



FACULTEIT
RECHTSGELEERDHEID

*Een vergelijkende studie tussen
georganiseerde misdaad en terroristische
groeperingen op vlak van organisatie en
financiering*

Masterproef neergelegd tot het behalen van
de graad van Master in de criminologische wetenschappen
door (01101783) Gosselin Nicolas

Academiejaar 2014-2015

Promotor :
Dr. Verhage Antoinette

Commissaris:
De Koker Cedric

Voorwoord

Deze masterproef kwam tot stand in het kader van de opleiding Criminologische Wetenschappen aan de Universiteit Gent, met als doelstelling een Masterdiploma in de Criminologische Wetenschappen te behalen.

In eerste instantie wens ik Doctor Antoinette Verhage te bedanken voor alle hulp die ze me heeft verleend doorheen dit jaar in het kader van de totstandkoming van deze masterproef. Ze heeft me bijgestaan door weer en wind en dit leidde tot een geweldig samenwerken.

Bijkomend wens ik elke respondent te bedanken die speciaal voor mij tijd heeft vrij gemaakt om hun expertise te kunnen verlenen in het kader van deze masterproef. Zonder hen zou deze masterproef niet het kwalitatieve niveau bereikt hebben dan dat het nu bezit.

Daarnaast wens ik ook journalist Jan Willems te bedanken die op regelmatige basis artikels doorstuurde via doctor Antoinette Verhage. Deze artikels gaven steeds een actuele kijk op de academische literatuur. Aansluitend wens ik ook Kim te bedanken om deze scriptie na te lezen op schrijffouten en op helderheid.

Verder wil ik mijn ouders bedanken voor alle steun en toeverlaat die ze me doorheen de vier jaren universiteit hebben verleend. Ze waren doorheen de jaren aanwezig bij de ups en downs en steunde me honderd procent bij de wegen die ik zelf wou inslaan.

Ten slotte wens ik Hanneke te bedanken voor alle steun die ze me verleende en voor alle momenten waarbij ze in mij geloofde. Haar aanwezigheid verlichtte alle zorgen en maakte van deze masterproef een prettige en voornamelijk interessante ervaring.

Trefwoorden

Terrorisme

Georganiseerde criminaliteit

Organisatie

Financiering

Gebruikte afkortingen

ADIV	Algemene Dienst Inlichting- en Veiligheid
AQAP	al-Qaida in the Arabian Peninsula
CFI	Cel voor Financiële Informatieverwerking
COT	Cel Organised Crime – Terrorism
CPI	Corruption Perceptions Index
DJF	Directie Economische en Financiële Criminaliteit
DJP	Directie van de Bestrijding van de Criminaliteit tegen Personen
DJSOC	Directie van de Bestrijding van Serious and Organised Crime
FGP	Federale Gerechtelijke Politie
FIU	Financial Intelligence Unit
IRA	Irish Republican Army
IS	Islamitische Staat
JIT's	Joint Investigation Teams
NAVO	Noord-Atlantische Verdragsorganisatie
OCAD	Coördinatieorgaan voor de Dreigingsanalyse
SHAPE	Supreme Headquarters Allied Powers Europe
PLO	Palestine Liberation Organization

Inhoudstafel

VERKLARING INZAKE TOEGANKELIJKHEID VAN DE MASTERPROEF CRIMINOLOGISCHE WETENSCHAPPEN	I
VOORWOORD	II
TREFWOORDEN	III
GEBRUIKTE AFKORTINGEN	IV
INHOUDSTAFEL	V
1. INLEIDING EN PROBLEEMSTELLING	1
2. METHODOLOGISCH LUIK	3
2.1 Centrale onderzoeksvragen en deelvragen	3
2.2 Doelstelling, Theoretische relevantie en praktische relevantie	3
2.3 Onderzoeksmateriaal, -strategieën en -technieken	5
2.3.1 Onderzoeksmateriaal	5
2.3.1.1 Interviews	6
2.3.1.2 Literatuurstudie	8
2.3.2 Onderzoeksstrategieën en -technieken	9
2.4 Validiteit, betrouwbaarheid en ethiek	11
2.5 De aanwezigheid van mogelijke beperkingen in deze scriptie	12
3. GEORGANISEERDE MISDAAD	15
3.1 Definiëring en inhoud van het begrip 'georganiseerde misdaad'	15
3.1.1 Definiëring van georganiseerde misdaad en haar aspecten	15
3.1.2 Politieke belangstelling voor georganiseerde misdaad	16
3.1.3 Beeldvorming van georganiseerde misdaad	17
3.2 De organisatie van georganiseerde misdaad	18
3.2.1 Rekrutering	18
3.2.2 Het netwerk binnen het criminele samenwerkingsverband	19
3.2.3 De hiërarchische orde	21
3.2.4 Samenwerking met gelijkende criminele organisaties	22
3.2.5 Het gebruik van corruptieve contacten en beïnvloeding	23
3.2.6 Het gebruik van rechtspersonen	26
3.2.7 Het gebruik van internet en media	27
3.2.8 Defensieve en offensieve contrastrategieën	28
3.2.8.1 Defensieve contrastrategieën	29
3.2.8.2 Offensieve contrastrategieën	30
3.2.8.3 Het categoriaal gebruik van afschermingsmethoden	31
3.2.8.3.1 Het gebruik van een valse identiteit	31
3.2.8.3.2 Het gebruik van ICT-middelen	32
3.2.8.3.3 Het gebruik van intimidatie en (bedreiging met) geweld	32
3.3 De financiering van georganiseerde misdaad	36
3.3.1 Insourcing en Outsourcing	36
3.3.2 Tussenkoms t van een derde partij	37
3.3.3 Symbiotische en parasitaire georganiseerde misdaad	38

3.3.3.1	Symbiotische georganiseerde misdaad.....	38
3.3.3.2	Parasitaire georganiseerde misdaad.....	39
3.3.4	Fraude en witwassen.....	39
4.	TERRORISME.....	41
4.1	<i>Definiëring en inhoud van het begrip ‘terrorisme’</i>	41
4.1.1	Definiëring van terrorisme en haar aspecten.....	41
4.1.2	Politieke belangstelling voor terrorisme.....	45
4.1.3	Beeldvorming van terrorisme.....	45
4.1.4	Soorten terrorisme.....	46
4.1.5	Foreign fighters.....	47
4.2	<i>De organisatie van terrorisme</i>	48
4.2.1	Rekrutering.....	48
4.2.2	Het netwerk binnen de terroristische groepering.....	54
4.2.3	De hiërarchische orde.....	58
4.2.4	Samenwerking met gelijkende terroristische groeperingen.....	58
4.2.5	Het gebruik van corruptieve contacten en beïnvloeding.....	59
4.2.6	Het gebruik van rechtspersonen.....	60
4.2.7	Het gebruik van internet en media.....	60
4.2.8	Defensieve en offensieve contrastrategieën.....	62
4.2.8.1	Defensieve contrastrategieën.....	62
4.2.8.2	Offensieve contrastrategieën.....	63
4.2.8.3	Het categoriaal gebruik van afschermingsmethoden.....	64
4.2.8.3.1	Het gebruik van een valse identiteit.....	64
4.2.8.3.2	Het gebruik van ICT-middelen.....	64
4.2.8.3.3	Het gebruik van intimidatie en (bedreiging met) geweld.....	64
4.3	<i>De financiering van terrorisme</i>	64
4.3.1	Tussenkomst van een derde partij.....	65
4.3.2	Bronnen van inkomsten.....	65
4.3.3	Fraude en witwassen.....	67
5.	EEN VERGELIJKING TUSSEN GEORGANISEERDE MISDAAD EN TERRORISME.....	68
5.1	<i>Op het vlak van organisatie</i>	68
5.2	<i>Op het vlak van financiering</i>	69
5.3	<i>Het samenkomen/samenwerken van georganiseerde misdaad en terrorisme</i>	70
6.	AANBEVELINGEN.....	73
6.1	<i>Aanbevelingen op lokaal niveau</i>	73
6.2	<i>Aanbevelingen op nationaal niveau</i>	76
6.3	<i>Aanbevelingen op Europees niveau</i>	84
6.4	<i>Aanbevelingen op academisch niveau</i>	90
6.5	<i>Aanbevelingen op inlichtingenniveau</i>	93
7.	CONCLUDEREND KADER.....	94
8.	BIBLIOGRAFIE.....	I
8.1	<i>Boeken</i>	i

8.2	<i>Bijdragen in verzamelwerken</i>	iii
8.3	<i>Tijdschriften</i>	vi
8.4	<i>Elektronische bijdragen</i>	viii
8.5	<i>Papieren mediaberichtgeving</i>	xvi
8.6	<i>Beleidsdocumenten en rapporten</i>	xvi
8.7	<i>Juridische bijdragen</i>	xvi
8.8	<i>Persoonlijke communicatie</i>	xvii
9.	BIJLAGEN	XVIII
9.1	<i>Figuren</i>	xviii
9.1.1	De drie basisvormen van netwerken van J. Arquilla & D. Ronfeldt (2001a).....	xviii
9.1.2	Boomdiagram van G. Löckinger (2005)	xix
9.2	<i>Interviewvragen inzake het lokale luik</i>	xx
9.3	<i>Interviewvragen inzake georganiseerde criminaliteit</i>	xxi
9.4	<i>Interviewvragen inzake terrorisme</i>	xxiv
9.5	<i>Questionnaire on the funding and organization of terrorism and organized crime</i>	xxvii

1. Inleiding en Probleemstelling

We leven in een dynamische geglobaliseerde wereld waar criminaliteit, al dan niet grensoverschrijdend, deel van uitmaakt (Onwudiwe, 2001; X, persoonlijke communicatie). Twee grensoverschrijdende criminaliteitsvormen, namelijk georganiseerde misdaad en terrorisme, komen dagelijks in beeld.

Georganiseerde misdaad is een complex verschijnsel, waar verscheidene criminaliteitsfenomenen onder gecategoriseerd kunnen worden. Voorbeelden zijn drugshandel, wapentrafiiek en mensenhandel (Dupuis, 2010). Dit criminaliteitsfenomeen komt in elke Belgische politiezone frequent voor (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). Sinds 1996 krijgt georganiseerde criminaliteit dan ook veel aandacht wat geleid heeft tot initiatieven als het ‘Actieplan tegen de georganiseerde criminaliteit’ (regering, 1996; Dienst voor Strafrechtelijk Beleid, 2015).

Terrorisme is een criminaliteitsfenomeen dat een grote impact teweeg bracht sinds 9/11 over de gehele wereld, maar waarschijnlijk al in één of andere vorm sinds mensenheugenis bestaat (Wright-Neville, 2010). Het is een fenomeen dat jaarlijks duizenden levens kost en ook na bijna vijftien jaar nog steeds razendactueel is. Als voorbeeld kunnen de cijfers rond de subgroep moslimterrorisme van professor Coolsaet (2004) een beeld geven over wat voor impact terrorisme heeft op de maatschappij. In een periode van elf september 2001 tot 2004 kwamen 7085 mensen om het leven en werden 10132 mensen gewond door een totaal van 393 aanslagen (Coolsaet, 2004). In 2013 vielen 18000 doden door terroristische aanvallen. Zesenzestig procent van het aantal doden viel door een aanslag van Islamitische Staat (IS), Boko Haram, al-Qaida en de Taliban (BVB & EVG, 2014).

Een actueel probleem binnen terrorisme is het fenomeen van *foreign fighters*. Bijna dagelijks komen *foreign fighters* in de media, door de praktijken die ze begaan en de wereld insturen. De laatste maanden was dit IS. Zij deinzen niet terug om regelmatig een duidelijk signaal de wereld in te sturen, via onthoofdingen van westerse personen, gaande van soldaten tot hulpverleners, op beeld vast te leggen (Bvb, 2014). Uit officiële cijfers van het ministerie van Binnenlandse Zaken wordt het aantal Belgische *foreign fighters* die naar Syrië reizen om te vechten aan de zijde van IS geschat op driehonderd à driehonderdvijftig zogenaemde ‘Syriëstrijders’ (Belga & RR, 2014).

Dit cijfer, dat sinds 2012 wordt bijgehouden, omvat zowel gedoodde Belgische Syriëstrijders, terug naar België gekeerde Syriëstrijders en Belgische Syriëstrijders die nog steeds residerende zijn te Syrië. Bij terugkomst in België worden deze Syriëstrijders gearresteerd of in het oog gehouden door de inlichtingendiensten, het parket of de lokale politie (Belga, 2014).

Deze twee grensoverschrijdende criminaliteitsvormen zijn niet lukraak gekozen om als onderwerp te dienen in deze scriptie, maar zijn beiden polycriminele structuren waartussen een soort kruisbestuiving bestaat. Terroristische groeperingen kunnen volgens de Dirjud van de FGP Bergen François Farcy enkel functioneren indien ze banden hebben met georganiseerde misdaadmilieus. Die kunnen er zijn om tal van redenen, zoals het bemachtigen van wapens, geld en valse papieren (Dupuis, 2010; Farcy, persoonlijke communicatie).

De probleemstelling die in deze scriptie centraal staat, is de volgende:

Wanneer we ervan uit gaan dat georganiseerde criminaliteit en terrorisme wellicht onderling verbonden zijn, valt op dat ze beiden onderzoeksmatig amper aan elkaar worden gelinkt. Dit vertaalt zich ook naar de praktijk. Binnen Belgische politie worden georganiseerde criminaliteit en terrorisme voornamelijk fenomeengericht benaderd, waarbij de fenomenen worden opgesplitst in aparte politionele cellen, namelijk DJSOC voor georganiseerde criminaliteit en DGJTerro voor terrorisme. Als beide fenomenen met elkaar verbonden zijn, zouden we mogelijk kennis over beide fenomenen met elkaar kunnen verbinden wat bijgevolg kan leiden tot een kennisvergroting en een betere bestrijding. Dit trachten we te benaderen door te kijken of er gemeenschappelijke kenmerken voorkomen tussen georganiseerde criminaliteit en terrorisme en welke aanbevelingen uit de literatuur en de interviews voorkomen.

2. Methodologisch luik

2.1 Centrale onderzoeksvragen en deelvragen

Hierbij focust deze masterproef zich op volgende onderzoeksvragen, met name:

- 1. Wat is en omvat georganiseerde misdaad?
 - 1a. Hoe is georganiseerde misdaad doorgaans georganiseerd?
 - 1b. Hoe ziet de financiering van georganiseerde misdaad eruit?
- 2. Wat is en omvat terrorisme?
 - 2a. Hoe is terrorisme doorgaans georganiseerd?
 - 2b. Hoe ziet de financiering van terroristische groeperingen eruit?
- 3. Wat zijn de vergelijkingen en verschillen tussen georganiseerde misdaad en terroristische groeperingen?
- 4. Komen hierbij aanbevelingen naar voren op lokaal, federaal en inlichtingenniveau inzake het bestrijden van beide criminaliteitsfenomenen?

2.2 Doelstelling, Theoretische relevantie en praktische relevantie

Het doel van deze thesis is om tot een geheel te komen van bestaande kennis en nieuwe kennis over de financiering en organisatie van criminele samenwerkingsverbanden en terroristische groeperingen. Hieruit kunnen vervolgens aanbevelingen getrokken worden die als hulpmiddel kunnen fungeren in de strijd tegen georganiseerde misdaad en terrorisme. De bevindingen van deze studie worden waar mogelijk getoetst aan IS, waardoor een vergelijking ontstaat tussen academische literatuur en nieuwe, moderne terroristische groeperingen.

De theoretische relevantie van deze thesis is om op basis van literatuur en interviews te kijken naar welke lessen er getrokken kunnen worden naar aanpak ter bestrijding van georganiseerde misdaad en terroristische groeperingen. We vertrekken hier dus niet vanuit een bepaalde theoretische stroming of criminologische theorie. Daarnaast wordt via deze scriptie duidelijk hoe terroristische groeperingen en criminele samenwerkingsverbanden financieren en zich organiseren aan de hand van een literatuurstudie en interviews. Door een literatuurstudie af te toetsen tegenover interviews, kan mogelijks nieuwe kennis ontstaan rond de twee criminaliteitsfenomenen. Deze scriptie vormt daardoor een bijdrage aan de criminologische kennis over dergelijke groeperingen. Ten slotte vormen de aanbevelingen voor het academisch niveau een mogelijk vertrekpunt voor verder onderzoek naar beide criminaliteitsfenomenen en hun onderlinge verband.

De praktische relevantie van deze scriptie ligt op lokaal, nationaal, inlichtingen- en Europees gebied. Uit de literatuurstudie en de kennis die naar voren komt uit de interviews, worden aanbevelingen getrokken op deze vier niveaus, zodat beleidsmakers op lokaal, nationaal en Europees niveau deze aanbevelingen kunnen implementeren in hun beleidsplan met als doel een hulpmiddel te vormen in de bestrijding van terrorisme en georganiseerde misdaad (Mortelmans, 2010). Daarnaast zijn deze aanbevelingen ook interessant voor inlichtingendiensten, zowel burgerlijk als militair. Inlichtingendiensten kunnen deze aanbevelingen meenemen in hun bestrijdingsstrategie. Deze relevantie bleek ook uit de interesse die de Algemene Dienst Inlichting- en Veiligheid (ADIV) had in deze scriptie. Deze interesse en relevantie zijn niet verwonderlijk omwille van vier redenen.

Ten eerste bevinden een groot aantal gebouwen van de Europese Unie, het hoofdkwartier van de Noord-Atlantische Verdragsorganisatie (NAVO) en het centrale commandocentrum van het militair personeel van de NAVO, oftewel *Supreme Headquarters Allied Powers Europe* (SHAPE), zich in België. De aanwezigheid van deze gebouwen verhogen de kans op aanslagen in België.

Ten tweede kan IS op veel steun rekenen vanuit België. *Voices from the Blogs*, een Italiaanse onderzoeksgroep verbonden aan de universiteit van Milaan, deed een onderzoek naar berichtgeving op sociale media rond IS. Van de onderzochte twee miljoen berichten op sociale netwerksites, is éénendertig procent van de berichten afkomstig uit België positief over IS (Voices from the Blogs, 2014; Tack, 2014). Dit cijfer ligt beduidend hoger dan onze buurlanden. Nederland verstuurt 12,5 procent positieve berichten over IS via sociale media, Duitsland 15,7 procent en Frankrijk 20,8 procent (Voices from the Blogs, 2014). Dit verontrustend fenomeen ontgaat ook andere Europese landen niet. Volgens cijfers van de Verenigde Naties zijn er al meer dan vijftienduizend *foreign fighters* naar Syrië en Irak getrokken om te strijden aan de zijde van IS (Bajekal, 2014). Daarom is er intussen een systematische uitwisseling van gegevens inzake Syriëstrijders gekomen tussen enkele Europese landen die zwaar getroffen worden in het aantal landgenoten die naar Syrië trekken om te vechten aan de zijde van IS (Belga, 2014).

Ten derde leidt het wegvallen van de grenzen binnen de Europese Unie tot een verhoogde mobiliteit, waar ook rondtrekkende dadergroepen gebruik van maken. Doordat België een klein land is waarbij je slechts in enkele uren in het buitenland zit, is België een perfect doelwit voor vormen van georganiseerde criminaliteit. Het Federaal Parket en de ‘Centrale Directie van de strijd tegen de criminaliteit tegen goederen’ van de Federale Politie besteden vanuit het strafrechtelijk beleid aandacht aan dit fenomeen via een gecentraliseerde aanpak (Van Daele & Vander Beken, 2010). De aanpak van rondtrekkende dadergroepen is opgenomen in een lijst van acht Europese prioriteiten in de strijd tegen georganiseerde misdaad met als doel het aantal criminele activiteiten die rondtrekkende dadergroepen ontplooien, te verminderen (Siegel, 2014).

Ten vierde is het aantal personen dat overleden is door terroristische aanslagen een verontrustend cijfer. Sinds de eerste waarnemingen in 2000 zijn het aantal slachtoffers van terroristische aanslagen en het aantal terroristische aanslagen nog nooit zo hoog geweest als in het jaar 2013 (BVB et al., 2014).

2.3 Onderzoeksmateriaal, -strategieën en –technieken

2.3.1 Onderzoeksmateriaal

In het theoretisch kader wordt ten eerste ingegaan op de beeldvorming, organisatie en financiering van georganiseerde criminaliteit. Ten tweede wordt ingegaan op de beeldvorming, organisatie en financiering van terroristische groeperingen. Ten derde wordt geanticipeerd op vergelijkingen en verschillen inzake organisatie en financiering tussen georganiseerde criminaliteit en terrorisme en wordt gekeken naar een mogelijk verband tussen beiden fenomenen. Ten vierde komen aanbevelingen naar voren inzake aanpak van beide criminaliteitsfenomenen. Ten slotte volgt een concluderend kader.

Deze thesis komt tot stand via basic intelligence, namelijk via onderzoek op basis van open bronnen. Deze open bronnen zijn literatuur en interviews met respondenten uit de professionele en academische wereld.

2.3.1.1 Interviews

In deze scriptie gebruiken we als interviewvormen de half gestructureerde interview en het e-mailinterview. Bij de halve gestructureerde interviews liggen de onderwerpen op voorhand al vast, maar de vragen niet. Door middel van een open beginvraag en open doorvragen worden de onderwerpen uitgediept. Een logische volgorde ligt vaak op het begin al vast aan de hand van een topiclijst. Echter is de onderzoeker vrij om de volgorde van de onderwerpen aan te passen indien dit in het gesprek beter uitkomt. De onderwerpen dienen wel allemaal behandeld te worden (Reulink & Lindeman, 2005). In ons onderzoek kwamen drie topiclijsten voor, namelijk het lokale luik, georganiseerde criminaliteit en terrorisme. Deze drie topiclijsten zijn te vinden in hoofdstuk 9 ‘bijlagen’.

