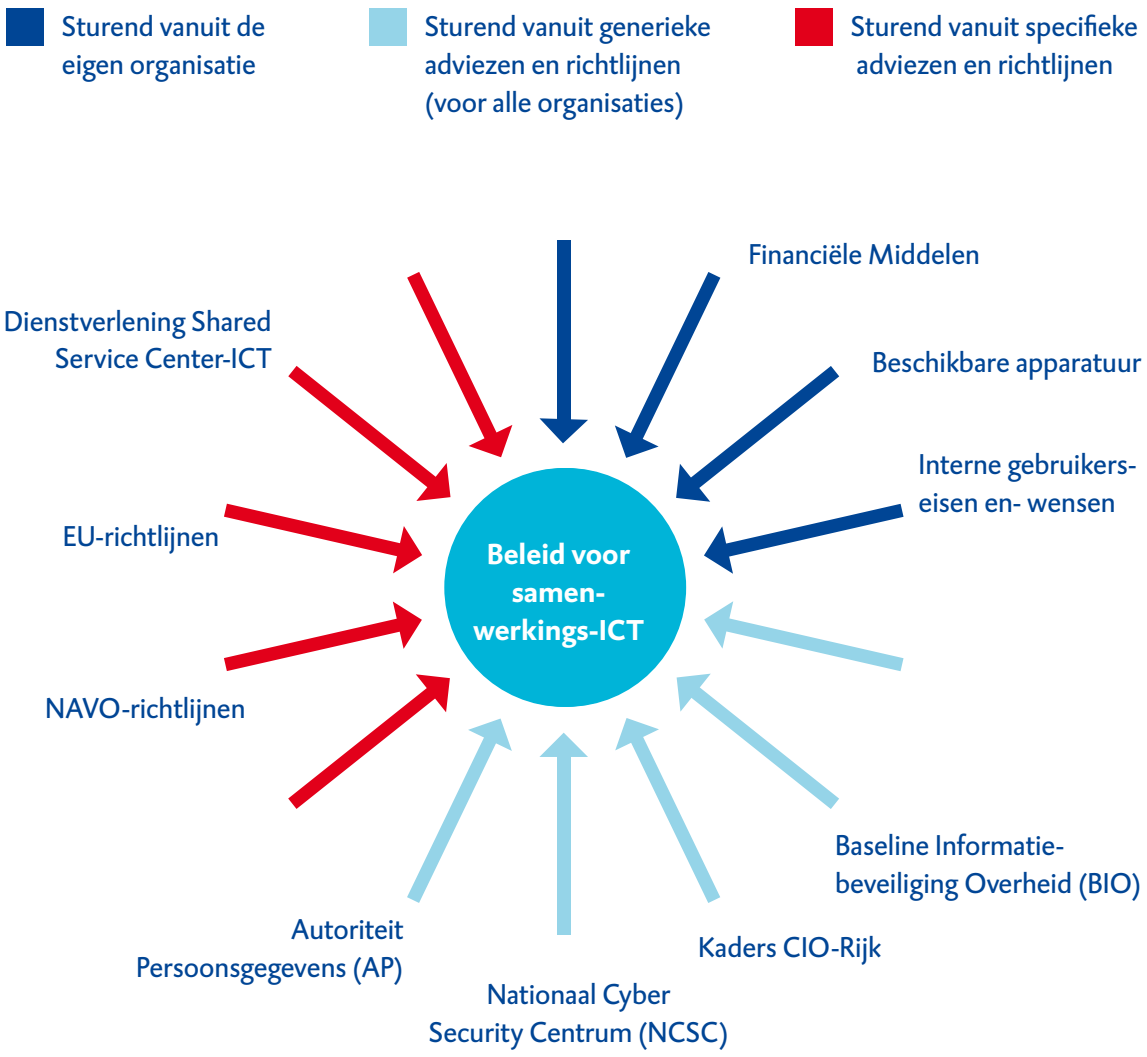
Wij onderzochten tussen juli en oktober 2020 welke ICT-middelen de medewerkers van ministeries en hoge colleges van staat gebruiken, waarvoor zij die gebruiken, welke beveiligingsrisico's dit oplevert en hoe de organisaties hun beleid hierover communiceren.

Uit ons onderzoek blijkt dat ambtenaren samenwerkings-ICT soms gebruiken op een manier die risico's voor de informatiebeveiliging met zich meebrengt. Zo deelt een deel tegen de afspraken in vertrouwelijke werkinhoudelijke informatie via WhatsApp. Verder kennen niet alle ambtenaren de voorschriften of vinden ze die in de praktijk niet goed

werkbaar. Ook verschilt het beleid voor samenwerkings-ICT van organisatie tot organisatie (figuur 1). Dit leidt tot onduidelijkheid bij ambtenaren over wat wel en niet mag en bemoeilijkt de communicatie tussen verschillende organisaties (figuur 2).

