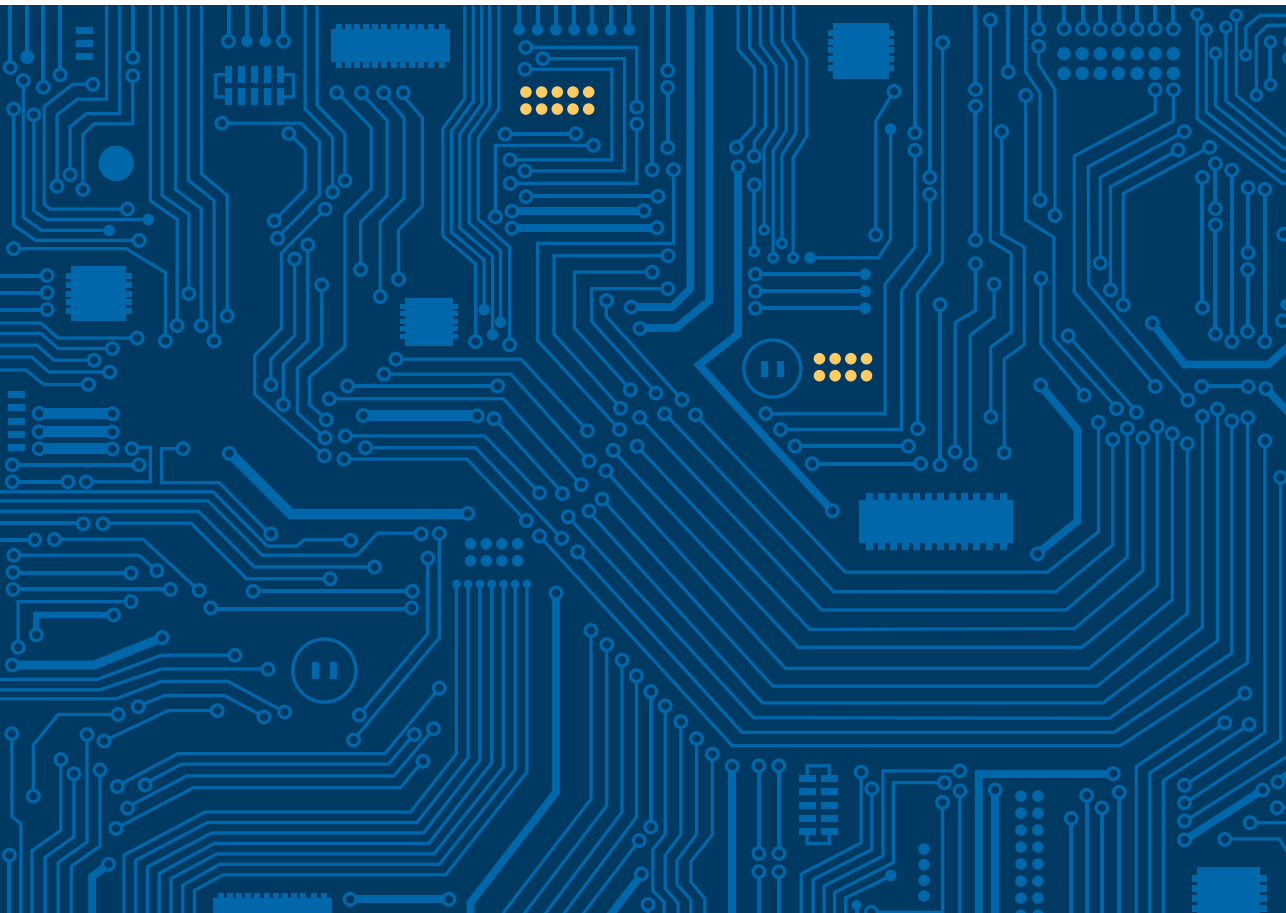
Algemene Inlichtingen- en
Veiligheidsdienst
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Offensief cyberprogramma

Een ideaal businessmodel voor staten



Inleiding

Dat de cyberdreiging tegen Nederland de afgelopen jaren sterk is toegenomen is algemeen bekend. Dat stelt de AIVD ook vast in zijn onderzoeken. De AIVD concentreert zich in het cyberdomein op de dreiging die uitgaat van digitale aanvallen door staten. Wij onderkennen in onze onderzoeken naar de statelijke cyberdreiging dat steeds meer staten een offensief cyberprogramma ontwikkelen en inzetten.

