Herbert Hamers
Department of Econometrics and Operations Research and TIAS School for Business and Society
Tilburg University
h.j.m.hamers@tilburguniversity.edu

Bart Husslage
Afdeling Data Science
CZ, Tilburg

Roy Lindelauf
Section Intelligence and Security
Nederlandse Defensie Academie, Breda
rha.lindelauf.01@mindef.nl

Coöperatieve speltheorie en terroristische netwerken

Een terroristisch netwerk is een voorbeeld van een verborgen netwerk: een netwerk waarvan weinig bekend is over de architectuur. Geheimhouding en organisatorische veerkracht zijn belangrijke kenmerken. In dit artikel beschrijven Herbert Hamers, Bart Husslage en Roy Lindelauf hoe coöperatieve speltheorie gebruikt kan worden voor de analyse van terroristische netwerken.

Het is een jaar voor de tragische gebeurtenissen op 9/11, ergens in een trainingskamp bij Kaboel. Een roodharige instructeur in spijkerbroek geeft les aan rekruten van de Afghaanse jihad. Hij noemt zich Abu Musab al-Suri (de Syriër). Op een whiteboard tekent hij een boom, een graaf waarin elk tweetal personen is verbonden door een uniek pad. “Zo moet je organisatie er niet uitzien”, zegt hij in een instructievideo die later is gevonden door Amerikaanse soldaten na de invasie van Afghanistan. Mustafa Setmariam Nasar, zoals hij werkelijk heet, is een van de architecten van de globale jihad en wordt verdacht van banden met Al Qaida, de Taliban en andere terroristische organisaties. Hij is de auteur van het bekende *Oproep tot Internationale Islamitisch Verzet*, een boekwerk van 1600 bladzijden waarvan de Engelse vertaling is te vinden op de internetbibliotheek archive.org. Geheimhouding en organisatorische veerkracht zijn volgens al-Suri de belangrijkste kenmerken van een verborgen organisatie. In de video legt hij uit hoe een organogram van een terroristische organisatie eruit moet zien. In plaats van een boomstructuur, die eenvoudig kan worden geïnfiltreerd en ontmanteld, pleit hij voor een netwerk van cellen. De organisatie moet decentraal zijn in plaats van hiërarchisch.

Een foto van Abu Musab al-Suri in 2004 uit een opsporingsbevel van de Amerikaanse overheid. Hij werd gearresteerd in 2005 in Pakistan en overgedragen aan de Amerikaanse autoriteiten. Wat er daarna met hem is gebeurd is niet bekend. Hij zit waarschijnlijk in een Syrische gevangenis.

Na 9/11 vielen de Verenigde Staten Afghanistan binnen en verwijderden de Taliban in een poging om Al Qaida te ontmantelen. Tot dan toe was de wereld gewend aan terroristische organisaties met een verticale commando structuur, zoals de IRA, de PLO, Hamas, Hezbollah en de Rode Brigades. Al-Suri, een werktuigbouwkundig ingenieur uit Aleppo, had een duidelijk andere visie. Analisten van de veiligheidsdiensten kregen te maken met een nieuwe organisatiestructuur, waarin leiders en volgers maar moeilijk van elkaar waren te onderscheiden. Het werd moeilijker om te bepalen welke individuen in de gaten moesten worden gehouden, waardoor destabilisatie of ontmanteling onmogelijk was. Na 9/11 werd Al Qaida het archetype van de moderne terroristische organisatie, waarvan nauwelijks betrouwbare data viel te verzamelen.

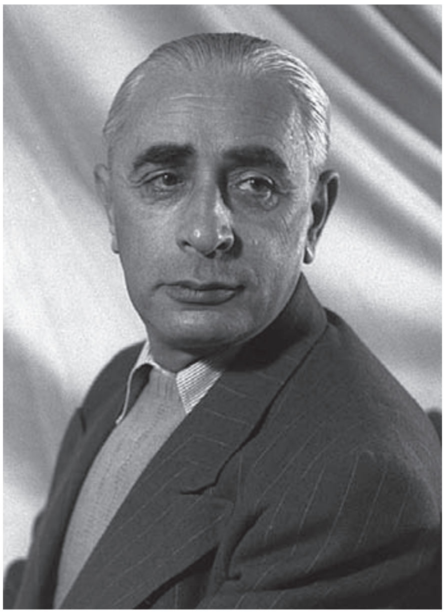
Ondertussen waren wetenschappers bezig om de structuur van verschillende sociale en biologische netwerken te ontrafelen [8, 16, 19]. Men realiseerde zich al snel dat deze inzichten belangrijk zouden kunnen zijn voor de analyse van terroristische netwerken [22]. Eerder onderzoek van terroristische netwerken richtte zich op destabilisatie [5,7], de karakterisatie van de organisatie [6,13,14] en methoden om sleutelfiguren te onderscheiden [1,4,18]. De netwerktopologie in deze onderzoeken was meestal een vast gekozen model. Soms werd historische data gebruikt, maar die is niet betrouwbaar en anekdotisch en bovendien zijn de datasets van de veiligheidsdiensten niet vrij toegankelijk.

