Transforming adaptation. Authoritative knowledge for climate change governance

Daan Boezeman
Promotie: Radboud Universiteit, 7 juli 2015
Promotoren: prof. dr. P. Leroy en dr. W. Halffman

Waar gaat het proefschrift over?

Klimaatadaptatie geniet steeds meer beleidsaandacht. Wetenschappelijke kennis speelt een cruciale rol in de identificatie van klimaatrisico's en het vormgeven van collectieve adaptatie-inspanningen. Die kennis is echter onzeker, complex, soms controversieel, en sluit vaak niet aan bij de behoeften van beleidsmakers. Met institutionele innovaties – zoals het opzetten van toegepaste wetenschapsprogramma's, grensorganisaties of kenniscocreatie – wordt geprobeerd de uitwisseling tussen wetenschappelijk aanbod en vraag vanuit beleid te verbeteren. Dit onderzoek bekijkt hoe gezaghebbende en relevante kennisclaims over klimaatverandering werden geproduceerd in de commissie-Veerman, hitteprojecten in steden en regionaal waterbeheer.

Wat waren de belangrijkste wetenschappelijke conclusies?

Het onderzoek concludeert dat het gangbare beeld van pakketjes wetenschappelijke kennis die moeten worden overgezet naar de beleidswereld, niet opging. Het 'wicked' probleem klimaatverandering werd door wetenschappers, beleidsmakers en andere belanghebbenden getemd en hanteerbaar gemaakt voor het beleidsveld waar klimaat een onderdeel van werd gemaakt. Zowel kennis als de kwestie klimaatverandering zelf werd daarbij *getransformeerd*. Vijf concepten helpen transformatie te analyseren: reductie, extensie, retorisch verpakken, herdefiniëren en modificeren. Transformatie heeft een januskop. Het geeft klimaatverandering lokale betekenis en maakt concrete adaptieve reacties mogelijk. Transformatie sluit echter ook af, is cognitief padafhankelijk en leidt tot blindheid voor sommige klimaatrisico's.

Wat kan de praktijk ermee?

Twee principes zijn momenteel leidend in adaptatiebeleid. Enerzijds worden klimaatonderzoeksprogramma's vormgegeven om kennis te produceren die dichter aansluit bij de behoeften van beleidsmakers: cocreatie. Anderzijds zijn sturingsstrategieën op 'mainstreaming' in bestaande beleidsinitiatieven gebaseerd: meekoppelen. Hoewel die strategie snelle acceptatie van klimaatoverwegingen en toe-

gesneden kennis kan opleveren, kent zij ook problemen. De onbekendere effecten zonder duidelijke probleemeigenaar blijven onderbelicht. Ook is het ontransparant welke belangen er met de nagestreefde kennisagenda's gediend zijn. Om blinde vlekken te verlichten is meer institutionele verandering nodig dan de mainstreamingsagenda voorstaat. Een verplichte en periodiek herhaalde risico- en kwetsbaarhedenbeoordeling, gecombineerd met een onafhankelijke review-organisatie voor kwaliteitsborging kan aanleiding geven voor een breder debat over relevante klimaatrisico's en adaptatiestrategieën. Voor inspiratie kijkt men in het VK, Noorwegen of Denemarken.

Bestuurskunde 2017 (26) 1
doi: 10.5553/Bk/092733872017026001019

ABSTRACTS

The price of openness: An introduction to the special issue on Cybersecurity
Haiko van der Voort, Wouter Kisteman & Henk Wesseling
Cybersecurity is daily news. Data leaks and hackers are common features in the media. We tend to look to the government when things go wrong: what is the government doing about it? In this special issue we also look to the government and ask ourselves whether we are ready for the challenges of cybersecurity. Asking this question is simple. Answering it, however, requires sophisticated knowledge. This includes knowledge about the technology of today and the future. It also includes knowledge about governance. Who should be prepared in the age of distributed responsibilities? Which public and private parties can enhance cybersecurity, including you and me? Finally, what is does 'being prepared' mean exactly? This special issue includes three academic articles, five interviews and a column. Cybersecurity is viewed from different academic perspectives and professional positions. In its entirety, this special issue provides state-of-the-art of academic and professional thinking on government cybersecurity.

Cybersecurity: where is the public administration?
Michel van Leeuwen & Nelly Ghaoui
In this article the case is made that, unjustly, there is a lack of interest in the topic of cybersecurity of on the part of public administration scholars and professionals in the topic of cybersecurity. ICT has become persistent in society and so has cybercrime, cyber sabotage and cyberespionage. The threats are real and growing. There is market failure and consequently there is a need for government intervention. This poses new challenges to governments as jurisdiction problems and sovereignty-issues arise, together with the dominance of private actors. The authors argue that a multistakeholder approach in such a networked environment is crucial but not sufficient. The concepts of Lessig and Thaler/Sunstein are used to sketch new and broader potential policy strategies.

