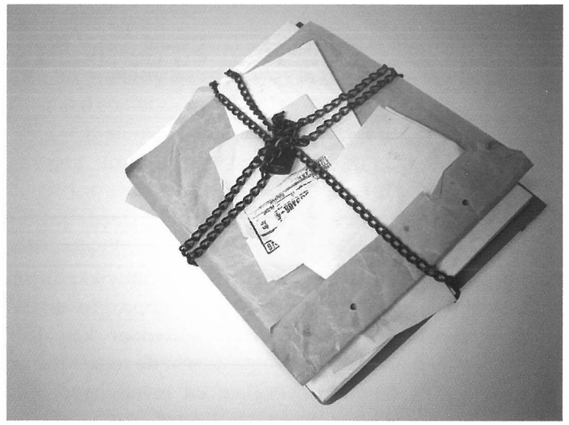
De twitterende wethouder

Duijn, W. van

verder uitdijen. "Het internet is groter dan ieder land of iedere groep van landen en ontwikkelt zich in een tempo buiten het bereik van zelfs het grootste technologiebedrijf" (Cornish et. al., 2010: 18). Doordat het internet voor steeds meer doeleinden wordt gebruikt en de complexiteit van de technologie alleen maar zal toenemen, is de kans op conflicten groot. Hoe kan de overheid haar netwerken, data en infrastructuur beschermen?



Het eerste probleem dat komt kijken bij cyberdefensie is het feit dat de cyberwereld sterk geïnternationaliseerd en wereldwijd onderling verbonden is waardoor de overheid en private stakeholders op elkaar aangewezen zijn (Cornish et. al., 2010). Het debat over cyberdefensie wordt voornamelijk gevoerd door technologen, de discussies zijn daardoor vaak technologisch van aard. Politici en beleidsmakers durven zich niet in dit debat te mengen terwijl juist zij de politieke grenzen moet trekken die bepalen tot waar defensie reikt en wanneer een aanval gerechtvaardigd is. Hoe moeten overheden dan met deze nieuwe dreiging omgaan? Leidende naties, zoals de Amerikaanse en Chinese overheden investeren fors in nieuwe technologieën en betere cyberdefensie (Cornish et. al., 2010). De Nederlandse overheid heeft hier, mede vanwege druk vanuit de Tweede Kamer, ook meer aandacht voor gekregen. Toch lijkt de Nederlandse overheid voornamelijk te participeren binnen een breder NAVO-verband. Als de Nederlandse overheid wordt aangevallen door een cyberaanval, die is gericht op het platleggen van infrastructuur of het verzamelen van data, is verdediging lastig. Het internet is namelijk toegankelijk voor iedereen en kent een hoge mate van anonimiteit. Dit maakt de attributie van professionele cyberaanvallen ingewikkeld en de toenemende complexiteit van het digitale netwerk zorgt er voor dat dit nog verder bemoeilijkt wordt. Het is lastig om te onderscheiden welke van de eerder genoemde typen bedreigingen verantwoordelijk is voor een aanval omdat zij dezelfde technieken gebruiken. Een andere complicatie komt voort uit de toenemende commercialisering van de kritieke (of nationale) infrastructuur, bestaande uit onder andere computernetwerken, dataopslag, telefoonnetwerken en satellieten (Cornish et. al., 2010). Toen het internet een steeds grotere rol kreeg in deze infrastructuur kwamen overheden er bij het beveiligen ervan achter dat veel van deze kritieke infrastructuur in private handen is. Overheden proberen nu samen te werken met grote private bedrijven om hun nationale belangen te verdedigen maar private bedrijven staan hier terughoudend tegenover. Daarnaast stopt het internet niet bij de landgrens waardoor systemen afhankelijk zijn van elkaar en geen enkele overheid de mogelijkheid heeft om de systemen goed te controleren (Cornish et. al., 2010).
Zo bezien zijn cyber-aanvallen een nieuwe militaire dreiging maar is de term 'cyber-warfare' misleidend. Er is veel discussie of de term 'oorlog' past binnen deze nieuwe context (Cornish et. al., 2010). Het is namelijk onduidelijk wanneer een cyberaanval een oorlogsdaad is, wie er verantwoordelijk voor is en wanneer een reactie geboden is. Had de aanval vanuit Rusland op het netwerk van Estland als een oorlogsdaad beschouwd moeten worden? Als het zo beoordeeld zou worden zou het een bewuste aanval zijn en direct het hart van de NAVO raken: artikel 5 roept immers op tot collectieve defensie. Men is daardoor terughoudend om te spreken over cyber-oorlog terwijl de voorbeelden van Estland en Iran laten zien dat dit wel degelijk een nieuwe vorm van oorlog kan zijn. Cornish et al. (2010) stellen in hun conclusie dat de defensie van de cyberwereld een nieuwe dimensie zal worden naast de vier dimensies die defensie al kent: land, water, lucht en ruimte.

