

Vergaderjaar 2025–2026

26 643

Informatie- en communicatietechnologie (ICT)

30 821

Nationale Veiligheid

Nr. 1434

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 november 2025

Tijdens het debat «Vaststelling van de begrotingsstaat van het Ministerie van Buitenlandse Zaken voor het jaar 2025» op 21 november 2024 heeft uw Kamer de motie van de leden Koekkoek (Volt) en Van der Burg (VVD) aangenomen waarin de regering wordt verzocht om in overleg te gaan met collega's in Estland en te onderzoeken welke mogelijkheden er zijn om een soortgelijke data-ambassade te creëren voor Nederland.¹ Met deze brief geef ik u aan op welke wijze het kabinet aan de motie uitvoering geeft.

Er is overleg geweest met het CIO Office van de Estse overheid om inzicht te krijgen in de Estse data-ambassade, welk doel deze dient, en hoe en op grond van welke overwegingen er besloten is tot het inrichten van de data-ambassade in Luxemburg. Tevens is er recent een bezoek geweest aan de overheid in Luxemburg, waar gesprekken zijn gevoerd inzake de data-ambassade, waarbij tevens het betrokken datacenter is bezocht.²

Data-ambassade in Luxemburg

Estland heeft een uitwijkomgeving gerealiseerd in Luxemburg om de integriteit en beschikbaarheid van basisregistraties en de continuïteit van kritische overheidsdiensten beter te (kunnen blijven) waarborgen.³ In een datacenter in Luxemburg is een IT-omgeving ingericht met servers en dataopslag, waarmee Estland in staat is de meest kritische data veilig te stellen en de continuïteit van de meeste overheidsprocessen te waarborgen indien de datacenters in Estland niet meer functioneren. De data die in Luxemburg is opgeslagen betreft de belangrijkste basisregistraties en een overzicht van wet- en regelgeving. Deze worden regelmatig

¹ Kamerstukken II 2024/25, 36 600 V, nr. 50.

² Inmiddels maakt naast Estland ook Monaco gebruik van een data-ambassade in Luxemburg

³ https://e-estonia.com/wp-content/uploads/factsheet_data_ambassy.pdf

bijgewerkt, zodat Estland in geval van nood kan beschikken over up-to-date data.

Uniek voor de data-ambassade is dat Estland en Luxemburg een verdrag getekend hebben, waarmee Luxemburg de systemen en data van Estland, aanwezig in het Luxemburgse datacenter, zal behandelen als ware het onderdeel van de Estse ambassade. Conform het Verdrag van Wenen zal Luxemburg de geheimhouding eerbiedigen en niets doen om de adequate werking te blokkeren. In het geval van verstoring van de Luxemburgse infrastructuur zal Estland prioriteit krijgen om de diensten te herstellen. Zo behoudt Estland zeggenschap over de diensten en de informatie.

Achtergrond noodzaak tot een buitenlandse uitwijkomgeving

Estland is de meest oostelijke van de Baltische staten en grenst direct aan Rusland, waarbij Estland een verleden heeft van Russische agressie en bezetting. Daarnaast heeft Estland in 2007 een zware cyberaanval ondergaan, die wordt gelinkt aan spanning tussen Estland en Rusland.⁴ Veel officiële overheidswebsites waren niet bereikbaar door geavanceerde DDoS-aanvallen.

De geografische ligging en dreiging was in het verleden de aanleiding voor Estland om kopieën van basisregistraties in het buitenland veilig te stellen door deze naar Estse ambassades te sturen. Om de gevolgen van een mogelijke herhaling van een dergelijke DDoS-aanval te mitigeren, besteed Estland ook veel aandacht aan het verbeteren van de beschikbaarheid en weerbaarheid van de overheids-IT infrastructuur in Estland. De moderne, gedistribueerde infrastructuur op basis van cloud technologie en verbeteringen in het monitoren en weerstaan van aanvallen, hebben er voor gezorgd dat meer recente aanvallen vrijwel geen uitval van diensten veroorzaakten.

Noodzaak uitwijkomgeving

Door de verbeteringen in de cyberweerbaarheid van de Estse overheid en samenleving, is er tot op heden geen noodzaak geweest de data-ambassade in Luxemburg daadwerkelijk te gebruiken. Als noodvoorziening blijft deze wel van belang, allereerst voor het veilig stellen van basisregistraties om ongeoorloofde wijziging daarvan te voorkomen en essentiële overheidsprocessen, ook tijdens een noodsituatie, te kunnen voortzetten.