Door middel van doorvragen, oftewel ‘*probing*’, wordt het gesprek in een bepaalde richting gestuurd. Dit doorvragen gebeurt in het geval een onduidelijk of onvolledig antwoord werd gegeven, het antwoord niet in gaat op de gestelde vraag en wanneer het vermoeden bestaat dat het antwoord op de gestelde vraag een sociaal wenselijk antwoord is (Beyens & Tournel, 2010).

Tijdens het onderzoek dat deze scriptie voorafgaat zal zoveel mogelijk ingezet worden op *face-to-face* interviews. Toch kan het voorkomen dat *face-to-face* interviews niet mogelijk zijn wanneer het op afstand aankomt. Sommige respondenten wonen namelijk in het buitenland waarbij reizen niet altijd een optie blijkt te zijn door een gebrek aan geld en tijd. Een oplossing hiervoor zijn interviews via Skype om toch te komen tot een virtuele versie van een *face-to-face* interview. Dit gebeurt enkel wanneer de respondent hier open voor staat. Bij e-mail interviews wordt er gestart met een korte vragenlijst elektronisch te versturen naar de respondent. Na het antwoord van de respondent, wordt er wederom een e-mail verstuurd met enkele bijkomende vragen. Op deze manier proberen e-mail interviews een interactief effect teweeg te brengen, wat neerkomt op een uitwisseling van e-mails (Flick, 2010).

De interviews worden afgenomen op een vertrouwelijke wijze. Om tegemoet te komen aan de geïnformeerde toestemming, oftewel ‘*informed consent*’, wordt aan de respondent op het begin van het interview mondeling meegedeeld dat hij/zij recht heeft op anonimiteit en op controle van de transcriptie. Hierdoor weet de respondent ten eerste in eer en geweten dat hij/zij alles kan vertellen zonder repercussies door zijn/haar mogelijke keuze voor anonimiteit en ten tweede dat hij/zij weet heeft dat het interview op een vertrouwelijke wijze wordt afgenomen (O’Gorman & Vander Laenen, 2010).

Deze geïnformeerde toestemming houdt in dat aan de respondent voldoende en gepaste informatie over de aard en het doel van het onderzoek wordt verschaft, waardoor de respondent een bewuste keuze kan maken om al dan niet deel te nemen aan dit onderzoek. Dit gebeurt niet aan de hand van een ‘*informed consent*’ formulier waarbij een handtekening van de respondent vereist is. In deze scriptie wordt de raad van de *American Anthropological Association* gevolgd die stelt dat de kwaliteit van de toestemming relevant is, en niet de vorm. Het is de bedoeling om de relatie die opgebouwd wordt tussen respondent en interviewer niet af te breken door een officiële handeling zoals het handtekenen van een formulier. Daarnaast kan het handtekenen van een formulier het vertrouwen bij de respondent tenietdoen, doordat de respondent twijfelt aan de anonimiteit die dit onderzoek wenst te garanderen (O’Gorman et al., 2010).

Indien de respondent aanwijst dat bepaalde commentaar niet opgeschreven mag worden, dient de interviewer zich aan deze keuze te houden. Op het einde van elk interview wordt toelating aan de participant gevraagd om zijn/haar naam en/of functie te vermelden doorheen de scriptie en in de bibliografie onder het onderdeel 8.8 ‘persoonlijke communicatie’. Een respondent kan verscheidene redenen hebben om anoniem te willen blijven. Zo kan hij/zij gebonden zijn aan beroepsgeheim of bang zijn om imagoschade te lijden door zijn/haar bijdrage. Indien hij/zij anoniem wenst te blijven, wordt hij/zij doorheen de scriptie en in de bibliografie onder het onderdeel 8.8 ‘persoonlijke communicatie’ aangeduid als ‘X’. Dit zonder de toekenning van een cijfer aan de ‘X’ om volledige anonimiteit te garanderen. Doorheen de scriptie zal vervolgens ook geen data vermeld worden wanneer het interview is afgenomen, om een optimale anonimiteit te verzekeren. Naar hem/haar zal doorheen de scriptie verwezen worden als ‘(X, persoonlijke communicatie)’.

Van elk interview wordt een transcriptie gemaakt, die vervolgens naar de respondent elektronisch wordt toegestuurd. De respondent heeft met andere woorden de mogelijkheid de transcriptie na te lezen, goed te keuren of aan te passen vooraleer het wordt geïmplementeerd in deze scriptie. Op deze wijze krijgt de respondent een grotere vrijheid over de inhoud van het gesprek en kan de respondent zeker zijn dat zijn/haar woorden op de juiste manier worden begrepen. De transcripties van de interviewgesprekken werden niet opgenomen in de bijlagen. Dit is een extra maatregel om de anonimiteit voor de respondent te garanderen.

Elke transcriptie citeert de respondent nooit letterlijk, aangezien het interviewgesprek niet wordt opgenomen. Deze keuze is gevallen wanneer bleek dat veel respondenten niet wensten dat het interview werd opgenomen met een recorder, om achteraf problemen inzake interpretatie en “Ik heb dit nooit gezegd” – “Maar het staat op recorder” -toestanden te vermijden. Deze werkwijze zou in het ergste geval kunnen leiden tot imagoschade. Daarom is de bewuste keuze gemaakt om alles te noteren op papier, met als gevolg dat alle transcripties geen letterlijke citering zijn van de respondent. Een oplossing hiervoor is bovenvermelde procedure inzake transcripties. Door de respondent macht te geven over de inhoud van de transcriptie en de kans te geven alle interpretatiefouten te verbeteren, leunen de transcripties dicht aan bij de citaten van de respondenten.

Daarnaast wordt na elk interview aan de respondent gevraagd of hij/zij personen kent die vanuit een praktisch of academisch kader kunnen bijdragen aan deze scriptie. Door op deze manier te werken, vertrouwen we op het principe van de sneeuwbalmethode.

Deze toepassing op *face-to-face* interviews wordt ook toegepast op interviews die in de vorm van e-mail interviews verlopen. De geïnformeerde toestemming is in dit geval de eerste e-mail naar de respondent.

2.3.1.2 Literatuurstudie

De literatuurstudie dat deze scriptie voorafgaat omvat verscheidene soorten bronnen. Om te komen tot een duidelijke en nauwkeurige scriptie, is de bibliografie onderverdeeld in meerdere onderverdelingen. Één daarvan is de persoonlijke communicatie die hierboven werd beschreven. De andere onderverdelingen zijn: boeken, bijdragen in verzamelwerken, tijdschriften, elektronische bijdragen, beleidsdocumenten en rapporten, juridische bijdragen en papieren mediaberichtgeving. Door middel van deze onderverdelingen is het voor de lezer van deze scriptie overzichtelijker om bronnen te raadplegen in de bibliografie. Bijkomend hebben de onderverdelingen tot doel een duidelijke scheidingslijn aan te brengen tussen academische bronnen en andere bronnen. Evenwel komt deze scheidingslijn niet tot zijn recht in de onderverdeling ‘elektronische bijdragen’. Dit komt door de toenemende hoeveelheid academische literatuur die te vinden is via het internet.

De bronnen uit de literatuurstudie worden op enkele manieren verworven. De eerste manier is via het gebruik van de website lib.ugent.be. Via deze website maakt deze scriptie gebruik van het materiaal dat aanwezig is in de bibliotheken van de Universiteit Gent en op materiaal waarop de Universiteit Gent een elektronisch abonnement heeft. De tweede manier is het gebruik van scholar.google.com. Via deze academische zoekmachine rakelt deze scriptie materiaal op die niet te raadplegen is via de Universiteit Gent. Een derde manier is via mediaberichtgeving afkomstig van de meest kwalitatieve nationale en internationale kranten. Een vierde manier bestaat uit het opzoeken van rapporten, wetteksten en beleidsdocumenten afkomstig van de sites van nationale, Europese en internationale instellingen. Een vijfde manier is informatie die verkregen wordt via interviews of die worden verkregen van journalist Jan willems.

2.3.2 Onderzoeksstrategieën en -technieken

Deze thesis is eerder een verkennend onderzoek, waarbij geen duidelijke link bestaat met een bepaalde criminologische stroming. Het is eerder exploratief, wat af te leiden valt door het gebruik van 'wat-vragen' bij de onderzoeksvragen. De interesse van de ADIV is een aanwijzing van de noodzakelijkheid om meer kennis te bekomen omtrent het onderwerp. Deze noodzaak aan meer kennis over een bepaald onderwerp, is een belangrijk kenmerk van exploratief onderzoek (Mortelmans, 2010).

Echter behoort deze scriptie ook tot een vorm van emancipatorisch onderzoek. Deze scriptie wenst namelijk hulpmiddelen aan te reiken, onder de vorm van aanbevelingen, om een probleem aan te pakken, namelijk georganiseerde criminaliteit en terrorisme. Op deze manier probeert deze scriptie een bijdrage te leveren aan sociale actie, waarbij sociale verandering de doelstelling vormt (Mortelmans, 2010).

De primaire gerichtheid, oftewel de functie, van dit onderzoek is praktijkgericht. Het onderzoek probeert een fase in het praktisch handelen te ondersteunen, door namelijk de problemen rond georganiseerde misdaad en terroristische groeperingen op vlak van organisatie en financiering in kaart te brengen en vanuit deze gegevens aanbevelingen te formuleren als hulpmiddel voor de bestrijding van georganiseerde misdaad en terroristische groeperingen vanuit lokaal, nationaal, Europees en inlichtingenniveau (Stokking, 2003). Dit onderzoek is dan ook bedoeld voor beleidsmakers, met name overheden, én praktijkmensen, met name inlichtingendiensten en politie (Mortelmans, 2010).

Dit onderzoek wordt benaderd vanuit een kwalitatief luik. Van de vijf belangrijkste strategieën die Verschuren en Doorewaard (2007) hebben uitgewerkt, komen twee strategieën in deze scriptie aan bod, namelijk het bureauonderzoek en de casestudie. Het bureauonderzoek is de strategie die in deze scriptie wordt toegepast op georganiseerde misdaad en terroristische groeperingen. De onderzoeker gebruikt bij deze onderzoeksstrategie bestaande informatie die al bewerkt is door anderen. Met dit materiaal probeert de onderzoeker te reflecteren en tot nieuwe inzichten te komen. Dit gebeurt aan de hand van een literatuuronderzoek (Verschuren et al., 2007; Decorte & Tieberghien & Petintseva, 2014).

Bijkomend komt een tweede strategie in deze scriptie naar voren. De tweede strategie, namelijk de vergelijkende casestudie, bekijkt in diepte de moderne terroristische groepering IS en wordt doorheen het hoofdstuk terrorisme behandeld. Deze tweede strategie vormt samen met de interviews het empirisch onderzoek van deze scriptie. Dit luik zoekt inzicht te krijgen in enkele tijdruimtelijk begrensde processen, namelijk de financiering en organisatie bij IS en deze tegelijkertijd te vergelijken met de academische literatuur hierover. De probleemstelling die in dit luik geldt is de vraag of de aanbevelingen toepasbaar op het bureauonderzoek en de interviews, ook gelden voor nieuwe terroristische groeperingen zoals IS en of ook daar samenhang is met georganiseerde criminaliteit.

Deze scriptie bevat met andere woorden een mengvorm van onderzoeksstrategieën. Zowel bureauonderzoek als de casestudie zijn vormen van kwalitatief onderzoek. Daarnaast zijn beide onderzoeksstrategieën ook toepasbaar in een praktijkgericht project (Verschuren et al., 2007; Decorte et al., 2014).

Zoals aangehaald in 2.3.1 “onderzoeksmateriaal”, zijn de methoden van gegevensverzameling de literatuurstudie en interviews. De bedoeling is om de literatuurstudie en de kennis verworven uit de interviews samen te brengen tot één geheel waarbij de literatuurstudie kan getoetst worden aan de kennis verworven uit de interviews en vice versa. De transcripties voortkomende uit de verworven interviews worden gelabeld aan de hand van enkele ‘*labels*’ oftewel onderwerpen. De gelabelde informatie wordt vervolgens vergeleken met de informatie afkomstig uit de literatuurstudie. Op deze manier wordt de bestaande informatie getoetst aan nieuwe informatie afkomstig van mensen uit de academische en praktijkwereld.

2.4 Validiteit, betrouwbaarheid en ethiek

Kwalitatieve onderzoekers hebben de betekenis van interne validiteit, namelijk de geloofwaardigheid van causale proposities, uitgebreid naar de algemene vraag of de uitspraken die de onderzoeker formuleert overeenkomen met een bepaalde ‘waarheidswaarde’ (Maesschalck, 2010). De interviews met respondenten uit de academische en praktijkwereld trachten deze interne validiteit te verhogen.

De externe validiteit bij de casestudie is niet aanwezig, aangezien er bij kwalitatief onderzoek niet kan worden gegeneraliseerd (Maesschalck, 2010). De casestudie, met name IS, wordt vergeleken met de veelvoorkomende kenmerken die voortkomen uit het bureauonderzoek. Evenwel dient bij het lezen deze scriptie steeds rekening gehouden te worden dat elke criminele of terroristische organisatie onderling kan verschillen op talrijke manieren. Elke organisatie is uniek, maar zal wel gemeenschappelijke kenmerken vertonen met andere organisaties.

Betrouwbaarheid is de stabiliteit van verschillende metingen van hetzelfde fenomeen. Binnen deze algemene term verwijst interne betrouwbaarheid naar de mate waarin ‘andere’ onderzoekers, in deze scriptie onderzoekers die niets met het onderzoek te maken hebben, tot dezelfde conclusies komen op basis van dezelfde data die gebruikt wordt in deze scriptie (Maesschalck, 2010). Interne betrouwbaarheid zal bij deze scriptie aanwezig zijn, maar enkel in beperkte mate. De bekomen primaire data (lees: getranscribeerde interviews) kunnen door andere onderzoekers enkel worden opgevraagd onder bepaalde voorwaarden. De getranscribeerde interviews zijn geanonimiseerd indien de respondent vragende partij was anoniem te blijven in de scriptie. Daarnaast vereist de opvraging van transcripties de toestemming van de geïnterviewde respondent. Deze maatregel dient om de privacy van de respondent te respecteren en te beschermen. Doch verhoogt een gedetailleerde rapportering over de methodologische keuzes doorheen deze scriptie de interne betrouwbaarheid van deze thesis. Deze gedetailleerde rapportering is terug te vinden in puntje 2.3 “onderzoeksmateriaal, -strategieën en –technieken” van deze scriptie.

Bij externe betrouwbaarheid moet een onderzoeker op basis van nieuwe data, die verzameld werd in een nieuw onderzoek, komen tot dezelfde conclusies als deze scriptie. Een dergelijke reproduceerbaarheid is moeilijk bij kwalitatief onderzoek, door het originele karakter van de inhoud van de interviews (Maesschalck, 2010).

Aangezien elke interactie uniek is, kan de onderzoeker bijgevolg niet komen tot een perfect reproduceerbaar onderzoek. Het enige wat in deze scriptie kan helpen bij het verhogen van de externe betrouwbaarheid, is een gedetailleerde opsomming van de gebruikte methodologische keuzes, de gebruikte onderzoeksobjecten in zoverre dit mogelijk is inzake anonimiteit en de vragenlijsten opgenomen in de bijlagen van deze scriptie die gebruikt werden tijdens de interviews (Maesschalck, 2010).

Door het gebruik van een geïnformeerde toestemming en een gegarandeerde anonimiteit indien de respondent dit wenst, besproken in het onderdeel 2.3.1.1 “interviews”, houdt deze scriptie in voldoende mate rekening met de ethische aspecten van het kwalitatief onderzoek (O’Gorman et al., 2010).

2.5 De aanwezigheid van mogelijke beperkingen in deze scriptie

Er dient te worden stilgestaan bij enkele problemen die zich voor (kunnen) doen in deze scriptie. Een eerste probleem is van ethische en praktische aard. Mogelijk zal er informatie zijn die niet te vinden is in open bronnen, maar enkel in het bezit is van inlichtingendiensten en politie. Interviews met experts in de praktijkwereld trachten dit probleem gedeeltelijk op te lossen. Het probleem volledig oplossen zal niet lukken door het vereiste beroepsgeheim. Bepaalde informatie bekomen via interviews met inlichtingofficieren of met politiepersoneel valt onder het beroepsgeheim. Informatie die onder het beroepsgeheim valt, zal niet gebruikt worden in deze scriptie. Dit zou leiden tot een onethische toon doorheen deze scriptie.

Een tweede probleem vormt zich bij de casestudie rond IS. IS bestaat sinds de jaren negentig, maar kreeg pas recent enorme media-aandacht sinds bleek dat een groot aantal *foreign fighters* die naar Syrië vertrokken zijn om daar te strijden in de Jihad, uit West-Europa komen. Ook aan wetenschappelijke aandacht was er een gebrek, waardoor wetenschappelijk onderzoek naar IS beperkt is. Daardoor is de informatie rond IS grotendeels eenzijdig en voornamelijk afkomstig van mediaberichtgeving. Dit tekort aan wetenschappelijk materiaal kan in deze scriptie niet opgelost worden door interviews met Syriëstrijders. De redenen hiervoor zijn: (1) een tekort aan tijd, (2) een tekort aan zoekmiddelen bij het traceren van dergelijke individuen, (3) een tekort aan middelen en (4) het bestaan van een gevarenrisico.

Aansluitend kan de vraag gesteld worden of de criminelen/terroristen die bereid zijn om geïnterviewd te worden, typische daders zijn (Mahan & Griset, 2008). Een studie brengt namelijk hun werkwijze en strategieën in gedrang. In deze scriptie vormen de interviews met experts in het praktijkveld de primaire data, wat leidt tot een oplossing van dit probleem. Hun visie en ervaringen vergelijken met de beschreven academische literatuur kan leiden tot vergelijkingen of net tot een contrast.

Het niet voldoende uitdiepen van de casestudie IS kan een vierde probleem vormen. Door rekening te houden met het voorgaande bureauonderzoek, houdt deze casestudie ook enkel rekening met de aspecten organisatie en financiering. Door het beperkt aantal aspecten, kan volgens sommige onderzoekers geargumenteed worden dat de gevallen, in casu IS, niet diep genoeg onderzocht worden (Leys et al., 2010). Evenwel vinden we dat in deze scriptie geen noodzaak bestaat om meerdere aspecten te onderzoeken, aangezien in het bureauonderzoek enkel deze twee aspecten worden onderzocht. Rekening houden met meer aspecten dan organisatie en financiering zou de kwaliteit van dit onderzoek teniet doen en zou het onderzoek onnodig uitbreiden.

Een vijfde probleem kan voorkomen bij het gebruik van e-mail interviews. Door het gebruik van e-mails, en het bijgevolg gebrek aan persoonlijk contact, wordt het contextualiseren van de verklaringen bemoeilijkt (Flick, 2010). Aan de hand van persoonlijk contact worden verklaringen duidelijker door het gebruik van emoties en lichaamstaal. Dit probleem wordt opgelost door bijkomende vragen te stellen via e-mail. Daarnaast vervalt dit probleem bij het interviewen via Skype.

Intervieweffecten kunnen een zesde probleem vormen. Zo dient de onderzoeker tijdens de interviews op te letten voor sociaal wenselijk antwoordgedrag (Heldens & Reyssoo, 2005). Sociaal wenselijk antwoordgedrag kan mogelijk voorkomen uit de angst imagoschade te lijden door zijn/haar eigen mening te geven. Deze intervieweffecten worden ondervangen door een goede voorbereiding van elk interview, een vergelijking met de literatuurstudie en de mogelijkheid geanonimiseerd te worden doorheen deze thesis.

Een zevende beperking zit in de veralgemening. Elke vorm van criminaliteit kan nooit verpakt worden in één allesomvattend concept. Dat is ook één van de redenen waarom criminaliteit moeilijk is te vermijden door middel van een beleid. Veelal worden georganiseerde criminaliteit en terrorisme uitgelegd door een allesomvattende uitleg, en ook deze masterproef verschilt hier in zekere mate niet in. Ook al probeert deze masterproef de brede variëteit weer te geven, zal het nooit de volledige lading kunnen dekken. Dit is ook niet de bedoeling van deze masterproef, aangezien het tracht veelvoorkomende eigenschappen bij terrorisme en georganiseerde criminaliteit met elkaar te vergelijken. De lezer mag tijdens het lezen van deze masterproef dus niet vergeten dat terrorisme en georganiseerde criminaliteit een brede waaier aan soorten individuen en groepen inhouden die allen kunnen leiden tot verschillende acties (Tilly, 2005).

3. Georganiseerde misdaad

“When societies get organized, so too do their criminals, and organized crime has evolved as the shadowy underside of modernization and order.”

– James O. Finckenauer (2007, foreword)

3.1 Definiëring en inhoud van het begrip ‘georganiseerde misdaad’

3.1.1 Definiëring van georganiseerde misdaad en haar aspecten

Onderstaande definities van georganiseerde misdaad en haar aspecten worden gehanteerd doorheen deze scriptie. Aangezien criminologie een humane wetenschap is, zijn de definities sociale constructies die vaak niet universeel gedefinieerd zijn (Onwudiwe, 2001; Hagan, 2006). Daardoor is het van belang om in deze paragraaf duiding te geven wat exact wordt verstaan onder de kernbegrippen van georganiseerde misdaad in deze scriptie.