De architectuur van decentrale netwerken is goed bestudeerd [20,21], maar dit betreft alleen openbare netwerken. Van verborgen netwerken is weinig bekend. De gebruikelijke sociale netwerken zijn te karakteriseren als *small-world networks*, met een hoge clustering en een kleine gemiddelde afstand. Het is maar de vraag of dit ook geldt voor verborgen netwerken en wat dit betekent voor de analyse ervan. Vanwege het gebrek aan goede data werd het noodzakelijk om theoretische modellen van verborgen netwerken te ontwikkelen. Wij benaderen dit probleem vanuit de *coöperatieve speltheorie*.

Nash-onderhandelingsoplossing

Geheime diensten beschikken ook over heimelijke netwerken die werken voor de overheid. De bekendste voorbeelden zijn de CIA, de KGB en de Mossad. Soms wordt een heimelijk netwerk ontdekt, zoals in de operatie Susannah, een Israëlische geheime missie in Egypte gedurende het begin van de jaren vijftig. Al snel na aanvang van de operatie werd het netwerk opgerold, omdat de Egyptische geheime dienst achter de namen kwam van de contacten van één verdacht persoon. Het probleem van de operatie was dat iedereen elkaar kende. Het netwerk was een volledige graaf. Dit bevordert de operationele slagkracht, maar het is niet goed voor de geheimhouding. De Israëlische minister van defensie, Pinhas Lavon, werd gedwongen tot opstappen als uiteindelijke verantwoordelijke van deze mislukte operatie. Dit staat nu bekend als de Lavon-affaire.

Het is duidelijk dat al-Suri een afweging maakte tussen geheimhouding en slagkracht van verborgen organisaties. Een dergelijke afweging wordt ook gemaakt in de *onderhandelingstheorie*, een onderwerp binnen de speltheorie. Als twee spelers een taart moeten verdelen, dan



Pinhas Lavon werd verantwoordelijk gehouden voor de operatie Susannah, waarin geheim agenten bomaanslagen zouden plegen in Egypte. De schuld zou worden gegeven aan de Moslimbroederschap.

ligt de helft voor beiden het meest voor de hand. Maar hoe is de verdeling bij verschillende preferenties? Een van de spelers is misschien op dieet en mag hoogstens een kwart taart. Of hoe verdeel je de taart als sommige delen slagroom bevat maar niet gelijk verdeeld over de hele taart? We zeggen dan dat de te verdelen taart asymmetrisch is. Uiteraard is ook een mogelijke uitkomst dat er geen verdeling wordt gevonden zodat beide spelers helemaal geen taart krijgen. In een onderhandelingsprobleem wordt een optimale verdeling $(\bar{u},\bar{v})$ in een verzameling F van alle mogelijke verdelingen (u,v) gezocht waarbij er een dreigpunt bestaat als de spelers niet tot een verdeling komen. Een optimale verdeling moet voldoen aan een aantal redelijke aannames. De volgende axioma's zijn opgesteld door John Nash, Nobelprijswinnaar in 1994 voor zijn werk op het gebied van de speltheorie, waarvan de onderhandelingstheorie een onderdeel is:

