Cyberwar en de risico's van de digitale overheid

Degen, T.

Since the massive introduction of Information and Communication Technological applications in state and society, the physical, demographic and jurisdictional boundaries of the modern state have been shifting.

The *territorial* basis of public administrations is affected by the installment of tracking, tracing and monitoring applications, such as Global Positioning Systems (GPS), put in orbit, through which all kinds of activities and developments on earth can be supervised.

The *demographic* basis of the state administration - at least in the Western world - is affected by a massive influx and outflow of, on one hand, asylum seekers and economically motivated immigrants and cross border workers, and on the other hand sun seeking pensioners.

The *jurisdictional* basis of the state – its paramount control and ultimate power basis – is affected by the globalizing developments in the world. Some of the side-effects of globalization are a growing-border crossing international criminality and terrorism, tax-evasion, traffic in women, etcetera. The jurisdictional limitations that nation states encounter when they fight the negative effects of a globalizing world are putting them under more and more pressure.

Conclusions

In 1998 the Dutch Scientific Council for Government Policy, the most important scientific advisory council of the Dutch government, published a report entitled "State without Country". The report focused especially on how the consequences affect the state's power to act. Modern state administrations are, in their essential dimensions, becoming "mobile state administrations" themselves.
Their territorial basis has been extended into virtual directions, their demographic basis
has become extended and more diversified, and their jurisdictional basis has only partly been strengthened by the still growing transparency in the relationships between state and society.
A more systematic study of the interrelationships between changes from e-government to m-government within countries, with changes in the role relationships of public officials and citizens, and with changes in state society relations, deserves our attention.

> "Modern state administrations are, in their essential dimensions, becoming 'mobile state administrations' themselves."

At the start of this paper the question raised was: does the deployment of mobile ICTs lead to fundamental changes? In the end of the paper the question was raised whether a re-conceptualization of the Weberian state–society relationship has to be considered.
The answers we found on these questions relate in the first place to the policy implementation aspects of public administration. The fundamental shifts we notice in these aspects is a growing functionalization of the role of citizens in the state society relationship, on one hand, and a growing infocratization (Zuurmond 1998) of the position of the street level bureaucrat on the other. Although these observations are based on quite recent developments, they point in a direction that has to be taken seriously.

The Weberian state society relationship is changing fundamentally as well. Governments are on the move outside their age honored geographical, demographic and jurisdictional boundaries. They are becoming more and more footloose. Those physical boundaries of the state are more and more replaced by virtual boundaries. This cannot remain without consequences for the quintessential dimensions of the state. ■

References

Franz, A. (2005), Mobile Kommunikation: Anwendungsbereiche und Implikationen für die Offentliche Verwaltung, Speyer.

Kaneko, Y. (2005), The Use of Space Technologies for More Effective and Efficient Public Administration, in: Petroni, G. and F. Cloete, New Technologies in Public Administration, IOS Press, Amsterdam, pp. 90-104.

Vedder et al.(2007) Van privacyparadijs tot controlestaat, Rathenau Institute, Den Haag.

Webster C.W.R. (1996) Closed Circuit Television and Governance: The Eve of a Surveillance Age. In: Information Infrastructure and Policy, vol.5, nr. 4 pp 253-63

WRR (Scientific Council for Government Policy) (1998). Staat zonder Land (State without Country)

Zuurmond A. (1994) De Infocratie. Een theoretische en empirische herorientatie op Webers ideaaltype. (The Infocracy. A theoretical and empirical re-orientation on Weber's ideal-type.) Rotterdam Phaedrus

Cyberwar en de risico's van de digitale overheid

door Tom Degen

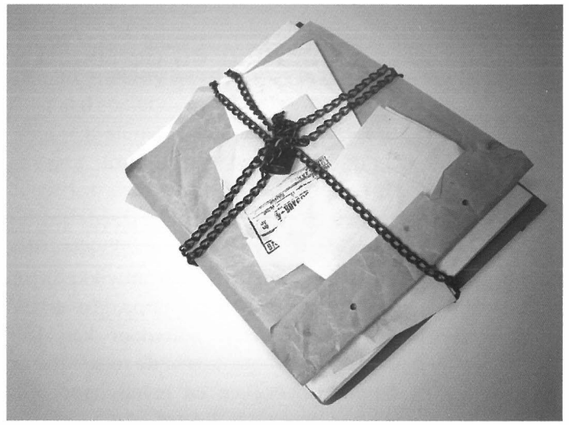
Binnen het openbaar bestuur neemt ICT een steeds grotere rol in en zij draagt daarmee bij aan de ontwikkeling van de informatiesamenleving. Nieuwe ICT-ontwikkelingen hebben telkens gevolgen voor de wijze waarop de overheid in de samenleving kan opereren. Hierdoor kan ICT ingrijpende veranderingen veroorzaken in de relatie tussen de overheid en burgers, bedrijven en maatschappelijke organisaties. Dit gebeurt doordat ICT nu al in alle primaire processen van de overheid betrokken raakt, zoals bij beleidsvorming, handhaving, toezicht en ook steeds meer in de democratische functie (Lips et. al, 2005). De overheid gebruikt ICT verder om data van burgers, bedrijven en haar eigen handelen op te slaan. Hiermee tracht zij efficiënter en effectiever te werken. Het openbaar bestuur verwordt zo tot een digitaal bestuur. De meeste aandacht gaat uit naar de mogelijkheden die ICT voor de overheid met zich meebrengt. De vraag wat de risico's zijn van deze digitalisering blijft vaak achterwege. In dit artikel zal ik ingaan op deze vraag. Eerst zal ik de achtergrond schetsen, vervolgens de risico's benoemen en tot slot de oplossingen en uitdagingen voor overheden formuleren.