Een offensief cyberprogramma is erop gericht om met digitale middelen andere staten te bespioneren, te beïnvloeden of in het ergste geval vitale infrastructuur te saboteren om zo eigen politieke, economische en financiële doelen te behalen. Rusland, China en Iran zijn voorbeelden van staten met een offensief cyberprogramma. Naast deze staten ontwikkelt een divers palet aan andere staten eveneens hun cybercapaciteiten.

Mede doordat steeds meer staten digitale aanvallen uitvoeren en hiermee direct of indirect Nederland tot doelwit maken, is de afgelopen jaren de cyberdreiging tegen Nederland toegenomen. Deze publicatie gaat dieper in op de aantrekkelijkheid van een offensief cyberprogramma voor staten en is bestemd voor een breed publiek.

Een offensief cyberprogramma is voor staten een ideaal businessmodel geworden: de kosten en de afbreukrisico's zijn laag, terwijl de reikwijdte en de opbrengst enorm zijn. Als gevolg daarvan worden digitale aanvallen in toenemende mate ingezet voor de verwezenlijking van de (heimelijke) politieke, economische en financiële doelen van staten. Deze publicatie eindigt met de inschatting dat de cyberdreiging de komende jaren aanhoudt. Redenen hiervoor zijn dat digitale aanvallen steeds anoniemer worden en hiermee moeilijker herleidbaar zijn tot de aanvaller, en dat staten in toenemende mate bereid zijn digitale aanvallen in te zetten.

Een statelijke digitale aanval is het ongeautoriseerd en vaak heimelijk toegang verkrijgen tot digitale systemen van een andere staat. Deze aanvallen kunnen ingedeeld worden in drie categorieën: digitale spionage, digitale beïnvloeding en digitale sabotage.

De AIVD verstaat onder digitale spionage het met digitale middelen verwerven van gevoelige of vertrouwelijke informatie van een andere staat voor het behalen van eigen strategische doelen. Denk aan het verkrijgen van belangrijke politieke of economische informatie. Daarnaast kan digitale spionage een eerste stap zijn richting beïnvloeding of sabotage.

Digitale beïnvloeding is het met digitale middelen inmengen in de belangen van een andere staat. Dit kan de vorm aannemen van het verspreiden van compromitterende informatie (informatie die niet gemanipuleerd is, maar waarvan het niet wenselijk is als die openbaar wordt gemaakt) of desinformatie (verzonnen of gemanipuleerde informatie). Zo kunnen bepaalde personen, regeringen of landen in een kwaad daglicht worden gesteld of kan onrust worden gecreëerd.

Digitale sabotage is het via digitale middelen beschadigen, verstoren of vernietigen van (vitale) systemen en processen in een ander land.

Offensief cyberprogramma gericht tegen Nederlandse belangen

Staten met een offensief cyberprogramma bedreigen onze nationale veiligheid. Zij kunnen direct of indirect een dreiging voor Nederland zijn. Direct doordat hun digitale aanvallen op Nederland gericht zijn. Indirect doordat Nederland nevenschade ondervindt van aanvallen die gericht zijn op andere staten of doordat staten bij aanvallen misbruik maken van Nederlandse internetinfrastructuur.

Internationaal staat de Nederlandse internetinfrastructuur hoog aangeschreven, omdat deze zeer snel, goedkoop en betrouwbaar is. Door dit misbruik wordt Nederland ongewild betrokken bij de verspreiding van digitale aanvallen die een inbreuk maken op de belangen van andere landen.

Nederland is een aantrekkelijk doelwit voor digitale aanvallen van andere staten. Nederland heeft een hoogwaardige kenniseconomie met een uitstekende (digitale) infrastructuur, participeert actief in diverse internationale gremia zoals de NAVO, de VN en de EU en huisvest diverse internationale bedrijven en organisaties.

De statelijke cyberdreiging richt zich met name op Nederlandse bedrijven en overheidsorganisaties. Zo worden bijvoorbeeld personen binnen het bedrijfsleven, de overheid of in Nederland gevestigde internationale organisaties digitaal aangevallen die vanuit hun functie toegang hebben tot waardevolle informatie. De statelijke cyberdreiging richt zich, in mindere mate, ook op individuele Nederlandse burgers. Bijvoorbeeld omdat zij vanwege hun afkomst (etnische en religieuze minderheden) of politieke opvattingen (dissidenten, activisten) tot doelwit worden gemaakt.