De term ‘georganiseerde misdaad’ bezit geen universele definitie (Onwudiwe, 2001; Hagan, 2006). Als synoniem wordt vaak ‘georganiseerde criminaliteit’ gebruikt. In deze scriptie gebruiken we daarom beide termen door elkaar. In deze thesis gebruiken we de definitie van Fijnaut, Bovenkerk, Bruinsma & van de Bunt uit de ‘Parlementaire Enquêtecommissie Opsporingsmethoden (PEO), Inzake opsporing: Enquête opsporingsmethoden’ van 1996, waarbij gesteld wordt dat: *“Er sprake is van georganiseerde criminaliteit indien groepen die primair gericht zijn op illegaal gewin systematisch misdaden plegen met ernstige gevolgen voor de samenleving, en in staat zijn deze misdaden op betrekkelijk effectieve wijze af te schermen, in het bijzonder door de bereidheid te tonen fysiek geweld te gebruiken of personen door corruptie uit te schakelen”* (Fijnaut, Bovenkerk, Bruinsma & van de Bunt, 1996, p25). In België dient een criminele organisatie enkele elementen te bevatten vooraleer het als georganiseerde criminaliteit wordt beschouwd. Ten eerste moet de organisatie actief zijn op de illegale markten. Ten tweede dient ze controle te hebben over een territorium. Ten derde moet ze minstens één jaar bestaan. Ten vierde moet er gebruik worden gemaakt van commerciële structuren. Ten vijfde dient geweld en/of intimidatie plaats te vinden. Ten zesde dient corruptie en/of beïnvloeding aanwezig te zijn (regering, 1996; Paternotte, persoonlijke communicatie). Voorbeelden van dit criminaliteitsfenomeen zijn onder andere mensenhandel, maffia, wapentrafiëk, handel in drugs, het witwassen van geld en rondtrekkende dadergroepen (Finckenauer, 2005; Europa, 2014).

3.1.2 Politieke belangstelling voor georganiseerde misdaad

Politieke belangstelling voor het fenomeen ‘georganiseerde criminaliteit’ kwam pas sinds de jaren negentig op in de Benelux (Kruisbergen, van de Bunt, Kleemans, Kouwenberg, Huisman, Meerts & de Jong, 2012; Dienst voor Strafrechtelijk Beleid, 2015). In deze periode werd georganiseerde criminaliteit gezien als een exotisch fenomeen dat geen sterke verbondenheid had met de maatschappij en hoe ze functioneert (Kruisbergen et al., 2012). Doch kwam dit criminaliteitsfenomeen in de jaren negentig op de voorgrond te staan nadat er alarmerende berichten uit Italië kwamen inzake maffia en hun invloed op politiek, media en bedrijfsleven (Dienst voor Strafrechtelijk Beleid, 2015). Het risico dat piramidaal opgebouwde misdaadorganisaties zouden binnendringen in politieke en economische instituties was zeer hoog. Deze piramidaal opgebouwde misdaadorganisaties zouden in dit verband optreden als een soort alternatieve overheid die een geweldsmonopolie handhaaft en zich het recht toewijst om belastingen te heffen. Dit fenomeen heet ook wel ‘*racketeering*’ (Kruisbergen et al., 2012).

Op beleidsniveau werden naar aanleiding van deze alarmerende berichten actieplannen uitgewerkt die een verzameling van maatregelen trachtte samen te brengen. Hieruit kwam voort dat verschillende landen een poging ondernamen om enerzijds efficiënte opsporings- en vervolgingsmiddelen te formuleren en anderzijds dit complexe criminaliteitsfenomeen in kaart te brengen. In België kwam dit naar voren via een Parlementaire Commissie van onderzoek naar georganiseerde criminaliteit en in het ‘Actieplan tegen de georganiseerde criminaliteit’ van 1996 (regering, 1996; Dienst voor Strafrechtelijk Beleid, 2015).

Door de opkomende politieke interesse en de daaruit volgende (parlementaire) onderzoeken bleek echter het dreigingsbeeld onrealistisch te zijn. Doch kwam men uit op een genuanceerd beeld, doordat uit onderzoek bleek dat bij dit criminaliteitsfenomeen omvangrijke netwerken betrokken waren en deze netwerken in grootsteden als Amsterdam belangrijke machtsposities verworven hadden (Kruisbergen et al., 2012). Ook hedendaags blijkt duidelijk in het Nationaal Veiligheidsplan 2012-2015 dat georganiseerde criminaliteit nog steeds onder grote politieke belangstelling staat, waarbij georganiseerde criminaliteit wordt aangeduid als een prioriteit (Federale Politie, 2012).

Echter staat georganiseerde criminaliteit niet enkel nationaal op de politieke agenda. Ook op Europees niveau is het criminaliteitsfenomeen een prioriteit en wordt het zowel repressief als preventief benaderd (Europa, 2014). Dit kan gaan over het meer algemene kader van Europese politionele samenwerking tot een specifieke benadering inzake georganiseerde criminaliteit (Europa, 2015a; Europa, 2015b).^{1 2} De aandacht die besteed wordt aan dit criminaliteitsfenomeen is een goede zaak, aangezien er jaarlijks honderd nieuwe criminele organisaties worden opgericht (Paternotte, persoonlijke communicatie).

3.1.3 Beeldvorming van georganiseerde misdaad

Voortvloeiend uit de definitie kan gesteld worden dat georganiseerde criminaliteit een structurele samenwerking heeft tussen individuen met als doelstelling materieel en/of financieel gewin te bekomen (Boerman, Grapendaal, Nieuwenhuis & Stoffers, 2012). Dit materiaal en/of financieel gewin kan bekomen worden door criminele activiteiten internationaal te plegen (Van Daele et al., 2010; Raad van de Europese Unie, 2010; Van Gestel, 2014).

Net zoals bij de term ‘terrorisme’ wordt de term ‘georganiseerde misdaad’ gebruikt als overkoepelende term voor verscheidene soorten criminaliteitsfenomenen. Door het gebrek aan een universele definitie zal niet onder elke definitie dezelfde soorten georganiseerde criminaliteit vallen. Denk onder andere aan handel in drugs, mensenhandel, georganiseerde vermogenscriminaliteit, wapenhandel, fraude en witwassen. Vaak zullen zelfs de criminaliteitsfenomenen die geplaatst kunnen worden onder de term ‘georganiseerde misdaad’ ook nog fungeren als koepelterm voor verscheidene subsoorten van het desbetreffende criminaliteitsfenomeen. Zo omvat bijvoorbeeld drugshandel onder andere de handel in heroïne en de handel in cocaïne, omvat fraude onder andere hypotheekfraude en beleggingsfraude en omvat georganiseerde vermogenscriminaliteit onder andere woninginbraak, autodiefstal en ramkraken (Boerman et al., 2012).

¹ EUR-LEX. Council framework decision on the fight against organised crime. 2008/831/JHA. Van 24 oktober 2008.

² EUR-LEX. *The prevention and control of organised crime: a European Union strategy for the beginning of the new millennium*. OJ C 124. Van 3 mei 2000.

Georganiseerde criminaliteit is een criminaliteitsfenomeen dat in elke politiezone in België vaak voorkomt (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). Zo is bijvoorbeeld in de politiezone Erpemere-Lede ongeveer de helft van de gemelde criminaliteit een vorm van georganiseerde criminaliteit (Lacaeyse, persoonlijke communicatie).

Georganiseerde misdaad bestaat om twee redenen. Ten eerste vervult georganiseerde misdaad behoeften die niet vervuld worden door de legale markt. Een voorbeeld hiervan is de handel in verdovende middelen (Finckenauer, 2007). Ten tweede kan georganiseerde misdaad “bescherming” bieden op plaatsen waar de staat faalt in het bieden van bescherming. Hier is de bescherming van een nachtwinkel tegen inbraken, in ruil voor een maandelijks bedrag, een voorbeeld van (Gambetta, 1996; Finckenauer, 2007). Georganiseerde misdaad is pas gevaarlijk als het niet enkel de zwakke plekken van de staat gaat benutten, maar deze vervolgens ook gaat vervangen (Finckenauer, 2007).

3.2 De organisatie van georganiseerde misdaad

3.2.1 Rekrutering

Er bestaan vijf rekruteringsvormen volgens professor Kleemans. Ten eerste kan een crimineel samenwerkingsverband rekruteren via werkrelaties. Dit kunnen bijvoorbeeld collega's zijn op het werk. Ten tweede via familiebanden. Ten derde via hobby's en nevenactiviteiten. Dit kunnen bijvoorbeeld individuen zijn die je kent vanop café. Ten vierde kan dit via levensloopgebeurtenissen zoals financiële tegenslagen. Ten vijfde kan dit via doelbewuste rekrutering (Kleemans, persoonlijke communicatie).

Een crimineel samenwerkingsverband kan bijvoorbeeld nieuwe leden rekruteren bij hun klanten. Zo kunnen drugsproducenten leden rekruteren bij hun druggebruikers. Op deze wijze kunnen deze gebruikers een levensstandaard opbouwen via het criminele milieu. Een andere reden om lid te worden van een crimineel samenwerkingsverband is om familie in het buitenland te kunnen ondersteunen door geld op te sturen (Pieteraerens, persoonlijke communicatie).

Daarnaast maakt Farcy (persoonlijke communicatie) een opsplitsing. Enerzijds heb je ervaring opgebouwde georganiseerde criminaliteit. Deze criminele samenwerkingsverbanden zijn stap per stap groter geworden. Hier zijn de leden individuen uit dezelfde wijk of stad, hebben ze voordien al kleine feiten gepleegd en kunnen gelinkt worden aan een bepaald milieu (bijvoorbeeld horeca). Anderzijds heb je maffiaorganisaties zoals de Albanese maffia. Hierbij behoren de leden tot dezelfde clan of familie. Soms zijn er ook buitenstaanders aanwezig, maar deze zijn gecoöpteerd omwille van een bepaalde vaardigheid (Farcy, persoonlijke communicatie).

Het lidmaatschap van een crimineel samenwerkingsverband kan soms worden bepaald door een specifiek kenmerk zoals etniciteit of kunnen relatief open zijn (Williams, 2001). In sommige gevallen hebben criminele samenwerkingsverbanden een homogene etnische herkomst die deels bestaat uit familieleden of een clan (Williams, 2001; Kruisbergen et al., 2012). Dit biedt twee voordelen aan de daders. Ten eerste beschikken de daders over contacten gesitueerd zowel in het land van herkomst als in België, waardoor het criminele samenwerkingsverband meer vat krijgt op het productie- en distributieproces, gemakkelijker transport kan regelen en gemakkelijker geld kan versluizen tussen beide landen. Ten tweede wordt niet elke activiteit die in België bestempeld wordt als een misdrijf, ook gezien als een misdrijf in het land van herkomst. Zo zal een mensensmokkelaar eerder een dienst verlenen aan gesmokkelde personen in het land van herkomst, wat in België wordt ervaren als een misdrijf (Kruisbergen et al., 2012). Een groot transnationaal netwerk is vaak multi-etnisch van aard wanneer instrumentele overwegingen zwaarder wegen dan de wens of behoefte om een hoge mate van exclusiviteit te behouden (Williams, 2001).

3.2.2 Het netwerk binnen het criminele samenwerkingsverband

Een crimineel netwerk is een (fictieve) plaats waar criminelen met elkaar kunnen samenwerken en dit in wisselende verbanden. In een crimineel netwerk ontstaat zowel stabiliteit in bepaalde samenwerkingsrelaties, alsook verandering. In de jaren negentig bestond de perceptie dat criminele samenwerkingsverbanden de vorm van traditionele Italiaanse maffiaorganisaties aannam, namelijk als piramidale organisaties met een sterke hiërarchie waar sprake is van een gedragscode, een intern strafsysteem en een duidelijke taakverdeling (Kruisbergen et al., 2012).

Deze soort criminele samenwerkingsverbanden bestaat wel, maar komt nog gering voor (Kleemans et al., 1998). Criminele organisaties zijn geëvolueerd van hiërarchische structuren naar flexibele netwerken (Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie).

De netwerken zijn vaak klein en worden zelden centraal gecoördineerd. Soms kan de coördinatie sterk zijn, wanneer de misdrijven lokaal gepleegd worden. Maar hoe meer een verscheidenheid aan criminele activiteiten (polycrimineel), hoe kleiner de waarschijnlijkheid is dat de coördinatie gecentraliseerd wordt (Felson, 2006).

Ten eerste kan een netwerk worden gecreëerd door een harde kern organisatoren die het netwerk willen gebruiken voor specifieke doeleinden. Dit soort netwerk wordt ook wel een '*directed network*' (of gericht netwerk) genoemd in de literatuur. Ten tweede kan een netwerk spontaan ontstaan als een mechanisme om efficiëntie toe te voegen aan het functioneren van een markt. Dit soort netwerk wordt ook wel '*transaction network*' (of transactienetwerk) genoemd in de literatuur. Een gericht netwerk kan deel uitmaken van een transactienetwerk (Williams, 2001; Farcy, persoonlijke criminaliteit). De aard van de criminele organisatie hangt dus af van de logistiek van het delict. Zo kan je bijvoorbeeld je vriendin in je eentje in de prostitutie brengen. Echter op het moment dat je meerdere meisjes in de prostitutie brengt, kom je terecht in een grotere cluster. In essentie worden de organisatievormen bepaald door het delict en hoe klein je het delict kan houden (Kleemans, persoonlijke communicatie).

In elk crimineel samenwerkingsverband verschilt echter de vorm, de grootte en het doel van het netwerk. Bijkomend kan een netwerk zich toespitsen op één crimineel feit, maar kan het ook polycrimineel zijn. De verscheidenheid van vormen gaat zelfs verder dan het criminaliteitsfenomeen, waarbinnen het per subsoort verschilt (Williams, 2001; Kruisbergen et al., 2012). Een netwerk kan dus variëren van een kleine, beperkte organisatie op lokaal niveau tot een transnationaal leveranciersnetwerk (Williams, 2001). Bijvoorbeeld zal je binnen de drugshandel verschillende vormen van netwerken aantreffen. De netwerkform van de productie van synthetische drugs zal verschillen van de netwerkform van invoer en uitvoer van cocaïne. De reden voor deze verscheidenheid is de grote variatie aan mogelijkheden en beperkingen die elke criminele activiteit kent, en die verschillen van criminele activiteit tot criminele activiteit. Er van uitgaan dat er een eenvormigheid bestaat inzake organisatie zou dan ook een foute redenering zijn (Kruisbergen et al., 2012). Met andere woorden bestaat er geen universeel toepasbare dominante organisatiestructuur (Williams, 2001).

Echter kan wel gesteld worden dat georganiseerde criminaliteit meer en meer evolueert van een vaste hiërarchische organisatie naar een flexibele netwerkstructuur. Zelfs typisch hiërarchische organisaties zoals de Italiaanse maffia laten steeds meer overleg met hun lokale afdelingen toe. Dit is ook niet verwonderlijk, aangezien een netwerk verdeeld in lokale afdelingen verder kan functioneren wanneer een deel wordt verwoest en het zich daarnaast relatief snel kan herstellen en gemakkelijk kan heropbouwen (Williams, 2001; Farcy, persoonlijke communicatie; Kleemans, persoonlijke communicatie).

Netwerken van enige omvang zullen in het algemeen bestaan uit een kern en een periferie, en kan je voorstellen als een buitencirkel (de periferie) rondom de binnenste cirkel (de kern). Waar je zit is een kwestie van macht, invloed en status binnen het netwerk (Williams, 2001; Farcy, persoonlijke communicatie; X, persoonlijke communicatie). De kern wordt gekenmerkt door dichte verbindingen tussen individuen. Bij een gericht netwerk geeft de kern richting aan het gehele netwerk. Meestal vormen de grondleggers van het crimineel samenwerkingsverband de kern van het netwerk en initiëren zij de specifieke criminele activiteiten, bemiddelen zij geschillen en geven zij richting aan het netwerk. Binnen deze kern bestaat een hoge mate van vertrouwen en samenhang (sociale cohesie). De periferie bezit in vergelijking met de kern meer losse relaties en minder compacte patronen van interactie. Daarnaast wordt door de periferie de geografische en sociale afstand van het netwerk vergroot waardoor het netwerk zich met een grotere variëteit aan activiteiten bezig kan houden (Williams, 2001). Vertrouwen speelt een belangrijke rol binnen criminele samenwerkingsverbanden (Paternotte, persoonlijke communicatie).

3.2.3 De hiërarchische orde

Hiërarchie kan dus zeker nog voorkomen bij georganiseerde criminaliteit. Zo heb je bij drugshandel grote vissen, tussendealers en koeriers die gevolgd worden door middel van *track & trace* systemen zoals GPS. Echter zal hiërarchie verschillen per criminaliteitsfenomeen binnen de georganiseerde criminaliteit (Pieteraerens, persoonlijke communicatie). Motorbendes bijvoorbeeld zijn ook hiërarchisch gestructureerd, waarbij functies bestaan als president en vice-president (Farcy, persoonlijke communicatie). Hiërarchie zal eerder voorkomen wanneer het crimineel samenwerkingsverband gebiedscontrole wenst te hebben (Kleemans, persoonlijke communicatie).

Verder kan een netwerk samenvallen met de familiestructuur (Farcy, persoonlijke communicatie; Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Hierbij heeft sociale invloed een impact op het netwerk. Zo kan het zijn dat bijvoorbeeld de vader de baas is. Al wat in die relaties meekomt, komt ook voor in het netwerk (Kleemans, persoonlijke communicatie). Bij de Albanese maffia is de oudste broer steeds de baas (Farcy, persoonlijke communicatie).

Wanneer het op geweld aankomt zijn het vaak de leidinggevende figuren binnen het criminele samenwerkingsverband die het geweld uitoefenen. Dit betekent evenwel niet dat andere leden van de organisatie geen geweld kunnen uitoefenen (Boerman et al., 2012; X, persoonlijke communicatie). Het agressieve karakter van de leider kan het functioneren van de groep sterk bepalen. Uit angst voor repercussies van het leidinggevende figuur durven sommige daders niet te stoppen met het uitvoeren van criminele activiteiten. Deze repercussies kunnen op zichzelf van toepassing zijn, maar ook op diens gezin of op diens familie (Kruisbergen et al., 2012).

3.2.4 Samenwerking met gelijkende criminele organisaties

Criminele samenwerkingsverbanden werken vaak samen (Farcy, persoonlijke communicatie; Kleemans, persoonlijke communicatie). Hoe groter de netwerkcluster, hoe meer nood er is aan samenwerking (Kleemans, persoonlijke communicatie). Criminele samenwerkingsverbanden werken samen wanneer het voordelig is voor hen (Williams, 2001). Deze criminele samenwerkingsbanden kunnen internationaal zijn (Kleemans, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie).

Daarnaast zijn er drie manieren om te zorgen dat gelijkende criminele organisaties zich aan elkaar binden. Ten eerste compenseren sterke sociale relaties tussen criminele samenwerkingsverbanden het gebrek aan formele periodegebonden samenwerkingscontracten. Hechte sociale relaties zijn een belangrijke voorwaarde binnen deze onzekere illegale wereld voor een duurzame samenwerking (Kruisbergen et al., 2012). Zoals eerder gesteld speelt vertrouwen een belangrijke rol (Paternotte, persoonlijke communicatie).

Een tweede bindingsmanier is het financieel gewin dat men gezamenlijk haalt uit samenwerken (Williams, 2001; Kruisbergen et al., 2012). Samenwerken moet een grotere winst opleveren dan hetzelfde zelfstandig doen. Inzake deze bindingsmanier wordt het principe van eerlijk delen tussen gelijkwaardige partners belangrijk bevonden (Kruisbergen et al., 2012). Financiële ongelijkheid kan leiden tot het verklikken aan politie of overlopen naar een concurrent (Zaitch, 2002; Kruisbergen et al., 2012). Voor dit principe dienen beide partners wel op ongeveer gelijke voet te staan. Bij bijvoorbeeld gedwongen prostitutie zullen andere verdelingscriteria heersen wanneer het gaat over het deel dat de slachtoffers krijgen in vergelijking met het deel dat de pooier krijgt (Kruisbergen et al., 2012).

Een derde bindingsmanier is het dreigen met en gebruik van geweld. Het uittreden door de ene handelspartner uit de samenwerkingsrelatie kan gevaarlijke gevolgen hebben voor de andere handelspartner, aangezien de uittredende handelspartner naar de politie kan stappen met informatie zoals routes, investeringen, namen en adressen. De uittredende handelspartner kan daarnaast ook gaan samenwerken met een andere concurrent en haar kennis gebruiken om zijn eerdere handelspartner te beconcurreren (Kruisbergen et al., 2012).

Het uittreden kan dus een bedreiging vormen voor het voortbestaan van het criminele samenwerkingsverband of leiden tot een verzwakking van de groep (Kruisbergen et al., 2012). Echter hoeft dit niet altijd het geval te zijn en vormt het uittreden voor sommige criminele samenwerkingsverbanden geen gevaar (Williams, 2001).

3.2.5 Het gebruik van corruptieve contacten en beïnvloeding

Één op vijf criminele samenwerkingsverbanden maakt gebruik van corruptieve contacten (Boerman et al., 2012; Kruisbergen et al., 2012; Paternotte, persoonlijke communicatie). Echter halen Williams (2001) en Ruggiero & Gounev (2012) aan dat corruptie een belangrijk element vormt binnen de georganiseerde criminaliteit (Williams, 2001; Ruggiero & Gounev, 2012). Doch hoeft een crimineel samenwerkingsverband soms niet gebruik te maken van corruptie als ze gebruik kan maken van legale goederenstromen (Kleemans, persoonlijke communicatie). Hoe vaak corruptieve contacten een rol spelen binnen de organisatie en werking van een crimineel samenwerkingsverband, valt niet vast te stellen door het *dark number*. Door het fragmentarisch beeld dat we rond corruptieve contacten hebben, is het onmogelijk te zeggen wat en hoe diep de gevolgen zijn voor onze maatschappij (Boerman et al., 2012).