Cybersecurity: The digital resilience of Dutch governments
Anne de Hingh & Arno Lodder
Cybersecurity is becoming increasingly vulnerable. DDos attacks, phishing e-mails, ransomware, Russian hacker attacks on the head office of a political party are all part of our daily online businesses, for governments too. Governments play various roles here. They are internet users and rely on information on the internet. They are also suppliers of online information and in these roles they are connected to citizens, companies and other governmental organisations. Because of the role they play in society, the government possesses huge quantities of – often sensitive – information. They have the legal and moral obligation to be careful with this information and to secure it properly. Providing adequate security for information, however, is not an easy task for governments, especially because they usually do not operate in isolation. What factors threaten the security of government information and the systems involved? And who is accountable for the security of the information chains that are becoming complex as a consequence of cooperation between organisations?

Will collaboration for digital security survive new challengers?
Bram Klievink, Rolf van Wegberg & Michel van Eeten
The speed and disruptive character of digital innovations affect social structures and practices faster than institutions can keep up with them. This results in an 'institutional void', i.e. a gap between the rules and institutions and their ability and the effectiveness of their measures. It also affects the institutional stability that is the basis for the paradigm of collaboration-based

types of governance. In this paper, we explore how parties are able to set up collaboration for digital security, which is inherently a topic that transcends organisational boundaries. Yet digital innovations constantly enable new challengers that might not share the same incentives for collaboration. Life in an institutional void is convenient for them and enables new business models. Hence, a key question is whether (institutionalised) collaboration is a sustainable model for addressing shared problems like digital security. We explore this question in the domain of financial cyber fraud. The new (regulatory) space currently being created for innovators suggests that the answer is 'no'. It is too early to say how this will play out specifically and we argue for further research into the antecedents for collaboration in institutional voids.

The system of cybersecurity: an essay about how we must learn to be prepared
Henk Wesseling, Jeroen Boot, Wouter Kisteman & Haiko van der Voort
Government cybersecurity requires action from many public and private actors. Both collective knowledge and collective priority are needed to ensure cybersecurity at a government level. This makes collective learning essential. There is a system of arrangements that includes all kinds of governmental organisations and private parties. How can learning be stimulated in this system? And what is the need for steering here? This article provides answers to these questions, based on the contributions in this special issue. We conclude that both central control and self-regulation are essential to cybersecurity, even if they are in conflict. We coin the term 'complimentary self-regulation'. We also conclude that many arrangements have been developed or are under development, however, it is difficult to institutionalise the coherence between these initiatives. There is a long road ahead in terms of gaining a collective understanding. Cybersecurity and its organisation will probably not vanish from the administrative agenda any time soon.

Determinants for non-take-up of informal help: a literature review
Mark Reijnders, Jelmer Schalk & Trui Steen
A major issue confronting Dutch municipalities is that informal help is not being accepted. This concerns potential clients who avoid or are reluctant to ask for support that can be provided by friends, family, neighbours or volunteers. This phenomenon of non-acceptance is still underexplored and our theoretical understanding is fragmented at best. We explore various explanations for why people avoid seeking help, drawn from various and – until now – largely separate bodies of literature. From an extensive literature review across the disciplines of psychology, sociology and public administration, we distil four possible causes for refusing to accept help. We conclude with a discussion of the practical implications and possible future research avenues.

Abstracts are also published in PA@BABEL the online EGPA-database for articles on public administration in European non-English journals. (http://soc.kuleuven.be/io/egpa/pnb/index.htm)

IN DIT NUMMER:

"Zijn we er klaar voor?" Deze eenvoudig klinkende vraag staat centraal in het themagedeelte van dit nummer, over informatieveiligheid bij de overheid, door velen ook cybersecurity genoemd. De logische vervolgvragen (Waarvoor? Wie zijn we? En wat is 'klaar'?) blijken ingewikkelde, welhaast existentiële vragen voor overheden die operationeel en strategisch verweven zijn met meerdere publieke en private partijen. Vier wetenschappelijke artikelen, vijf interviews en een column verschaffen u een tour door de problematiek en de hedendaagse denkrichtingen voor informatieveiligheid in de toekomst. De tour gaat vele paden af, van het lokale tot het mondiale, van het theoretische tot het praktische, van het operationele tot het strategische en van het sociale tot het technische domein, en verschaft u zo noodzakelijke kaartkennis van dit onderwerp.

De overige bijdragen exploreren vele andere gebieden. Mark Reijnders, Jelmer Schalk en Trui Steen bestudeerden psychologische, sociologische en bestuurskundige literatuur in hun zoektocht naar verklaringen waarom hulpbehoevenden niet om hulp vragen, zelfs wanneer het hulpaanbod voldoende is. Thomas Schillemans sluit de cyclus over de toekomst van de bestuurskunde af met een persoonlijke samenvatting. Stavros Zouridis geeft in de kroniek een bestuurskundige reflectie op twee rapporten van de commissie Oosting, onder meer over de gevaren van normen-, feiten en oordeelscontaminatie.

Lof voor goed werk is er in het Laudatio bij de uitreiking van de L.P. van de Spiegelprijs 2016 aan Em. Prof. dr. W.J.M.Kickert en het juryrapport van de Van Poeljeprijs 2017. De auteurs van de drie genomineerde proefschriften, Nanke Verloo, Nina van Loon en Daan Boezeman, pitchen hun onderzoek in deze editie.

Boombestuurskunde