– *Pareto-optimaal*. Er is geen $(u,v)\in F$ met $u\geq\bar{u}$ en $v\geq\bar{v}$ anders dan $(\bar{u},\bar{v})$. Ofwel, als een oplossing Pareto-optimaal is dan kan een speler zichzelf alleen verbeteren ten koste van de andere speler.
– *Symmetrie*. Als F invariant is onder de spiegeling $(u,v)\mapsto(v,u)$ dan $\bar{u}=\bar{v}$. Ofwel, als de verzameling van alle mogelijke verdelingen symmetrisch is dan verdelen de spelers gelijk.
– *Onafhankelijkheid van onbelangrijke alternatieven*. Als $G\subset F$ en als $(\bar{u},\bar{v})\in G$, dan is dit ook de optimale verdeling voor F. Ofwel, als de optimale oplossing in een deelverzameling zit van alle mogelijke verdelingen, dan zijn alle mogelijke verdelingen buiten deze deelverzameling irrelevant. Immers, de oplossing wordt al gevonden uit alle mogelijke verdelingen in deze deelverzameling.
– *Schaalinvariant*. Als $\tau(x,y)=(ax,bx)$ voor positieve a en b, dan is de optimale verdeling in $\tau(F)$ gelijk aan $\tau(\bar{u},\bar{v})$. Ofwel, het verhogen van alle verdelingen met dezelfde factoren verhoogt tevens het optimum met deze factoren.

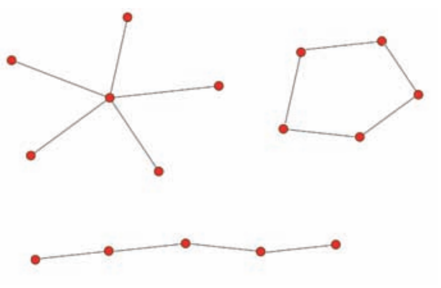
Nash introduceerde de Nash-onderhandelingsoplossing [15] als de oplossing die het product uv maximaliseert. Bovendien toonde hij aan dat de Nash-onderhandelingsoplossing de enige oplossing is die aan de vier genoemde axioma's voldoet. In de volgende paragraaf zullen we de geheimhouding en de slagkracht van een netwerk definiëren. Hierbij gebruiken we de kennis van de Nash-onderhandelingsoplossing waarbij een optimaal netwerk het product van deze twee kenmerken maximaliseert.

Geheimhouding en informatie in een graaf

Een netwerk of graaf G bestaat zoals welbekend uit een verzameling knopen N en zijden E tussen de knopen. In ons geval staat N voor de leden of voor afzonderlijke cellen in een terroristisch netwerk. De zijden E staan voor de directe informatiekanalen binnen het netwerk. Binnen het netwerk wordt informatie uitgewisseld en we nemen aan dat de tijd die het duurt om informatie te sturen van i naar j proportioneel is met de afstand van l_{ij} (het minimaal aantal zijden tussen i en j). Hoe groter de afstand, hoe waarschijnlijker de onderschepping van de informatie. We stellen n gelijk aan het aantal knopen en $T(G)$ gelijk aan de som over alle afstanden $\sum_{i,j\in N} l_{ij}$. We definiëren de informatie-afstand in de graaf als

$$I(G)=\frac{n(n-1)}{T(G)}.$$

Met andere woorden, $I(G)$ is de reciproke waarde van de gemiddelde afstand. Merk op dat $0<I(G)\leq 1$ en dat $I(G)=1$ dan en slechts dan als G een volledige graaf is.



Figuur 1 Stergraaf, cyclische graaf en lineaire graaf.

Voorbeeld. Beschouw de stergraaf S_n, de cyclische graaf C_n en de lineaire graaf L_n zoals in Figuur 1. Als n oneven, dan zijn de informatie-afstanden van deze grafen gelijk aan

$$I(S_n) = \frac{n}{2(n-1)},$$
$$I(C_n) = \frac{4}{n+1},$$
$$I(L_n) = \frac{3}{n+1}.$$

Nu definiëren we de mate van geheimhouding. Hierbij spelen twee factoren een rol. Ten eerste de kans op ontmaskering van een individueel lid. Ten tweede, de kans dat bij ontmaskering ook andere leden van het netwerk in beeld komen. Neem bijvoorbeeld het geval van Nawaf al-Hazmi, een van de kapers van 9/11. In het rapport van de Nationale Commissie Terreuraanslagen [9] staat: “U.S. intelligence would analyze communications associated with Mihdhar whom they identified during this travel, and Hazmi, whom they could have identified but did not.” Khalid al-Mihdhar was een boezemvriend van Nawaf, die wel was afgereisd naar de Verenigde Staten, maar op het laatste moment afzag van de 9/11-aanslag. Hij was onder surveillance, maar toch ontsnapte Nawaf aan de aandacht. We hebben hier te maken met een kans op detectie α_i van knoop i. In geval van detectie wordt ook een fractie $1-u_i$ van het netwerk zichtbaar. De kans op detectie is klein en we nemen aan dat er slechts één knoop kan worden gedetecteerd. We definiëren de geheimhouding $S(G)$ van de graaf als de verwachte fractie die onzichtbaar blijft, gegeven dat één van de knopen wordt gedetecteerd,

