Merel Koning
Radboud Universiteit Nijmegen
Merel Koning Consultancy
www.merelkoning.nl

AAN: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Betreft: Inbreng consultatie conceptvoorstel wijziging Wiv2017

Utrecht, 18 Augustus 2018

Geachte heer Rutte, mevrouw Ollongren, mevrouw Bijleveld en heer Grapperhaus,

Graag maak ik gebruik van de door u geboden mogelijk om te reageren op het conceptvoorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2017.

Tijdens het raadgevend referendum van 21 maart 2018 liet een meerderheid van de stemmers zich negatief uit over de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Hierna: Wiv2017). Jullie zijn aan de slag gegaan om de referendumuitslag tegemoet te komen. Op een aantal punten wordt voorgesteld de wet aan te passen doormiddel van het ter consultatie liggende conceptvoorstel en de Beleidsregels Wiv 2017.

Tot mijn verontrusting – en ik voel mij in dit gevoel gesteund door een grote groep kiezers (Zie uitslag referendum Wiv Maart 2018) – is een groot gedeelte van mijn reactie op de internet consultatie over de Wiv in 2015 nog steeds relevant. Het is drie jaar later en de argumenten gaan nog immer op. Ik heb mijn reactie op de internet consultatie over de Wiv uit 2015 als bijlage toegevoegd.[1]

Vanuit mensenrechtenoogpunt is het zorgelijk dat het voor de diensten nog steeds mogelijk wordt gemaakt om op grote schaal gegevens te verzamelen en te analyseren van burgers die geen bedreiging vormen voor de nationale veiligheid. Daarnaast blijft de mogelijkheid bestaan om ongeëvalueerde gegevens met buitenlandse veiligheidsdiensten te delen. Beiden bevoegdheden vormen een dreiging voor o.a. het recht op bescherming van de persoonlijke levenssfeer. De door het kabinet voorgestelde waarborgen in het conceptvoorstel en de Beleidsregels Wiv 2017 nemen

1 Inzending ME Koning, Radboud Universiteit Nijmegen, 1 september 2015 18:41. Beschikbaar op:

https://www.internetconsultatie.nl/wiv/reactie/0e73b0d3-71d1-4591-9f50-d0e5b5a25884. Laatstelijk geraadpleegd op 18 Augustus 2018.

de zorgen niet weg. Voor een meer gedetailleerde uitwerking van de mensenrechten aspecten verwijs ik u naar de consultatie inzending van Amnesty International en Bits of Freedom, welke ik grotendeels onderschrijf.

De Wiv2017 brengt tevens veiligheidsrisico's met zich mee die moeten worden meegenomen in het wetgevend proces en vertaald naar juiste afwegingen in de wet. Het conceptvoorstel en de Beleidsregels Wiv 2017 doen dit onvoldoende. In mijn inbreng zet ik een aantal cybersecurity risico's uiteen.

Ik hoop dat de wetgever deze risico's – naast de mensenrechten aspecten – in het wetgevend proces meeweegt en een aantal keuzes uit de Wiv2017 herziet.

Uiteraard ben ik bereid om een en ander nader toe te lichten, indien daar behoefte aan is.

Met vriendelijke groet,

Merel Koning

BIJLAGE 1: Inzending ME Koning, Radboud Universiteit Nijmegen, 18 augustus 2018.
BIJLAGE 2: Inzending ME Koning, Radboud Universiteit Nijmegen, 1 september 2015.