Corruptie kan gaan van de transportsector tot de logistieke sector, van douane tot justitie. Met andere woorden hoeft corruptie niet gebonden te zijn aan een overheid, maar komt het net voornamelijk voor in het private zakenleven (Ruggiero et al., 2012; Kleemans, persoonlijke communicatie; X, persoonlijke communicatie). Een voorbeeld zijn bankiers en advocaten die criminelen helpen om het geld te verbergen of juist te investeren (Williams, 2001). Deze corruptie strekt zich niet enkel nationaal, maar gaat over de grenzen heen. Zo blijkt bijvoorbeeld uit Nederlandse gegevens dat er criminele samenwerkingsverbanden cocaïne smokkelen naar Nederland en hiervoor contacten hebben in zowel Nederlandse luchthavens als in de Antwerpse haven. Het gebruik van buitenlandse corruptieve contacten komt voornamelijk voor in de drugshandel (Boerman et al., 2012). Corruptieve contacten bieden door hun kennis of vaardigheden een oplossing voor specifieke knelpunten of problemen waar criminele samenwerkingsverbanden mee te maken krijgen (Kruisbergen et al., 2012). Corruptie helpt met andere woorden om de activiteiten van het crimineel netwerk te faciliteren, te vermenigvuldigen of net te beschermen (Williams, 2001; Ruggiero et al., 2012).

Het takenpakket van een corruptief contact verschilt naargelang zijn/haar jobfunctie. Ze kunnen een specifieke rol spelen en een cruciale schakel vormen in het productie- of distributieproces. Zo zal een corruptief contact op de luchthaven bijvoorbeeld informatie kunnen lekken over de controles en kan hij/zij bagage waarin cocaïne is verstopt, doorlaten. Corruptieve contacten kunnen ook overheidspersoneel zijn en hebben doorgaans als doel het criminele samenwerkingsverband af te schermen van de autoriteiten. Zo zijn er in Nederland feiten aan het licht gekomen waarbij agenten politie-informatie verkochten aan criminele samenwerkingsverbanden. Deze informatie kon bijvoorbeeld gaan over waar en wanneer een huiszoeking zou plaatsvinden. Op deze manier neutraliseren de corruptieve contacten op tactische wijze de aandacht en acties van de bevoegde autoriteiten (Boerman et al., 2012; Kruisbergen et al., 2012). Daarnaast zal het soort corruptief contact ook afhangen van de criminele feiten waar het criminele samenwerkingsverband zich schuldig aan maakt (Boerman et al., 2012; Gounev, 2012). Zo zal bij fraude eerder bankiers optreden als corruptieve contacten (Boerman et al., 2012). Echter zal corruptie bij bankiers amper voorkomen, doordat de meeste financiële instituties beschikken over anti-witwassystemen. Echter, wanneer het toch voorkomt, zal deze vorm van corruptie eerder succesvol zijn door bank collusie of door onvoldoende effectieve anti-witwasmaatregelen (Gounev, 2012).

Een andere groep corruptieve contacten zijn vrijberoepsbeoefenaars. Dit kunnen bijvoorbeeld advocaten, makelaars en belastingadvieskantoren zijn. Vrijberoepsbeoefenaars beschikken namelijk over bepaalde expertise en privileges bij wet, waarbij zij kunnen helpen bij het bouwen van bruggen (Boerman et al., 2012). Advocaten kunnen aan criminele samenwerkingsverbanden aangeven wat de uiterste grenzen zijn van een wet, zodat deze criminele samenwerkingsverbanden kunnen opereren in de schemerzone tussen legaliteit en illegaliteit (Kruisbergen et al., 2012).

Uit de interviews van Gounev (2012) komt voor dat de meeste corruptieve contacten uit de transportsector komen (Gounev, 2012). Zo kan het voorkomen dat bijvoorbeeld een corruptief contact een container moet gaan halen op de haven. Hiervoor krijgt hij dan een vergoeding en kan het zijn dat hij de restinhoud van de container, die dient om bijvoorbeeld de drugs of wapens te verbergen, krijgt (X, persoonlijke communicatie).

Wanneer het gaat over corrupt overheidsoptreden zijn er twee soorten relaties tussen overheid en criminele netwerken: sporadische en symbiotische relaties. Bij een sporadische relatie zullen criminelen door middel van corruptie tegen een vergoeding ongemerkt opereren of een overheidscontract binnenhalen. Bij een symbiotische relatie zullen criminelen betalen voor ongestoord te kunnen werken terwijl ze lange termijn vriendschappen creëren met politici. Deze laatste relatievorm komt vaak voor op lokaal niveau in veel Europese lidstaten. Overheidsopdrachten, zoals het bouwen van sociale woningen, worden dan gegeven aan lokale bedrijven die voor de burgemeester of regerende politieke partij stemmen. Echter zijn deze bedrijven soms crimineel van aard. Verder komt het vaak voor dat criminelen participeren in stadsbesturen, waarmee ze het lokale politieke proces corrumperen (Bezlov & Gounev, 2012). Een grote overheidsdienst is politie, waarbij politieagenten een afspiegeling van de maatschappij vormen. Het uniform maakt je daarbij niet anders, waardoor er steeds wel enkelen zijn die zich tot corruptie wenden. Echter komt corruptie op lokaal politieniveau niet vaak voor, aangezien een lokaal politiekorps meestal klein en beheersbaar is, waardoor een snelle detectie volgt (Pieteraerens, persoonlijke communicatie). Uiteraard betekent dit niet dat het nooit voorkomt. Corruptie kan steeds voorkomen, ook bij wijkagenten (X, persoonlijke communicatie).

Bijkomend is België een land waar binnen de douane weinig corruptie voorkomt. Door de grote ladingen die de Antwerpse haven binnenkomen, is de statistische kans dat een criminele lading ongedetecteerd douane passeert enorm hoog. Daarom vinden criminele netwerken het onnodig om geld uit te geven aan het corrumperen van douane (Bezlov et al., 2012). Daarnaast weten douaniers niet welke containers ze morgen gaan controleren (Kleemans, persoonlijke communicatie).

Verder mag corruptie niet worden gezien als een slachtofferloos misdrijf. Het kan zijn dat het criminele netwerk een potentieel corruptief contact beïnvloedt corruptie te plegen door middel van intimidatie en/of geweld (Ruggiero et al., 2012).

Ten slotte dient een onderscheid gemaakt te worden tussen corruptie en beïnvloeding. Sommige criminele netwerken proberen zich positief te profileren in de buurt of gemeente, waarmee ze meer invloed proberen te bereiken in de buurt of gemeente. Zo kunnen bijvoorbeeld motorbendes hun controle op een territorium (bijvoorbeeld een gemeente) beïnvloeden door te helpen in de gemeente, waardoor hun aanzien in de gemeente stijgt (Paternotte, persoonlijke communicatie). Een ander voorbeeld is drugsbaron Pablo Escobar die over een hele cocaïne-industrie beschikte. Echter wordt hij in de Colombiaanse gemeente Medellín door sommigen nog steeds bekeken als een held, doordat hij voor duizenden arme mensen huizen liet bouwen en hij mensen in nood hielp (Moreno, 2014).

3.2.6 Het gebruik van rechtspersonen

Uit een Nederlands onderzoek van Boerman, Grapendaal, Nieuwenhuis en Stoffers (2012) blijkt dat een meerderheid van de criminele samenwerkingsverbanden gebruik maakt van één tot meer rechtspersonen. Verder heeft kwart van de leden van criminele samenwerkingsverbanden zeggenschap over één of meer ondernemingen die zijn ingeschreven bij de Nederlandse Kamer van Koophandel (Boerman et al., 2012). Ook andere studies bevestigen dat rechtspersonen een rol spelen binnen criminele samenwerkingsverbanden (Kleemans, Van den Berg, van de Bunt & Brouwers, 1998; Boerman, Grapendaal & Mooij, 2008; Farcy, persoonlijke communicatie; X, persoonlijke communicatie). Één onderzoek stelt zelfs dat het gebruik/misbruik van ondernemingen en rechtspersonen een belangrijke voorwaarde vormt voor het bestaan en de continuïteit van criminele samenwerkingsverbanden (Boerman et al., 2008).

Het veelvuldig gebruik van rechtspersonen biedt verschillende voordelen. De onderneming kan fungeren als dekmantel, kan dienen om illegaal verkregen opbrengsten uit te geven of het logistiek proces van een criminele activiteit verzorgen. Wederom zal het soort onderneming/rechtspersoon afhangen van de criminele feiten die de criminele samenwerkingsverbanden plegen. Zo maken criminele samenwerkingsverbanden die zich schuldig maken aan mensenhandel gebruik van bordelen en escortebedrijven, maken criminele samenwerkingsverbanden die zich schuldig maken aan mensensmokkel gebruik van uitzendbureaus en maken criminele samenwerkingsverbanden die zich schuldig maken aan hennepteelt gebruik van coffeeshops en transportbedrijven om drugs internationaal te transporteren. Daarnaast worden ook ondernemingen van familieleden gebruikt om illegaal verkregen opbrengsten wit te wassen. Deze ondernemingen kunnen praktisch alles zijn, zoals onder andere kledingzaken, broodjeszaken en kapsalons (Boerman et al., 2012). Bijkomend kunnen criminelen bij onder andere fraude een bedrijf oprichten die ze op een postbus domiciliëren, maar waarbij ze vanuit een andere locatie opereren (X, persoonlijke communicatie). Ook wordt er gebruik gemaakt van VZW's, die vervolgens dienen als het hoofdkwartier van de criminele organisatie (Farcy, persoonlijke communicatie).

3.2.7 Het gebruik van internet en media

Het internet wordt als informatietechnologie meer en meer gebruikt. Door middel van internet kan een crimineel netwerk haar activiteiten uitvoeren met meer efficiëntie en dat tegen een lagere kostprijs (Williams, 2001). Daarnaast kunnen criminelen elkaar ook ontmoeten via het internet, ook al blijven sociale relaties wel een belangrijke rol spelen binnen criminele samenwerkingsverbanden (Kleemans, persoonlijke communicatie).

Meestal heeft het gebruik van media bij een crimineel samenwerkingsverband als doel om het imago van politie en justitie in diskrediet te brengen (Boerman et al., 2012). Maar daarnaast kan het gebruik van media dienen om de algemene opinie te beïnvloeden en reclame te maken voor klanten aan te trekken (Kruisbergen et al., 2012). Media is een handig communicatiemiddel waarbij het risico op een relatie bestaat tussen aan de ene kant journalisten, die nood hebben aan criminelen om te publiceren, en aan de andere kant criminelen, die nood hebben aan journalisten om via hen geruchten te verspreiden over en druk uit te oefenen op opsporings- en vervolgingsdiensten (Boerman et al., 2012). Maar voor media te kunnen gebruiken, is een crimineel samenwerkingsverband wel afhankelijk van journalisten (Kruisbergen et al., 2012).

Wanneer media dient om reclame te maken zodat een crimineel samenwerkingsverband klanten naar zich toe kan trekken, beschrijft Felson (2006) dat een dilemma ontstaat tussen in de schaduwzijde van de maatschappij opereren en klanten te trekken in het openbaar (Felson, 2006; Kruisbergen et al., 2012). Een voorbeeld van reclame is klanten aantrekken via zogezegde legitieme beleggingsprojecten waarbij mensen hun geld verliezen door beleggingsfraude. Door deze reclame op televisie uit te zenden, zorgt het voor een schijn van betrouwbaarheid waardoor meer mensen geneigd zijn hun geld te beleggen bij deze daders (Kruisbergen et al., 2012). Door de verdere digitalisering van media wordt de speelruimte van criminelen vergroot, waardoor de bestrijding van georganiseerde misdaad steeds moeilijker wordt (Boerman et al., 2012). Zo wordt sociale media ook gebruikt door criminele organisaties, wat de drempel voor mogelijke klanten over de streep te trekken enkel verlaagt. Zo blijkt uit een klein onderzoek van VRT-journalist Majd Khalifeh dat een mensensmokkelaar vinden om uit Syrië naar Europa te vluchten relatief gemakkelijk is. Khalifeh vond verscheidene (besloten en toegankelijke) pagina's op Facebook en andere sociale media waar hij aan allerlei informatie geraakte zoals telefoonnummers en de dienstregelingen van de vluchtelingenboten (Maerevoet, 2015).

3.2.8 Defensieve en offensieve contrastrategieën

Criminele samenwerkingsverbanden kunnen maatregelen aanwenden om opsporing door politie en vervolging door justitie te voorkomen. Deze maatregelen noemt men ook wel contrastrategieën of afschermingsmethoden (Boerman et al., 2012; Farcy, persoonlijke communicatie; X, persoonlijke communicatie). In Nederlands onderzoek gebruikte minstens de helft van de criminele samenwerkingsverbanden contrastrategieën. Over de aard en de omvang van contrastrategieën is de informatie beperkt, doordat de strafbare feiten die als contrastrategieën fungeren doorgaans niet de criminele hoofdactiviteiten uitmaken. Dit terwijl de focus van een opsporingsonderzoek net ligt op de criminele hoofdactiviteiten waar het criminele samenwerkingsverband zich schuldig aan maakt. Criminele samenwerkingsverbanden die gebruikmaken van dergelijke geavanceerde contrastrategieën zijn vaak sterk positioneel verankerd in de boven- en onderwereld en zijn daarbij vrij succesvol. Er bestaan twee soorten maatregelen: defensieve contrastrategieën en offensieve contrastrategieën (Boerman et al., 2012).

3.2.8.1 Defensieve contrastrategieën

Defensieve contrastrategieën trachten criminele activiteiten te verbergen. Van de voorheen besproken helft van criminele samenwerkingsverbanden die gebruikmaken van contrastrategieën, maakt van deze helft tachtig procent gebruik van defensieve contrastrategieën (Boerman et al., 2012).

De meest gebruikte defensieve contrastrategie is het afschermen van communicatie van het criminele samenwerkingsverband. Dit kan een crimineel samenwerkingsverband bekomen door het gebruik van codetaal en van verschillende telecommunicatiemiddelen (Boerman et al., 2012; Kruisbergen et al., 2012; X, persoonlijke communicatie). Verder kunnen criminelen op het *darkweb* illegale goederen verkopen. Hierbij maken ze gebruik van virtuele betalingssystemen zoals Bitcoin, aangezien dit geen sporen nalaat (Kleemans, persoonlijke communicatie; X, persoonlijke communicatie). Voorlopig blijft het aantal meldingen inzake gebruik van nieuwe betaalsystemen bij de Cel voor Financiële Informatieverwerking (CFI) beperkt (Cel voor Financiële Informatieverwerking, 2013). Andere defensieve contrastrategieën zijn: het kopen van informatie zoals waar en wanneer een huiszoeking zal plaatsvinden, contra-observatie en het gebruik van vervalste identiteitspapieren zoals identiteitskaarten (Boerman et al., 2012).

Verder kan een crimineel samenwerkingsverband zich ook verbergen door zich bezig te houden met legale producten. Hierdoor vallen de illegale activiteiten minder op en fungeren de legale producten als dekmantel (Williams, 2001). Daarnaast kunnen netwerken relatief gemakkelijk verhuizen van gebieden waar het risico op politie groot is naar gebieden waar het risico op politie minder groot is (Williams, 2001).

Ten slotte kunnen criminele netwerken een gemeenschap vormen, waarin intern een sterke sociale cohesie kan bestaan met als gevolg dat criminele activiteiten makkelijker zijn af te schermen (Williams, 2001; Kruisbergen et al., 2012; Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Elementen zoals de afwezigheid van overheid(sinterventies) maken het mogelijk dat structuren hechter en duurzamer worden (Kleemans, persoonlijke communicatie). Deze gemeenschap kan gevormd worden door een specifiek kenmerk zoals etniciteit (Williams, 2001). Binnen deze gemeenschap kunnen ook subcultuurgemeenschappen ontstaan, zoals bijvoorbeeld een motorbende binnen een achterbuurt in Anderlecht (Kruisbergen et al., 2012).

In dit geval ontstaat op een vrij sociale of letterlijk ontoegankelijke locatie voor buitenstaanders een sterke sociale cohesie die onderworpen is aan een reputatiesysteem waarbij dit laatste tot angst leidt om verklaringen bij de politie af te leggen (Kruisbergen et al., 2012). Binnen deze gemeenschap kan sprake zijn van een omerta, zwijgplicht (Paternotte, persoonlijke communicatie). Al deze zaken maken het makkelijker voor een crimineel samenwerkingsverband om hun criminele activiteiten af te schermen en onderling af te spreken (Felson, 2006; Kruisbergen et al., 2012).

3.2.8.2 Offensieve contrastrategieën

Offensieve contrastrategieën trachten de activiteiten van opsporings- en vervolgingsambtenaren te verhinderen. Deze soort contrastrategieën komen over het algemeen minder voor. Zo gebruikten amper twintig procent van de criminele samenwerkingsverbanden, die aan bod kwamen in ons aangehaalde Nederlandse onderzoek, offensieve contrastrategieën (Boerman et al., 2012).

De meest gebruikte offensieve contrastrategie bij een crimineel samenwerkingsverband is het omkopen van ambtenaren, het onder druk zetten van ambtenaren of diens familieleden en het bekomen van relaties met strategisch-geplaatste individuen (Williams, 2001; Boerman et al., 2012; Ruggiero et al., 2012; Paternotte, persoonlijke communicatie). Andere voorbeelden van offensieve contrastrategieën zijn het creëren van omstandigheden die de positie van justitie- en politieambtenaren ondermijnen en het verspreiden van geruchten. Deze laatste is een strategie die volgens het Nederlands onderzoek sinds 2008 aan populariteit won. Door het verspreiden van geruchten trachten criminele samenwerkingsverbanden overheidsdiensten en ambtenaren belast met opsporing en vervolging in diskrediet te brengen via *social media* en media (Boerman et al., 2012).

Bijkomend creëren sommige transnationale criminele samenwerkingsverbanden jurisdictionele verwarring, zodat het moeilijk wordt voor een nationale politie-eenheid om effectief en efficiënt te werken. Dit kan bijvoorbeeld door geld wit te wassen doorheen een serie van bedrijven en banken gelocaliseerd in meerdere jurisdicties (Williams, 2001; X, persoonlijke communicatie).

Daarnaast kunnen criminele netwerken gebruik van encryptieprogramma's, waarmee het crimineel netwerk op een goedkope manier haar gesprekken en informatie probeert te beschermen tegen autoriteiten. Dergelijke programma's geven criminele netwerken een strategisch voordeel (Williams, 2001). Verder kunnen criminele organisaties gebruikmaken van het *darkweb*. Hierbij zijn alle gegevens van de websites gecodeerd en met wachtwoorden verborgen (Farcy, persoonlijke communicatie). Bijkomend kunnen criminele samenwerkingsverbanden meerdere gsm's gebruiken, waarbij één gsm gebruikt wordt per contact. Deze gsm's worden regelmatig vervangen (Farcy, persoonlijke communicatie; X, persoonlijke communicatie). Vervolgens rijden leden van een crimineel samenwerkingsverband soms tweemaal rond een rotonde om te zien of ze achtervolgd worden (Farcy, persoonlijke communicatie).

Ten slotte kunnen criminele samenwerkingsverbanden hun kennis en informatie compartimenteren. Zo kan bijvoorbeeld het ene luik van het netwerk bepaalde informatie in handen hebben over het transport en een ander luik informatie over de productie. De bedoeling hierachter is dat de politie voornamelijk een lokaal effect heeft op het netwerk, in plaats van heel het netwerk lam te leggen (Williams, 2001).

3.2.8.3 Het categoriaal gebruik van afschermingsmethoden

In deze paragraaf kijken we naar de drie hoofdcategorieën die aan afschermingsmethoden kunnen worden gelinkt. Door deze drie hoofdcategorieën te behandelen, beschrijven we de afschermingsmethoden in zijn totaliteit, in plaats van elke afschermingsmethode te linken aan één bepaald criminaliteitstype binnen de georganiseerde misdaad. Dit laatste doen we niet, omdat elke criminaliteitstype binnen de georganiseerde misdaad gebruik maakt van verschillende varianten van afschermingsmethoden, in plaats van gebruik te maken van één (of enkele) specifieke afschermingsmethoden. De drie hoofdcategorieën van afschermingsmethoden zijn het gebruik van: een valse identiteit, ICT-middelen en intimidatie en (bedreiging met) geweld (Boerman et al., 2012).

3.2.8.3.1 Het gebruik van een valse identiteit

Binnen het gebruik van vervalste paspoorten en identiteitsbewijzen, zoals rijbewijzen en identiteitskaarten, zijn een drietal ontwikkelingen in de Nederlandse maatschappij aan te treffen. Ten eerste komt de stickermethode steeds vaker voor. Bij deze methode gaat de crimineel een bedrukte folie plakken over de originele personaliabladzijde in het paspoort (Boerman et al., 2012; Farcy, persoonlijke communicatie).

Ten tweede worden er meer personen betrappt met een vals rijbewijs. Ten derde komen zogenaamde fantasiedocumenten vaker voor. Fantasiedocumenten zijn documenten die authentiek ogen, maar niet toebehoren aan een bestaande instantie of een bestaand land (Boerman et al., 2012; Farcy, persoonlijke communicatie).

3.2.8.3.2 Het gebruik van ICT-middelen

Bij het gebruik van ICT-middelen als afschermingstechniek kan je denken aan onder andere het gebruik van anonieme chatdiensten, encryptie van mails, het gebruik van geëncrypteerde browsers zoals Tor, *gps-jammers* en af luisterzenders om politieberichten te horen (Williams, 2001; Boerman et al., 2012; Tor, 2015). Ook door de opkomst en verdere evolutie van ICT-middelen wordt het steeds moeilijker om georganiseerde misdaad te bestrijden. Wederom vergroot ook hier de speelruimte voor criminelen (Boerman et al., 2012; Farcy, persoonlijke communicatie).