$$S(G) = \sum_{i \in N} \alpha_i u_i.$$

Volgens het Nash-onderhandelingsprincipe zijn $I(G)$ en $S(G)$ optimaal als het product maximaal is. Daarom definiëren we

$$\mu(G) = S(G) I(G) \tag{1}$$

als de prestatiemaatstaf van de graaf. Een optimaal verborgen netwerk maximaliseert $\mu(G)$.

Enkele optimale verborgen netwerken

We beschouwen enkele voorbeelden. Stel dat de ontmaskering van individu i ook leidt tot het openbaar maken van al zijn d_i buren. De fractie ongedetecteerde knopen is dan

$$1 - \frac{d_i + 1}{n}.$$

Als de kans op ontmaskering voor elke knoop even groot is, dan is de geheimhouding gelijk aan

$$S_1(G) = \sum_{i \in N} \frac{1}{n}\Big(1 - \frac{d_i+1}{n}\Big) = \frac{n^2 - n - 2m}{n^2},$$

waarbij m het aantal zijden is. De prestatiemaat is in dit geval

$$\mu_1(G) = S_1(G) I(G) = \frac{n^2-n}{n^2} \cdot \frac{n^2-n-2m}{T(G)}.$$

Het optimale netwerk voor deze maat is de stergraaf.

Als de ontmaskering van een knoop leidt tot het openbaar maken van een buur met kans p, dan krijgen we te maken met de binomiale verdeling op d_i. De prestatiemaat is nu

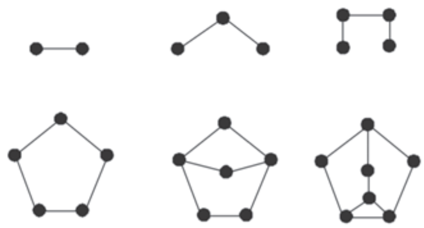
$$\mu_2(G) = S_2(G) I(G) = \frac{n^2-n}{n^2} \cdot \frac{n^2-n-2pm}{T(G)}.$$

Voor lage waarden van p is de volledige graaf optimaal. De geheimhouding is dan uitstekend en de informatiestroom is maximaal voor de volledige graaf. De hieronder vermelde resultaten kunnen worden gevonden in [11]:

Stelling. *Als $p \le \frac{1}{2}$ dan is de volledige graaf optimaal onder μ_2. Als $p \ge \frac{1}{2}$ dan is de stergraaf optimaal onder μ_2.*

We vinden hier dus ofwel een volledige graaf ofwel een boom. De ene kennen we uit de Lavon-affaire en de andere wordt afgekeurd door al-Suri. De beschouwde prestatiematen zijn relevant voor de initiele fase van een operatie. Dan zijn leden van het netwerk passief met een minieme kans op detectie. Gedurende de operatie worden sommige leden meer zichtbaar. We modelleren deze ‘informatie-centraliteit’ via de evenwichtsverdeling van een standaard random walk op een graaf. De prestatiemaatstaf wordt dan

$$\mu_3(G) = \frac{2m(n-2) + n(n-1) - \sum_{i \in N} d_i^2}{n(2m+n)} \cdot \frac{n(n-1)}{T(g)}.$$



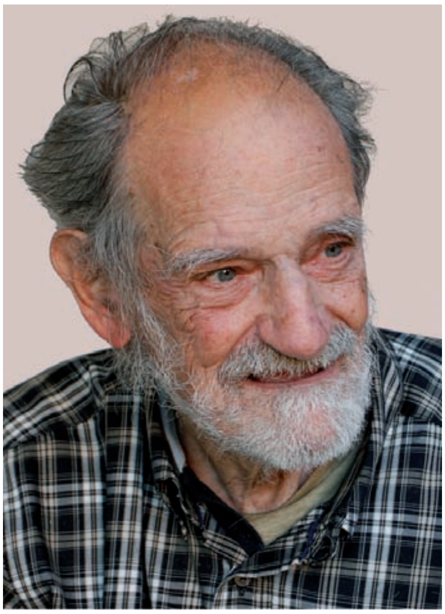
Figuur 2 Optimale netwerken tot en met $n = 7$.

