Samenvatting

Een toenemend aantal cyberaanvallen bedreigde het afgelopen decennium de wereldeconomie. Voor organisaties is het lastig om een optimaal niveau van veiligheid te bepalen. Om dit te verbeteren, bepleit deze studie dat het noodzakelijk is om de informatie over de aard van het cyberrisico en het rendement van de investering in maatregelen om het risico te verminderen te delen onder relevante actoren, waarbij men de kosten van deze kennisdeling in acht neemt. Op dit moment is er onvoldoende kennisdeling in cybersecurity. Daarom zoekt deze studie oplossingen voor efficiënte stimulering van kennisdeling in cybersecurity. Kennisdeling heeft sterke trekken van een publiek goed: degene die de informatie deelt, heeft er zelf weinig baat bij. Dit bemoeilijkt deze uitdaging.

Allereerst moet de rechtseconomie beter verbonden worden met de economie van cybersecurity. Onderzoekers in de economie van cybersecurity zouden gebruik moeten maken van de theoretische en methodologische kennis uit de rechtseconomie. En onderzoekers in de rechtseconomie zouden moeten leren van de inzichten met betrekking tot de dynamiek, empirie en specifieke micro-economische aspecten van de economie van cybersecurity. We moeten een flinke inspanning doen om de twee gebieden bij elkaar te brengen.

Deze *rechtseconomie van cybersecurity* moet de taak op zich nemen om een gemeenschappelijke 'cybersecurity kennisdelingsagenda' te definiëren voor zowel wetenschap als overheid en bedrijfsleven. Elke partij in deze 'triple helix' heeft verschillende rollen, verantwoordelijkheden en middelen om kennisdeling te stimuleren. De ontwikkeling van die individuele middelen, gecombineerd met intensieve samenwerking, zal de beste resultaten opleveren. Deze studie heeft in de drie inhoudelijke delen een eerste stap in deze richting gezet.

Deel 1 richt zich op de rol van de wetenschap zelf en presenteert een pionierende analyse die zes aspecten in de wettekst van 71 persoonsgegevensbeschermingswetten ontsluit. Het deel deelt informatie met betrekking tot concepten binnen deze wetten en maakt ze gereed voor statistische analyse, wat de verbinding tussen rechtseconomie en de economie van cybersecurity ten goede komt. De laatste heeft namelijk veel empirische data die op deze manier verbonden kunnen worden met de effecten van wetgeving. Hierna richt Deel 2 zich op de rol van de overheid en bestudeert de nieuwe Europese meldplicht datalekken, verankerd in de Europese Algemene Verordening Gegevensbescherming. De studie openbaart dat deze Europese meldplicht prikkels kan geven om organisaties te stimuleren om informatie te delen, maar alleen als deze slim gehandhaafd wordt door de nationale autoriteiten. Ik spoor deze autoriteiten dan ook aan om slimme beloningen te ontwerpen en ook te kijken naar de expressieve functie van de wet als alternatieve manieren om de juiste prikkels te geven aan de organisaties die de wet moeten naleven. Een laatste punt is dat de drempel om te melden relatief hoog moet zijn en in ieder geval duidelijk. Als laatste focust Deel 3 op de rol van de industrie, en in het bijzonder onderzoekt dit deel cyberverzekeringen en cyberriskpooling (risicoverschuiving zonder tussenkomst van een verzekeraar). De empirische analyse van cyberverzekering laat zien dat de markt voor het midden- en kleinbedrijf nog in de

kinderschoenen staat en dat de kennisdeling tussen de verzekeraar en de verzekerde nog zeer beperkt is. Cyberriskpooling kan een belangrijke rol spelen in situaties waarin organisaties meer (of gelijke) informatie over het cyberrisico hebben dan de verzekeraar. Met cyberriskpooling kunnen organisaties een gewenste hybride vorm van risicoallocatie kiezen, waarin ook cyberverzekeringen en eigen beheer van het risico een rol spelen. De analyse schetst welke voorwaarden en ontwerpvragen bij cyberriskpooling in acht moeten worden genomen.

De verdere verbondenheid van onze analoge levens met de digitale wereld zal zich onvermijdelijk voortzetten. Zo ook de nadelen hiervan, in de nabije en verre toekomst. De rechtseconomie van cybersecurity kan deze ontwikkeling van een fundament voorzien waardoor we verdere welvaart- en welzijnsgroei in het digitale tijdperk kunnen realiseren.