Offensief cyberprogramma als ideaal businessmodel

Een offensief cyberprogramma is een ideaal 'businessmodel' voor staten. De verregaande digitalisering van onze maatschappij biedt staten veel nieuwe mogelijkheden voor spionage, beïnvloeding en sabotage. Dit businessmodel ziet er als volgt uit:

Kosten

De kosten voor het opzetten en uitvoeren van een digitale inlichtingenoperatie zijn relatief laag in vergelijking met andere inlichtingenmiddelen die een staat kan inzetten. Een klein budget, een paar computers met een internetverbinding en een handvol hackers volstaat in principe voor een succesvolle cyberoperatie. Hierdoor zijn offensieve cyberoperaties een laagdrempelig middel voor staten.

Tijds- en arbeidsextensief

De benodigde tijd en arbeid voor het opzetten en uitvoeren van een digitale inlichtingenoperatie zijn eveneens beperkt in vergelijking met andere inlichtingenmiddelen. Waar het rekruteringsproces van een menselijke bron in een organisatie enkele jaren kan omvatten, kan infiltratie van computernetwerken binnen enkele uren of dagen gerealiseerd worden door één of enkele hackers. Daarnaast biedt de inzet van malware (kwaadaardige software) legio mogelijkheden om inlichtingenactiviteiten (deels) te automatiseren. Naar verwachting zal de inzet van kunstmatige intelligentie ervoor zorgen dat toekomstige digitale inlichtingenoperaties minder tijd en menskracht vergen.

Eenmaal binnen in een netwerk, kunnen de aanvallers vervolgens diverse digitale 'achterdeurtjes' realiseren die moeilijk te onderkennen en te

verwijderen zijn waardoor zij in staat zijn om onopgemerkt toegang te houden tot die netwerken. De AIVD heeft in diverse onderzoeken vastgesteld dat deze toegang enkele jaren behouden kan blijven. Een dergelijke langdurige toegang is renderend omdat het de aanvallers in staat stelt om over een langere periode gevoelige informatie buit te maken. Niet voor niets worden statelijke digitale aanvalsgroepen vaak aangeduid met de term *Advanced Persistent Threat* (APT).[1]

Opbrengst

Als gevolg van toenemende digitalisering is belangrijke en vertrouwelijke informatie steeds vaker enkel digitaal beschikbaar en wordt deze informatie steeds vaker via het internet toegankelijk gemaakt. Daarnaast neemt de publieke en private communicatie via digitale middelen nog steeds sterk toe, worden steeds meer productie-, vervoers- en huishoudelijke systemen aan het internet gekoppeld (het zogenoemde *Internet of Things*), wordt data steeds vaker *in the cloud* opgeslagen en worden interne bedrijfsprocessen uitbesteed aan digitale dienstverleners. Dit alles zorgt ervoor dat de mogelijkheden en opbrengsten van digitale spionage, sabotage en beïnvloeding enorm zijn toegenomen.

Bereik

In principe is elk digitaal systeem waar ook ter wereld dat verbonden is met het internet, kwetsbaar voor aanvallen. Hierdoor is fysieke nabijheid tot het doelwit niet langer meer een vereiste voor een succesvolle digitale inlichtingenoperatie. Dit heeft de actieradius van spionage, sabotage en beïnvloeding enorm vergroot. Als gevolg van het *Internet of Things* komen steeds meer systemen in het bereik van digitale aanvallen.

Toegankelijkheid

Digitale aanvalsmiddelen zijn relatief eenvoudig verkrijgbaar. De afgelopen jaren zijn diverse statelijke *hacktools* openbaar geworden. Ook zijn *zerodays*[2] en andere aanvalstools te koop. Informatiebeveiligingsbedrijven publiceren daarnaast met grote regelmaat en zeer gedetailleerd over dit soort middelen met als doel de weerbaarheid tegen dergelijke aanvallen te verhogen. Deze informatie kan echter worden misbruikt voor het uitvoeren van digitale aanvallen. Door deze (vrij) toegankelijke kennis over digitale aanvalsmiddelen kunnen staten snel een eigen offensief cyberprogramma ontwikkelen.