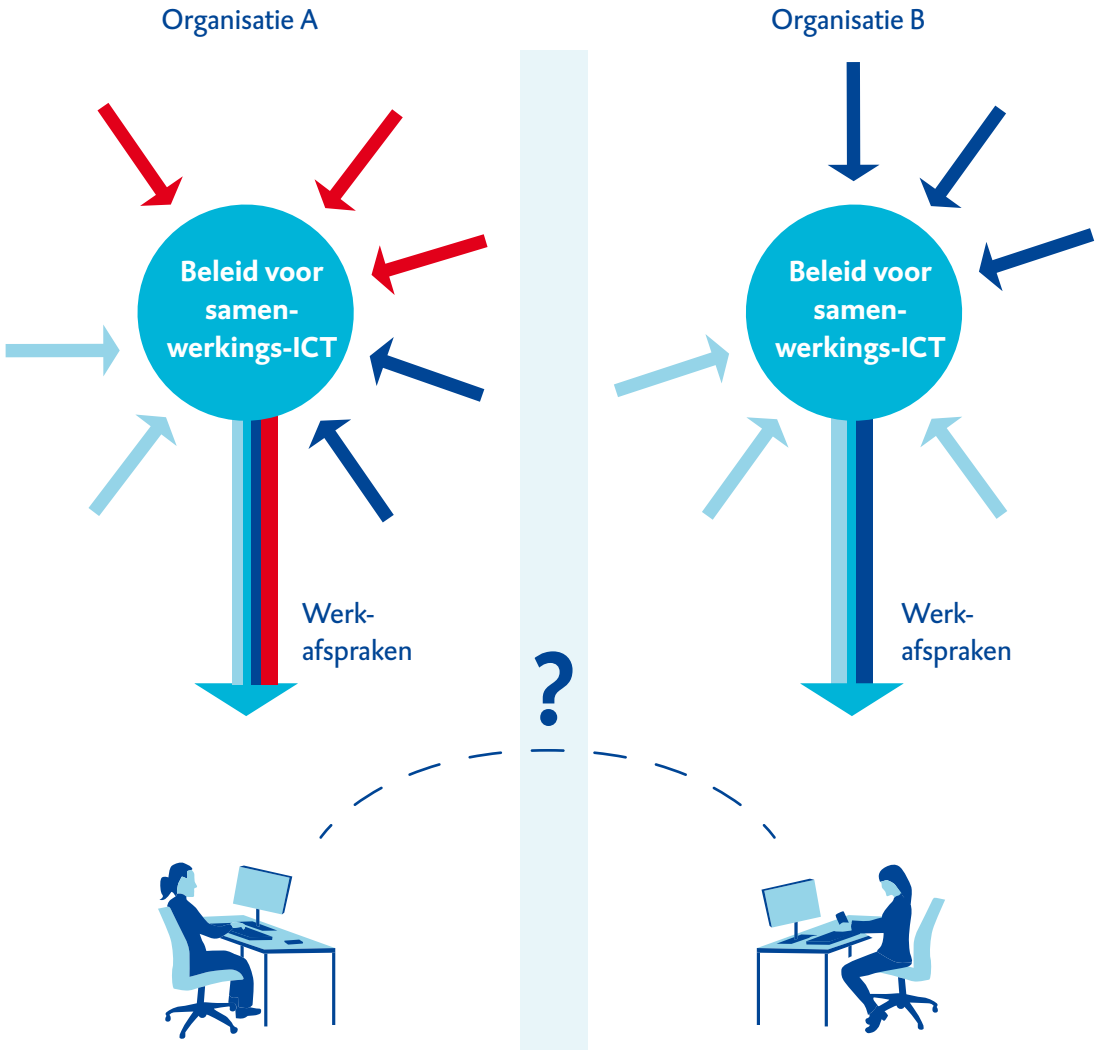
Door de coronacrisis heeft samenwerkings-ICT definitief zijn plek opgeëist binnen de Nederlandse samenleving. Met dit onderzoek willen we bijdragen aan de doorontwikkeling van digitale samenwerking binnen de rijksoverheid.

Verschillende factoren beïnvloeden de keuzes van organisaties rondom samenwerkings-ICT



Figuur 1 *Factoren die het beleid voor samenwerkings-ICT beïnvloeden*

Verschillen in werkafspraken bemoeilijken samenwerking tussen organisaties



Figuur 2 *Verschillen in beleid en werkafspraken*

Een focusonderzoek is een type onderzoek van de Algemene Rekenkamer dat zich onderscheidt van reguliere onderzoeken door een aanzienlijk kortere doorlooptijd (circa 14 weken), aansluiting bij de actualiteit en een scherpe en afgebakende vraagstelling. Een focusonderzoek leidt tot een heldere, bondige publicatie zonder conclusies en aanbevelingen.

