Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

Lotte Houwing
+31 6 8320 7546
lotte@bitsoffreedom.nl

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Schriftelijke inbreng Bits of Freedom voor het rondetafelgesprek op woensdag 5 april 2023 inzake de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma tegen Nederlandse belangen.

Bits of Freedom maakt graag van de gelegenheid gebruik om een aantal zorgen te delen over zowel het proces waarbij dit wetsvoorstel tot stand komt als de inhoud ervan.

1. Het warrige wetgevingsproces

Het voorstel dat voorligt is een tijdelijke wet die de Wet op de inlichtingen- en veiligheidsdiensten 2017 als hoofdwet deels aanvult en deels wijzigt. Het is geschreven terwijl er reeds een proces tot herziening van de hoofdwet is gestart. En nog voordat deze tijdelijke wet uw Kamer heeft bereikt, is er al een wijziging op aangekondigd. Tezamen ontstaat er een beleidslabyrinth dat ten koste gaat van duidelijkheid over wat de geheime diensten mogen, in welke context en op basis van welke wettelijke grondslag. Dat bemoeilijkt democratische controle door uw Kamer, journalisten en maatschappelijk middenveld.

Ook maakt het een zorgvuldige behandeling van het voorstel zelf moeilijker. Helaas heeft de Kamer niet willen wachten tot de nota van wijziging om het voorstel in zijn totaliteit in behandeling te nemen. Het voorstel dat nu voorligt bespreekt de mogelijkheden van de geheime diensten om toegang te krijgen tot IT-infrastructuur, apparaten en grote hoeveelheden gegevens. De nota van wijziging bespreekt hoe er vervolgens met deze gegevens moet worden omgegaan. **Bits of Freedom dringt daarom vriendelijk aan om de verdere behandeling te pauzeren tot de nota van wijziging bij u bekend is.**

2. De uitbreiding van de bevoegdheden

Al bij de totstandkoming van de Wiv 2017 werden bezwaren geuit over de zogenaamde OOG-interceptie bevoegdheid. De destijds minister van Binnenlandse Zaken beloofde uw Kamer en ook ons dat dit absoluut geen ongerichte interceptie inhield. Nu wordt er een bevoegdheid tot kabelinterceptie voorgesteld die per definitie ongericht is.

De ministers maken het met dit voorstel ook op een andere manier veel makkelijker voor de geheime diensten om toegang te krijgen tot de gegevens van heel veel mensen. Op dit moment is het zo dat, wanneer de diensten toegang willen tot bijvoorbeeld een server die *niet exclusief* door een “target” in gebruik is, ze een verzwaarde proportionaliteitstoets moeten doorlopen. Met dit voorstel wordt een loophole gecreëerd waardoor deze verzwaarde toets soms pas maanden na de start van de activiteiten hoeft te worden uitgevoerd.

Bits of Freedom adviseert het “bijschrijven” van apparaten/infrastructuur op een reeds verkregen toestemming alleen toe te staan, wanneer bij de initiële toestemming een gelijke of zwaardere proportionaliteitstoets is uitgevoerd dan voor de bijschrijving noodzakelijk zou zijn.

3. De afbraak van het toezicht vooraf

We zijn zeer blij met de bindende bevoegdheden die aan de CTIVD worden toegekend. Nederland laat hiermee zien kennis te hebben genomen van internationale standaarden.

Met het afschalen van het toezicht vooraf toont Nederland zich juist weer van haar slechtste kant. Nergens is toezicht beter in staat schade te voorkomen, dan voordat de diensten aan het werk gaan. We geven twee voorbeelden.

Wanneer de diensten een aanvraag doen om te mogen hacken, zijn ze verplicht inzicht te geven in de technische risico's. Heel belangrijk, want dit heeft ook gevolgen voor andere mensen en bedrijven die van die infrastructuur gebruik maken. Het voorstel dat nu voorligt schrapt deze verplichting. Maar de afweging over welke risico's voor de samenleving aanvaardbaar zijn, kunnen de diensten helemaal niet alleen maken. Zij hebben, nog meer dan wij allen door de grote belangen die met hun werk gemoeid gaan, baat bij een blik van buitenaf. Een partij die een stapje achteruit kan zetten en de bredere context mee kan nemen. Zeker waar het vitale digitale infrastructuur betreft wil je schade voorkomen, niet achteraf de brokken hoeven oprapen.

Toetsing vooraf is ook heel belangrijk bij geautomatiseerde data-analyse van gegevens die "in bulk" zijn verzameld. Sterker nog: vanwege de grote risico's die hiermee gepaard gaan, is het toezicht vooraf een bewust geïntroduceerde barrière. Terwijl de overheid elders het toezicht op algoritmen juist versterkt, zou dit voorstel toezicht op het algoritmegebruik door de geheime diensten verzwakken.

Het belang van toetsing vooraf is glashelder. Daar tegenover staat het argument dat toetsing het werk soms vertraagt. Wij zien elders voldoende kansen voor versnelling, bijvoorbeeld door de interne processen te stroomlijnen, of om vaker gebruik te maken van de spoedprocedure. Zorgvuldigheid en snelheid moeten hand in hand kunnen gaan, juist bij werk dat zo'n grote maatschappelijke urgentie heeft.

Bits of Freedom adviseert om de CTIVD bindende bevoegdheden toe te kennen, maar om ook de TIB in stand te houden.

4. Het vertrouwen van de burger geeft democratische legitimiteit

Bij het referendum in 2018 stemden burgers de Wiv 2017 weg vanwege grote zorgen over de nieuwe mogelijkheden voor de diensten om op heel grote schaal gegevens te verzamelen. Deze wet doet er nog een schepje bovenop. De verplichting om altijd zo gericht mogelijk te tappen komt te vervallen. En de toezichthouder vooraf, die juist werd geïntroduceerd als tegenwicht voor de uitdijende bevoegdheden, wordt beknot.

In het coalitieakkoord wordt naast "operationele slagkracht" van de diensten, ook gesproken over waarborgen voor goed en effectief toezicht en over digitale burgerrechten. De ministeries hebben hun aandacht duidelijk gelegd bij die slagkracht. **Bits of Freedom roept de Tweede Kamer daarom op om het voorstel te behandelen met extra nadruk op sterk toezicht en burgerrechten.**