Schaalbaarheid

Statelijke digitale aanvallen richten zich niet alleen op individuele gebruikers van digitale systemen maar steeds vaker op de producenten van dergelijke systemen zelf. Denk hierbij bijvoorbeeld aan ontwikkelaars van hard- en software. Ook richten hun aanvallen zich steeds vaker op digitale dienstverleners die een cruciale rol vervullen in de verwerking, opslag en communicatie van digitale informatie. Voorbeelden van dergelijke dienstverleners zijn internet service providers, telecomproviders en *managed service providers*. Deze bedrijven hebben vanwege hun dienstverlening vaak een diepgravende, omvangrijke en structurele toegang tot (de digitale netwerken van) hun klanten.

Deze producenten en dienstverleners zijn een aantrekkelijk doelwit van statelijke digitale aanvallen, omdat zij vaak wereldwijd klanten bedienen en hiermee schaalvergroting binnen inlichtingenoperaties kunnen faciliteren. Deze dreiging neemt toe wanneer deze producenten en dienstverleners afkomstig zijn uit landen die een offensief cyberprogramma hebben dat gericht is tegen Nederland. Overheden uit dergelijke landen

[1] Een Advanced Persistent Threat is een actorgroep die verantwoordelijk is voor geavanceerde en langdurige digitale aanvallen, waarbij deze groep ongemerkt en voor lange tijd toegang krijgt tot een computernetwerk.

[2] Zerodays zijn onbekende kwetsbaarheden in hard- of software die kunnen worden misbruikt om ongeautoriseerd toegang te krijgen tot deze hard- of software.

kunnen deze producenten en dienstverleners verplichten om samen te werken met de inlichtingendiensten waardoor zij bijvoorbeeld heimelijk digitale 'achterdeurtjes' kunnen realiseren. Hiermee kunnen deze staten ongezien de schaalbaarheid van hun digitale aanvallen verder vergroten.

Herbruikbaarheid

De bij digitale aanvallen gebruikte tools en werkwijzen zijn vaak opnieuw te gebruiken. Deze herbruikbaarheid geldt niet alleen voor de aanvaller, maar net zo goed voor het doelwit. De aanvaller kan dezelfde tools en werkwijzen tegen verschillende doelwitten inzetten. Staten die doelwit zijn (geweest) van deze digitale aanvallen kunnen de gebruikte tools en methodes bestuderen, reproduceren, verfijnen en vervolgens aan hun eigen digitale wapenarsenaal toevoegen. Dit werkt verspreiding (proliferatie) en daarmee de beschikbaarheid van deze tools en methodes in de hand.

Anonimiteit

Veel staten voeren digitale aanvallen uit onder een dekmantel. Zo zetten diverse staten bedrijven in voor digitale inlichtingenoperaties om overheidsbetrokkenheid te maskeren. Hierdoor is het moeilijk te achterhalen wie nu precies met welk doel een aanval uitvoert. Digitale aanvallen zelf kunnen nagenoeg anoniem worden uitgevoerd: digitale sporen kunnen eenvoudig worden gewist of in ieder geval moeilijk traceerbaar worden gemaakt - denk hierbij onder meer aan encryptie en TOR[3]. Dit alles bemoeilijkt de attributie van statelijke digitale aanvallen (het vaststellen / bepalen welke statelijke actor achter een aanval zit).

Laag afbreukrisico

Door de anonimiteit waarmee staten digitale aanvallen kunnen uitvoeren, is het niet eenvoudig om de verantwoordelijke staten en de hackers achter deze aanvallen te herkennen en te bestraffen. Het internationale sanctieregime tegen dit soort aanvallen is nog in ontwikkeling. Op dit moment is slechts een beperkt aantal maatregelen mogelijk. Voorbeelden van deze maatregelen zijn het saboteren van digitale aanvalsnetwerken (*notice and take down*), strafrechtelijke aanklachten en diplomatieke maatregelen. Dergelijke maatregelen hebben echter meestal een beperkt effect. Hierdoor is het afbreukrisico relatief laag, wat de inzetbereidheid van staten vergroot.