1 Gebruik van samenwerkings-ICT

In een online enquête vroegen we ambtenaren bij ministeries en hoge colleges van staat naar hun gebruik van samenwerkings-ICT. Samen met interviews en documenten gaf ons dit een beeld van het huidige gebruik van samenwerkings-ICT. De citaten van respondenten in dit rapport illustreren de praktijk.

1.1 Werkgerelateerd video-overleg veelal via de aanbevolen applicaties

Wij constateren dat rijksambtenaren die op onze enquête reageerden[1] dit jaar 42 verschillende IT-applicaties gebruikten om te videovergaderen met collega's. 69% van de respondenten gebruikte het programma *Webex* voor werkgerelateerd overleg. Verder worden *Skype for business* en *Microsoft Teams* het meest gebruikt. De meeste organisaties bevelen hun medewerkers deze applicaties aan als voorkeursapplicatie. Respondenten gebruiken met name deze applicaties voor videovergaderen voor vertrouwelijke werkinhoudelijke communicatie, in lijn met deze adviezen.

1.2 Vertrouwelijke informatie gedeeld via berichtenapps

Berichtenapps worden vooral gebruikt voor informele communicatie. 7% van de respondenten die *WhatsApp* gebruiken gaf aan de app gebruikt te hebben voor vertrouwelijke werkinhoudelijke communicatie. Dit gebeurde terwijl het niet is toegestaan binnen ministeries of hoge colleges van staat. De gebruikers van *MS-Teams* en berichtenapp *Signal* gebruiken deze applicaties veel voor korte berichten met vertrouwelijke en niet-vertrouwelijke werkinhoudelijke informatie. Sommige organisaties adviseren *Signal* voor werkinhoudelijke communicatie.

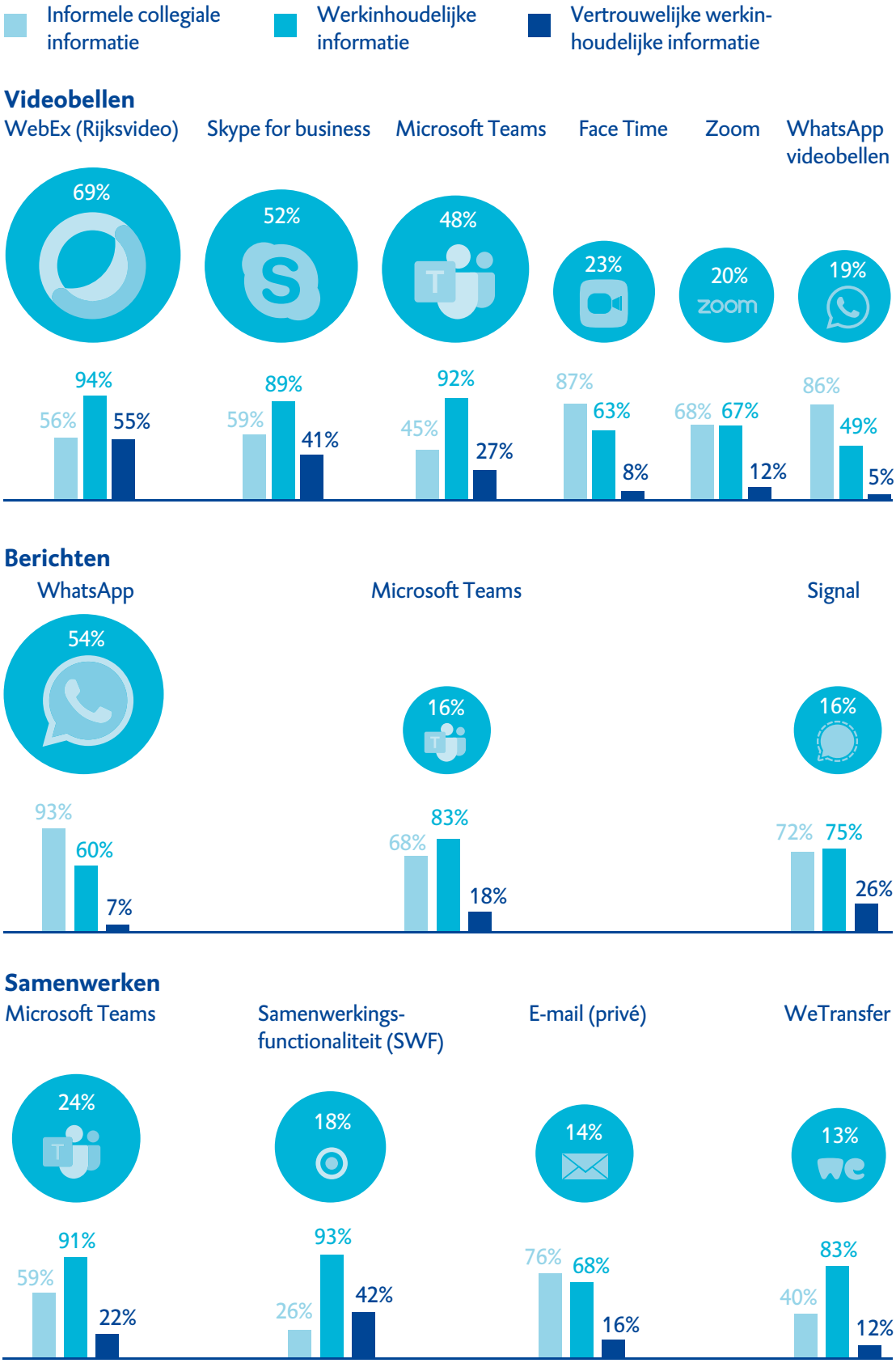
> *"WhatsApp is niet toegestaan voor werkinhoudelijke communicatie, maar de functionaliteit is van te veel toegevoegde waarde om te kunnen missen."*