3.2.8.3.3 Het gebruik van intimidatie en (bedreiging met) geweld

Ook het gebruik van intimidatie en/of (het bedreigen met) geweld is een afschermingsmethode. Het begrip ‘geweld’, toegepast op georganiseerde misdaad, is zeer gevarieerd en wordt verschillend gebruikt naargelang type misdrijf. Geweld omvat in deze context onder andere ernstig geweld, geweld met dodelijke afloop, mishandeling, gedwongen seks, gijzeling en het uiten van bedreigingen inzake het gebruik van geweld (Kruisbergen et al., 2012). Deze contrastrategie kan onder andere betrekking hebben op journalisten, politieagenten en getuigen (Boerman et al., 2012; Ruggiero et al., 2012; X, persoonlijke communicatie). Maar ook daders van georganiseerde criminaliteit kunnen het slachtoffer worden van geweld (Kruisbergen et al., 2012). Paternotte (persoonlijke communicatie) geeft aan dat in vijftig procent van zijn dossiers geweld en/of intimidatie voorkomt (Paternotte, persoonlijke communicatie).

Indien er problemen voorkomen, zouden daders inzake georganiseerde criminaliteit weinig medelijden vertonen met hun handelspartners of slachtoffers (Kruisbergen et al., 2012). Zoals aangehaald onder 3.2.3 “hiërarchische orde” zijn het vaak de leidinggevende figuren binnen het criminele samenwerkingsverband die het geweld uitoefenen. Doch betekent dit niet dat andere leden van de organisatie geen geweld kunnen uitoefenen. Daarnaast huren sommige criminele samenwerkingsverbanden, voornamelijk op de drugsmarkt, externe contacten in om voor hen geweld uit te oefenen (Boerman et al., 2012).

Uit een Nederlands onderzoek van Kruisbergen et al. (2012) gebruikt de helft van de onderzochte criminele samenwerkingsverbanden geweld (Boerman et al., 2012; Kruisbergen et al., 2012). Dit om de samenwerking met andere criminelen te reguleren en de continuïteit van hun criminele activiteiten veilig te stellen (Boerman et al., 2012). Echter dient geweld niet in elk crimineel samenwerkingsverband voor te komen. Ten eerste kunnen criminele samenwerkingsverbanden bij het verkrijgen van meer macht overstappen op andere en meer subtiele vormen van overtuiging. Ten tweede ligt de frequentie en ernst van geweld niet bij alle criminele samenwerkingsverbanden even hoog. Zo zullen mensensmokkelaars en ondergronds bankieren minder gebruik maken van geweld door een lagere mogelijkheid aan conflicten (Kruisbergen et al., 2012).

Wanneer het aankomt op het plegen van geweld, plegen criminele samenwerkingsverbanden die zich schuldig maken aan fraude het minste geweld (Boerman et al., 2012). Een respondent haalde echter aan dat inzake BTW-fraude bedreigingen frequent voorkomen (X, persoonlijke communicatie). Criminele samenwerkingsverbanden die zich schuldig maken aan mensenhandel plegen het meeste geweld. Driekwart van mensenhandelaars maakt zich schuldig aan het plegen van geweld. Daarnaast zijn criminele samenwerkingsverbanden die zich schuldig maken aan mensenhandel ook het meest gewelddadig. Dit kan gaan van fysieke mishandeling en verkrachting tot psychische mishandeling en gedwongen abortussen. Dit geweld beperkt zich niet tot de slachtoffers van mensenhandel, maar wordt ook gepleegd tegenover eigen groepsleden of concurrenten. Doch dient de kantmelding gemaakt te worden dat criminele samenwerkingsverbanden die zich schuldig maken aan mensenhandel meer dreigen met geweld dan dat ze daadwerkelijk geweldsfeiten plegen (Boerman et al., 2012).

Over het gebruik van intimidatie en (bedreiging met) geweld bestaan er twee vaak voorkomende invalshoeken in de literatuur. De ene invalshoek wordt ook wel '*self-help*' genoemd. Deze invalshoek ziet het geweld door criminele samenwerkingsverbanden als het gevolg van het illegale karakter waar daders zich bezig mee houden. Dit kan gaan over illegale markten tot het illegaal opereren op legale markten. Daders kunnen vanwege deze illegaliteit geen beroep doen op de bescherming van de overheid die ze normaliter aan elk individu biedt. Conflicten rond aansprakelijkheid en interpretatieverschillen kunnen niet bemiddeld worden door deze beschermende overheid, maar dienen door de daders opgelost of uitgevochten worden waarbij het gebruik van fysiek geweld kan voorkomen (Kruisbergen et al., 2012).

De andere invalshoek concludeert dat daders binnen criminele samenwerkingsverbanden enkel geringe mogelijkheden hebben om geweld te gebruiken. Hiervoor kunnen verschillende redenen bestaan. Zo zal een crimineel samenwerkingsverband niet de aandacht willen trekken van media en/of politie, bestaat de mogelijkheid op wraak en zal het haar reputatie niet willen tenietdoen zodat handelspartners niet afgeschrikt worden om zaken te doen. Het gebruik van geweld wordt omwille van deze redenen een risico (Kruisbergen et al., 2012).

Echter zijn beide invalshoeken niet allesomvattend. Waarom zou een Mexicaans drugskartel geweld gebruiken tegen vijand en politie als er zo een grote risico's aan zijn verbonden (Kruisbergen et al., 2012)? Elk voorval van geweld zal afhangen van historische, culturele en economische feiten, het type misdrijf en van de sociale strata waar de dader uit afkomstig is (Andreas & Wallman, 2009; Kruisbergen et al., 2012). Wanneer daders van georganiseerde criminaliteit afkomstig zijn uit sociale strata waar het gebruik van geweld als normaal wordt bevonden, zal dit verband houden met de aard en de omvang van geweld dat een crimineel samenwerkingsverband gebruikt (Andreas et al., 2009). Er zijn daarnaast grote internationale verschillen inzake omvang, aard en functie van geweld. Juist om deze reden mag men niet georganiseerde criminaliteit in België vergelijken met georganiseerde criminaliteit in bijvoorbeeld Mexico. Ook binnen de Europese Unie zijn er verschillen inzake geweld vast te stellen. Zo behoort het gebruik van geweld door Italiaanse maffia tot een belangrijk onderdeel van de modus operandi, terwijl dit niet het geval is in de Benelux. In Italië is geweld gericht op het beïnvloeden van overheid, op het vestigen en handhaven van machtsposities en afpersing om financieel gewin. In bijvoorbeeld de Benelux speelt geweld een andere rol, aangezien daar criminele activiteiten meer gericht zijn op het faciliteren van illegale handelspraktijken in plaats van het onder controle houden van gebieden, sectoren en burgers (Kruisbergen et al., 2012).

Het gebruik van geweld zal daarnaast afhankelijk zijn van de functie die het geweld heeft. Zo kan geweld 'helpen' om (1) misdrijven uit te voeren, (2) mensen in het gareel te houden, (3) conflicten te beslechten, (4) de onthulling van misdrijven te voorkomen en (5) als reactie op verraad en bedrog. De eerst vier functies zijn instrumenteel van karakter. Deze functies van geweld dienen te zorgen dat niemand een klacht indient of een getuigenis aflegt bij de politie, de leden niet uittreden en afspraken worden nagekomen. De vijfde functie van geweld is emotioneel van karakter, waarbij een ervaring van bedrog en verraad leidt tot een gewelddadige handeling (Kruisbergen et al., 2012).

Bij de eerste functie van geweld zal het gebruik van of de dreiging met geweld een onlosmakelijk onderdeel zijn van de *modus operandi*. Het misdrijf kan zonder de dreiging met of het gebruik van geweld niet uitgevoerd worden. Denk bijvoorbeeld aan een ontvoering voor losgeld. Dit soort geweld komt voornamelijk voor bij afpersing en bij mensenhandel. Echter is deze functievorm eerder uitzonderlijk en zijn de meeste criminele feiten die criminele samenwerkingsverbanden plegen vormen van *crimes without victims* (Kruisbergen et al., 2012).

De tweede functie van geweld is de derde bindingsmanier zoals aangehaald in 3.2.4 “samenwerking met gelijkende criminele organisaties”. Medewerkers kunnen van de ene op de andere dag uittrekken, aangezien er geen concurrentiebedingen of opzeggingstermijnen bestaan binnen de criminaliteit. Ook handelspartners kunnen plots de samenwerking stoppen wat gevaarlijke gevolgen kan hebben voor het crimineel samenwerkingsverband. Handelspartners kunnen de groep verzwakken en informatie doorspelen aan politie en concurrenten (Kruisbergen et al., 2012).

De derde functie van geweld komt vaak voor binnen criminele samenwerkingsverbanden. Deze conflicten ontstaan steeds uit misverstanden en onvermogen. Dit kan gaan over onder andere betaling, nakoming tot betaling en leveringen (Kruisbergen et al., 2012).

De vierde functie van (bedreiging met) geweld dient als afschermingsstrategie om personen te ‘overtuigen’ die aan politie of in de rechtbank informatie wensen te verschaffen over de illegale praktijken waar bepaalde criminele samenwerkingsverbanden zich schuldig aan maken. Deze ‘overtuigingswijze’ kan leiden tot het intrekken van klachten of getuigenissen (Kruisbergen et al., 2012).

De vijfde functie van geweld is de enige emotionele functie in deze lijst. De ervaring om bedrogen en/of verraden te worden leidt tot wraak en woede waarbij een crimineel samenwerkingsverband tot de keuze kan komen een gewelddadige handeling te stellen (Kruisbergen et al., 2012).

3.3 De financiering van georganiseerde misdaad

3.3.1 Insourcing en Outsourcing

Criminele samenwerkingsverbanden passen verscheidene methoden toe om hun illegale ‘bedrijf’ te financieren. Echter hebben legale en illegale bedrijven volgens Naylor (2002) een verschillend doel voor ogen. Legale bedrijven zoeken naar opportuniteiten om winstmaximalisatie te bekomen. Illegale criminele bedrijven zullen net risicominalisatie nastreven, in plaats van winstmaximalisatie. De winstmaximalisatie bij reguliere bedrijven zorgt voor een streven naar het in handen nemen van tussenliggende schakels die tussen product en consument liggen met als doel de winst te vergroten. Bij risicominalisatie zullen criminele samenwerkingsverbanden proberen aan *outsourcing* te doen, waarbij ze net zo min mogelijk proberen activiteiten in eigen beheer te bezitten. Om meer scheiding te bekomen tussen organisatie en autoriteiten, proberen criminele samenwerkingsverbanden dus via *outsourcing* zo min mogelijk directe controle te hebben over het productie- en distributieproces en zoveel mogelijk activiteiten uit te voeren buiten de eigen organisatie (Naylor, 2002).

Maar Kruisbergen et al. (2012) spreken deze risicominalisatie tegen. Zij stellen dat schakels buiten de eigen organisatie kunnen leiden tot risicomaximalisatie, aangezien de scheiding tussen autoriteit en crimineel samenwerkingsverband nooit waterdicht is. Een mensenhandelaar die via een derde partij ramen huurt om zijn prostituees aan het werk te stellen, loopt het risico dat deze derde partij mogelijk verklaringen aflegt bij de politie. Elke derde vormt dan een mogelijk risico voor het voortbestaan van het crimineel samenwerkingsverband. Kruisbergen et al. (2012) stellen vervolgens dat juist risicominalisatie misschien zelfs kan bekomen worden door zoveel mogelijk activiteiten in eigen beheer te hebben. Daarnaast hangt alles af van de kennis, mogelijkheden en capaciteiten dat het crimineel samenwerkingsverband bezit. Om iets te beheren, moet je het ook kunnen. Ten slotte leidt *insourcing*, het eigen beheer van de activiteiten, tot meer winstmarge. In dit laatste geval kunnen we ook spreken van ‘universele zelfdoeners’ die elke stap binnen het productie- en distributieproces van hun product beheersen (Kruisbergen et al., 2012). Denk hier bijvoorbeeld aan een crimineel samenwerkingsverband dat in cocaïne handelt, waarbij het in Colombia de cocaïne versnijdt, naar België via de Antwerpse haven smokkelt om vervolgens zelf te distribueren in het Gentse uitgangleven.

De keuze van *in-* en *outsourcing* zal verschillen van crimineel samenwerkingsverband tot crimineel samenwerkingsverband (Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Enerzijds haalt professor Kleemans (persoonlijke communicatie) aan dat we het proces uitbesteden (*outsourcing*) minder zien (Kleemans, persoonlijke communicatie). Anderzijds halen zowel Farcy (persoonlijke communicatie) als Paternotte (persoonlijke communicatie) aan dat criminele organisaties net wel hun activiteiten gaan verdelen, mits er voldoende financiële middelen aanwezig zijn (Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Net als op de economische markt is het een kwestie van vraag en aanbod (Kleemans, persoonlijke communicatie; Pauwels, persoonlijke communicatie; X, persoonlijke communicatie). Zo zal bijvoorbeeld een criminele onderneming gespecialiseerd in witwassen meer geld vragen, maar zal het risico op betrapping lager liggen (X, persoonlijke communicatie). Verder hangt alles af van de vertrouwensband (Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie).

In sommige gevallen zal de tussenschakel niet weten dat hij/zij zich schuldig maakt aan criminele activiteiten. Dit kan bijvoorbeeld een vrachtwagenfirma zijn die de goederen van punt A naar punt B brengt voor zijn klant, onwetende dat de goederen bestaan uit drugs. Sommige tussenschakels zullen doelbewust meewerken voor financieel voordeel of uit dwang (Kruisbergen et al., 2012).

3.3.2 Tussenkomst van een derde partij

Om leverings- of betalingsproblemen te vermijden, zetten sommige criminele samenwerkingsverbanden een onpartijdige derde in om de partijen bij elkaar te brengen. Deze onpartijdige derde is vervolgens ook aanwezig wanneer deze partijen zakelijke afspraken maken. Soms kan een derde partij ook een ‘depot functie’ vervullen. In dit geval zal de derde partij een rekening hebben waar personen die bijvoorbeeld zaken doen met mensensmokkelaars vooraf geld op kunnen storten. De som geld bedoeld om de persoon over een bepaalde landsgrens te smokkelen wordt dan door deze derde partij overgemaakt aan de mensensmokkelaars wanneer de gesmokkelde persoon hiervoor zijn toestemming geeft (Kruisbergen et al., 2012).

Criminele samenwerkingsverbanden kunnen ook beroep doen op gespecialiseerde financiële diensten wiens taak het witwassen van illegale inkomsten is. Dit witwassen via een gespecialiseerde derde komt vaker voor dan dat criminele samenwerkingsverbanden het geld afkomstig uit hun criminele activiteiten zelf witwassen. Maar dit gebeurt doorgaans binnen eigen bedrijven die als dekmantel fungeren. Dit kan bijvoorbeeld een autohandelaar zijn die voertuigen verhuurt, maar die niet te herleiden zijn naar de verhuurder/dader. Daarnaast zullen deze financiële specialisten zorgen voor het oprichten van rechtspersonen, het fiscaal afschermen van het crimineel vermogen en het crimineel vermogen doorsluizen en investeren (Kruisbergen et al., 2012; Christensen, 2012).

3.3.3 Symbiotische en parasitaire georganiseerde misdaad

Georganiseerde criminaliteit kan symbiotisch of parasitair zijn (Kruisbergen et al., 2012). Aansluitend zijn criminele samenwerkingsverbanden hedendaags polycrimineel (Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Dit wilt zeggen dat ze zich niet enkel meer focussen op één criminele activiteit, maar op meerdere tegelijkertijd. De manieren waarop een crimineel samenwerkingsverband aan geld komt, kan in een schemerzone liggen. Zo kan een crimineel samenwerkingsverband een volledig officieel bedrijf hebben met legale inkomsten, waarbinnen het ook aan illegale praktijken doet. Zo kan je bijvoorbeeld een transportfirma hebben en naast legale goederen ook drugs vervoeren (Farcy, persoonlijke communicatie).

3.3.3.1 Symbiotische georganiseerde misdaad

Symbiotische georganiseerde misdaad zijn georganiseerde criminaliteitsvormen die marktgeoriënteerd zijn. Ze spelen daarbij in op de vraag via de levering van een dienst of goed. Er dient dus een economische voedingsbodem aanwezig te zijn. Denk maar aan drugs- en wapenhandel (Kruisbergen et al., 2012).

Net als Nederland heeft België te maken met voornamelijk transitcriminaliteit. België speelt daarbij de rol als productie, doorvoer- of bestemmingsland (Dienst voor het strafrechtelijk beleid, 2010; Kruisbergen et al., 2012; Pieteraerens, persoonlijke communicatie). Goederen worden dan in een land gekocht waar het goed een lage waarde heeft en doorverkocht in België waar het goed een hogere waarde heeft. Bij drugshandel is de productiekost laag, maar door het illegale karakter van het goed kunnen criminele samenwerkingsverbanden de drugs verkopen aan woekerprijzen (Kruisbergen et al., 2012).

De winst hoeft niet steeds gehaald te worden uit de verkoop van goederen, maar kan ook bestaan uit de productie van het goed of het transport naar België, waarbij andere criminele samenwerkingsverbanden of individuen het goed verkopen (Kruisbergen et al., 2012). Zo zal je bijvoorbeeld in een gemeente als Temse zowel productie, doorvoer als gebruik aantreffen. Hier spelen de harde maatregelen in Nederland zeker een rol in, waardoor je uitkomt op een ‘waterbedeffect’ waarbij de drugsproductie van Nederland naar België verhuist (Pieteraerens, persoonlijke communicatie).

3.3.3.2 Parasitaire georganiseerde misdaad

Parasitaire georganiseerde misdaad zijn georganiseerde criminaliteitsvormen die niet marktgeoriënteerd zijn. Financieel voordeel wordt hier bekomen door iets af te nemen of te onthouden van anderen. Denk maar aan fraude, mensenhandel, diefstal en afpersing (Kruisbergen et al., 2012).

3.3.4 Fraude en witwassen

Fraude komt tot stand via bedrijven of vennootschappen. Deze bedrijven kunnen eigen bedrijven zijn, maar kunnen ook bedrijven zijn waar de dader in dienst is/was. Soms worden ondernemingen opgericht met als enige doel fraude te plegen, waardoor deze ondernemingen als dekmantel fungeren voor criminele activiteiten (Kruisbergen et al., 2012; X, persoonlijke communicatie).

De vrije kapitaalmarkt stimuleerde in deze geglobaliseerde wereld grensoverschrijdende financiële stromingen. Tussen 1990 en 2006 zijn deze financiële stromingen verachtvoudigd en bereikten samen een waarde van 8.2 biljoen dollar waarvan één/vijfde illegaal geld is, ook wel *dirty money* genoemd. Het witwassen van dit illegaal bekomen geld op industriële schaal krijgt volgens Christensen (2012) weinig politieke aandacht aangezien de politiek zich stort op de grensoverschrijdende geldstromen van mensenhandel en terrorisme (Christensen, 2012). Om dit geld wit te wassen verplaatsen criminele samenwerkingsverbanden het illegaal bekomen geld naar belastingparadijzen die fiscaal-juridisch afgeschermded jurisdicties vormen. In deze belastingparadijzen is er weinig regulering, lage belastingtarieven voor buitenlands kapitaal en is er bankgeheim om de inhoud van de rekening te verdoezelen (Christensen, 2012, Kruisbergen et al., 2012; Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie; X, persoonlijke communicatie).

Een transnationaal crimineel samenwerkingsverband zal dan ook steeds op zoek gaan naar landen waar de regelgeving en/of de maatregelen zwak zijn (Williams, 2001; X, persoonlijke communicatie). Een gevestigde vennootschap opgericht in een belastingparadijs of het geld op een bankrekening in een belastingparadijs zijn door alle voornoemde juridische voordelen moeilijk te herleiden tot het crimineel samenwerkingsverband. In het onderzoek van Kruisbergen et al. (2012) was er in achtentwintig van de honderdvijftig cases sprake van een rechtspersoon of bankrekening in een belastingparadijs afkomstig van een crimineel samenwerkingsverband (Kruisbergen et al., 2012). Het risico dat een crimineel samenwerkingsverband loopt met het illegaal bekomen geld grensoverschrijdend te investeren in bijvoorbeeld een vennootschap op de Kaaimaneilanden is bijzonder laag. Er wordt bijvoorbeeld geschat dat amper 0,01 procent van de *dirty money* dat door Zwitserland passeert, daadwerkelijk gedetecteerd wordt (Christensen, 2012).

Een vorm van fraude is het witwassen van illegale inkomsten. Zoals aangehaald in 3.3.2 “tussenkost van een derde partij” wordt het witwassen van illegale inkomsten vaak uitbesteed aan financiële specialisten. Het doel van witwassen is om van zwart geld, afkomstig uit criminele activiteiten, een legale vorm van inkomsten te maken. Het geld dat verdiend werd met criminele activiteiten wordt dan de winst die de eigen witwasonderneming, bijvoorbeeld een autoverhuurbedrijf, heeft gemaakt. Dit voorbeeld is niet uit de lucht gegrepen, aangezien uit het onderzoek van Kruisbergen et al. (2012) blijkt dat autobedrijven vaak voorkomen als witwasondernemingen (Kruisbergen et al., 2012). Inzake witwassen speelt contant geld een grote rol en wordt ook fysiek aan geldtransport gedaan (Kleemans, persoonlijke communicatie).

4. Terrorisme

“When it comes to terror, the beginning of wisdom is to recognize it as a strategy”

– Charles Tilly (2005, p27)

4.1 Definiëring en inhoud van het begrip ‘terrorisme’

4.1.1 Definiëring van terrorisme en haar aspecten

Onderstaande definities van terrorisme en haar aspecten worden gehanteerd doorheen deze scriptie. Aangezien criminologie een humane wetenschap is, zijn de definities sociale constructies die vaak niet universeel gedefinieerd zijn (Onwudiwe, 2001; Mahan & Griset, 2008; Sinai, 2008; Schmid, 2012). Daardoor is het van belang om in deze paragraaf duiding te geven wat exact wordt verstaan onder de kernbegrippen van terrorisme in deze scriptie.