De optimale netwerken zijn nu minder eenvoudig te beschrijven. Figuur 2 toont de optimale netwerken tot en met $n = 7$ personen.

Centraliteit in een netwerk

Naast de structuur van verborgen netwerken is het ook van belang te bepalen welke knopen cruciaal zijn. Welke individuen moeten in de gaten worden gehouden? Het is onmogelijk om iedereen te surveilleren dus moet er een selectie worden gemaakt. Hoe meet men het belang van een knoop in een netwerk? Een van de eerste onderzoe-

Kurt Lewin (1890–1947) was een van de grondleggers van de sociale psychologie. Hij introduceerde het begrip groepsdynamica. Zijn student Alex Bavelas probeerde dit in de praktijk meetbaar te maken.



Lloyd Shapley (1923–2016) was een Amerikaans wiskundige. Hij kreeg de Nobelprijs voor de economie in 2012 vanwege zijn werk aan coöperatieve speltheorie. Deze theorie raakt aan combinatorisch optimaliseren. Een bekend voorbeeld is de Edmonds–Shapley-stelling over het basispolyeder van een submodulaire functie. In coöperatieve speltheorie representeert dit polyeder alle 'redelijke' verdelingen van $v(N)$. Het heet de *core* van het spel.

kers die zich dit afvroeg was Alex Bavelas, een socioloog van MIT die grafentheorie gebruikte om groepen te analyseren [2,3]. Hij definieerde de centraliteit van een knoop als de reciproke waarde van de gemiddelde afstand tot alle andere knopen. Sindsdien zijn er veel van dit soort *centraliteitsmaten* gedefinieerd, een bekend voorbeeld is de PageRank. De meeste centraliteitsmaten zijn niet bruikbaar voor de analyse van verborgen netwerken, omdat ze te veel kennis van het netwerk eisen. Hier presenteren we een benadering van centraliteit via de *coöperatieve speltheorie*.

Een coöperatief spel kan worden gedefinieerd als een paar (N,v), waarbij N de verzameling spelers is en v een functie die een waarde $v(S)$ toekent aan elke coalitie $S \subset N$. Vaak worden extra eisen opgelegd aan v. Het is gebruikelijk dat $v(\emptyset)=0$ en dat v monotoon is, dat wil zeggen, $v(A) \leq v(B)$ als $A \subset B$. Daarmee is de waarde van de grote coalitie N de maximaal haalbare opbrengst. De kernvraag is dan hoe $v(N)$ moet worden verdeeld over alle spelers. Met andere woorden, wat is de individuele bijdrage van elke speler aan $v(N)$. Lloyd Shapley stelde voor om deze waarde als volgt uit te rekenen [17]. Laat π een random permutatie van N zijn. Met andere woorden, zet de spelers random op een rij. Speler i staat op plaats $\pi(i)$ en speler j staat voor speler i als $\pi(j) < \pi(i)$. Definieer nu $F(i)$ als de verzameling spelers die voor i staan. De marginale bijdrage van i in deze permutatie π is $m_i^\pi(v) = v(F(i) \cup \{i\}) - v(F(i))$. De *Shapley-waarde* van i is dan de verwachte marginale bijdrage van speler i. Ofwel, de gemiddelde marginale bijdrage van i wanneer we alle mogelijke permutaties beschouwen. In formule, voor alle $i \in N$,

$$\phi_i(N,v) = \frac{1}{n!} \sum_{\pi \in \Pi(N)} m_i^\pi(v),$$

waarbij $\Pi(N)$ de verzameling van alle permutaties van N is.

Om een waarde v aan iedere coalitie S toe te kennen, kiezen we een functie v die het onderliggende netwerk, de personen in het netwerk en de aanwezige informatie over personen en relaties meeneemt. In [12] wordt een gewogen graaf met gewichten w_i op de knopen en k_{ij} op de zijden beschouwd. Om deze gewichten mee te kunnen nemen in de analyse is gekozen voor het definiëren van een zogenaamde *weighted connectivity game* op de gewogen graaf.