Het digitale bestuur is de toekomst, maar geen toekomst zonder gevaren. Het zal voor iedere overheid uitdagingen met zich meebrengen om haar data, netwerken en eigen systemen te beveiligen. De Wikileaks-affaire heeft laten zien dat het internet buiten het bereik ligt van overheden en dat de informatiesamenleving zich verder ontwikkelt met alle nieuwe kansen en risico's van dien. Cyberdefensie moet een bijdrage leveren aan de veiligheid van het openbaar bestuur en haar functioneren maar zal ook een bijdrage leveren aan de ontwikkeling van nieuwe vormen van oorlog. Het is aan overheden om de juiste beveiliging te creëren en te bepalen welke risico's reëel zijn en derhalve antwoord behoeven. ■

Referenties:

- Buckland, B.S., F. Schreier en T.H. Winkler (2010), Democratic Governance and Challenges of Cyber Security, the Geneva Centre for the Democratic Control of Armed Forces, Genève
- Cornish, P., D. Livingstone, D. Clemente, C. Yorke (2010), On Cyber Warfare, Royal Institute for International Affairs, London
- Lips, M., V. Bekkers en A. Zuurmond (2005), ICT en openbaar bestuur, Utrecht: Uitgeverij Lemma
- The meaning of Stuxnet', The Economist, 2 oktober 2010.
- UK Home Office, Cyber Crime Strategy (London: The Stationery Company, Cm 7842, Maart 2008).

De twitterende wethouder

Dhr. Willem van Duijn
Wethouder Gemeente Katwijk

Het gebruik van de sociale media door een bestuurder.

Communicatie naar de burger is een onderwerp dat de gemoederen van politici al eeuwen bezighoudt. Hoe vertel ik aan de burgers wat ik doe en waar ik voor sta? Daar zijn veel manieren voor. De gemeente heeft een website en in de lokale krant wordt van alles geplaatst. Ook aan de regionale pers kun je een persbericht opsturen en tevens heeft iedere partij een eigen website en folders.

Als je nog meer kwijt wilt, dan open je tegenwoordig een blog of een twitter-account. Het maakt een wethouder zichtbaarder voor een bepaalde doelgroep en meer persoonlijk.

Maar als je niet handig genoeg bent of niet het juiste gevoel hebt voor de nieuwe media moet je dat misschien maar beter niet doen. Want wie zit te wachten op een bloggende wethouder die eens in de maand een berichtje schrijft? Of een twitterende wethouder die de wereld laat weten dat hij die ochtend naar het zwembad is geweest?

Het is niet waarschijnlijk dat daar mensen op zitten te wachten. Communiceren kan je op veel manieren, maar je moet wel iets te melden hebben. Bovendien schuilen er een aantal gevaren in het gebruik van bijvoorbeeld Twitter. Het gebruik van het medium heeft iets impulsiefs. Dat impliceert het gevaar dat je iets ondoordachts twittert met onbedoelde consequenties.

Ten tweede is het aantal woorden in een tweet beperkt. Dit heeft gevolgen voor de nuancering die (niet) in een tweet kan worden aangebracht. Een tweet kun je ook moeilijk vooraf kortsluiten met medebestuurders, die daardoor kunnen worden verrast, zowel aangenaam als onaangenaam.
Daarnaast worden nieuwe media nog vooral door jonge mensen gebruikt. Dat vraagt een goed inlevingsvermogen in het taalgebruik van deze groep om geen averechts effect op te roepen. Tot slot is besturen voortdurend zaken tegen elkaar afwegen. Dat vraagt om tijd en bedachtzaamheid.

Het is de vraag hoe bovenstaande vereisten zich verhouden tot de nieuwe media. Het antwoord op deze vraag zal moeten blijken met de tijd. Maar het is zeker aan te raden om bedachtzaam om te gaan met het gebruik van nieuwe media.

De moraal van dit verhaal: *Weet wat je Tweet*