Het definiëren van de term ‘terrorisme’ is net als bij de term ‘georganiseerde misdaad’ ambigu. Deze term heeft geen universeel geaccepteerde definitie, waarbij ook rekening gehouden dient te worden met de laatste trends in de doelstellingen die terroristische groeperingen wensen te bereiken en in de oorlogsvoering tegen terrorisme (Mahan et al., 2008; Sinai, 2008; Schmid, 2012). De Verenigde Naties zijn nooit tot een internationaal legaal verbonden definitie van terrorisme gekomen (Schmid, 2011; Holtmann, 2014). Dit is niet verwonderlijk aangezien terrorisme een begrip is, waarbij de begripsinvulling fluctueert doorheen de tijd (Rapoport, 2001; Horgan, 2005; Mahan et al., 2008). Daarnaast bestaat er niet één, maar verschillende vormen van terrorisme, wat de invulling nog verder bemoeilijkt (Löckinger, 2005; Horgan, 2005; Mahan et al., 2008; Kleemans, persoonlijke communicatie; Schmid, persoonlijke communicatie). Ook Walter Reich (1998) stelt dat terrorisme een complex en divers fenomeen is dat zich niet laat vatten in een simpele universele definitie. Het is zowel een uitdaging voor onze intellectuele inzet om het fenomeen te doorgronden als voor onze collectieve inzet om het fenomeen te controleren (Reich, 1998). Maar het definiëren van het begrip terrorisme is van belang, doordat de invulling van de definitie reële gevolgen heeft. Zo zal bijvoorbeeld het coördineren van internationale *counterterrorism* operaties geaccepteerde standaarden en definities behoeven (Mahan et al., 2008).

Voor deze scriptie gebruiken we de vaak gebruikte definitie van het Ministerie van Buitenlandse Zaken van de Verenigde Staten uit 1983. Deze definitie definieert ‘terrorisme’ als met voorbedachte rade, politiek gemotiveerd geweld uitgevoerd tegen ongewapende doelwitten door provinciale groeperingen of clandestiene agenten, meestal bedoeld om een publiek te beïnvloeden (Sinai, 2008). Enkele termen die onderdeel vormen van deze definitie hebben nood aan iets meer verduidelijking.

- De term ‘ongewapend’ bestaat zowel uit burgers als uit militair personeel dat ongewapend is of niet dienstdoende is op het moment van de aanslag (Sinai, 2008).
- De term ‘internationaal terrorisme’ refereert naar terrorisme waarbij burgers of territoria betrokken is van meer dan één land (Sinai, 2008).
- Onder de term ‘terroristische groepering’ verstaan we een groepering, of significante subgroeperingen, bestaande uit minstens twee individuen die geëngageerd zijn in terrorisme-gerelateerd geweld en zich schuldig maken aan internationale terrorisme (Sinai, 2008).

Ondanks we een vaak gebruikte definitie van de term ‘terrorisme’ hanteren, dienen we rekening te houden met een gebrek dat eigen is aan deze definitie. Met de mogelijke oplossingen voor dit gebrek houden we gedurende de gehele scriptie rekening, waardoor we binnen de grenzen van onze definitie, de term ‘terrorisme’ zo ruim mogelijk benaderen en hanteren. De meeste definities, waaronder onze definitie uit 1983, zien het beïnvloeden van een bepaald publiek en het verspreiden van angst onder dat bepaald publiek als de maatschappelijke focus van terroristische groeperingen. Echter hebben de aanslagen van 9/11 te New York en de aanslagen van 3/11 te Madrid aangetoond dat groeperingen zoals al Qaida niet enkel angst wensen te verspreiden onder een welbepaald publiek en dat welbepaalde publiek wensen te beïnvloeden. Dergelijke groeperingen wensen ook massaal menselijke slachtoffers en fysieke schade te veroorzaken bij hun vijanden. Hieruit komt voort dat we bij de term ‘terrorisme’ mede rekening houden met een component van ‘massavernietiging’, naast de componenten ‘beïnvloeding’ en ‘angst’ (Sinai, 2008).

Indien we spreken van de term ‘terrorisme’ of ‘terroristische groepering’ dienen we ook rekening te houden met de term ‘terrorist’. Onder de term ‘terrorist’ verstaan we een individu dat aangesloten is bij een groepering die zich schuldig maakt aan terrorisme-gerelateerd geweld en aan internationaal terrorisme, alsook toebehorende aan een ondersteunende infrastructuur wiens activiteiten bijdragen aan geweld in termen van training, planning, fondsenwerving, logistiek (Sinai, 2008). Daarnaast vallen ook volgende individuen onder de term ‘terrorist’ volgens Sinai (2008):

- Individuen die militaire training krijgen van terroristische groeperingen.
- Individuen die ambiëren geweld te plegen en dit meedelen via *internet chat rooms*.
- Individuen die behoren tot politieke, sociale of andere groeperingen die aanhang vertonen voor terroristische activiteiten.
- Individuen die terroristische activiteiten steunen of anderen overtuigen om deel te nemen aan terroristische activiteiten of deze te ondersteunen.
- Individuen die weet hebben van een dreigende terroristische operatie door anderen, maar die niet de autoriteiten hierover verwittigen.
- “Zelf-gerekruteerde” individuen (“*lone wolf*”) die zich schuldig maken aan terroristische activiteiten.

De term ‘contraterrorisme’ duidt de offensieve strijd door een overheid of overheden tegen terrorisme aan met als indirect doel het verdedigen van nationale en internationale belangen (Sinai, 2008). In de Verenigde Staten wordt deze offensieve strijd ook wel de ‘*war on terror*’ genoemd. Er bestaan vijf verschillende mogelijkheden om contraterrorisme te benaderen: een dwingende benadering (oftewel ‘*coercive counterterrorism*’), een proactieve benadering (oftewel ‘*proactive counterterrorism*’), een overredende benadering (oftewel ‘*persuasive counterterrorism*’), een defensieve benadering (oftewel ‘*defensive counterterrorism*’) en een lange termijn benadering (oftewel ‘*long-term counterterrorism*’) (Crelinsten, 2014).

- De dwingende benadering van contraterrorisme vertrouwt op de monopolie van de staat om geweld te gebruiken (Crelinsten, 2014).
- De proactieve benadering van contraterrorisme heeft als doel terroristische aanslagen te verhinderen, met andere woorden vóór de aanslagen gepleegd worden (Crelinsten, 2014).
- De overredende benadering van contraterrorisme probeert terrorisme te bedwingen via communicatie, aan de hand van propagandacampagnes en het gebruik van beloningen (Crelinsten, 2014).

Dit door bijvoorbeeld terroristen een beloning te geven wanneer ze geweld verlaten en geweldloze wegen gebruiken om hun ideologie en ideeën over te dragen (Crelinsten, 2014).

- De defensieve benadering van contraterrorisme neemt aan dat een terroristische aanslag onvermijdelijk is. Daarom bereidt deze benadering zich voor op een terroristische aanslag door het beïnvloeden van de variabelen die de aard van de aanslag of de identiteit van het doelwit bepalen (Crelinsten, 2014).
- De lange termijn benadering bij contraterrorisme draait rond initiatieven die geen snelle oplossingen beloven, maar oplossingen op lange termijn beloven. Dergelijke initiatieven betreffen bijvoorbeeld de basisoorzaken van terrorisme en de structurele factoren die instaan voor een geschikt klimaat voor het gebruik van terrorisme (Crelinsten, 2014).

'Foreign fighters' zijn mensen die onbetaald willen strijden in een conflict waar ze geen duidelijk verband mee hebben, uitgezonderd van hun religieuze affiniteit met de islam (Hegghammer, 2010). Evenwel kan het verband ook historisch zijn (Pauwels, persoonlijke communicatie).

De term 'jihad' wordt in de Westerse wereld aanzien als een vorm van terrorisme, gevoed door een religieuze affiniteit met de islam, en wordt ook wel 'de heilige oorlog' genoemd. Doch betekent 'jihad' niet voor iedereen hetzelfde en wordt het niet door iedereen als een vorm van terrorisme aanzien (Holtmann, 2014).

De term 'jihad' kan verdeeld worden in: de strijd van het hart en de ziel (als in het bestrijden van het kwade), de strijd van de tong en de pen (als in het verspreiden van het woord van de islam), de strijd van de hand (als in het ondernemen van politieke actie of protest) en de strijd van het zwaard (als in het vechten met wapens). Nochtans is de dominante betekenis van de term 'jihad' in de Soennitische moslim cultuur die van een islamitische oorlogsvoering, met de intentie om te doden (Holtmann, 2014). In deze scriptie houden we ons bij de dominante betekenis, omdat deze dominante betekenis aansluit bij de term 'terrorisme'.

4.1.2 Politieke belangstelling voor terrorisme

De Europese Unie maakt heel wat strategieën en actieplannen voor de strijd tegen terrorisme. Hierbij wordt aandacht besteed aan verschillende luiken zoals repressie en preventie (Europa, 2015c). Ook het grensoverschrijdend witwassen van het illegaal bekomen geld bij terrorisme krijgt volgens Christensen (2012) veel politieke aandacht en dat zie je ook in de actieplannen die de Europese Unie bekend maakt op haar website. Zo zijn er actieplannen rond het bevrozen van het vermogen van terroristen of hoe dient te worden omgegaan met witwassen (Christensen, 2012; Europa, 2015c).

4.1.3 Beeldvorming van terrorisme

Aan terrorisme wordt immens veel aandacht besteed sinds de aanslagen in New York op 11 september 2001. Nochtans waren de New Yorkse aanslagen niet de geboorte van het fenomeen terrorisme. Waarschijnlijk bestaat terrorisme in één of andere vorm sinds de organisatie van mensen in hiërarchische samenlevingen (Wright-Neville, 2010). Terrorisme is geëvolueerd in golven, waarbij elke golf de politieke, technologische en sociale omstandigheden van die periode reflecteert (Rapoport, 2001; Horgan, 2005; Mahan et al., 2008). Geschiedenis leert ons dat terrorisme eigen is aan de mens en niet geëlimineerd kan worden door gebruik van de juiste strategieën, maar mogelijk ten minste tijdelijk gehandhaafd kan worden (Mahan et al., 2008).

Terrorisme globaliseert tegelijkertijd met de wereldglobalisering. Waar de wereldglobalisering tracht mensen dichterbij te brengen, tracht terrorisme een ideologie te verspreiden of net die wereld te verkleinen in kleinere oppervlaktes (Mahan et al., 2008). Barber (1992) spreekt hier over "*McWorld*", het globaliseren van de wereld door economie en internet, versus jihad. De meeste hedendaagse terroristen zien de begripsinvulling van jihad als het gevecht ten opzichte van de vijanden van de Islam, waarbij in casu de globalisering wordt aanschouwd als een vijand (Barber, 1992; Mahan et al., 2008).

Terroristische activiteiten maken meestal deel uit van een campagne gevoed door geweld, dat door middel van een opeenvolgend karakter aan geweldsdaden en dreigingen, een doordringend klimaat van angst creëert (Schmid, 2011; Schmid, 2012).

Deze angst wordt gecreëerd door de aard van de misdrijven, door haar zinloosheid, de wijze waarop deze misdrijven worden gepleegd en haar onverschilligheid ten opzichte van de waarde van het menselijke leven. Dit doordringende klimaat van angst is de bron van macht voor terroristen en maakt het mogelijk voor terroristen om de politieke gang van zaken te manipuleren (Schmid, 2011; Schmid, 2012). Dit is ook de reden waarom dit hoofdstuk begint met een citaat van Charles Tilly (2005): “*When it comes to terror, the beginning of wisdom is to recognize it as a strategy*” (Tilly, 2005, forword). Terrorisme zorgt via terreur voor angst, langs waar het onder andere haar politieke agenda naar buiten tracht te brengen.

Redenen voor terrorisme kunnen divers zijn. Terrorisme kan gepleegd worden om collectieve redenen, individuele redenen, morele redenen en om ‘gebruiksnuttige’ redenen waarbij bij dit laatste terrorisme een werkinstrument is om een bepaald doel te bereiken (Mahan et al., 2008; Crenshaw, 2008). Wanneer terrorisme als werkinstrument wordt gebruikt, kan het zijn dat terrorisme dient als een *ultimum remedium*. De terrorist heeft om een doel te bereiken al verschillende methoden ondernomen, maar faalden telkens, waardoor hij/zij overging op hun ‘enige laatste keuze’, namelijk terrorisme. Dit zagen we bijvoorbeeld in Ierland bij het falen van het constitutionalisme van Parnell (Crenshaw, 2008).

4.1.4 Soorten terrorisme

Net als de term ‘georganiseerde misdaad’ wordt de term ‘terrorisme’ gebruikt als verzamelnaam voor een verscheidenheid aan vormen van terrorisme. Net als bij georganiseerde criminaliteit kan elk aspect, van rekrutering tot financiering, in elke terroristische groepering verschillen (Löckinger, 2005; Horgan, 2005; Kleemans, persoonlijke communicatie; Schmid, persoonlijke communicatie). Aangezien elk aspect van elke terroristische groepering ter wereld invullen enorm veel tijd en data zou vragen, kijken we, net als in het hoofdstuk ‘georganiseerde criminaliteit’, naar meer algemene opvattingen. De grootte van het begrip terrorisme kan aangetoond worden aan de hand van het boomdiagram van Löckinger (2005) die je kan terugvinden in de bijlagen onder puntje 9.1 ‘figuren’. Löckinger (2005) splitst terrorisme op in subgroepen door middel van enkele specifieke elementen: betrokken actoren, middelen en gebruikte methoden, motieven en geografisch bereik. Zo vallen onder terrorisme waarbij het specifieke kenmerk is welke actor betrokken is: staatsterrorisme, *state-sponsored terrorism* en revolutionair terrorisme (Löckinger, 2005).

Wanneer het specifieke element methode is, kan er een opdeling gemaakt worden tussen zelfmoordterrorisme, cyberterrorisme en *CBRN terrorism*. Deze laatste vorm van terrorisme is een verzamelnaam voor bio-terrorisme, nucleair terrorisme en chemisch terrorisme. Wanneer je gaat opdelen op basis van motief kan je opdelen in religieus terrorisme, drugsterrorisme en politiek terrorisme, waarbij politiek terrorisme kan opgedeeld worden in *single-issue terrorism* waarbij de groepering één doel zoekt te verwezenlijken, *left-wing terrorism* en *right-wing terrorism*. Ten slotte kan je terrorisme ook opdelen door haar geografische bereik. In dat geval kan je terrorisme opdelen in *domestic terrorism* en *international terrorism* (Löckinger, 2005).

Aangezien terrorisme een evoluerend begrip is dat door de tijd heen fluctueert, leidt het ook tot het ontstaan van nieuwe soorten terroristische groeperingen (Rapoport, 2001; Horgan, 2005; Mahan et al., 2008). Zo zal de toename van het gebruik van ICT ook haar impact hebben op de soorten terroristische groeperingen, zoals het ontstaan van *terrorist cum hackers*. Dit zijn individuen die beschikken over technische vaardigheden om via het hacken terrorisme te ondersteunen (Zanini & Edwards, 2001). Zo hebben strijders van IS op 9 april 2015 de sociaalnetwerkkanalen, zender en website van de Franse zender TV5 Monde gehackt, waarbij de hackers via deze media propaganda verspreidde (Knack, 2015). Op 15 april 2015 hebben strijders van IS geprobeerd om Nederlandse, Britse en Amerikaanse sites te hacken door middel van cyberaanvallen, en hebben tegelijkertijd de Twitterpagina van de populaire Egyptische radiozender Nugoum gehackt (Terrorismemonitor, 2015a; Terrorismemonitor, 2015b).

4.1.5 Foreign fighters

Het fenomeen van *foreign fighters* is een actueel relevant fenomeen. In deze context passeren in de media IS en Boko Haram vaak de revue. Volgens cijfers van de Verenigde Naties zijn er al meer dan vijftienduizend *foreign fighters* afkomstig uit meer dan tachtig landen naar Syrië en Irak vertrokken om daar te strijden aan de zijde van IS (Bajekal, 2014). Dit fenomeen is echter niet nieuw (Stern, 2003; Pauwels, persoonlijke communicatie). Zo rekruteerde in 1994 Spaanse extremisten die lid waren van al Qaida, individuen in de Abu Bakr moskee in Spanje en stuurde hen naar trainingskampen in Bosnië, Pakistan en de Filipijnen (Stern, 2003).

Verder streden in Belfast Amerikanen mee, aangezien hun grootouders afkomstig waren van Ierland en ze dus historische banden hadden met Ierland. Het grote verschil met vroeger is de technologische innovatie, waardoor rekrutering en verspreiding van ideeën gemakkelijker gaat dan voorheen (Pauwels, persoonlijke communicatie).

De Verenigde Naties stelt dat de kern van al-Qaida zwak is en dat deze verzwakking leidt tot een toename van jihadistische steun aan IS. IS is een afgesplinterde groepering van al-Qaida, maar beide groeperingen streven naar gelijkende strategische doelen, maar wel met tactische verschillen (Bajekal, 2014). Een andere voorbeeld van een dergelijke groepering is Boko Haram. Boko Haram is een groepering die gelooft dat de politiek in Noord-Nigeria ingenomen wordt door corrupte, valse moslims. Het wenst daardoor een oorlog met Nigeria, met als doel een pure islamitische staat te creëren die de sharia hanteert (Walker, 2012).

Religieus terrorisme probeert dan ook misbruikt te maken van een wereldgodsdienst. Deze godsdienst biedt een grote wereldwijde vijver om leden uit te wisselen. Dit is een belangrijk element dat verschilt afhankelijk van de soort terrorisme. Bij extreemlinkse of –rechtse groeperingen is de vijver klein aangezien het bestaat uit lokale burgers. Zo zal je bij bijvoorbeeld ETA geen grote volksverhuizing zien als bij IS (Pauwels, persoonlijke communicatie).

Niet enkel op Belgisch nationaal niveau is er een belangstelling voor het fenomeen van *foreign fighters*, echter ook op internationaal niveau. Zo is er op Europees niveau een systematische uitwisseling van gegevens inzake Syriëstrijders opgezet tussen België, Nederland, Groot-Brittannië, Ierland, Spanje, Duitsland, Frankrijk, Denemarken en Zweden. Deze negen Europese landen zijn het zwaarst getroffen in aantal Syriëstrijders (Belga, 2014).

4.2 De organisatie van terrorisme

4.2.1 Rekrutering

Uit een onderzoek van Post, Sprinak en Denny (2010) bestaande uit interviews met vijfendertig terroristen actief in het Midden-Oosten kwam naar voren dat de achtergronden van de ondervraagde terroristen enorm verschilden en geen invloed hadden op hun beslissing om toe te treden tot een terroristische beweging (Post, Sprinak & Denny, 2010).

Dertig procent van de seculiere respondenten en twintig procent van de religieus-geïnspireerde respondenten gaven aan dat familie een primaire rol speelde bij de rekrutering in een terroristische groepering (Post, Sprinak & Denny, 2010). Er kan druk uit de familie voortkomen dat de gerekruteerde geen goede moslim is, waardoor hij mogelijk zich buitenstaander kan voelen. Door zich te rekruteren kan hij zich tegenover zijn familie bewijzen als goed moslim (Pieteraerens, persoonlijke communicatie). Het merendeel van de ondervraagden hadden wel familieleden die gerespecteerd werden binnen de moslimgemeenschap en steunden vaak de keuze van de respondent om terrorist te zijn. Deze steun kwam voornamelijk voor bij familieleden die politiek actief waren. Evenwel waren familieleden die niet politiek actief zijn, niet ontradend. In tachtig procent van de interviews was de respondent het enige familielid dat een terroristische groepering vervoegde. Wanneer toch een (vaak) jongere broer of zoon ook gaat strijden bij een terroristische groepering, vervoegt hij zich voornamelijk bij dezelfde terroristische groepering als zijn oudere broer of vader. Indien niet, zal hij eerder opteren voor een meer radicalere groepering (Post et al., 2010).

Meer dan familie blijkt sociale omgeving en vriendengroep (*peers*) een grote invloed te spelen op de rekrutering (Post et al., 2010; Rajakumar, persoonlijke communicatie). In veel gevallen blijkt het een vriend of kennis in de vriendengroep te zijn die een persoon zal rekruteren. Meer dan de helft van de respondenten kenden hun ronselaar al vóór de rekrutering. Deze bekende hoeft geen vriend te zijn, maar kan een kennis of familielid zijn. Vierenzestig procent van de seculiere terroristen en drieënveertig procent van de religieuze terroristen in het onderzoek van Post, Sprinak en Denny (2010) verklaarde dat de groepering waar ze toebehoorden het meest actief was in hun gemeenschap. Iets meer dan de helft van de seculiere respondenten gaf aan dat hun gemeenschap en/of een jongerenclub in de gemeenschap de primaire rol speelde bij rekrutering. Wanneer het aankwam op de religieus-geïnspireerde respondenten gaf ongeveer de helft aan dat de moskee, Moslim Broederschap of een andere religieuze invloed centraal stond bij de rekrutering. Twintig procent van de religieus-geïnspireerde respondenten gaf aan dat de universiteit of een professionele school de primaire rol speelde bij de rekrutering (Post et al., 2010). Ook Rajakumar (persoonlijke communicatie) haalt aan dat rekrutering kan voorkomen op scholen en universiteiten (Rajakumar, persoonlijke communicatie).

Radicalisering aan een universiteit was bijvoorbeeld het geval bij Saïd Kouachi, die de aanslag op Charlie Hebdo pleegde, toen hij in Yemen aan de Iman universiteit studeerde en les kreeg van de fundamentalistische predikant Abdel Majeed al-Zindani. Deze laatste staat op de Amerikaanse terreur *blacklist* (Burke, 2015).