BIJLAGE 1: Inzending ME Koning, Radboud Universiteit Nijmegen, 18 augustus 2018. [2]

Het eerste veiligheidsprobleem wordt gevormd door de uitgebreide hackbevoegdheid die de diensten toestaat om via onbekende kwetsbaarheden binnen te dringen op apparatuur en in netwerken. Deze kwetsbaarheden hoeven zij niet te melden bij de producenten en ontwikkelaars van de apparatuur of software. Door dit stilhouden blijft niet alleen het spionagedoelwit kwetsbaar maar ook talloze burgers in binnen- en buitenland. De kans is reëel dat anderen van diezelfde kwetsbaarheid gebruik maken voor andere doeleinden. Cybercriminelen en minder frisse inlichtingendiensten zullen ofwel zelf de kwetsbaarheid vinden ofwel de databank van de diensten hacken om deze informatie te stelen. De meerdaagse cyberaanval op de containerterminal in de Rotterdamse haven van afgelopen zomer wordt in verband gebracht met informatie over kwetsbaarheden die eerder bij de Amerikaanse dienst NSA is buitgemaakt. Het niet melden van kwetsbaarheden is een gevaar dat ernstige economische schade veroorzaakt en moeilijk te verenigen is met de veiligheidstaak van de diensten. Het gebruik van kwetsbaarheden in apparaten en software door de overheid kan ook nieuwe kwetsbaarheden veroorzaken. In Duitsland heeft men dit ondervonden met de Bundestrojaner: opsporingssoftware die de Duitse overheid in het geniep plaatste op computers van verdachten, maar waarvan de controle gemakkelijk door derden was over te nemen. Dit veiligheidsrisico wordt versterkt door een nieuwe bevoegdheid in de Wiv. De wet staat de diensten toe om de apparaten van derden te hacken die zelf geen doelwit van de diensten zijn. Het gaat dan om apparaten die met een doelwit in verbinding staan, bijvoorbeeld de netwerkapparatuur die door een systeembeheerder wordt onderhouden. Personen met een sleutelrol binnen de IT, zoals systeembeheerders, worden door de toevoeging van overheidssoftware nog kwetsbaarder voor aanvallen van buitenaf.

Het tweede veiligheidsprobleem houdt verband met de onderzoeksopdrachtgerichte interceptie. Om het dataverkeer in bulk van de kabel op te pikken worden tappunten in het netwerk aangebracht. Binnen de cybersecurity is ieder tappunt een extra kwetsbaarheid. Hoe weten we zeker dat hackers niet ook van die taps gebruik maken? Bovendien kleven aan de opslag van de in bulk verworven data zwaarwegende veiligheidsrisico's, want die bergen data zijn ook voor andere spionnen en cybercriminelen een goudmijn. Met welke mate van zekerheid kunnen de Nederlandse diensten het niet lekken van deze data garanderen? De dreiging van datalekken wordt groter nu de opgeslagen bulkinformatie (ook zonder dat ernaar gekeken is) gedeeld mag worden met buitenlandse diensten. Dit gaat Nederland naar alle waarschijnlijkheid doen met o.a. de Britten en de Amerikanen. Beide landen hebben echter een rijke geschiedenis van datalekken bij de overheid. Data delen met deze landen is dus niet

2 Deze inbreng is gebaseerd op die brief van https://veiligheid-en-de-wiv.nl/ die door tientallen cybersecurityonderzoekers, computerwetenschappers en security professionals is ondertekend in de aanloop naar het referendum in Maart 2018.

zonder veiligheidsrisico voor Nederland.

Daarnaast wordt steeds meer communicatie effectief versleuteld en metadata wordt gemaskeerd, zeker door criminelen en (potentiële) terroristen. Hierdoor vult het sleepnet zich al snel met data van willekeurige burgers. Dit geeft overheden met een sleepnet de prikkel om beveiligingstechnieken zoals end-to-end versleuteling en VPN's te verbieden. We zien dit momenteel in China gebeuren. Deze technieken zijn echter broodnodig voor een veilig internet en het verbieden hiervan levert een groot beveiligingsrisico op voor burgers en de maatschappij.