De Nederlandse situatie

Het huidige dreigingsbeeld voor een fysieke aanval op Nederland is een andere dan die voor Estland. De buurlanden van Nederland zijn sterke bondgenoten. Het risico van een inval door een vijandelijke mogendheid is dan ook vele malen kleiner. Een van de belangrijkste redenen van Estland tot het opzetten van een data-ambassade is het veiligstellen van een aantal basisregistraties in geval van een fysieke inval en bezetting. Dat risico is kleiner voor Nederland.

Het risico van een sabotageactie of een cyberaanval tegen de Nederlandse internetinfrastructuur is wel aanwezig. Nederland als transportland, ook voor de logistieke voorzieningen ten behoeve van de NAVO, kan mogelijk een doelwit worden. Het verschil in geografische ligging geeft Nederland andere mogelijkheden om te zorgen voor continuïteit van dienstverlening en het bewaken van de integriteit en beschikbaarheid van de data in de basisregistraties. Rijksorganisaties nemen al maatregelen om de

⁴ Cyberaanvallen: dit gebeurt er bij sabotage | Rathenau Instituut

weerbaarheid tegen cyberaanvallen te verbeteren en de beschikbaarheid van belangrijke gegevens veilig te stellen.

Momenteel hebben we te maken met een verhoogde dreiging. Om de impact van uitval, gerichte cyberaanvallen of sabotageacties te weerstaan, is het van belang om de uitwijkmogelijkheden van kritische systemen van de overheid te verbeteren. Dit is daarom een belangrijke prioriteit binnen de Nederlandse Digitaliseringsstrategie.⁵ De digitale weerbaarheid en autonomie van de overheid, ook in tijden van crisis, behoeft versterking.^{6, 7} Op basis van de realisatie van een overheidsbrede, gecoördineerde aanpak voor cyberveiligheid, wordt een beter inzicht in kritieke dienstverlening gecreëerd. De continuïteit van de kritieke dienstverlening, onder normale en ongunstige omstandigheden, wordt verbeterd. Als onderdeel daarvan wordt bekeken of en voor welke data en diensten er een noodzaak van een uitwijkoptie op geografische afstand van Nederland is. Dat kan dan bijvoorbeeld meegenomen worden in onder meer het ontwerp van een eigen overheidsbrede soevereine cloud.⁸ Door het verbeteren van de onderlinge uitwijkmogelijkheden, kunnen de risico's van uitval door bijvoorbeeld een sabotage- of cyberaanval worden gemitigeerd en kan gebruik worden gemaakt van de geografische spreiding van de datacenters van de Nederlandse overheid.

De meerwaarde voor Nederland om dit in het buitenland te doen is minder dan de Estse situatie, gezien de verschillen in geografische ligging, geopolitieke dreigingen en risico-inschatting. Onderdelen van de Rijksoverheid, m.n. Defensie en organisaties in het veiligheidsdomein, kiezen wel al voor een gespreide implementatie van hun digitale dienstverlening.

In een latere fase wordt beoordeeld of het voor specifieke kritische processen gewenst is om tevens een uitwijkmogelijkheid buiten Nederland te realiseren. Een dergelijke locatie zal een ander risicoprofiel dan Nederland moeten hebben en ook op grotere afstand moeten liggen dan Luxemburg. In deze analyse zal ook moeten worden meegenomen of een dergelijke faciliteit gecombineerd kan worden met de data-ambassadestructuur, inclusief verwijzing naar het Verdrag van Wenen, zoals overeengekomen tussen Estland en Luxemburg.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van Marum

⁵ Kamerstukken II 2024/2025, 26 643, nr. 1366

⁶ Zie ook «Digitale Kroonjuwelen – Gegevens, documenten en registraties van Nationaal Belang», 6 juni 2023

⁷ Zie ook de Kamerbrief «Weerbaarheid tegen militaire en hybride dreigingen», Kamerstukken II 2024/2025, 30 821, nr. 249

⁸ Kamerstukken II 2024/25, 26 643, nr. 1316.