1.3 Groot aantal samenwerkingsplatforms in gebruik

Als het gaat om online samenwerkingsplatforms zoals *MS-Teams*, *Sharepoint* of *Dropbox* gebruiken respondenten tientallen verschillende programma's om mee samen te werken.[2] Dit komt doordat deze categorie van applicaties breed is. Zo zijn er programma's om samen te werken in documenten, om (grote) bestanden te delen of om planningen te beheren. Een tweede verklaring voor dit grote aantal gebruikte applicaties is dat er bij de rijksoverheid weinig samenwerkingsplatforms bestaan waarop organisaties onderling veilig kunnen samenwerken.

Het valt op dat privé-e-mail in de praktijk regelmatig gebruikt wordt voor het uitwisselen van (vertrouwelijke) werkinhoudelijke informatie. Dit is niet toegestaan volgens de richtlijnen.

Percentage van de respondenten dat aangeeft in 2020 een communicatiemiddel te hebben gebruikt voor werk



Figuur 3 *Gebruik van communicatiemiddelen*

2 Werkafspraken gebruik samenwerkings-ICT

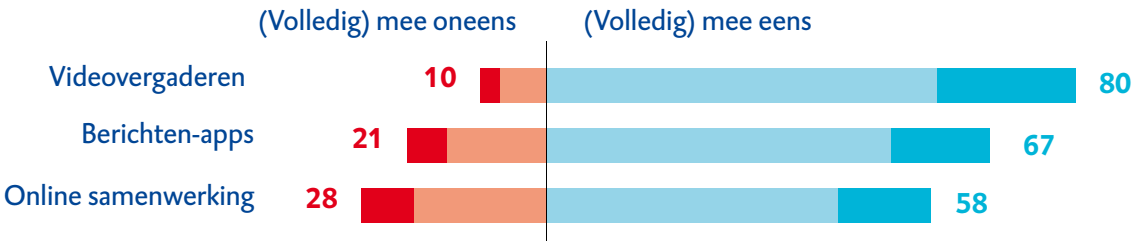
Ministeries en hoge colleges van staat zijn ieder afzonderlijk bevoegd de eigen bedrijfsvoering in te richten. Ook in het gebruik van ICT-middelen mogen zij hun eigen keuzes maken. Het geheel aan voorschriften, afspraken en adviezen voor medewerkers vanuit deze keuzes noemen we hier 'werkafspraken'. We vroegen rijksambtenaren naar hun ervaringen met de werkafspraken voor het gebruik van samenwerkings-ICT. In de onderstaande figuren (4 t/m 7) gebruiken wij het woord 'ambtenaren' voor de respondenten die onze enquête hebben ingevuld.[3]

Gemiddeld 20% van de respondenten zegt niet op de hoogte te zijn van de werkafspraken voor het gebruik van samenwerkings-ICT (figuur 4). 22% is niet tevreden met de communicatie van de werkafspraken (figuur 5).

"Te veel regels, te veel op verschillende plekken, wanneer je zoekt naar specifieke informatie zoek je je een slag in de rondte en of je dan het juiste vindt …"

Een vijfde ambtenaren vindt werkafspraken samenwerkings-ICT niet duidelijk

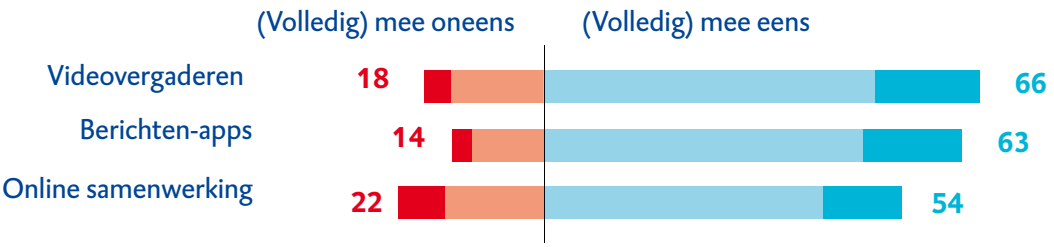
"Ik ben op de hoogte van de geldende werkafspraken."
Verdeling van antwoorden in %