Hoog slagingspercentage

Potentiële slachtoffers investeren vaak in cybersecurity om statelijke digitale aanvallen te weerstaan. Desondanks is dit dikwijls onvoldoende om te voorkomen dat statelijke hackers zich toegang weten te verschaffen tot computersystemen. Zo worden steeds weer nieuwe kwetsbaarheden in hard- en software ontdekt. Ook neemt de AIVD bijvoorbeeld regelmatig waar dat statelijke digitale aanvallen worden uitgevoerd door misbruik te maken van bekende kwetsbaarheden in hardware en software. Daarbij geldt dat de snelheid waarmee dit soort kwetsbaarheden kan worden ingezet meestal hoger is dan het vermogen van potentiële slachtoffers om tegenmaatregelen te nemen. Hierdoor is het aantal statelijke digitale aanvallen dat succesvol is groot.

Offensief cyberprogramma draagt bij aan (heimelijke) doelen

Als gevolg van dit ideale businessmodel worden digitale aanvallen in toenemende mate ingezet voor de verwezenlijking van de doelen van een staat. Sommige van die doelen zijn bekend, andere worden geheim gehouden. Al deze doelen zijn grofweg onder te verdelen in politieke, economische en financiële doelen. Per doel wordt een aantal praktijkvoorbeelden gegeven die de AIVD in zijn onderzoeken heeft onderkend en die illustratief zijn voor de mate waarin digitale aanvallen bijdragen aan de realisatie van (heimelijke) overheidsdoelen.

[3] TOR (The Onion Router) zorgt ervoor dat de herkomst en bestemming van netwerkverkeer wordt versluierd.

Politieke doelen

Vaak worden cyberaanvallen vanuit een politiek motief uitgevoerd. De AIVD heeft bijvoorbeeld in zijn onderzoeken onderkend dat een bepaalde staat op de hoogte wil zijn van de internationale beleidsvorming ten aanzien van deze staat binnen een internationaal gremium. Deze staat verschaft zich middels digitale aanvallen toegang tot het overheidsnetwerk van één staat binnen dit gremium dat een slechte ICT-beveiliging heeft. Vervolgens infiltreert deze aanvallende staat de internationale communicatie met de andere staten binnen dit gremium. Deze strategische positie geeft de aanvallende staat inzicht in de beleidsstandpunten van alle staten binnen dit gremium, waaronder Nederland.

In een ander praktijkvoorbeeld tracht een bepaalde staat geëmigreerde (ex-)landgenoten in Nederland digitaal te bespioneren en monddood te maken. Hierdoor voelen de slachtoffers zich in Nederland niet veilig, geremd in hun handelen en passen zij hun gedrag aan. De AIVD beschouwt dit als ongewenste buitenlandse inmenging en een aantasting van de burgerrechten van betrokkenen.

Daarnaast neemt de AIVD waar dat diverse staten zich bekwamen in, voorbereidingen treffen voor en in sommige gevallen daadwerkelijk overgaan tot digitale sabotageoperaties. Zo heeft de AIVD vastgesteld dat een staat zich innestelt in Europese vitale infrastructuur voor mogelijke sabotagedoeleinden. Hierdoor kunnen aan het internet gekoppelde besturings- en controlesystemen van vitale infrastructuren, zoals drinkwatervoorziening en elektriciteitsdistributie, verstoord worden.

Economische doelen

Cyberaanvallen kunnen vanuit een economisch motief worden uitgevoerd. Zo heeft de AIVD in zijn onderzoeken onder meer onderkend dat bepaalde staten hun economie versneld willen moderniseren en hierbij bereid zijn heimelijk en op soms bijna industriële schaal innovatieve westerse en Nederlandse technologieën te stelen. Met behulp van deze gestolen kennis willen deze staten die technologieën integreren in hun eigen economie en/of zelf gaan produceren tegen een lagere marktprijs. Dit bedreigt het Nederlands economisch innovatievermogen en de werkgelegenheid.

In een ander onderkend voorbeeld probeert een staat met behulp van een staatsbedrijf een internationale onderneming over te nemen. Deze staat voert tegelijkertijd heimelijke digitale aanvallen uit op het advocatenkantoor dat deze overname juridisch begeleidt met als doel vertrouwelijke informatie te verkrijgen over de overname. Hierdoor is deze staat precies op de hoogte van alle bedrijfsresultaten en -risico's. Hiermee heeft deze staat zicht op de overnameconcurrenten en hun overnamevoorwaarden en -biedingen. Hierdoor kan deze staat zijn overnamestrategie aanpassen en precies het juiste overnamebod met de juiste voorwaarden uitbrengen. Dergelijke praktijken bedreigen het *level playing field* van het Nederlandse bedrijfsleven.

