Een internationale rechtsorde voor cyberspionage en *intelligence*

8 De inlichtingen- en veiligheidsdiensten (AIVD en MIVD) haalden recentelijk het nieuws. Zo was er aandacht voor het kritische rapport van de CTIVD, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (Buruma, vorige aflevering op deze plaats). Prominent was ook de berichtgeving over de hack bij de MIVD. Het Ministerie van Defensie meldde dat bij de dienst geavanceerde malware was aangetroffen waarmee een 'Chinese statelijke actor' spionageactiviteiten uitvoerde.

Dat statelijke actoren uit landen als China en Rusland offensieve cyberprogramma's voor spionage inzetten is al langer bekend. Maar inmiddels zijn intensiteit en karakteristieken hiervan zodanig dat AIVD en MIVD benadrukken dat Poetin weliswaar niet met grondtroepen aan onze grenzen staat, maar in de digitale wereld Nederland wel degelijk in de oorlog verzeild is geraakt. Het digitale slagveld levert echter (nog) geen indringende beelden van puinhopen en menselijke slachtoffers op. En dus: alhoewel feitelijk heel dichtbij, is de oorlog in de beleving van politiek en samenleving nog immer iets dat Nederland nauwelijks tot niet raakt.

Gelukkig wordt wel werk gemaakt van een steviger wettelijk instrumentarium om op het nieuwe strijdtoneel enigszins staande te blijven. Sinds december 2022 ligt een wetsvoorstel in de Tweede Kamer voor een zelfstandige strafbaarstelling van spionageactiviteiten (36280). En bij de Eerste Kamer is de Tijdelijke wet cyberoperaties (36263) momenteel in behandeling. Deze beoogt op onderdelen tijdelijk van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2017) af te wijken. De aanpassing moet bijdragen aan meer 'operationele snelheid en wendbaarheid' in het onderzoek door de AIVD en MIVD, onder meer door enkele cyberbevoegdheden te verruimen. Ook beogen de diensten met het nieuwe regime een meer integraal beeld te kunnen verkrijgen van dreiging, intenties en capaciteiten van landen met offensieve cyberprogramma's. De tijdelijke regels zien daarom niet alleen op specifieke onderzoeken naar dergelijke programma's, maar op alle onderzoeken naar landen met een offensief cyberprogramma.

Hoe verhouden de nieuwe regels zich tot de cyberbevoegdheden van andere landen? Zeker in de vernetwerkte digitale wereld is internationale samenwerking tussen gelijkgezinde landen wezenlijk. Het ontbreekt aan goed rechtsvergelijkend onderzoek, maar een globale blik toont de nodige verschillen tussen landen. Zo is in ons land het kader voor het opereren van de diensten publiekrechtelijk verankerd. Dat is in lang niet alle (Westerse) landen het geval. Verder ontbreekt het her en der aan een met Nederland vergelijkbaar stelsel van toezicht met elementen van publieke verantwoording. En lang niet overal heeft de toezichthouder, zoals in ons land, voor de eigen taakvervulling zelfstandig toegang tot de data en informatie waar de diensten over beschikken. Ten slotte maken sommige landen, zowel de VS als in Europa, een strak onderscheid tussen binnenland en buitenland. Onderzoek naar (groepen van) personen die zich in eigen land bevinden is aan regels gebonden, maar daarbuiten is veel – zo niet alles – toegestaan. Dit laatste wordt in de hand gewerkt door het ontbreken van internationaalrechtelijke kaders voor spionage en *intelligence*. Waar voor tal van oorlogsgerelateerde handelingen internationale afspraken gelden, blijft de daarmee nauw verbonden praktijk van spionage en *intelligence* 'deeply steeped in secrecy' en 'deliberately ignored in terms of international law and governance', aldus de Leidse hoogleraar Broeders. Hij schetste vorig jaar maart in zijn oratie een indringend beeld van het mondiale machtstoneel van cyberspionage.[1] Zonder internationale kaders geldt daar als norm hetgeen staten zichzelf aan bevoegdheden toe-eigenen dan wel elkaar feitelijk toestaan. En juist bij cyber brengt dat specifieke risico's met zich mee. Zo ontwikkelt het instrumentarium voor spionage zich in rap tempo en zijn het vooral landen met veel innovatiecapaciteit (ook van private partijen – waaronder de Big Tech – aldaar) die daarin de toon zetten. De overige landen hebben in dit offensieve geweld niet alleen geen positie, maar met het ontbreken van internationale afspraken beschikken ze ook niet over een instrumentarium om tegenwicht te bieden tegen hetgeen grote spelers toelaatbaar achten. Dat is niet alleen vanuit rechtsstatelijke optiek problematisch. Ook is het zorgelijk omdat bij cyberspionage de grens tussen enerzijds het verzamelen van inlichtingen in het belang van nationale veiligheid en anderzijds het meekijken voor economisch gewin nogal eens diffuus blijkt te zijn. Natuurlijk gebeurt spionage nog steeds op de conventionele manier: personen die personen benaderen om toegang te krijgen tot informatie. Maar met digitalisering – en zeker artificiële intelligentie – kan een vrijwel oneindige hoeveelheid slimme en nauwelijks te traceren spionage-applicaties een ontelbaar aantal systemen, bedrijven en organisaties binnendringen en informatie verzamelen.

Terug naar de genoemde voorstellen waarmee onze regering het wettelijk instrumentarium voor het digitale strijdtoneel beoogt te versterken. Bij beide voorstellen gaat het om nationale regelingen. De wat mij betreft noodzakelijke volgende stap is die naar het internationale niveau. Om tal van redenen kunnen de kaders niet beperkt blijven tot de huidige – variëteit aan – nationale regelingen. Nog afgezien van voornoemde zorgen, gaat het – gezien vanuit Europees en westers belang – niet alleen over spionage maar ook om *intelligence*. En juist daarvoor is cruciaal het vermogen tot een gecoördineerd functioneren als geheel om inlichtingen in te winnen, in plaats van als separate lidstaten met versnipperde bevoegdheden. En nu het om cyber gaat lijkt er bij uitstek voor ons land een voortrekkersrol te liggen. We zijn met de digitalisering van onze samenleving en economie een koploper binnen Europa. In ons land komen cruciale kabels voor de Europese digitale infrastructuur aan land. Maar bovenal heeft Nederland een reputatie hoog te houden in het initiëren en faciliteren van voor vrede en veiligheid noodzakelijke verdragen en instituties.

Corien Prins

1. hdl.handle.net/1887/3572085.