Figuur 4 *Mening respondenten over duidelijkheid geldende werkafspraken*

Een vijfde ambtenaren vindt werkafspraken samenwerkings-ICT niet altijd uitvoerbaar

"De werkafspraken zijn voor mij in de praktijk (bijna) altijd uitvoerbaar."
Verdeling van antwoorden in %



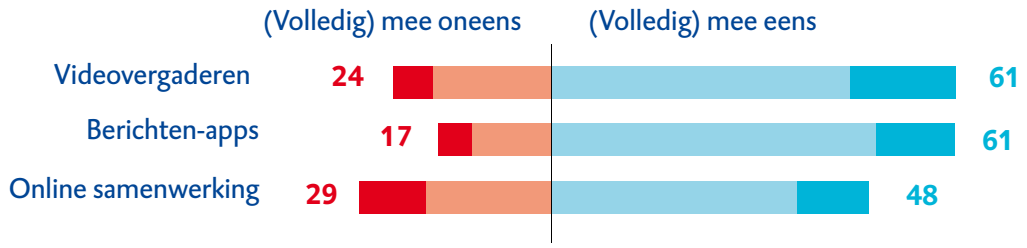
Figuur 5 *Mening respondenten over communicatie van werkafspraken*

Circa 20% van de respondenten geeft aan dat de werkafspraken niet altijd uitvoerbaar zijn (figuur 6). Zo blijkt dat ambtenaren enerzijds verplicht zijn de beveiligde thuiswerkomgeving te gebruiken (*Citrix*), maar anderzijds het advies krijgen daar buiten – in een privé-omgeving – te videobellen. Dit videobellen in de privé-omgeving brengt risico's met zich mee. Applicaties voor videobellen slaan soms standaard de chatberichten uit een videogesprek op in het gebruikte apparaat. Informatie uit deze berichten kan dus terecht komen op privé-ICT van ambtenaren, waar de werkgever geen invloed heeft op het beveiligingsniveau.

"Beveiligingsafspraken kunnen consistenter. De ene keer mogen wij in een systeem niet onze namen koppelen aan het ministerie, maar een andere keer moet dat wel of is het zelfs al gedaan. Veel moeite voor de ene instructie die vervolgens door een andere instructie teniet gedaan wordt."

Kwart ambtenaren niet tevreden over de mogelijkheden voor samenwerking die de werkafspraken bieden

"Ik ben tevreden over de mogelijkheden die de werkafspraken me bieden."
Verdeling van antwoorden in %



Figuur 6 *Mening respondenten over uitvoerbaarheid van werkafspraken*

Verder verschillen aanbevolen applicaties en adviezen aan ambtenaren van organisaties tot organisatie. Ambtenaren weten op deze manier niet meer welke IT-applicaties ze wel of niet mogen gebruiken. Zo staat op de interne website van de rijksoverheid (het Rijksportaal) dat het zakelijk gebruik van *WhatsApp* onder voorwaarden is toegestaan. Bij meerdere organisaties zijn berichtenapps zoals *WhatsApp*, echter expliciet niet toegestaan.

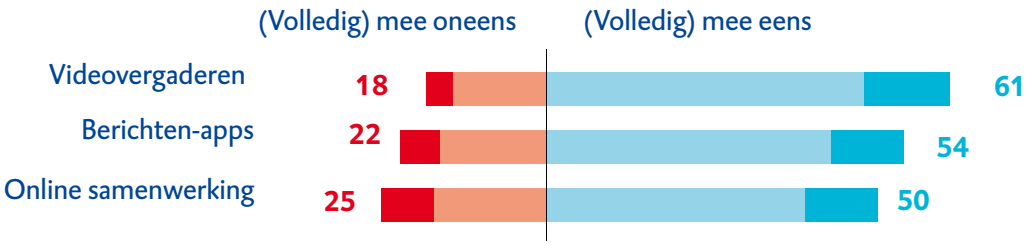
"Werkafspraken moeten duidelijk op het Rijksportaal komen te staan. Nu zijn er verschillende interpretaties naargelang met welk rijksonderdeel je moet vergaderen."

Van de respondenten zegt 23% dat de (werkafspraken voor) aanbevolen samenwerkings-ICT niet voldoende mogelijkheden bieden voor samenwerking (figuur 6). Onderzoeksliteratuur noemt onvrede over de mogelijkheden van door de werkgever aangeboden IT-applicaties als een belangrijke reden om zelf alternatieven te zoeken of om werkafspraken in de wind te slaan.[4] Een voorbeeld hiervan is het Interdepartementaal Samenwerking Platform (ISWF) waarmee ambtenaren van verschillende ministeries veilig kunnen samenwerken.