De vervlechting van ICT als onderdeel van de verandering naar een informatiesamenleving heeft ervoor gezorgd dat de overheid en de samenleving steeds afhankelijker zijn geworden van informatiesystemen, datasystemen en digitale netwerken. De risico's van gepubliceerde informatie op internet zijn duidelijk te zien in de Cablegate affaire, waarbij vertrouwelijke documenten van de Amerikaanse diplomatieke dienst in de handen zijn gekomen van WikiLeaks. Niet de inhoudelijke onthullingen in deze documenten, maar het feit dát deze informatie ter beschikking staat van een onbereikbaar extern netwerk is het meest interessante aspect aan deze kwestie. Het laat de onmacht zien van de staat om dergelijke informatieverspreiding tegen te gaan wanneer internetgebruikers op collectieve en individuele basis de informatie verspreiden en beschermen. Acties van verschillende overheden om verspreiding tegen te gaan, leidden tot cyberaanvallen op de websites van Mastercard, Paypal, en ook het Openbaar Ministerie in Nederland. Globalisering en de netwerksamenleving hebben er toe geleid dat er serieuze zorgen zijn over de mogelijkheden van overheden om data, informatie en processen te beveiligen. De Cablegate affaire lijkt deze zorgen opnieuw onder de aandacht te brengen.
De aandacht voor en bezorgdheid over cyberveiligheid onder burgers en media is een ontwikkeling die al langer speelt (Cornish et al., 2010). Overheden en internationale organisaties focussen zich steeds meer op deze nieuwe dreiging. Zo hebben het Verenigd Koninkrijk en de Verenigde Staten aangekondigd fors te investeren in cyberbeveiliging en heeft de NAVO een Cyber Security Centre of Excellence in Tallinn opgezet. De keuze om dit centrum in Estland te vestigen, heeft deels een symbolisch karakter. In 2008 werden overheidssites en netwerken van Estland vanuit Rusland geïnfiltreerd en platgelegd. Dit wordt gezien als één van de eerste cyber-aanvallen in een nieuwe dimensie van cyber-oorlog (Buckland et al., 2010). In juni 2010 werd de Stuxnet-worm via USB-sticks verspreid naar computers wereldwijd. Dit virus was dermate complex dat er wordt gesuggereerd dat het alleen door overheid gesteund werk kan betreffen. Het was ontworpen om een specifiek industrieel controlesysteem te infecteren en daarmee een bepaalde installatie te onderbreken. Gezien het feit dat de uitbraak geconcentreerd was in Iran, lijkt het erop dat de nucleaire faciliteiten het doelwit waren. De Verenigde Staten en Israël zijn potentiële daders. "This, it seems, is what cyber war looks like. Get used to it." was het commentaar van The Economist (2010). Bij dergelijke cyberaanvallen is de dader vaak onbekend, gezien deze virtueel en vaak anoniem handelt. Het is daardoor lastig om te onderscheiden welke acties daadwerkelijk een aanvallend karakter hebben en welke voornamelijk criminele activiteiten ontplooien. De nieuwe dreigingen die het digitale netwerk meebrengen zijn: cyberaanvallen gesteund door of uitgevoerd vanuit een staat, extremisme (vaak cyberterrorisme genoemd), georganiseerde criminaliteit en individuele criminaliteit (Cornish et.. al., 2010).

Deze dreigingen zorgen ervoor dat verschillende overheden fors investeren in cyberdefensie. Zo investeert de Amerikaanse overheid de komende vijf jaar al 50 miljard dollar in haar cyberdefensie. Op dit moment wordt het globale netwerk van het Amerikaanse ministerie van Defensie wereldwijd miljoenen keren per dag aangevallen en in de toekomst zal dit naar verwachting alleen maar toenemen. Dit alles terwijl de rol van cybertechnologie binnen het defensieapparaat al aanzienlijk is. Cybertechnologie is gedurende conflictsituaties van essentieel belang omdat wapensystemen, satellieten en communicatienetwerken allen afhankelijk zijn van deze technologie.
Doordat het aantal gebruikers ieder jaar met tientallen miljoenen toeneemt, zal het globale netwerk steeds >

> "This, it seems, is what cyber war looks like. Get used to it."

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*