Financiële doelen

Cyberaanvallen kunnen ook vanuit een financieel motief worden uitgevoerd. Zo heeft de AIVD in zijn onderzoeken onderkend dat een staat die nauwelijks beschikt over internationale deviezen, zeer succesvol digitale aanvallen uitvoert die als motief financieel gewin hebben. Bij deze aanvallen worden gehuurde Nederlandse servers ingezet. De tientallen miljoenen euro's die deze staat zo verdient, vloeien rechtstreeks naar de staatskas. Hoewel de huidige omvang en impact relatief beperkt zijn, kunnen dergelijke aanvallen een potentiële dreiging vormen voor de beschikbaarheid en continuïteit van het internationale betalingsverkeer.

Statelijke cyberdreiging neemt ook de komende jaren toe

De inschatting is dat de komende jaren het aantal staten met een offensief cyberprogramma verder toeneemt. De AIVD ziet in zijn onderzoeken twee trends die deze inschatting onderbouwen.

Aanvallen steeds anoniemer; attributie steeds moeilijker

Digitale aanvallen worden steeds anoniemer en deze anonimiteit bevordert de inzetbaarheid van dit middel. Zo investeren veel staten niet alleen kwantitatief in hun cybercapaciteiten (meer hackers en andere ICT-specialisten), maar ook kwalitatief. Er is een toenemende specialisatie op diverse terreinen van *hacking* te zien en er worden steeds innovatievere technieken toegepast om de aanvallen niet herleidbaar te maken. Hierdoor wordt de attributie van een aanval moeilijker.

Attributie wordt ook bemoeilijkt doordat staten steeds vaker elkaars tools en werkwijzen 'recyclen'. Succesvolle onderdelen uit malware van de ene staat worden door een andere staat verder ontwikkeld en toegepast. Daarnaast constateert de AIVD een kruisbestuiving met criminele aanvalsmiddelen, zo wordt bijvoorbeeld *ransomware*[4] ingezet bij statelijke digitale sabotageaanvallen. Deze wereldwijde proliferatie van digitale aanvalsmiddelen bemoeilijkt attributie.

Er is nog een ontwikkeling die de anonimiteit bevordert waarmee staten digitale aanvallen kunnen uitvoeren. In de afgelopen jaren ziet de AIVD een toename van het aantal *supply chain attacks* door statelijke actoren. Bij dergelijke aanvallen worden externe digitale dienstverleners, zoals internet service providers, telecomproviders en *managed service providers*, ingezet als springplank om doelwitorganisaties te infiltreren. Nadat eerst het netwerk van de dienstverlener is geïnfiltreerd, wordt van daaruit het netwerk van het slachtoffer benaderd. Dit soort indirecte aanvallen via vertrouwde dienstverleners is uiterst moeilijk te detecteren, tegen te gaan en toe te schrijven aan een bepaalde staat. Een andere vorm van *supply chain attacks* zijn aanvallen die worden uitgevoerd met behulp van digitale 'achterdeurtjes' in hard- of software. Dergelijk aanvallen kunnen geheel anoniem worden uitgevoerd.

Toegenomen bereidheid tot inzet van digitale aanvallen

Steeds meer staten zien digitale aanvallen als een 'normaal' overheidsmiddel dat ze op grote schaal in kunnen zetten. Dit geldt met name voor digitale spionage. Steeds meer staten beschouwen dit als een gangbaar inlichtingenmiddel dat ze ongelimiteerd, bijna anoniem en veelal straffeloos kunnen inzetten. Bij diverse statelijke actoren is een toenemende verwevenheid te zien tussen klassieke en digitale spionage. Zo worden klassieke (menselijke) spionageoperaties voorafgegaan door (verkennende) digitale spionageoperaties. Naast digitale spionageaanvallen voeren staten steeds vaker digitale beïnvloedings- en sabotageaanvallen uit en die zijn steeds vaker succesvol.