Het derde veiligheidsrisico zit in het verlies van controle op het gebruik van de gedeelde bulkinformatie door buitenlandse diensten. Opgeslagen bulkinformatie, inclusief bijvangst, mag nog steeds (ook ongeëvalueerd) gedeeld worden met buitenlandse diensten. Misbruik van gunsten door bevriende diensten is in de wereld van spionnen niet ongewoon. Zo verleende de Duitse dienst BND nietsvermoedend toegang aan de Amerikaanse dienst NSA tot haar databases in de strijd tegen het terrorisme. Later bleek dat die toegang werd misbruikt door de Amerikanen voor industriële spionage tegen Duitsland. De nieuwe toetsingscommissie (de TIB) noch de toezichthouder (CTIVD) kan controleren wat er buiten de landsgrenzen met onze gedeelde data gebeurt. Dit veiligheidsrisico moet worden vertaald in betere waarborgen.

Tot zover een aantal veiligheidsgevaren van de nieuwe wet. Er zijn ook sterke aanwijzingen dat nut en noodzaak van OOG-interceptie in de strijd tegen terrorisme door de voorstanders worden overdreven. Er is geen bewijs dat ongerichte bulkverzameling en de geautomatiseerde (meta)analyse daarvan het meest geschikte middel is. Niet alleen biedt het geen uitkomst om de zogenaamde "lone wolves" eruit te vissen. Ook blijkt achteraf vaak dat aanslagplegers al bekend waren bij de geheime diensten. Met traditionele en gerichte tapbevoegdheden - waarover de Nederlandse geheime diensten reeds beschikken - zouden zij hen in het vizier moeten kunnen krijgen.

Uit onderzoek uitgevoerd door de New America Foundation naar de effectiviteit van bulkinterceptie bij meer dan 200 strafrechtelijke onderzoeken naar terrorismeverdachten in de Verenigde Staten bleek dan ook dat traditionele onderzoeksmethoden veelal de initiële drijfveer waren, denk aan het gebruik van informanten, tips van lokale gemeenschappen en gerichte surveillanceoperaties. Zelfs het Anderson review report roept scepsis op over de noodzaak van dit zeer ingrijpende middel in de strijd tegen terrorisme. Voorstanders van de wet citeren dit onderzoek omdat het het nut van bulkinterceptie door de Britse inlichtingendiensten aan zou tonen. Van de vijf onderzochte contraterrorisme-casussen - die de diensten zelf hadden aangedragen als succesvoorbeelden - bleek dat het sleepnet vooral toegepast werd in gevallen waarbij de uiteindelijke verdachten al deel uitmaakten van een bestaand

terrorismenetwerk of contact hadden met doelwitten, waardoor gericht tappen hetzelfde resultaat zou hebben gehad. De noodzaak van OOG-interceptie is dus op z'n minst discutabel.

BIJLAGE 2: Inzending ME Koning, Radboud Universiteit Nijmegen, 1 september 2015. Beschikbaar op: https://www.internetconsultatie.nl/wiv/reactie/0e73b0d3-71d1-4591-9f50-d0e5b5a25884.

Consultation input for the Wet op de inlichtingen- en veiligheidsdiensten

The Dutch government has proposed a new intelligence bill. Having an open and transparent debate on this topic is something I encourage and I would like to take the opportunity to share my thoughts on the proposal via the Internet consultation.

Mass Surveillance (bulk interception)
The proposal to intercept communication in bulk should be withdrawn by the Dutch government. Collecting communication data at a large scale undermines the human rights of individuals. These rights are of fundamental importance in a constitutional democracy. Mass surveillance via bulk interception violates human rights, in particular privacy, the right to protection of personal data and freedom of speech.

A government should protect individuals against such violations. Nevertheless in exceptional situations it might be necessary and proportionate to infringe on these rights by the government in pursuance of a legitimate aim, such as national security. If such an exception would emerge, the measure should be specifically aimed at targets against whom a concrete suspicion is held. Collection, interception and analysis must exclude internet messages, communication and data of individuals for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with crime or national security threats. With a three-step collection-filter-analyze approach this still holds true.