Dit platform vinden gebruikers niet gebruiksvriendelijk. Het gebruik van niet aanbevolen alternatieven zoals *Dropbox* ligt dan voor de hand, terwijl deze niet aan de gestelde (beveiligings)eisen van de ministeries voldoen.

Een vijfde ambtenaren is niet tevreden met de manier waarop werkafspraken worden gecommuniceerd

"Ik ben tevreden met de manier waarop de werkafspraken aan mij worden gecommuniceerd."
Verdeling van antwoorden in %



Figuur 7 *Mening respondenten over mogelijkheden die werkafspraken bieden*

"Het ontbreekt (al jaren) volledig aan een goedgekeurde chatoplossing voor mobiele toestellen geschikt voor departementaal vertrouwelijke informatie. Hierdoor kiezen gebruikers zelf voor een oplossing, met alle gevolgen van dien."

3 Kansen en risico's samenwerkings-ICT

De belangrijkste risico's van het gebruik van ICT voor samenwerking op afstand zijn die op het gebied van informatiebeveiliging, privacy en (adequate) archivering van informatie. Nauwere samenwerking tussen ministeries biedt kansen om te komen tot gemeenschappelijke, veilige samenwerkings-ICT en eenduidige werkafspraken. Ook doorontwikkeling van de techniek helpt hierbij.

3.1 Informatiebeveiliging en privacy

De voornaamste risico's bij samenwerkings-ICT bevinden zich op het vlak van de informatiebeveiliging en privacy. Door het gebruik van onveilige middelen of het onjuist gebruik van de aanbevolen ICT-voorzieningen kan informatie in handen van onbevoegden komen. Ook kunnen commerciële partijen inzicht krijgen in persoonlijke gegevens van gebruikers. Het gebruik van berichtenapps op mobiele telefoons wordt hierbij gezien als grootste risico. Een concreet voorbeeld zijn werknemers die de organisatie verlaten maar in app-groepen blijven meelezen met werkgerelateerde (vertrouwelijke) informatie.

Uit onze gesprekken blijkt bovendien dat hogere ambtenaren en bewindspersonen vaak niet de voorgeschreven IT-middelen gebruiken. Dit terwijl hun voorbeeldfunctie van belang is voor het gebruik van veilige IT-applicaties in de rest van de organisatie. Zo merkt een *chief information officer* (CIO) van een ministerie op dat er veel tijd, geld en energie geïnvesteerd is om veilig (staatsgeheim) te kunnen communiceren, maar dat sterk beveiligde faciliteiten, zoals de Sectra Tiger telefoon, in de praktijk weinig worden gebruikt omdat ze niet makkelijk in het gebruik zijn. Populaire berichtenapps, tablets en smartphones hebben bij hoge ambtenaren en bewindspersonen vaak de voorkeur boven de sterk beveiligde middelen omdat ze gemakkelijker, sneller en gebruiksvriendelijker zijn.

Na het begin van de coronacrisis bleek uit mediaberichten dat bewindspersonen Zoom en *WhatsApp* gebruiken.[5] Het gebruik van deze applicaties wordt binnen de rijksoverheid afgeraden voor vertrouwelijke communicatie. Iets langer geleden bleek een bewindspersoon vertrouwelijke stukken in *Gmail* op te slaan.[6] In een van onze gesprekken voor dit onderzoek bleek dat een van de ministeries in het voorjaar van 2020, op verzoek van CIO-Rijk, een extra beveiligde omgeving voor videovergaderingen inrichtte. Deze omgeving bood het ministerie aan voor vertrouwelijke communicatie binnen en tussen de politieke top van ministeries. Bij de kabinetsleden bleek geen behoefte aan een dergelijk systeem. In de praktijk gebruiken bewindspersonen ICT-middelen niet volgens de richtlijnen. Dit is lastig want bewindspersonen geven leiding aan een departement; ze zijn formeel geen ambtenaar en vallen niet onder de verantwoordelijkheid van de secretaris generaal of *chief information (security) officer*.

We constateren dat ambtenaren van ministeries en hoge colleges van staat behalve de aanbevolen middelen ook gebruik maken van alternatieve samenwerkings-ICT. Een afdoende niveau van informatiebeveiliging en privacy is daarbij niet vanzelfsprekend en veel organisaties zijn zich hiervan bewust. Het is vrijwel onmogelijk te controleren welke samenwerking-ICT ambtenaren precies gebruiken. Soms is gebruik van een 'ontraden'

middel zelfs onontkoombaar. Een rijksambtenaar bepaalt bij interactie met de omgeving niet altijd zelf welke middelen worden gebruikt. Een voorbeeld is *Zoom*, een programma dat bij internationale organisaties vaak standaard in gebruik is voor videovergaderingen. Ministeries en hoge colleges van staat ontkomen dan moeilijk aan het gebruik ervan, terwijl dit formeel ontraden wordt. Het gevolg van een keuze om *Zoom* niet te gebruiken zou anders zijn dat Nederland niet zou kunnen deelnemen aan bepaalde internationale overleggen.

