Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 496

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 november 2017

Met deze brief voldoet het kabinet aan de toezegging gedaan door de Minister-President aan het lid van de Tweede Kamer Van Haersma Buma (CDA) in het debat over de regeringsverklaring van 2 november 2017 (Handelingen II 2017/18, nr. 17, Debat over de regeringsverklaring (inclusief algemene Politieke Beschouwingen)) over de invloed vanuit andere landen op de publieke opinie in Nederland, daarbij verwijzend naar de mogelijke rol van Rusland bij het Brexit-referendum in het Verenigd Koninkrijk en de presidentsverkiezingen in de Verenigde Staten.

Politieke beïnvloeding door statelijke actoren in Nederlandse interne aangelegenheden of democratische processen (waaronder de verkiezingen) vindt het kabinet volstrekt onwenselijk. Hier zal het kabinet in voorkomende gevallen tegen optreden. Er zijn meerdere statelijke actoren die belang hebben bij beïnvloeding van bevolkingsgroepen, politieke besluitvorming en van de publieke opinie in Nederland. Deze vorm van politieke beïnvloeding omvat de integrale, veelal heimelijke inzet van (drog-) argumenten, selectieve informatie en desinformatie (omtrent politiek gevoelige thema's) ten behoeve van het realiseren van politieke doeleinden richting een vooraf bepaald publiek. Het is geen nieuw fenomeen. De opkomst van het internet heeft het echter wel een nieuwe dynamiek gegeven; brede verspreiding van desinformatie kan makkelijk, anoniem, snel en goedkoop.

De afgelopen jaren is in diverse publicaties zoals de jaarverslagen van de Nederlandse inlichtingen- en veiligheidsdiensten en het Cyber Security Beeld Nederland (CSBN) 2017 gerapporteerd over statelijke heimelijke politieke beïnvloeding. Een van de kernbevindingen van het CSBN 2017 is zelfs dat digitale aanvallen worden gebruikt om democratische processen te beïnvloeden. In het jaarverslag 2016 van de AIVD (Kamerstuk 30 977, nr. 149) is voorts gesteld dat digitale beïnvloeding door statelijke actoren in toenemende mate een bedreiging vormt voor de nationale veiligheid.

kst-26643-496
ISSN 0921 - 7371
's-Gravenhage 2017

Geconstateerd is ook dat overheidsinstellingen herhaaldelijk doelwit waren van omvangrijke en hardnekkige digitale cyberaanvallen.

Nederland staat in het vizier van onder meer Russische inlichtingendiensten. In Nederland zijn structureel Russische inlichtingenofficieren aanwezig, die zich in uiteenlopende geledingen van de samenleving begeven om onder valse vlag informatie te verzamelen die voor Rusland van belang is. Naast deze klassieke inlichtingenoperaties via inlichtingenofficieren zet Rusland ook digitale middelen in voor beïnvloeding van besluitvormingsprocessen, beeldvorming en de publieke opinie. Ook in Nederland zijn er dossiers en (politieke) processen die voor Rusland van belang zijn en waarbij beïnvloeding en manipulatie een voorstelbare dreiging zijn, bijvoorbeeld het MH-17 proces.

Zo is in het verleden een gefingeerde website in Rusland waargenomen. De website wekte de indruk een officiële Nederlandse overheidssite te zijn. De vervalste website bevatte onder meer desinformatie over MH17.

Zoals in het rapport van de Amerikaanse inlichtingen- en veiligheidsdiensten van 7 januari 2017 beschreven laten de gebeurtenissen rondom de presidentsverkiezingen in de Verenigde Staten zien dat statelijke actoren niet alleen de intentie en de capaciteit hebben om zich via digitale middelen actief te mengen in democratische processen, maar dat ook daadwerkelijk doen.

Nederland heeft een hoogwaardige en goedontwikkelde ICT-infrastructuur en is daarmee aantrekkelijk als doorvoerhaven van digitale aanvallen. De AIVD heeft dan ook diverse statelijke actoren gedetecteerd die via de Nederlandse digitale infrastructuur andere landen aanvallen. Vaak worden daartoe meerdere servers of serviceproviders tegelijk gebruikt, waardoor attributie niet of nauwelijks mogelijk is.

Om zicht te krijgen en houden op dit fenomeen is onderzoek naar de intenties en de capaciteiten van statelijke actoren nodig. De Nederlandse inlichtingen- en veiligheidsdiensten doen dit onderzoek. De AIVD onderzoekt de digitale dreiging en deelt – indien mogelijk – informatie over aanvalskenmerken met overheids- en private organisaties opdat zij over kunnen gaan tot het treffen van maatregelen.
In dat kader wordt nauw samengewerkt met de MIVD en het NCSC in het Nationaal Detectie Netwerk (NDN) zodat vroegtijdig aanvallen onderkend worden en betrokken instanties geïnformeerd. In voorkomende gevallen kunnen de inlichtingen- en veiligheidsdiensten ook verstorende activiteiten ondernemen. Voor het blijven verrichten van dit onderzoek is het wettelijke kader van de Wiv 2017 noodzakelijk. Over de uitgangspunten die het kabinet heeft opgenomen in het regeerakkoord aangaande de Wiv zal ik u zoals toegezegd op korte termijn nader schriftelijk informeren.

Het is van belang dat de maatschappij zich bewust is dat de digitale dreiging zich in de volle breedte ook in Nederland kan manifesteren. Het kabinet blijft zich dan ook inspannen om dit bewustzijn te stimuleren, zoals ook gemeld in de Kamerbrief van 21 juni 2017 bij verschijning van het CSBN 2017 (Kamerstuk 26 643, nr. 477). Tegelijkertijd spelen media en technologiebedrijven een belangrijke rol bij de afweging of er sprake is van bijvoorbeeld valse berichtgeving op social media. Het kabinet zal in gesprek gaan met deze partijen over hoe (heimelijke) politieke beïnvloeding kan worden tegen gegaan.

In het Regeerakkoord zijn extra middelen beschikbaar gesteld ten behoeve van digitale veiligheid. Hiervoor wordt structureel 95 miljoen euro gereserveerd. De middelen worden onder andere ingezet voor de

uitbreiding van personele capaciteit en ICT-voorzieningen en verdeeld over de departementen Justitie en Veiligheid (NCTV), Defensie, Binnenlandse Zaken en Koninkrijksrelaties (AIVD), Buitenlandse Zaken, Infrastructuur en Waterstaat en Economische Zaken en Klimaat.

Begin 2017 is uw Kamer geïnformeerd (Kamerstuk 26 643, nr. 441) dat het kabinet in de aanloop naar de Tweede Kamerverkiezingen van 15 maart 2017 een analyse heeft gemaakt van mogelijke kwetsbaarheden in het verkiezingsproces en de daaraan gekoppelde maatregelen. Zo is er voorlichting gegeven om de digitale weerbaarheid van politieke partijen en organisaties betrokken bij de verkiezingen te vergroten. Ook in aanloop naar de gemeenteraadsverkiezingen en het referendum van maart 2018 zal het kabinet de opgedane ervaringen meenemen en blijven zorgdragen voor een integer verloop van het verkiezingsproces.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren