Een gezamenlijke rekening?

Over digitale innovatie en samenwerking in een institutional void

Klievink, Bram; van Wegberg, Rolf; van Eeten, Michel

Publication date
2017

Document Version
Publisher's PDF, also known as Version of record

Published in
Bestuurskunde

Citation (APA)
Klievink, B., van Wegberg, R., & van Eeten, M. (2017). Een gezamenlijke rekening? Over digitale innovatie en samenwerking in een institutional void. Bestuurskunde, 2017(1).

Een gezamenlijke rekening?
Over digitale innovatie en samenwerking in een institutional void

Bram Klievink, Rolf van Wegberg & Michel van Eeten

Informatieveiligheid lijkt in ieders belang. Gegeven het organisatie-overstijgende karakter ervan lijkt samenwerking dan ook een noodzakelijke route. In dit artikel verkennen we hoe die route zich verhoudt tot steeds nieuw opkomende innovaties waarvan de ontwikkeling vooruitloopt op wat de geïnstitutionaliseerde regels en praktijken kunnen bijbenen. Als we erin slagen om samenwerking ten behoeve van informatieveiligheid te institutionaliseren, vullen we dan daarmee ook de 'institutionele leegte' die kan ontstaan door toedoen van technische innovaties die elkaar in hoog tempo opvolgen? We verkennen en illustreren dit vraagstuk aan de hand van het voorbeeld van digitale financiële fraude en veiligheid. De institutionele omgeving lijkt daar te veranderen ten faveure van de partijen die juist geen prikkel tot samenwerking hebben. Institutionele stabiliteit is echter wel een pijler van collaboratieve vormen van governance. De vraag is dan ook of een dergelijk model houdbaar is in een toekomst met meer en meer disruptieve digitale innovaties.

[English summary at the end of the document]
[This is the author's version of the accepted manuscript. The full and final paper was published in 'Bestuurskunde', issue 1, 2017, and can be found here]

Inleiding

Grote technische en maatschappelijke veranderingen – zoals industrialisatie, globalisering en urbanisatie – hebben in het verleden geleid tot perioden van buitengewone institutionele en sociale innovaties. Datzelfde valt op te merken bij het digitaal tijdperk, dat grote wijzigingen met zich meebrengt op economisch, sociaal, democratisch en governance vlak (Nye, 1999). Digitale technologie is letterlijk grenzeloos en trekt zich daardoor veel minder dan soortgelijke historische 'revoluties' aan van de grenzen die voor (openbaar) bestuur van belang zijn, zoals die tussen landen, de publieke en de private sector, en organisaties (Fountain, 2001). Deze technologie creëert nieuwe kansen en mogelijkheden tot actie en innovatie buiten – en zelfs zonder – traditionele structuren en organisaties. De snelheid waarop digitale innovaties plaatsvinden en het (soms) intrinsieke disruptieve karakter, beïnvloeden sociale structuren en praktijken sneller dan bestaande instituties en processen van bestuur bij kunnen benen. Het gevolg daarvan is een gat tussen bestaande regels en instituties en hun effectiviteit en legitimiteit; digitale innovaties leiden tot een *institutional void* (Hajer, 2003).

Die institutionele leegte is natuurlijk niet écht leeg; we doelen hiermee op de situatie dat heersende instituties, regels en structuren niet meer passen bij een nieuwe werkelijkheid die door uitdagers wordt gecreëerd (Fremeth & Marcus, 2011).

Belangrijker nog, bij tal van aan informatie- en communicatietechnologie (ICT) gerelateerde innovaties zoeken uitdagers nadrukkelijk die leegte op. Bekende voorbeelden daarvan zijn Airbnb en Uber, die razendsnel een grijs gebied in de bestaande (wettelijke) regels opzoeken en op eigen wijze vullen. Dat staat op gespannen voet met de partijen (publiek en privaat) die hun rol en belangen juist in die regels en instituties hebben vastgelegd. Dat betekent ook dat die uitdagers er soms weinig belang bij hebben dat die institutionele leegte weer ingevuld kan worden. Zij ervaren weinig prikkels tot samenwerking, juist omdat het zo lucratief kan zijn om activiteiten te ontplooien in zo'n leegte.

Soms is echter ook te verwachten dat de belangen van zowel de zittende instituties als van de uitdagers sterk overeenkomen. Een van die situaties doet zich voor bij informatieveiligheid. Kwaadwillende actoren niet meegerekend, is er juist rond dat probleem een duidelijk gedeeld belang: processen, diensten en infrastructuren zo goed mogelijk beschermen tegen die kwaadwillenden. Neem bijvoorbeeld het financiële domein: ondanks hevige concurrentie tussen banken is het in ieders belang dat de digitalisering van de financiële wereld, inclusief ontwikkelingen als bitcoin, niet tot grote veiligheidsrisico's leidt. Terwijl elektronische dienstverlening en innovatie zeer concurrentiegevoelig zijn, slaagt men er in deze sector in om op het gebied van internet- en informatieveiligheid grootschalige samenwerking op te tuigen, waarin deze partijen niet elkaars concurrenten maar elkaars collega's zijn. Dat is essentieel, niet alleen voor de banken zelf, maar uiteraard ook voor alle anderen die belang hebben bij financiële diensten: de cliënten van een bank. Gelet op de grote financiële stromen binnen, van en naar de overheid zijn overheidsorganisaties daar ook bij gebaat. Dit nog naast een justitiële rol en naast het algemene publieke belang van een goed werkend betaalsysteem. Omdat de digitale wereld zich weinig van grenzen aantrekt, is samenwerking tussen organisaties, sectoren en over landsgrenzen heen noodzakelijk.

Gegeven de structuur en de vele en complexe afhankelijkheden in de netwerkmaatschappij, zijn overheden gewend geraakt te moeten afstemmen en samenwerken om uitdagingen het hoofd te bieden, bijvoorbeeld onder de noemer van *collaborative governance* (Agranoff, 2006; Ansell & Gash, 2007; Mcguire, 2006). Zeker voor informatieveiligheid lijkt samenwerking een noodzakelijke route. In dit artikel willen we verkennen hoe die route zich verhoudt tot steeds nieuw opkomende innovaties, waarvan de ontwikkeling vooruitloopt op wat de geïnstitutionaliseerde regels en praktijken kunnen bijbenen. Dat zal gevolgen hebben voor de uitgangspunten (zoals institutionele stabiliteit) van collaboratieve vormen van governance en daarmee voor de houdbaarheid van een samenwerkingsmodel. Als we er toch in slagen om samenwerking ten behoeve van informatieveiligheid te institutionaliseren, hebben we de leegte dan afdoende gevuld?

We verkennen en illustreren dit vraagstuk aan de hand van het voorbeeld van digitale financiële fraude. Voor dat vraagstuk werken banken, overheden en anderen samen

aan een veilig en weerbaar financieel stelsel. Het optuigen van dergelijke samenwerking is uitdagend maar nu dat er eenmaal staat, geeft dat op zijn minst een basis voor het borgen van informatieveiligheid. Daarmee zijn we dus klaar voor toekomstige veiligheidsdreigingen. Toch?

Digitale financiële fraude

Fraude met online betaaldiensten is een van de meest kostbare vormen van cybercrime (Anderson et al., 2013; Europese Centrale Bank, 2015). Een bij cybercriminelen populair instrument is het gebruik van malware. Dit is kwaadaardige software, waarmee vaak langdurig toegang tot een computer van een slachtoffer verkregen kan worden. Dergelijke malware kan via verschillende kanalen bij het slachtoffer terechtkomen, zoals via phishing[1] of spear-phishing.[2] De malware gebruikt (of in dit licht: misbruikt) een kwetsbaarheid of achterdeur in bestaande software, waardoor de cybercrimineel toegang tot de computer kan krijgen. Op die manier kan er bijvoorbeeld nog meer kwaadaardige software op de computer worden geïnstalleerd of kan de computer worden ingezet bij cyberaanvallen. Om dat voor elkaar te krijgen bestaat er een aanvalsinfrastructuur, met zogenoemde command & control (C&C) servers.[3] De extra software die wordt geïnstalleerd, kan bijvoorbeeld worden gebruikt om inloggegevens te verkrijgen, om meer rechten op de computer of zelfs het netwerk te verkrijgen, of om internetverkeer te onderscheppen. Dat laatste is een veelgebruikte vorm van innovatieve financiële fraude. Een aanvaller kan dan bijvoorbeeld een internetbankieren-sessie omleiden via een eigen systeem (een zogenaamde man-in-the-middle aanval) en zo transacties proberen te manipuleren of toegang tot een rekening te krijgen. Hierbij is het belangrijk op te merken dat het dus niet om een directe aanval op de systemen van de bank gaat, maar dat de crimineel er alles aan doet om het voor de bank te laten lijken of er een gewone klant met zijn of haar eigen rekening bezig is.

Is een cybercrimineel er eenmaal in geslaagd om in te breken en geld te bemachtigen, dan moet dat worden weggesluisd. Daarvoor zijn verschillende kanalen denkbaar. Het meest traditionele kanaal maakt gebruik van zogenoemde *money mules*,[4] ofwel geldezels die te vergelijken zijn met katvangers. De crimineel sluist het vervolgens weer verder door of zet het om in contant geld of andere middelen van waarde (Van Wegberg, Klievink, & Van Eeten, 2017). Een andere zogenoemde 'cash out'-strategie is de gestolen middelen te gebruiken om (anonieme) bitcoins te kopen.

[1] In grote hoeveelheden en ongericht verstuurde e-mails die tot doel hebben om slachtoffers te verleiden inlogcodes te verstrekken, soms ook gecombineerd met een kwaadaardig bestand of een link waarmee malware wordt geïnstalleerd.

[2] Phishing e-mails die gericht worden verstuurd, zoals naar klanten of medewerkers van een specifieke bank.

[3] Computerservers die gebruikt worden door criminelen om een netwerk aan geïnfecteerde computers aan te sturen of instructies te geven.

[4] Mensen die tegen betaling hun rekening of bankpas ter beschikking stellen aan een crimineel.

Het voert voor dit artikel te ver om het hele scala aan mogelijke aanvalspaden uit te werken. Het bovenstaande dient slechts om te illustreren dat er een aantal basisingrediënten zijn die de crimineel gebruikt, waaronder de malware zelf, de software die men vervolgens gebruikt voor de fraude, de specifieke servers die men gebruikt in zo'n aanval en de cash-out-kanalen die worden gebruikt.

In het gegeven dat in die instrumenten de bouwstenen liggen voor cyberaanvallen op (klanten van) verschillende banken, ligt ook de basis voor samenwerking. Veel informatie over hoe die aanvallen werken en dus ook hoe aanvallen of bijbehorende transacties gedetecteerd en geblokkeerd kunnen worden, kan worden verkregen door bijvoorbeeld de malware uit elkaar te halen en te onderzoeken. Ook kan er veel worden geleerd van de analyse van de modus operandi van deze aanvallen en het uitwisselen van zaken als informatie over de eerdergenoemde *money mules*. Hoewel financiële instellingen ieder afzonderlijk een commercieel belang hebben en internetbankieren ook ten behoeve van het halen van concurrentievoordeel kan worden ingezet, is hier tevens een duidelijk gedeeld belang. Het imago van online bankieren in het algemeen hangt ook samen met die van de eigen instelling. Ook het financiële belang is groot, gegeven de grote kosten, zowel als gevolg van de beveiliging, maar ook van de directe en indirecte schade, zoals in veel gevallen als gevolg van het compenseren van klanten en zo mogelijk terugdraaien van frauduleuze betalingen.

Samenwerken tegen fraude

In dat gedeelde belang ligt de basis voor (inmiddels) geïnstitutionaliseerde samenwerkingsverbanden. Het uitwisselen van (operationele) informatie over cyberdreigingen, kwetsbaarheden en concrete aanvallen is van groot belang voor een effectieve aanpak van digitale financiële fraude. Immers, als de ene bank een bepaald rekeningnummer heeft geïdentificeerd als behorend bij een *money mule*, dan heeft het zin als ook andere instellingen dit weten en transacties naar of vanaf die rekening monitoren en zelfs blokkeren. Zo ook met de informatie die opsporingsdiensten, het NCSC (Nationaal Cyber Security Centrum), of private cybersecurity-bedrijven hebben, zoals mogelijke doelwitten die in blootgelegde instructiesets voor malware gevonden zijn.

Een samenwerkingsarrangement op dit domein is het ISAC (Information Sharing and Analysis Centre) voor de financiële sector: FI-ISAC. Dit is een publiek-privaat samenwerkingsverband en wordt per sector georganiseerd, al dan niet op Europees niveau. In de FI-ISAC delen de financiële sector, de politie en de CERT-gemeenschap (CERT staat voor Computer Emergency Response Team*)* good practices, informatie over modus operandi, incidenten, dreigingen en kwetsbaarheden die zijn gericht op de financiële sector (CPNI, 2012). Naast dit soort samenwerking op tactisch/strategisch niveau is er ook op operationeel niveau samenwerking tussen de betrokken partijen.

Dergelijke samenwerkingsverbanden lijken een probaat middel om in een sector waar ICT vooral ingezet wordt voor concurrentievoordeel, toch samen te werken waar het gaat om cyberveiligheid. De condities waaronder deze spelers – die soms regelrechte concurrenten zijn – toch samenwerken (tenminste, tot op zekere hoogte), zijn te duiden aan de hand van een aantal van de condities die Ansell en Gash (2007, p. 550) in hun model voor collaborative governance onderscheiden:

- Startcondities. Er is een duidelijk gedeeld belang en onderlinge afhankelijkheid om dat te realiseren. Tevens is er een publiek belang, wat de betrokkenheid van de overheid ten goede komt, Daar komt bij dat er in Nederland een aantal grote banken zijn, waardoor geen sprake is van grote machtsasymmetrie. Als die grote banken in staat zijn om iets op te tuigen waarin ze hun individuele belang ontstijgen, kunnen ze ook kleinere banken meenemen.
- Institutioneel ontwerp. Een belangrijk instrument in de samenwerking is een non-concurrentiebeding op de veiligheid van de betaaldiensten. Hier zit wel enig verschil in het niveau van de samenwerking: de meer strategische en tactische samenwerking is gebaseerd op inclusiviteit en vaste momenten, terwijl de meer operationele samenwerking deels incident-gedreven is en evenzeer op een proces van samenwerking leunt, als op de instituties daartoe.
- Collaboratief proces. Ten slotte valt op te merken dat na een periode waarin online bankieren vooral een instrument voor concurrentievoordeel was, er steeds meer historie van samenwerking is. Denk bij dat laatste bijvoorbeeld aan iDeal als betaalmiddel en andere technische innovaties die door de banken gezamenlijk gedragen en ontplooid worden. Dit helpt om vertrouwen op te bouwen en een dialoog open te houden, wat de basis is voor nieuwe uitingen van samenwerking.

Dit schept licht op de voorwaarden waaronder deze concurrenten samenwerken. Of we daarmee ook een toekomstbestendig model voor deze uitdagingen hebben, is echter de vraag.

Zijn we er dan klaar voor?

In de inleiding introduceerden we het idee van een institutionele leegte die ontstaat doordat digitale innovaties zich sneller ontwikkelen dan de instituties – in brede zin – kunnen bijbenen. Een eerste versie van die *void* in het financiële domein valt wellicht te zien in de opkomst van online bankieren, waar in het zwaar gereguleerde financiële domein in eerste instantie de regelgeving en jurisprudentie niet goed aansloten op de ontwikkeling. Daardoor was er redelijk wat ruimte voor de banken om gebruik te maken van de mogelijkheden die internet hen bood voor het digitaliseren van de dienstverlening. Niet in de laatste plaats speelden concurrentieoverwegingen een rol, zeker in de vorm van de hoop op flinke kostenbesparingen. De uitdagingen die dat op het gebied van cybersecurity met zich mee bracht en het gebrek aan instituties om die adequaat te adresseren, zijn inmiddels opgepakt in samenwerkingsverbanden als het FI-ISAC alsook in ad hoc verbanden binnen de financiële sector.

Informatieveiligheid is een organisatie-overstijgend vraagstuk. Organisaties zijn wederzijds afhankelijk en gezamenlijk optrekken kan tot grote voordelen leiden in de snelheid en effectiviteit van de reactie op nieuwe veiligheidsproblemen. Het in het leven roepen van ISAC's, zoals in de financiële sector, lijkt dan ook een belangrijke stap in het trachten te vergroten van de digitale veiligheid van met name online bankieren. Daarmee lijkt een weg gevonden om verschillende partijen met verschillende belangen te laten samenwerken aan een gedeeld vraagstuk. Die samenwerking is zowel operationeel als tactisch van aard. Doordat deze samenwerkingsverbanden steeds verder geïnstitutionaliseerd raken, geeft dat het beeld dat we er klaar voor zijn om ook het inter-organisationele aspect van informatieveiligheid het hoofd te bieden.

We lijken er dus klaar voor te zijn. Dat wil zeggen: we lijken effectieve instrumenten te hebben om met huidige en toekomstige veiligheidsvraagstukken om te gaan, even los van de staat van de implementatie daarvan. Maar zijn we er wel echt klaar voor?

Er staan inmiddels weer nieuwe uitdagers aan de poort te rammelen. Die uitdagers zien zich niet gehouden aan die samenwerking en missen een deel van de *incentives* die eerdere deelnemers wel hebben. Met die uitdagers komen uiteraard weer nieuwe veiligheidsuitdagingen. Maar de vraag is of die in voldoende mate geïnvolveerd willen en kunnen worden om die uitdagingen met dezelfde instrumenten aan te kunnen.

Nieuwe uitdagers in een groter wordende *void*

De ontwikkelingen van digitale innovaties gaan in onvermoeibaar tempo door. In het financieel domein worden die zelfs geholpen door een nieuwe wettelijke EU-richtlijn (Revised Payment Service Directive; PSD2), die de *de facto innovaties* in betaaldiensten volgt door de vernieuwing te codificeren, te reguleren en de ruimte te creëren voor innovaties die concurrentie kunnen vergroten. Zo moet de richtlijn het gemakkelijker maken om als betaalaanbieder te gaan opereren en nieuwe betaalmiddelen te accepteren. Dit maakt het voor de TPP's – third party payment service providers, dus 'derden' in het betaalverkeer, naast de bank of creditcardmaatschappij, de koper en de verkoper – makkelijker om een *seat at the table* en daarmee een rol te krijgen in het nog steeds toenemende online betaalverkeer.

Relevant voor het veiligheidsvraagstuk hierin is vooral welke rol en ruimte voor deze TPP's worden voorzien. Er zijn grofweg twee smaken: ten eerste kunnen TPP's toegang krijgen tot de gegevens van een bankrekening, bijvoorbeeld om diensten als digitale huishoudboekjes te kunnen aanbieden. Daarnaast is voorzien dat TPP's elektronische betalingen kunnen starten. Er zijn inmiddels al een aantal jaren *fintech*-bedrijven op de markt die online betalingen afhandelen en die markt groeit snel. De diensten van deze bedrijven kunnen namens hun klanten transacties opstellen en indienen bij de banken. Dit zou – overeenkomstig de memorie van toelichting bij deze richtlijn – innovatie en concurrentie onder aanbieders moeten bevorderen.

Echter, in technisch opzicht lijkt een transactie die wordt geïnitieerd door een dienst van een betaalaanbieder, ontzettend veel op een transactie die wordt geïnitieerd door de software van een cybercrimineel; in beide gevallen gaat het immers om een zogeheten *man-in-the-middle*. In het ene gunstigste geval is dat precies de bedoeling, in het donkerste scenario is het een aanval. De banken hebben de afgelopen jaren – al dan niet gezamenlijk – flink geïnvesteerd in het detecteren van frauduleuze transacties en dit lijkt nu bemoeilijkt te worden door de komst van deze richtlijn. Hiermee lijkt in de strijd tegen cybercriminaliteit wederom een nieuw hoofdstuk aan te breken. Banken worden voor de cyberveiligheid deels afhankelijk van de afstemming met en detectie door nieuwe aanbieders. De banken hebben hier wat tegenstrijdige prikkels voor: enerzijds zijn die nieuwe aanbieders ook concurrenten, anderzijds worden banken vaak aansprakelijk gehouden voor gestolen geld – in het geval van particulieren althans.

Nieuwe betalingsverwerkers hebben echter juist *weinig incentives* om te investeren in samenwerking ten behoeve van informatieveiligheid, juist omdat de regels zo zijn ingericht dat het risico en de kosten bij de 'oude' instituties – in dit geval de banken – liggen. Hier doet zich het interessante geval voor dat een deel van de nieuwe regels op dit terrein nieuwe ruimte creëren of codificeren, zonder dat de rest van de instituties en regels mee evolueren. Als gevolg daarvan zijn er eigenlijk twee speelvelden, die voor een deel van de partijen veel comfortabeler is dan voor de partijen die (institutioneel) gebonden zijn aan het oude speelveld. Banken, overheden en anderen die samenwerken, zitten opeens in hetzelfde schuitje: samen vormen ze de bestaande instituties die worden uitgedaagd. De uitdagers hebben geen direct belang om daaraan deel te nemen – al willen sommigen graag hun verantwoordelijkheid nemen – waar de bestaande deelnemers aan de geïnstitutionaliseerde samenwerking dat wel hadden. Geholpen door PSD2 is er een gerede kans dat fintech-ontwikkelingen de sector dus weer die void intrekken; voor de uitdagers is dat immers een comfortabele plek.

De institutionele omgeving (Ansell & Gash, 2007) lijkt aan het veranderen ten faveure van de partijen die daar nu geen rol in hebben en ook niet noodzakelijk een rol willen spelen. Stabiliteit in die institutionele omgeving is echter wel een uitgangspunt voor collaboratieve vormen van governance. Er bestaat dan ook een kans dat het in plaats van richting een verder uitgebreide samenwerking, meer in de richting van conflict gaat (Hensmans, 2003). Tegelijkertijd zou samenwerking met dergelijke partijen hierin erg kunnen helpen omdat individuele partijen niet de hele betaalketen kunnen zien. De vraag is echter of zij het net zo goed monitoren als banken doen, zonder dat ze daar een direct belang bij hebben maar wel de kosten zullen voelen. Tegelijkertijd is het de vraag of de banken er veel trek in hebben de kastanjes uit het vuur te moeten halen voor hun nieuwe concurrenten.

Wat betekent dat voor de informatieveiligheid bij de overheid?

De hier beschreven casus is slechts illustratief maar wel effectief in het beschrijven van een patroon van samenwerking en conflict in het licht van nieuwe innovaties en uitdagers. 'We' lijken gewend geraakt om dit soort complexe vraagstukken met samenwerking tegemoet te treden. Dat lijkt soms naïef, maar blijkt ook wel effectief. Hoe dan ook leunt het wel op het idee dat er gesprekspartners zijn die ook belang hebben bij samenwerking, die stabiel en aanspreekbaar zijn, en die zich überhaupt aangesproken voelen om mee te spelen.

Wegens het gebrek aan incentives voor nieuwkomers lijkt meer inclusieve samenwerking echter niet te werken. Als die partijen niet meedoen, heeft dat gevolgen voor de stabiliteit van de institutionele omgeving, waarin de basis voor samenwerking ligt. Een samenwerkingsmodel lijkt dan ook niet of slechts ten dele houdbaar. Daar zijn andere mechanismen nodig. Het is nog te vroeg om vast te kunnen stellen welke mechanismen dat in het hier beschreven domein kunnen zijn. Misschien moeten 'we' het ook gewoon laten gebeuren; de *void* zal zichzelf op enige wijze vullen. Dat zal wellicht gepaard gaan met een terugtrekkende beweging van de nu samenwerkende partners, die ieder voor zichzelf moeten gaan proberen de informatieveiligheid te regelen zonder op samenwerking te kunnen vertrouwen. Een ander instrument kan zijn meer aandacht te besteden aan de nieuwe regels die deze *void* introduceren, te vergezellen van wijzigingen in gerelateerde regels die direct of indirect tot het huidige systeem voor informatieveiligheid hebben geleid. Ten slotte heeft informatieveiligheid ook economische waarde die eventueel meer aan de markt overgelaten kan worden, waar zich dan ongetwijfeld nieuwe modellen, diensten en producten zullen vormen. Kortom, als de geijkte samenwerking niet meer werkt, kunnen we ten minste vier richtingen op: op zoek naar nieuwe incentives en spelregels voor samenwerking; het laten gebeuren; de wet- en regelgeving juist versterken; of het aan de markt overlaten. Hoe deze wegen kunnen uitpakken en welke factoren mede bepalen welke kant het op gaat, is voor ons onderwerp van nader onderzoek. Zonder die antwoorden zijn we nog niet klaar voor nieuwe stabiliteit in een voortdurend spel tussen instituties, uitdagers en disruptieve technische innovaties.

Literatuur

Agranoff, R. (2006). Inside collaborative networks: Ten lessons for public managers. *Public Administration Review*, *66*(s1), 56-65.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M.J.G. van, Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer.

Ansell, C., & Gash, A. (2007). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*(4), 543-571. http://doi.org/10.1093/jopart/mum032

CPNI. (2012). *Jaarbericht 2011 CPNI.NL – Platform voor Cybersecurity*. Werkendam.

Europese Centrale Bank. (2015). Fourth report on card fraud. Retrieved from https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

Fountain, J.E. (2001). *Building the virtual state: Information technology and institutional change*. Washington, DC: Brookings Institution Press.

Fremeth, A.R., & Marcus, A.A. (2011). Institutional void and stakeholder leadership: Implementing renewable energy standards in Minnesota. In *Stakeholders and scientists* (pp. 367-392). New York: Springer. http://doi.org/10.1007/978-1-4419-8813-3

Hajer, M. (2003). Policy without polity? Policy analysis and the institutional void. *Policy Sciences*, *36*, 175-195. Retrieved from http://link.springer.com/article/10.1023/A:1024834510939

Hensmans, M. (2003). Social movement organizations: A metaphor for strategic actors in institutional fields. *Organization Studies*, *24*(3), 355-381. http://doi.org/10.1177/0170840603024003908

Mcguire, M. (2006). Collaborative public management: Assessing what we know and how we know it. *Public Administration Review*, *66*(s1), 33-43. http://doi.org/10.1111/j.1540-6210.2006.00664.x

Nye, J. (1999). Information technology and democratic governance. In E.C. Kamarck & J.S. Nye (Eds.), *Governance.com: Democracy in the Information Age* (pp. 1-18). Brookings Institution Press.

Wegberg, R. van, Klievink, B., & Eeten, M. van. (2017). Discerning novel value chains in financial malware. *European Journal on Criminal Policy and Research*, 1-20. http://doi.org/10.1007/s10610-017-9336-3

English summary:

Will collaboration for digital security survive new challengers?

The speed and disruptive character of digital innovations impact social structures and practices faster than institutions can keep up with. This results in an 'institutional void'; a gap between the rules and institutions and their ability and effectiveness of their implementation. This will also affect the institutional stability that is the basis for the paradigm of collaboration-based forms 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. New (regulatory) space currently being created for innovators, suggests that the answer is 'no'. It is too early to say how this plays out specifically and we argue for further research into the antecedents of collaboration in institutional voids.

Keywords: collaboration, digital security, institutional void, collaborative governance, financial cyber fraud

Over de auteurs

Dr. ing. B. Klievink is universitair hoofddocent collaborative digital governance en sectieleider bij de sectie Policy, Organisation, Law & Gaming, faculteit Techniek, Bestuur en Management van de TU Delft.

R. van Wegberg, MSc is criminoloog, werkt bij TNO en is als promovendus verbonden aan de faculteit Techniek, Bestuur en Management van de TU Delft.

Prof. dr. M. van Eeten is hoogleraar economics of cyber security aan de faculteit Techniek, Bestuur en Management van de TU Delft.