Ambtenaren doen, in de wetenschap dat regels niet alles kunnen afdekken, een beroep op gezond verstand: bewustzijn en werken aan de hand van principes in plaats van harde regels.

"Het zou helpen als de gebruiker zich meer bewust is van de gevaren van het delen van informatie via bepaalde bronnen. Het lijkt mij belangrijk dat we werken vanuit verantwoordelijkheid in plaats van het naleven van regeltjes."

3.2 Gebrekkig archivering van samenwerkings-ICT

Het gebrek aan ordelijke archivering van informatie bij samenwerkings-ICT kent risico's. Als er geen archivering is ingericht, leidt dat tot een gebrekkige inzicht in wat is afgesproken en het besluitvormingsproces daarbij. Hieruit volgen problemen met de navolgbaarheid (*audit trail*). Daardoor is het niet meer mogelijk volledig verantwoording af te leggen binnen een ministerie, aan inspecties en auditinstanties, aan de media en aan parlement. Bij relatief nieuwe samenwerkings-ICT is het minder vanzelfsprekend dat de archivering op orde is dan bij applicaties die langer in gebruik zijn, zoals e-mail.

"Iedereen gaat werken met Dropbox / Google Drive waardoor er geen enkel zicht is op wat er gebeurt en er geen centrale archivering plaatsvindt."

3.3 Kansen voor gemeenschappelijke samenwerkings-ICT

Uit ons onderzoek komt een behoefte aan gemeenschappelijke samenwerkings-ICT naar voren waarmee ambtenaren van ministeries en hoge colleges van staat veilig met elkaar kunnen samenwerken. Hierbij gaat het niet zo zeer om uniformering in het gebruik van applicaties (allemaal hetzelfde) als wel 'interoperabiliteit': het hanteren van dezelfde standaarden zodat verschillende applicaties op elkaar aansluiten. Een voorbeeld hiervan zijn de applicaties voor videobellen *Webex* en *Jabber* die door gebruik van dezelfde techniek op elkaar aansluiten. Gebruikers van deze twee applicaties kunnen, elk vanuit hun eigen applicatie, onderling communiceren.

Uniformeren is overigens binnen het Rijk niet altijd haalbaar door specifieke eisen en wensen bij individuele organisaties. Zo moeten sommige ministeries voldoen aan eisen van de NAVO of de EU die strikter zijn dan de Nederlandse regelgeving. Het Ministerie van Buitenlandse Zaken kon bijvoorbeeld voor de uitwisseling van vertrouwelijke informatie niet meedoen aan gemeenschappelijke oplossingen om documenten te printen en te videobellen omdat deze niet voldoen aan technische beveiligingseisen van zowel NAVO als EU.

Epiloog

De coronacrisis bracht digitaal werken bij de rijksoverheid en de daaraan verbonden organisaties vanaf maart 2020 in een stroomversnelling. Dit vergde een enorm aanpassingsvermogen van tienduizenden medewerkers en tientallen ondersteunende diensten. Ambtenaren moesten een permanente thuiswerkplek inrichten, tegelijkertijd vaak in beslag genomen door thuisonderwijs voor hun kinderen en zorgen over kwetsbaren in hun omgeving. Ondersteunende diensten zetten alle zeilen bij om de ICT-infrastructuur overeind te houden bij het enorme aantal thuiswerkers en om verzoeken om ondersteuning van medewerkers af te handelen. Wij vinden daarom een compliment op zijn plaats voor de wijze waarop ministeries, CIO-Rijk, individuele ambtenaren en dienstverleners als SSC-ICT hebben gereageerd op de crisis.

Manieren van werken die begin dit jaar nog uitzonderlijk waren, werden in april gemeengoed. Voor velen is videovergaderen nu dagelijkse realiteit, maar ook de elektronische handtekening is – nadat hier op ministeries jaren over geaarzeld is – aan een opmars bezig. Werken op afstand is definitief doorgebroken en gaat niet meer weg.[7] Uit ons onderzoek blijkt dat meer eenduidige en begrijpelijke communicatie aan ambtenaren nodig is over welke samenwerkings-ICT zij, onder welke voorwaarden, kunnen gebruiken.