Als de coalitie $S \subset N$ samenhangend is, dus alle personen in de coalitie kunnen direct of indirect met elkaar communiceren, dan definiëren we

$$f(S) = \left(\sum_{i \in S} w_i \right) \cdot \max_{ij \in E_S} k_{ij},$$

anders is $f(S) = 0$. Definieer nu $v(S) = \max_{T \subset S} f(S)$. Ofwel, kies een samenhangende coalitie binnen S met de hoogste waarde $f(T)$. Als centraliteitsmaat voor persoon i kunnen we dan de Shapley-waarde van deze persoon berekenen.

In dit model moeten de gewichten op een of andere manier worden bepaald uit gegevens, zoals individuele vaardigheden, financiën, frequentie van communicatie en dergelijke. Dit is het werk voor analisten van de veiligheidsdienst.

Shapley-waarde toegepast op Al Qaida

De berekening van de Shapley-waarde kan soms lastig zijn afhankelijk van het spel. De reden is dat het aantal permutaties exponentieel toeneemt. Bijvoorbeeld, voor een spel met 50 spelers ($n = 50$) heeft een redelijk snelle computer al jaren nodig om de Shapley waarde te berekenen. Bij 100 spelers ($n = 100$) is er geen enkele computer op aarde die de Shapley waarde kan vinden binnen duizenden jaren.

Echter, soms heeft een spel een mooie structuur. Dit is gelukkig ook hier het geval. Echter de wiskunde voor deze methode gaat iets te ver om in dit artikel te vertellen. Er wordt bij deze methode gebruikgemaakt van de *treewidth* van een netwerk. Als deze niet al te groot is, en dat is het geval voor dit Al Qaida netwerk, dan kunnen we de Shapley waarde snel en exact uitrekenen [23].

Het terroristisch netwerk van de aanslag van 9/11 bestond uit 69 spelers. In Tabel 1 staan de 15 leden met de hoogste waarde.

De top 10 bevat bekende namen zoals Mohamed Atta (piloot van vlucht 11, WTC

Ranking	Naam	Geschatte Shapley-waarde
1	Mohamed Atta	0,114099473
2	Essid Sami Ben Khemais	0,111249806
3	Hani Hanjour	0,110702087
4	Djamal Beghal	0,107273424
5	Khalid Almihdhar	0,107153568
6	Mahmoun Darkazanli	0,106635302
7	Zacarias Moussaoui	0,101188122
8	Nawaf Alhazmi	0,099594346
9	Ramzi Bin al-Shibh	0,098434678
10	Raed Hijazi	0,094777059
11	Hamza Alghamdi	0,008901234
12	Fayez Ahmed	0,008790340
13	Marwan Al-Shehhi	0,004533725
14	Satam Suqami	0,003693424
15	Saeed Alghamdi	0,003666945

Tabel 1 De vijftien leden van het 9/11-netwerk met de hoogste Shapley-waarde.

De vier kopstukken achter de 9/11-aanslag, volgens de coöperatieve speltheorie.

North), Hani Hanjour (piloot van vlucht 77, Pentagon), Khalid Almihdhar and Nawaf Alhazmi (beiden kapers van vlucht 77). Zacarias Moussaoui, die werd gearresteerd voor de WTC aanval plaats vond en die bekend staat als de twintigste kaper, staat ook in de top 10. Naast de actieve leden, de piloten en de kapers, staan ook andere leden van het netwerk als Essid Sami Ben Khemais en Djamal Beghal in de top 10. De eerste was hoofd operaties voor Al-Qaida in Italië en de tweede was betrokken bij aanslagen in Frankrijk. Beiden zijn geïdentificeerd door de Amerikaanse overheid als organisatoren van aanvallen op diverse Amerikaanse ambassades.