Stern, J. (2003), Mullins, S. (2009), Jaak Raes, administrateur-generaal van de Staatsveiligheid (2015), Pauwels (persoonlijke communicatie), Farcy (persoonlijke communicatie) en Rajakumar (persoonlijke communicatie) halen net als Post et al. (2010) de sociale omgeving, zoals moskeeën, jongerenclubs en fitnessen, aan als sleutelfiguur in de radicalisering van een persoon (Stern, 2003; Mullins, 2009; nadb, 2015; Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Ook de Poot, Sonnenschein, Soudijn, Bijen & Verkuylen (2009) halen het belang van semi-openbare plaatsen zoals moskeeën aan als belangrijke eerste ontmoetingsplaats voor jihadisten (de Poot, Sonnenschein, Soudijn, Bijen & Verkuylen, 2009). Daarnaast haalt Mullins (2009) aan dat de belangrijkste radicaliseringshypothese inhoudt dat individuen worden geïdentificeerd vanuit een grote groep die mogelijk beïnvloedbaar zijn voor radicalisering om hen daarna privé in kleinere groepen te radicaliseren (Mullins, 2009). Deze hypothese wordt ook gevolgd door Stern (2003). Zij haalt aan dat een groepering individuen kan rekruteren in een moskee (grote groep) en deze individuen vervolgens naar trainingskampen sturen waar ze verder geradicaliseerd worden (Stern, 2003). Deze hypothese komt niet goed overeen met het onderzoek van Post et al. (2010). Zij stellen namelijk dat een minderheid op dergelijke manier gerekruteerd werd (Post et al., 2010).

Verder vormt de straat een goede plaats om te rekruteren en ligt dus in de lijn met Mullins' Sterns hypothese (Stern, 2003; Mullins, 2009; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Ook Michael Delefortrie, een Belgische teruggekeerde Syriëstrijder, gaf aan dat Sharia4Belgium, veroordeeld als netwerk dat individuen rekruteerde om in Syrië mee te vechten in de jihad, voorbijgangers op straat probeerden bewust te maken van hun geloof door middel van flyers uit te delen. Dit wordt ook wel een *street dawah* genoemd (Alde'emeh, 2014). Bij deze *street dawah's* pleegde Sharia4Belgium op een gestructureerde wijze propaganda en voorzag het vervoer richting Syrië (nadb, 2015; Pieteraerens, persoonlijke communicatie).

Ook professor Pauwels (persoonlijke communicatie) haalt de straat aan als rekruteringsplatform. Hij stelt dat de boodschap verkondigt kan worden en de persoon beïnvloed kan worden door neutrale vragen te stellen zoals: “Wat vind jij van dit probleem? Wil jij je niet aansluiten voor het goede doel?” (Pauwels, persoonlijke communicatie).

Door de grote toegankelijkheid en invloed van internet dringt verder ook het internet zich op als middel om potentiële leden te rekruteren (Weimann, 2006; Farcy, persoonlijke communicatie). Sociale media vormen hier een goed rekruteringsplatform (n.d., 2015; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Ronselaars rekruteren dus vaak op plaatsen waar veel jongeren zitten (Pauwels, persoonlijke communicatie). Ten slotte worden ook penitentiaire inrichtingen en asielcentra als rekruteringsplatformen aangehaald door de Poot et al. (2009). Daar zouden jihadisten op zoek gaan naar potentiële nieuwe leden die vatbaar zijn voor hun religieuze boodschap (de Poot et al., 2009). Zo is bijvoorbeeld IS ontstaan in de Iraakse gevangenissen (Dettmer & Schindler, 2015; Trends, 2015). Dit laatste ligt in de lijn met wat Dirjud Farcy zegt. Hij haalt aan dat heel wat strijders van IS komen uit het criminele milieu (Farcy, persoonlijke communicatie).

Om iemand te rekruteren, zal de terroristische organisatie een boodschap dienen over te dragen. Deze boodschap komt over in drie stappen. Eerst geeft de terroristische groepering aan wat er scheef zit in de samenleving. Vervolgens haalt de groepering aan wat een mogelijke oplossing is voor dit probleem. Ten slotte vertelt de groepering op welke manier deze oplossing kan bekomen worden. Zo is bijvoorbeeld een Islamitisch kalifaat de oplossing en valt dit te bereiken door terrorisme. Dit is echter niet nieuw, aangezien de boodschap in de jaren zeventig en tachtig door de Rode Brigades op dezelfde wijze werd overgebracht. Toen was de oplossing het communisme (Pauwels, persoonlijke communicatie).

Omtrent Kennismaking met het ‘goede doel’, groeiden bijna alle terroristen uit het Midden-Oosten in het onderzoek van Post et al. (2010) op in dorpen of vluchtelingenkampen waar het probleem voelbaar was. Amper tien procent van de respondenten kwamen niet uit een dergelijk dorp of vluchtelingenkamp. Het gevoel van slachtofferschap draagt bij aan het samenvloeien van de persoonlijke identiteit met de identiteit van de groepering (Post et al., 2010). Een reden tot dit slachtofferschap kan onderdrukking zijn (Onwudiwe, 2001; Horgan, 2005).

Terroristische groeperingen als IS gebruiken zeer professionele videoboodschappen om potentiële leden kennis te laten maken met het ‘goede doel’. Deze professionaliteit werkt in op de jeugd. Zo stelt professor Pauwels (persoonlijke communicatie) dat IS er bijna een game van maakt, waardoor je uitkomt op een zekere ‘*gamingfication* van de jihad’. Bijkomend gebruikt de groepering de mediakanalen die de huidige generatie gebruikt om hun boodschap over te brengen. Dit is een groot verschil van werken met andere terroristische groeperingen zoals al Qaida, waarbij de videoboodschappen van zeer slechte kwaliteit waren (Pauwels, persoonlijke communicatie).

Bij deze fusie van de individuele identiteit met de groeperingsidentiteit hebben terroristen moeite om een onderscheid te maken tussen persoonlijke doelstellingen en de groepsdoelstellingen (Tucker, 2008; Koomen & van der Plicht, 2009; Post et al., 2010). Deze fusie is een traag proces, waarbij het potentiële lid gradueel meer betrokken raakt in de groepering (Horgan, 2005). Deze fusie zorgt voor een voldoende rechtvaardiging om terroristische misdrijven te plegen. Als de groepering zegt dat een bepaalde actie nodig en gerechtvaardigd is, dan is het ook nodig en gerechtvaardigd (Tucker, 2008; Post et al., 2010). Niemand wilt achterblijven, want achterblijven kan worden gepercipieerd als trouweloosheid (Tucker, 2008). Ook leden van Sharia4Belgium waren zoekende naar een eigen identiteit en gingen zich net extreem engageren om zich in de groep te bewijzen (Pieteraerens, persoonlijke communicatie). De leden van een terroristische groeperingen komen dan in een polariserend “wij-zij”-verhaal terecht. Zo zal dit bijvoorbeeld bij moslimterrorisme het ‘wij’ de heilige oorlog zijn en het ‘zij’ de ongelovigen (Aquila et al., 2001b; Koomen et al., 2009; Pauwels, persoonlijke communicatie). Door middel van de fusie naar een groepsidentiteit krijgen de nieuwe leden beloningen zoals status, respect en bewondering (Horgan, 2005).

Een andere reden om zich aan te sluiten bij een terroristische groepering is wanneer men zich buitenstaander voelt binnen de samenleving (Horgan, 2005; Wright-Neville, 2010; Pauwels, persoonlijke communicatie). Zo stelt bijvoorbeeld Ahmad al-Haznawi al-Ghamidi, een terrorist betrokken bij 9/11, in een videoboodschap dat “de tijd van vernedering voorbij is” (Wright-Neville, 2010). Een mogelijke oorzaak van dit buitenstaandersgevoel is racisme. Sommige moslimterroristen haalden aan dat Islam hen hielp om vooruit te gaan in hun leven wanneer ze geconfronteerd werden met racisme (Wieviorka, 2004; Horgan, 2005; Koomen et al., 2009; Wright-Neville, 2010; Pauwels, persoonlijke communicatie).

In combinatie met de afwezigheid van andere etniciteiten in de media, spelen geïdealiseerde vormen van religie een belangrijke rol bij het vormen van een alternatief gevoel van gemeenschapsidentiteit. Bijkomend kan ook de sociaaleconomische status en werkgelegenheid bijdragen aan een gevoel van ongenoegen, een gevoel van sociale onrechtvaardigheid, een gevoel van buitenstaander en leiden tot frustraties met de kerninstituties van de samenleving (Horgan, 2005; Wright-Neville, 2010; Pauwels, persoonlijke communicatie). Terroristische groeperingen halen aan dat het ‘Westen in oorlog is met de Islam’. De groepering gaat dus polariseren en komt vervolgens uit op een zwart/wit-verhaal. Door te polariseren, vergroot de groepering net het ongenoegen bij de (potentiële) gerekruteerde (Pauwels, persoonlijke communicatie).

Gerekruteerd worden, is dus ook een kwestie van zelfselectie. De gerekruteerde zit met een ongenoegen en gaat zelf op zoek naar contacten. Hierbij heeft hij de kans om niet verder te gaan met het rekruteringsproces, wanneer hij vindt dat het te radicaal wordt (de Poot et al., 2009; Pauwels, persoonlijke communicatie). Echter wordt deze zoektocht gemakkelijker gemaakt door de propagandamachines die terroristische groeperingen hedendaags bezitten (Pauwels, persoonlijke communicatie).

In het onderzoek van Post et al. (2010) kwam naar voren dat bij de seculiere respondenten vijftien procent en bij de religieus-geïnspireerde respondenten dertig procent gerekruteerd werd op een formele manier. Deze formele rekrutering hield een eedaflegging en/of een probatieperiode in. Sommige respondenten gaven aan dat ze verschillende interviews moesten doorlopen waarbij ze geobserveerd werden door waarnemers achter een gespiegeld raam. Wanneer je al een familie- of gezinslid hebt in de groepering, kan het zijn dat je geen rekruteringsproces moet doorlopen. Wanneer dit voorkomt, gaat de groepering er vanuit dat je betrouwbaar bent, en dat je ‘lidmaatschap’ een gegeven is binnen de familie, gemeenschap en groepering (Post et al., 2010). Ook komt het voor dat er een screening plaatsvindt waarbij enerzijds wordt gekeken naar veiligheid en anderzijds naar geschiktheid van het individu (Horgan, 2005). Rekrutering in terroristische organisaties gebeurt dus soms niet zo anders dan bij gewone organisaties (Pauwels, persoonlijke communicatie).

Een strijder dient bij rekrutering ook niet bang te zijn of zijn ‘heldhaftige’ dood gevolgen kan hebben voor zijn familieleden post mortem. Terroristische groeperingen zijn zodanig georganiseerd dat ze familieleden van overleden strijders materieel en financieel ondersteunen. De familie in kwestie krijgt ook een respectvol aanzien binnen de groepering (Post et al., 2010; Pauwels, persoonlijke communicatie).

Ten slotte dient hier nog het belang van trainingskampen aangehaald te worden. Trainingskampen voor terroristen bestaan nog steeds, maar zijn moeilijk te verbergen door bijvoorbeeld het gebruik van satellieten (Pauwels, persoonlijke communicatie). Zo werden in 2011 Saïd en Chérif Kouachi, de terroristen achter de aanslag op Charlie Hebdo van 9 januari 2015, opgeleid in Yemen (Borger, 2015; Burke, 2015). Zoals later wordt aangehaald heeft IS momenteel een kamp in de Mexicaanse staat Chihuahua (Terrorismemonitor, 2015c).

4.2.2 Het netwerk binnen de terroristische groepering

Een trend die de laatste jaren voorkomt is dat terroristische groeperingen die zeer hiërarchisch en georganiseerd van aard zijn meer en meer evolueren naar terroristische groeperingen waarbij het netwerk lossier wordt. Een andere trend is dat de terroristische netwerken kleinschaliger worden, waarbij onder deze terroristische ‘cellen’ eenzelfde ideologische opvatting wordt gevolgd. Dergelijke groeperingen worden ook wel *leaderless networks* genoemd in de literatuur (Stern, 2003; Schmid, 2011; Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie). Deze evolutie naar kleinere groeperingen komt onder andere door de opkomst van steeds betere, steeds meer beschikbare en meer gesofisticeerde technologische middelen. Hierdoor kunnen de cellen onderling communiceren en activiteiten coördineren zonder een centraal commandocentrum. Er heerst dus een lokale autonomie, waarbij besluitvorming en activiteiten worden gedecentraliseerd, maar waarbij de cellen afhankelijk zijn van een constitutieve consensusvorming (Zanini et al., 2001; Marsden & Schmid, 2011). In tegenstelling tot een traditioneel hiërarchisch organisatie-model, beschikken netwerkmodellen over een grotere flexibiliteit, een grotere mogelijkheid tot aanpassing en een verhoogde mogelijkheid om gebruik te maken van de volle potentie/talenten van de leden (Zanini et al., 2001). Deze vorm van coördinatie en structurering wordt door Arquilla en Ronfeldt (2001a) ‘*netwar*’ genoemd. Deze *netwars* zijn meestal staatloos, worden niet door staten gefinancierd en kunnen zich internationaal focussen (Arquilla & Ronfeldt, 2001a).

Elke netwerkorganisatie heeft drie gemeenschappelijke elementen. Ten eerste vloeien coördinatie en communicatie niet via verticale of horizontale relaties, maar vloeien ze samen en veranderen ze afhankelijk van de voorliggende specifieke taak of doelstelling. Hierbij zijn de relaties voornamelijk informeel van aard. Ten tweede hebben interne netwerken ook linken naar de buitenwereld toe, waarbij deze linken vaak van internationale aard zijn. Ten derde zijn interne en externe banden mogelijk door middel van gedeelde waarden en normen en een tweezijdig vertrouwen (Monge & Fulk, 1999; Zanini et al., 2001). Volgens Zanini en Edwards (2001) zien we deze opkomst ook bij terroristische groeperingen. Deze transformering van hiërarchisch gevormde organisaties naar netwerkorganisaties is deel van het afstappen van formeel georganiseerde staatsgesponsorde groeperingen naar privaat-gefinancierde losse netwerken bestaande uit individuen en subgroeperingen die een tactische onafhankelijkheid bezitten (Zanini et al., 2001). In deze netwerkstructuren mogen terroristen operationele details in vraag trekken, zolang het niet gaat over ofwel de operatie al dan niet wordt uitgevoerd. Evenwel zullen netwerkstructuren variëren naargelang het soort terrorisme. Religieus-geïnspireerde terroristen zijn minder tolerant op de meningen van hun medestrijders, maar zijn vrijer om keuzes te maken in de lage cellen van de organisatie in vergelijking met seculiere terroristen. Seculiere groeperingen zijn dan weer hiërarchischer georganiseerd in vergelijking met religieus-geïnspireerde terroristen (Post et al., 2010).

Bij oudere groeperingen, ontstaan in de jaren zestig en zeventig, zoals de Palestine Liberation Organization (PLO), zien we een bureaucratische hiërarchisch gestructureerde organisatie. De PLO gebruikte wel autonome cellen als deel van hun georganiseerde structuur, maar deze werden geleid door een hiërarchie waarbij de nadruk lag op verticale relaties. Bij jongere actieve groeperingen zoals Hamas en Hezbollah is de organisatie minder hiërarchisch en bureaucratisch gestructureerd, maar meer los gestructureerd, waarbij religieuze en ideologische motieven worden gebruikt als gedeelde waarden en waarbij horizontale relaties de overhand nemen (Zanini et al., 2001).

In de literatuur worden drie netwerkstructuren herhaaldelijk aangehaald: dit zijn het *kettingnetwerk* (of *chain network*), het *ster- of hubnetwerk* en het *all-channel network*. Voorstellingen van deze soorten netwerken kan je terugvinden in de bijlagen onder 9.1 ‘figuren’. In het *kettingnetwerk* passeert informatie persoon per persoon zoals een *ketting*. In het *ster- of hubnetwerk* zijn groepen of individuen gelinkt aan een centraal punt. Ten slotte zijn in het *all-channel network* alle knooppunten gelinkt aan elkaar (Arquilla et al., 2001a; Marsden et al., 2011).

Het uitgangspunt van deze drie netwerkstructuren is dat organisaties samen worden gehouden door de linken die bestaan tussen verschillende knooppunten. Dit laat de organisatie toe om te communiceren, informatie uit te wisselen, om gezag over te brengen en het gedrag van de organisatie vorm te geven. Elk knooppunt binnen deze netwerkstructuren kan refereren naar een individu, een deel van een groep, een groep, een organisatie of een staat (Arquilla et al., 2001a; Marsden et al., 2011). Deze losjes gekoppelde netwerkorganisaties kunnen gekoppeld worden aan wat we voorheen zagen onder *leaderless networks*. Hun operaties worden gekarakteriseerd door een afwezigheid van controle op het tactische niveau, een zwakke beïnvloeding op het operationele niveau en met een strategische inbedding door leiders in de religieuze, sociale of politieke beweging (Marsden et al., 2001; Schmid, 2011; Farcy, persoonlijke communicatie).

In de literatuur wordt vervolgens gesteld dat inzake gezag drie types van groepen zijn in een organisatie: strak gecontroleerde groepen, gekoppelde netwerken en losjes gekoppelde netwerken. Strak gecontroleerde groepscommandanten oefenen tactische, strategische en operationele controle uit en plannen complexe operaties. Strak gecontroleerde groepen wordt voornamelijk gevonden in organisaties die onderhevig zijn aan hiërarchie. Gekoppelde netwerken hebben lossere relaties onder eenheden en beschikken over minder rechtstreekse vormen van communicatie. Losjes gekoppelde organisaties tonen een streven naar gezamenlijke doelen waarbij een gelijke ideologie heerst (Arquilla et al., 2001a; Marsden et al., 2011).

Een goed voorbeeld van een *netwar* is het netwerk van Osama bin Laden. Zijn terroristisch netwerk, genaamd al Qaida, was een multinationale samenwerking tussen islamextremisten. Het bestond uit relatief autonome groepen die allen gefinancierd werden door private bronnen en met een gedeelde ideologie, namelijk de “heilige oorlog” tegen het Westen en tegen alles wat een “dreiging” vormt voor de Islam. Ondanks dat de financiën via Osama bin Laden liepen, speelde bin Laden in dit verhaal niet een alles-controlerend commandocentrum. Hij speelde eerder een sleutelfiguur in de coördinatie en steun bij enkele knooppunten in het netwerk. Informatie kon via twee netwerken gaan: via een *hub-and-spoke* structuur of via een wielstructuur. In geval van de *hub-and-spoke* structuur ging de informatie via bin Laden en zijn dichtste adviseurs. In geval van de wielstructuur ging de informatie niet via bin Laden (Zanini et al., 2001; Kenney, 2007). Met andere woorden hebben niet alle knooppunten een gelijke vorm van autoriteit. Dit betekent dus dat al Qaida wel in het bezit was van een harde kern die een autoritair gezag had (Kenney, 2007; Tucker, 2008).

Deze autoritaire kern is ook het geval bij IS (Pauwels, persoonlijke communicatie). Dit is een belangrijk detail, aangezien het aantoont dat hoewel terroristische groeperingen van een pure hiërarchische orde zijn geëvolueerd naar een flexibele netwerkstructuur, deze flexibele netwerkstructuur steeds nog in het bezit is van een kleine hiërarchische kern (de Poot et al., 2009; Post et al., 2010; Pauwels, persoonlijke communicatie, Rajakumar, persoonlijke communicatie). Dit is niet verwonderlijk, aangezien een gedecentraliseerde organisatie de beste optie is voor het mobiliseren van middelen en voor rekrutering, maar de slechtste optie is voor veiligheid en om strategische richting aan de groepering te geven. Bij een hiërarchisch georiënteerde groepering zal dit net het omgekeerde zijn. Een middenweg dient gekozen te worden om succesvol te zijn (Tucker, 2008). de Poot et al. (2009) introduceren daarom de term ‘afhankelijkheid-ontvankelijkheidsrelaties’ om aan te duiden dat de sociale betrekkingen niet horizontaal of gelijkwaardig zijn, maar toch afwijken van strakke verticale verhoudingen (de Poot et al., 2009).

Verder komt het vaker voor dat een terroristische groepering haar netwerk gaat compartimenteren in cellen die onderling samenwerken zoals we zagen bij criminele samenwerkingsverbanden (Kenney, 2007; Farcy, persoonlijke communicatie). Net als bij criminele samenwerkingsverbanden vermindert compartimenteren de kans op infiltratie en limiteert het de schade aan de terroristische groepering. Voorbeeld van groeperingen die een gecompartmenteerd netwerk hadden zijn al Qaida, PLO, Hamas, Hezbollah en de Irish Republican Army (IRA) (Kenney, 2007).

Doch loert er een nieuw gevaar rond de hoek: namelijk *homegrown terrorism* (Pauwels, persoonlijke communicatie). In het voorjaar van 2015 werden vrijdelingen van terrorisme in West-Europa schering en inslag. Zo bewees ook het vrijdelen van een aanslag door de Duitse politie op 29 april 2015 (Deredactie.be, 2015b). Daarnaast werd op 22 april 2015 een aanslag in Frankrijk op kerken vrijdeld, waarbij de dader naar Syrië wou vertrekken (WB, 2015). Dit is niet verwonderlijk, aangezien groeperingen als IS en al-Shabaab juist via internetboodschappen oproepen om ‘thuis’, in het land waar je woont, aanslagen te plegen in naam van ‘het goede doel’ en op deze manier een individueel luik aan terrorisme koppelt (Dunham, Beech & Kerry, 2015; Jalil, 2015; Swaine, 2015; Pauwels, persoonlijke communicatie). Dergelijk *homegrown terrorism* kan leiden tot *lone wolf*-aanvallen, waarbij maar één individu noodzakelijk is om een aanslag te plegen (Dunham et al., 2015).