> *"Waarom wel voor de burger 1 overheid en niet voor de medewerkers?"*

Dat we steeds meer op afstand werken raakt de samenleving en de rijksoverheid op allerlei terreinen. Zo zal het waarschijnlijk gevolgen hebben voor (de inrichting van) de huisvesting en het vastgoed van verschillende organisaties. In het programma Rijksdienst 2022 vertaalt de rijksoverheid deze toekomst in concrete plannen. Hieraan is ook een investeringsplan gekoppeld, bijvoorbeeld om vergaderzalen gereed te maken voor hybride vergaderen.

In dit rapport geven we geen oordeel over het gebruik van samenwerkings-ICT of de rechtmatigheid van daarmee samenhangende uitgaven. We geven die oordelen pas als onderdeel van ons Verantwoordingsonderzoek 2020, in mei 2021.

Reactie staatssecretaris van BZK

De staatssecretaris van BZK heeft op 30 oktober 2020 gereageerd op dit rapport, vanuit zijn coördinerende verantwoordelijkheid met betrekking tot ICT binnen de Rijksdienst.

De staatsecretaris dankt ons voor het rapport en beaamt dat de door COVID-19 ontstane situatie een groot aanpassingsvermogen van de rijksoverheid als werkgever en dienstverlener vergde. Hij dankt ons ook voor het compliment voor de wijze waarop thuis werken voor zoveel ambtenaren binnen korte tijd mogelijk is gemaakt.

De staatsecretaris geeft aan dat in de beginfase van de crisis diverse maatregelen zijn getroffen, waarbij op de middellange termijn bezien moet worden of en hoe deze gecontinueerd, aangescherpt of afgeschaald moeten worden. Volgens de staatsecretaris heeft het beheersen van de risico's op het gebied van informatiebeveiliging, privacy en adequate archivering binnen de Rijksoverheid structurele aandacht. Zo wijst hij op de campagne 'bewust veilig werken' die op 21 oktober 2020 gestart is en aanvullende maatregelen voor goede archivering van overheidsinformatie die verband houdt met de COVID-19-aanpak.

Voorts schetst de staatsecretaris dat het programma Rijksdienst 2022 ook voor de middellange termijn een visie op grenzeloos, hybride werken binnen de Rijksdienst ontwikkelt. Om die reden waardeert hij hoe ons onderzoek inzicht geeft en aandachtspunten schetst bij het actuele gebruik van video-overlegapplicaties, berichtenapps en samenwerkingsplatforms. Ook het geschetste beeld van de hiermee verband houdende werkafspraken binnen de rijksoverheid draagt bij aan de doorontwikkeling van digitale samenwerking en onderstreept het belang van een rijksbrede integrale aanpak.

Tot slot verwacht de staatsecretaris dat het opnemen van digitaal thuiswerken in het rijksbrede verantwoordingsonderzoek over 2020 nader inzicht zal geven in de mate waarin de door ons genoemde risico's en kansen zich manifesteren. Met de uitkomsten van dit focusonderzoek zal verder gewerkt worden aan bewustwording in het veilige gebruik van samenwerkings-ICT binnen de rijksoverheid.

De volledige bestuurlijke reactie is te vinden op www.rekenkamer.nl

Eindnoten

1. Ter verduidelijking is 'die op onze enquête reageerden' toegevoegd na vaststelling van de rapportagetekst door de Algemene Rekenkamer. Zie ook de methodologische verantwoording die te vinden is op www.rekenkamer.nl.
2. Een exact aantal konden we niet vaststellen omdat we vermoeden dat sommige respondenten dezelfde platforms anders benoemden.
3. Deze zin is ter verduidelijking toegevoegd na vaststelling van de rapportagetekst door de Algemene Rekenkamer. Zie ook de methodologische verantwoording die te vinden is op www.rekenkamer.nl.
4. Kopper en Westner (2016); *Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature*.
5. Zie bijvoorbeeld: Het Parool (4 juni 2020) *Halsema en Grapperhaus ruzieden via de app over demonstratie dam* en Volkskrant (18 juli 2020) *Minister Koolmees van Sociale Zaken: 'Dit is geen gezonde baan'*.
6. NRC (17 november 2016) *Staatsgeheim in privé-mail minister Kamp*.
7. Zie bijvoorbeeld het KIM-onderzoek Thuiswerken en de coronacrisis – Een overzicht van studies naar de omvang, beleving en toekomstverwachting van thuiswerken in coronatijd.

Afdeling Communicatie
Postbus 20015
2500 EA Den Haag
telefoon (070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

De tekst van de publicatie *Focus op Digitaal thuiswerken* is op 30 oktober 2020 door de Algemene Rekenkamer vastgesteld en op 2 november 2020 aangeboden aan de Voorzitter van de Tweede Kamer.
Bij deze publicatie hoort een bijlage 'Methodologische verantwoording'.
Op www.rekenkamer.nl zijn de methodologische verantwoording bij de onderzoek en de (geanonimiseerde) enquêteresultaten als open data te vinden.