The societal costs of mass surveillance exceed the returns. So far, governments have failed to demonstrate the necessity of mass surveillance. The Explanatory Notes of the proposal state that the MIVD and AIVD have to catch up with technological developments and so it appears, that the means justify the ends. This is unacceptable in a democracy. Without a concrete need that can be demonstrated in a transparent manner, restrictive measures — such as the Wiv proposal — should not be adopted. Research into mass surveillance shows that interception of data of individuals who are not suspected is ineffective. See for example the report of the White House's Privacy and Civil Liberties Oversight Board. Instead of introducing these disproportionate

restricting measures, the Dutch government should protect its citizens against human rights violations. The proposal suggests public-private cooperation and mandatory decryption and transfers of data by private entities to the intelligence services. This leads to the undesirable situation where commercial parties are forced to assist is mass surveillance and push their costumers into the surveillance dragnet.

The United States of America (US) is often pointed to as a country that has a more repressing surveillance regime, and this is true with regard to surveillance on foreigners and the ultra vires surveillance activities of the National Security Agency (NSA) that were exposed by whistleblower Edward Snowden. These activities are being challenged in US courts as we speak. As far as the constitutionality of the proposed intelligence gathering and sharing under US law is concerned, it is highly doubtful whether this will pass the fourth amendment test in the US. If the US government would propose such dragnet surveillance for their own citizens — as the Dutch government is doing for Dutch citizens in this proposal— it is likely to be held unconstitutional.

Collaboration between secret services
Intelligence services collaborate at a global scale. The past years multiple conspiracies of intelligence services have come to light, including nine eyes, in which the Dutch take part. This knowledge cannot be ignored in the drafting process of new legislation. Four important points should be taken into account:

Firstly, Other intelligence services have an interest in the Dutch having extensive powers, this includes NSA and the British GCHQ. The latter advised the Dutch intelligence services on 'legislative issues' that relate to mass surveillance in 2009. The Dutch legislator should prevent that the intelligence position is becoming a goal in itself without evaluating the necessity of having such a position. The idea of competing with other Nations over measures that encompass severe human rights infringements is unacceptable.

Secondly, measures that infringe on human rights have to meet the criterion of necessary in a democratic society as put forward by the European Convention on Human Rights. This treaty guarantees minimum safeguards to human rights protection in the Member States. However, because of the Dutch constitutional structure, this treaty provides effectively maximum protection in case of restricting measures for the aim of national security. Taking the requirements seriously is therefore pivotal to human

rights protection in the Netherlands. The proposal allows for a culture of extensive data exchange between the MIVD and/or AIVD and foreign intelligence services. The question is for which democratic society the data processing is necessary and whether the entities that are responsible for approval and oversight on the powers, are capable of making this assessment. It is likely that these entities do not want to question matters touching upon national security in another State. This renders the safeguards ineffective.

Thirdly, the proposal encompasses the authority to collect, filter and analyse internet traffic, but also the authority to share this information with foreign intelligence services right after collection and prior to the assessment of the proportionality and necessity of the further data processing. It is therefore impossible for the data exchange between the Dutch AIVD and/or MIVD and foreign intelligence services to be proportionate.

Lastly, Government action that restricts the enjoyment of human rights must be foreseeable and the individual should be granted an effective remedy to his case. The current international practice of 'I'll spy on your citizens, if you'll spy on mine' deprives individuals of an effective remedy and cannot meet the criteria of foreseeability.

Oversight
Without effective and complete oversight safeguards have little meaning. The proposal grants the minister — member of the executive branch of the government — powers to override the judgment of the better-equipped oversight committee on the lawfulness of the interception. When the minister disregards the opinion of the oversight committee the Parliament is asked to decide on the legitimacy of the interception. This needlessly politicizes the oversight on human rights infringements. In a democracy under the Rule of Law an independent oversight committee or judge should assess the legitimacy of restricting measures.

I truly hope the Dutch legislator takes the input of all submissions into consideration and takes a leading role in protection human rights and the Rule of Law.