Als gevolg hiervan hebben conflicten tussen staten steeds vaker een digitale component. De bereidheid tot en de keuze van doelwitten voor digitale aanvallen is daarmee deels afhankelijk van geopolitieke ontwikkelingen. De sterk verschuivende geopolitieke machtsposities in de wereld leiden tot een diffuser dreigingsbeeld. De AIVD heeft vastgesteld dat Nederland ineens een digitaal doelwit kan worden na een internationaal of diplomatiek conflict waarbij het betrokken is (geraakt).

[4] Ransomware of gijzelsoftware is kwaadaardige software waarmee een digitale aanvaller een computer en/of de gegevens die erop staan vergrendelt en in ruil voor geld weer vrijgeeft.

Conclusie

De AIVD concludeert dat steeds meer staten een offensief cyberprogramma ontwikkelen en inzetten. De reden hiervan is dat een dergelijk programma een aantrekkelijk businessmodel voor staten is en bijdraagt aan het behalen van hun (heimelijke) politieke, economische en financiële doelen. Mede door de toename van het aantal staten met zo'n programma is de cyberdreiging tegen Nederland de afgelopen jaren toegenomen. Nederland is vooral om politieke en economische redenen een aantrekkelijk doelwit voor deze staten. Naar inschatting van de AIVD houdt de statelijke cyberdreiging de komende jaren aan omdat digitale aanvallen steeds anoniemer worden en hiermee moeilijker herleidbaar zijn tot de aanvaller, en er bij staten een toenemende bereidheid is om digitale aanvallen in te zetten.

De cyberdreiging tegen Nederland neemt verder toe wanneer voor de uitwisseling van gevoelige informatie of binnen vitale processen gebruik wordt gemaakt van ICT-producten en -diensten uit staten waarvan is vastgesteld dat ze een offensief cyberprogramma hebben. Veel van deze staten verplichten namelijk bedrijven in hun land door middel van wetgeving samen te werken met de inlichtingendiensten. ICT-producten en -diensten uit deze staten kunnen daarom bijvoorbeeld zijn voorzien van digitale 'achterdeuren'. Hiermee kan eenvoudig en anoniem de toegang tot gevoelige informatie of vitale processen in Nederland verkregen worden. Om deze redenen vindt de AIVD het onwenselijk dat Nederland afhankelijk is of wordt van ICT-producten en -diensten uit staten met een offensief cyberprogramma dat gericht is tegen Nederland.

Wat doet de AIVD tegen deze cyberdreiging?

Digitale veiligheid is essentieel voor het functio neren van onze maatschappij. De AIVD investeert in zijn onderzoekscapaciteit om de dreiging van staten met een offensief cyberprogramma al in een vroeg stadium te kunnen herkennen, te duiden en waar mogelijk weg te nemen. Zo assisteert de AIVD bij de detectie en mitigatie van dergelijke aanvallen bij bedrijven en overheden, informeren wij slachtoffers van digitale aanvallen en geven wij bewustwordingspresentaties aan mogelijke doelwitten van deze aanvallen. Wij verstrekken informatiebeveiligingsadviezen op maat aan de Nederlandse overheid en andere belanghebbenden, zoals vitale bedrijven. Het doel van deze adviezen is de weerstand tegen statelijke digitale aanvallen te verhogen en (digitale) schade te beperken of te voorkomen. Door onze toegang tot geheime informatie geven wij uniek en gedegen beveiligingsadvies en stellen wij anderen in staat te handelen.

Nauwe samenwerking met de MIVD is cruciaal bij het uitvoeren van deze taken. Daarnaast werken we intensief samen met andere nationale partners zoals het Nationaal Cyber Security Centrum (NCSC), de Cyber Security Raad en internationale partners. Zo is er het Nationaal Detectie Netwerk (NDN) waarbinnen de AIVD, de MIVD en het NCSC nauw samenwerken om overheden en vitale bedrijven digitaal veiliger te maken. Binnen het NDN wordt relevante dreigingsinformatie gedeeld, waardoor de aangesloten organisaties in staat zijn gericht maatregelen te treffen tegen digitale dreigingen. De AIVD en deze partners kunnen de statelijke cyberdreiging echter niet alleen aanpakken; die vraagt om structurele investeringen door alle geledingen van de Nederlandse samenleving heen.

Algemene Inlichtingen- en Veiligheidsdienst
aivd.nl

Postbus 20010
2500 EA Den Haag

juni 2019