Slot

In dit artikel zijn we kort ingegaan op de bijdrage die wiskundige modellen kunnen leveren aan de kwantitatieve analyse van terroristische netwerken. Het grote probleem met dit soort heimelijke netwerken, net zoals heimelijke criminele en andersoortige netwerken, is dat ze in de schaduw opereren en zodanig hun structuur, communicatiepatronen en *modus operandi* hebben ingericht. Elementen uit de coöperatieve speltheorie zijn de revue gepasseerd en het nut ervan in deze context is geïllustreerd. Zowel in het geval dat er geen of onvoldoende complete informatie over dergelijke netwerken beschikbaar is en voor de analyse van deze incomplete informatie kunnen technieken als Nash-onderhandeling en speltheoretische centraliteit ingezet worden. Deze technieken ondersteunen de inlichtingenanalist bij het complexe besluitvormingsproces over heimelijke organisaties: wat is de meest waarschijnlijke organisatievorm van een dergelijk netwerk? Welke personen moeten (meer) onder surveillance komen? Hoe kunnen we beter zicht krijgen op heimelijke netwerken en hoe destabiliseren wij ze? De heterogene en incomplete data die dergelijke heimelijke netwerken genereren kunnen niet alleen handmatig en kwalitatief geanalyseerd en geduid worden. Daarvoor is het probleem te diffuus. Modellen uit de speltheorie en netwerkanalyse leveren belangrijke bouwstenen voor de data-analyse ten behoeve en bevordering van het inlichtingenproces.

Referenties

1 C. Ballester, A. Calvó-Armengol en Y. Zenou, Who's who in networks. Wanted: the key player, *Econometrica* 74(5) (2006), 1403–1417.

2 A. Bavelas, A mathematical model for group structures, *Applied Anthropology* 7 (1948), 16–30.

3 A. Bavelas, Communication patterns in task-oriented groups, *The Journal of the Acoustical Society of America* 22 (1950), 725–730.

4 S.P. Borgatti en M.G. Everett, A graph-theoretic framework for classifying centrality measures, *Social Networks* 28 (2006), 466–484.

5 K.M. Carley, J. Reminga, N. Kamneva, Destabilizing terrorist networks, in: *NAACSOS Conference Proceedings*, Pittsburgh, 2003.

6 W. Enders en X. Su, Rational terrorists and optimal network structure, *Journal of Conflict Resolution* 51(1) (2007), 33–57.

7 J.D. Farley, Breaking Al Qaeda cells: a mathematical analysis of counterterrorism operations, *Studies in Conflict and Terrorism* 26 (2003), 399–411.

8 B. Jasny en B. Ray, Life and the art of networks, *Science* 301 (2003), 1863.

9 T.H. Kean, L.H. Hamilton, R. Ben-Veniste, B. Kerrey, F.F. Fielding, J.F. Lehman, J.S. Gorelick, T.J. Roemer, S. Gorton en J.R. Thompson, *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks upon the United States*, W.W. Norton and Company, 2002.

10 V.E. Krebs, Uncloaking terrorist networks, *First Monday* 7 (2002), 1–10.

11 R.H.A. Lindelauf, P. Borm en H. Hamers, The influence of secrecy on the communication structure of covert networks, *Social Networks* 31 (2009), 126–137.

12 R. Lindelauf, H.J.M. Hamers en B.G.M. Husslage, Game theoretic centrality analysis of terrorist networks: the cases of Jemaah Islamiyah and Al Qaeda, *European Journal of Operational Research* 229(1) (2013), 230–238.

13 G. McCormick en G. Owen, Security and coordination in a clandestine organization, *Mathematical and Computer Modelling* 31(6–7) (2000), 175–192.

14 C. Morselli, C. Giguère en K. Petit, The efficiency/security trade-off in criminal networks, *Social Networks* 29(1) (2007), 143–153.

15 J. Nash, Two person cooperative games, *Econometrica* 21 (1953), 128–140.

16 M.E.J. Newman, Analysis of weighted networks, *Physical Review E* 70 (2004), 56–131.

17 L. Shapley, A value for n-person games, *Annals of Mathematics Studies* 28 (1953), 307–317.

18 M. Sparrow, The application of network analysis to criminal intelligence: an assessment of the prospects, *Social Networks* 13 (1991), 251–274.

19 S. Strogatz, Exploring complex networks, *Nature* 410 (1991), 268–276.

20 D. Watts en S. Strogatz, Collective dynamics of 'small-world' networks, *Nature* 393 (1998), 440–442.

21 D. Watts, The 'new' science of networks, *Annual Review of Sociology* 30 (2004), 243–270.

22 G.L. Zacharias, *Behavioral Modeling and Simulation: From Individuals to Societies*, National Academy of Sciences, 2008.

23 T. van der Zanden, H. Bodlaender en H. Hamers, 'Efficiently computing the Shapley value of connectivity games in low-treewidth graphs', working paper, 2019.