Personen thuis laten radicaliseren is dan ook de goedkoopste optie in tijden waarin trainingskampen opzetten en explosieven op het vliegtuig meenemen moeilijker zijn geworden (Kleemans, persoonlijke communicatie; Pauwels, persoonlijke communicatie). Het bekendste voorbeeld van *homegrown terrorism* is de aanslag in Parijs op Charlie Hebdo en tegelijkertijd de aanslag op een supermarkt op 9 januari 2015. De terroristen achter de aanslagen, waren leden van IS (Amedy Coulibaly) en van al-Qaida in the Arabian Peninsula (AQAP) (Chérif Kouachi en Saïd Kouachi) en hadden allen de Franse nationaliteit (Borger, 2015).

4.2.3 De hiërarchische orde

Het ICT-tijdperk heeft een grote invloed op de wijze waarop een terroristische cel zich organiseert en structureert. Terroristische groeperingen benutten de informatietechnologie om zich minder hiërarchisch te oriënteren en in de plaats zich net meer richten op netwerkvorming om juist hun weerstand, responsiviteit en flexibiliteit te vergroten. Net hierdoor stappen groeperingen af van hiërarchisch piramidale structuren en stappen over naar platte gedecentraliseerde netwerkstructuren waarbij ze met andere cellen een gemeenschappelijk doel of ideologie nastreven (Zanini et al., 2001).

Ondanks de losse en flexibele netwerkstructuren is er evenwel nog een hiërarchische structuur aanwezig in de bovenste kringen van de groepering, waarbij bevelen worden doorgegeven naar onderen toe en waar een leider aanwezig is (Tucker, 2008; de Poot et al., 2009; Post et al., 2010; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie).

4.2.4 Samenwerking met gelijkende terroristische groeperingen

Internationale samenwerking tussen terroristische groeperingen kan voorkomen. Dit is echter niet noodzakelijk (Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Een voorbeeld kan hier gevonden worden in de jonge samenwerking van Boko Haram met IS, ondanks hun verschillende geografische situering (Boffey, 2015; Pauwels, persoonlijke communicatie). Kleine netwerken helpen elkaar wel en er is bijkomend ook hulp te vinden via het internet. Echter geldt wel het principe van “ons kent ons”. Vertrouwen speelt hier een belangrijke rol (Pauwels, persoonlijke communicatie).

Dit is een evolutie van de laatste jaren. Terrorisme is geëvolueerd van grote goede gestructureerde terroristische netwerken naar kleinere onafhankelijke cellen die strijden met dezelfde ideologie. Deze kleine netwerken werken onderling samen (Farcy, persoonlijke communicatie). Ook kan het zijn dat terroristische groeperingen één gelijke ideologie volgen en daardoor hetzelfde doel nastreven. Dan heb je geen één groot terroristisch netwerk meer, maar allemaal kleine losse netwerken die allen in dezelfde naam strijden. Dit kan leiden tot samenwerking tussen de gelijkende terroristische afdelingen (Pauwels, persoonlijke communicatie).

4.2.5 Het gebruik van corruptieve contacten en beïnvloeding

Net als georganiseerde criminaliteit komt corruptie bij terroristische groeperingen veelvuldig voor (Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Ook experts kunnen aan terroristische groeperingen hun vaardigheden verlenen. Dit hoeft niet altijd om geld te gaan, maar kan ook voorkomen door een gelijkende ideologie. Zo kreeg het netwerk van Osama bin Laden hulp van Egyptische computer-experts die hem steunde gedurende het Afghaans conflict om een communicatienetwerk uit te bouwen dat bestond uit het internet, email en elektronische *bulletin boards* (Zanini et al., 2001). IS roept dan weer iedereen, van fiscaal experts tot dokters, op om aan hun zijde te staan. IS probeert dan ook een samenleving te creëren, waarbij er behoefte is aan alle diensten die ook in een normale samenleving nodig zijn (Pauwels, persoonlijke communicatie). Verder kunnen corruptieve contacten helpen bij het oversteken van grenzen voor nieuwe leden en illegale handel (Dettmer et al., 2015; Trends, 2015).

Naast corruptie speelt ook beïnvloeding een rol. Het beïnvloeden van burgers kan zoals eerder gezegd leiden tot rekrutering, maar kan ook leiden tot het vergroten van het aanzien van de groepering en tot corruptief gedrag. Deze beïnvloeding gebeurt bijvoorbeeld bij IS via videoboodschappen en hun online magazines 'Dabiq' en 'Dar al Islam'. Zo vertelt Hayat Boumeddiene, de vrouw van de terrorist Amedy Coulibaly die de aanslag op een joodse supermarkt in Parijs pleegde, in een artikel voor 'Dar al Islam' hoe blij ze is om te leven bij IS en vertelt ze over haar dode echtgenoot zijn verlangen om samen met zijn 'broeders' te vechten tegen de vijanden van het 'islamitische kalifaat' (Jalil, 2015; Drury, 2015).

Ze tracht mensen aan te sporen naar Syrië te komen door te zeggen hoe makkelijk ze in Syrië geraakte en te stellen dat de beloning, namelijk het wonen in een territorium geregeerd door de Islam, het waard is. ‘Dar al Islam’ werd dan ook speciaal ontworpen om mensen aan te sporen te reizen naar territoria die gecontroleerd worden door IS (Drury, 2015).

4.2.6 Het gebruik van rechtspersonen

Ook terroristische groeperingen kunnen rechtspersonen, zoals vennootschappen, gebruiken (Farcy, persoonlijke communicatie; X, persoonlijke communicatie). Echter zijn deze rechtspersonen moeilijk te linken aan terroristische groeperingen. Een voorbeeld zijn de raffinaderijen die IS in handen heeft. IS financiert zich deels via de verkoop van petroleum en olie. Tussen het bezetten van raffinaderijen en de uiteindelijk verkoop van de petroleum zitten rechtspersonen. Op papier kan dit een gewone vennootschap lijken, terwijl het mogelijks kan dienen ter financiering van IS (X, persoonlijke communicatie). Verder gebruiken terroristische organisaties ook VZW’s om hun groepering te financieren (Winer, 2002; Stern, 2003; Mahan et al., 2008; de Poot, et al., 2009; Kleemans, persoonlijke communicatie; Rajakumar, persoonlijke communicatie; X, persoonlijke communicatie).

4.2.7 Het gebruik van internet en media

Internet werkt als een katalysator inzake terrorisme (Pauwels, persoonlijke communicatie). Het ICT-tijdperk geeft dan ook veel mogelijkheden en opportuniteiten aan terroristische cellen, is gemakkelijk toegankelijk, wordt amper gecensureerd en is bovendien goedkoop (Denning, 2001; Weimann, 2006). In eerste instantie laat het gebruik van ICT en media een leerproces toe voor terroristen. Terroristen leren op het internet of via berichtgeving hoe andere terroristen aanslagen plegen of wat voor contrastrategieën ze gebruiken. Deze verspreiding van kennis creëert een ketting van besmetting (Zanini et al., 2001; Crenshaw, 2008; Marsden et al., 2011; Burke, 2015). Deze ketting van besmetting kan leiden tot ‘*self-starter*’ groups. Dit zijn groepen die, door de afwezigheid van een top-down-invloed, via het internet operationele en ideologische informatie bekomen (Mullins, 2009). Echter hoeft dit leerproces niet enkel betrekking te hebben van terrorist naar terrorist, maar kan het ook gaan over van doelwit/overheid naar terrorist. Zo kan een terrorist via de enorme bibliotheek die het internet is, te weten komen wat exact de counterstrategies zijn tegen terrorisme of wat bijvoorbeeld het tijdschema is van hun doelwit (Weimann, 2006).

Het gebruik van internet, dat een handige aanpak vormt om know-how en ideologie te verspreiden, is aan een opmars bezig de laatste jaren (Schmid, 2011).

Verder laat het internet toe dat de groepering belangrijker en omvangrijker lijkt dan dat het in realiteit is, waardoor het bedreigender overkomt (Weimann, 2006). ICT heeft invloed op de soorten doelen die ze willen bereiken, op het soort wapens dat ze willen gebruiken aangezien ze er gemakkelijker aan kunnen geraken, maar ook in de wijze waarop een groepering opereert en zich structureert. Het verhoogt de snelheid van mobilisatie en laat meer dialoog toe tussen leden. Dit kan bijvoorbeeld gebeuren aan de hand van *chat rooms* (Zanini et al., 2001; Weimann, 2006). Zo deelt bijvoorbeeld Hamas operationele informatie via het internet en gebruikt het *chat rooms* om aanslagen te plannen (Zanini et al., 2001).

Daarnaast is ICT een handig middel om propaganda en ideeën te verspreiden. Het internet laat groeperingen toe om rechtstreeks hun bericht over te brengen naar een groot publiek, waarbij het een grote controle behoudt over de inhoud van het bericht (Zanini et al., 2001; Weimann, 2006; Kenney, 2007; Mahan et al., 2008; Marsden et al., 2011). Het publiek bestaat uit de internationale gemeenschap (namelijk burgers), de vijanden van de groepering (namelijk overheden) en potentiële leden. Met andere woorden is het publiek wereldomvattend en kent de zoektocht naar een publiek geen grenzen. Zo is bijvoorbeeld een website van Hamas, al-Fateh, gericht op kinderen waarbij het naast tekeningen en kinderliedjes “discussieert over jihad en de beste heldenverhalen vertelt die nergens anders worden vertelt” (lees: verheerlijking van jihad) (Weimann, 2006). IS riep bijvoorbeeld in een videoboodschap die verspreid werd via het internet Westerse moslims op om aanslagen te plegen in het land waar ze wonen, zo ook in België (Jalil, 2015). Echter hoeft dit niet altijd via het internet te gebeuren, maar kan het ook gebeuren via radio- en televisie-uitzendingen (Zanini et al., 2001; Km, 2015). Dit wordt in de literatuur ook wel het ‘CNN effect’ genoemd. Grote mediabedrijven als CNN geven terroristische groeperingen een platform om mensen kennis te laten maken met hun ideologie (Mahan et al., 2008). Een actueel voorbeeld hiervan is het eigen televisiekanaal van IS waarop het berichten over militaire operaties en preken verspreidt (Km, 2015). Echter zijn niet alle terroristische groeperingen enkel uit op publiciteit. Zo zijn er in Noord-Ierland verscheidene aanslagen nooit opgeëist (Horgan, 2005).

Verder kan ICT ook helpen bij het verwerven van fondsen door zich duidelijk te profileren op het internet. Het internet laat toe om individuen, bedrijven of staten te vinden die eenzelfde ideologie delen, om hun vervolgens een donatie te vragen (Marsden et al., 2001; Weimann, 2006; Kenney, 2007; Mahan et al., 2008).

Bijkomend kan het gebruik van ICT leiden tot economische schade, psychologische schade (zoals angst opwekken) en fysieke schade, wanneer een groepering bijvoorbeeld een systeem hackt (Zanini et al., 2001; Weimann, 2006; Mahan et al., 2008; Marsden et al., 2011). Zo zien we deze ICT-elementen samenvloeien in het hacken door IS van de website, sociale mediakanalen en televisiezender van TV5 Monde op 9 april 2015. Dit hacken kon ten eerste leiden tot economische schade voor de zender door de pro-terroristische uitspraken die door IS op de sociaalnetwerksites en op de website van TV5 Monde werden gepubliceerd. Ten tweede dienen deze uitspraken als propaganda om aanhangers te werven en ten derde kan deze hacking angst inboezemen bij de bevolking daar deze geconfronteerd wordt met in hoeverre de mogelijkheden strijken van IS (n.d., 2015). Zo had bijvoorbeeld de 'Islamic State Hacking Division' een lijst van honderd personeelsleden van het Amerikaanse leger bekendgemaakt, waarbij het Amerikaanse moslims aanspoort om deze personeelsleden te vermoorden. Over het daadwerkelijk hacken werd getwijfeld, maar het zaait, naast het aansporen tot geweld, ook angst bij de Westerse bevolking. Indien dit hacken niet voorkwam, toont het daarnaast aan dat ICT toelaat om bedreigender over te komen dan de realiteit (Dunham et al., 2015).

4.2.8 Defensieve en offensieve contrastrategieën

Ook terroristische groeperingen gebruiken defensieve en offensieve contrastrategieën. Een groepering zal uit de radars proberen blijven en hierbij alle opties gebruiken die ze kan gebruiken (Pauwels, persoonlijke communicatie). De keuze welke contrastrategieën gebruikt worden is afhankelijk van de jurisdictie waarbinnen de groepering te werk gaat (Rajakumar, persoonlijke communicatie). Ook zal niet elk onderdeel van een groepering contrastrategieën gebruiken. Zo komt het voor dat identiteitspapieren gevonden worden van zelfmoordterroristen bij zelfmoordaanslagen (Pauwels, persoonlijke communicatie).

4.2.8.1 Defensieve contrastrategieën

Zoals eerder gesteld in 3.2.8.1 trachten defensieve contrastrategieën criminele activiteiten te verbergen (Boerman et al., 2012).

Sommige groeperingen raden hun leden aan om zich aan te passen aan de omgeving waar ze wonen, geen onnodige aandacht te trekken en hun communicatie te beschermen. Zo raadde al Qaida haar leden in het Westen aan om hun baard af te scheren, contact met burens te vermijden, bidden te beperken en codewoorden te gebruiken aan de telefoon wanneer ze gevoelige informatie communiceerde (Kenney, 2007). Ook de Poot et al. (2009) halen beperkte communicatie en codetaalgebruik aan (de Poot et al., 2009).

Verder proberen terroristen veelvuldig *face-to-face* ontmoetingen te regelen in een besloten ruimte in een semi-openbare plaats of in een woning (de Poot et al., 2009).

Ten slotte dient een groepering het achterlaten van digitale sporen te beperken, aangezien digitalisering ook een risico kan vormen voor het verdere bestaan van de groepering. Dit kan onder andere voorkomen in de vorm van harde schijven, e-mails en cd-roms wat mogelijk kan beschikken over strategische informatie of over informatie inzake trainingskampen (Zanini et al., 2001).

4.2.8.2 Offensieve contrastrategieën

Zoals eerder gesteld in 3.2.8.2 trachten offensieve contrastrategieën de activiteiten van opsporings- en vervolgingsambtenaren te verhinderen (Boerman et al., 2012).

Wanneer het gaat over het gebruik van internet proberen terroristische groeperingen hun anonimiteit te vrijwaren en communicatie te anonimiseren door encryptie-programma's te gebruiken (Zanini et al., 2001; Arquilla et al., 2001b; Stern, 2003; Klausen, 2015). Bijkomend zitten ook terroristische groeperingen op het *dark web* (Farcy, persoonlijke communicatie). Daarnaast kunnen terroristen proberen anonimiteit te bereiken via verschillende soorten telefonie. Zo gebruikte bijvoorbeeld het bin Laden netwerk satelliettelefoons (Zanini et al., 2001). Vervolgens kan een groepering verscheidene gsm's laten circuleren doorheen een groep personen om onderzoek te bemoeilijken. Verder komt het ook voor dat *prepaid-gsm's* of telefooncellen worden gebruikt (de Poot et al., 2009). Het kan voorkomen dat een terroristische groepering haar leden vraagt om gsm, tablet en pc af te geven om op deze manier niet gelokaliseerd te kunnen worden. Deze werkwijze gebruikt IS (Alde'emeh, 2014).

Bijkomend zullen groeperingen hun communicatie proberen af te schermen door codetaal te gebruiken (Kenney, 2007; de Poot et al., 2009). Ten slotte zal een lid door de aanname van meerdere namen of identiteiten het onderzoek bemoeilijken (de Poot et al., 2009).

4.2.8.3 Het categoriaal gebruik van afschermingsmethoden

4.2.8.3.1 Het gebruik van een valse identiteit

Jihadisten die binnen de Europese Unie verblijven krijgen vervalste paspoorten, visa's, rijbewijzen en identiteitskaarten. In sommige gevallen beschikt men zelfs over apparatuur waarmee de jihadisten kwalitatieve valse documenten kunnen produceren (de Poot et al., 2009). Verder hebben leden van een terroristische groepering vaak twee aliaten, wat politieel onderzoek moeilijker maakt. Verder kan men ook meerdere identiteiten aannemen of opgeven (de Poot et al., 2009; Klausen, 2015).

4.2.8.3.2 Het gebruik van ICT-middelen

Zoals eerder gesteld zullen groeperingen communicatie proberen te anonimiseren door encryptie-programma's te gebruiken om hun anonimiteit te vrijwaren (Zanini et al., 2001; Arquilla et al., 2001b; Stern, 2003; de Poot et al., 2009). Een mogelijke manier is het gebruik van een anonieme browser zoals Tor (Tor, 2015). Verder komt het voor dat terroristen '*dead letter boxes*' nalaten. Dit zijn conceptberichten die ze niet verzenden, maar laten staan voor de volgende gebruiker. De informatie is dus nooit verzonden, maar wel overgekomen (de Poot et al., 2009). Ten slotte komen ook nieuwe communicatiemiddelen naar voren die nog niet geregeld zijn in de wetgeving. Voorbeelden zijn Skype, Whatsapp, Paltalk en Voice over IP (de Poot et al., 2009; Klausen, 2015; Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie; X, persoonlijke communicatie).

4.2.8.3.3 Het gebruik van intimidatie en (bedreiging met) geweld

In deze scriptie vonden we maar één voorbeeld inzake het gebruik van intimidatie en (bedreiging) met geweld. Terroristische organisaties proberen door middel van te dreigen met aanslagen of geweld, overheden aan te zetten hun acties tegen hen te staken (Duffin & Ross, 2014).

4.3 De financiering van terrorisme

De aanslagen van 9/11 onthulde dat de financiering van terrorisme geglobaliseerd is (Winer, 2002). De financiering van terrorisme is van groot belang voor de terroristische groeperingen, aangezien aanslagen, strijden zoals jihad en het ondersteunen van familieleden van overleden strijders geld kosten (Dettmer et al., 2015; Trends, 2015; Pauwels, persoonlijke communicatie).

Het bekomen van inkomsten, die daarna aangewend worden voor de aankoop van producten zoals wapens, zijn een belangrijk element dat langdurende terroristische groeperingen van verdwijnende terroristische groeperingen onderscheidt (Stern, 2003; Keatinge, 2014; Pauwels, persoonlijke communicatie). Echter dient aangehaald te worden dat training en aanslagen relatief weinig kosten in vergelijking met de impact die het heeft op de samenleving (Dettmer et al., 2015; Trends, 2015; Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Zo kocht Coulibali, voor de aanslag op de joodse supermarkt, wapens met het geld dat hij had van een banklening (Paternotte, persoonlijke communicatie).

4.3.1 Tussenkomst van een derde partij

Een derde partij kan ook een overheid zijn. Maar ICT kan de nood aan staatsfinanciering beperken doordat ten eerste encryptering zorgt voor een hogere veiligheid en een verhoogde heimelijkheid inzake opereren en ten tweede financiering over het internet toelaat (Zanini et al., 2001). Dit hoeft echter geen overheid te zijn, maar kan ook een organisatie uit de private sector zijn. Zo werkte Hamas en Hezbollah in de jaren tachtig samen met enkele banken (Pauwels, persoonlijke communicatie). Tussenkomst van een derde partij kan voorkomen, maar hoeft dit niet. De derde partij is vaak niet op de hoogte dat hij financiële voordelen teweeg brengt voor een terroristische groepering (Rajakumar, persoonlijke communicatie). Aansluitend haalt Farcy (persoonlijke communicatie) aan dat terroristische groeperingen liefst alles in eigen beheer doen, omdat ze een permanent wantrouwen hebben tegenover de buitenwereld (Farcy, persoonlijke communicatie).

4.3.2 Bronnen van inkomsten

Er zijn voornamelijk vier manieren waarmee terroristische groeperingen worden gefinancierd. Ten eerste kan dit gebeuren via het criminele luik (van drugsmokkel tot prostitutie) (Winer, 2002; Stern, 2003; Mahan et al., 2008; De Poot et al., 2009; Levitt, 2013; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Zo verkocht al Qaida bijvoorbeeld heroïne aan de Amerikaanse en West-Europese markt en verzorgde het transport voor de drugszaken van de Taliban (Stern, 2003). Een ander voorbeeld is dat IS pornografie smokkelt en gestolen kunst verhandelt (Dettmer et al., 2015; Trends, 2015). Verder doet Hezbollah aan wapentrafiëk en drugshandel in Europa (Levitt, 2013).

Evenwel mag ook het belang van kidnapping niet vergeten worden. Dit is een goedverdienende manier om terrorisme te financieren, waar onder andere ook IS en FARC zich schuldig aan maken (Dettmer et al., 2015; Rollins & Rosen, 2015; Trends, 2015; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Ook kwam in het onderzoek van de Poot et al. (2009) naar voren dat documentvervalsing, woninginbraak, diefstal, drugshandel en drugsproductie gebruikt worden om internationaal jihadisme te financieren. Omwille van criminele activiteiten heeft een terroristische groepering financiële zekerheid en is ze niet afhankelijk van donaties van derden (Dettmer et al., 2015; Trends, 2015; de Poot et al., 2009).

Ten tweede kan financiering ook gebeuren via het legitieme luik (van constructiebedrijven tot banken) (Stern, 2003; Mahan et al., 2008). Zo bezat bijvoorbeeld Osama bin Laden verschillende legitieme bedrijven, zoals een constructiebedrijf dat wegen en bruggen bouwde en een transportbedrijf (Stern, 2003). IS doet dan weer in de handel van olie en bezit elektriciteitscentrales (Van de Cloot, 2014; Dettmer et al., 2015; Trends, 2015; Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie; X, persoonlijke communicatie).

Hier dient wel de kanttekening gemaakt te worden dat, net als bij georganiseerde criminaliteit, activiteiten die in België illegaal zijn, legaal kunnen zijn in sommige landen (Rajakumar, persoonlijke communicatie).

Ten derde kan terrorisme gefinancierd worden door staten door middel van donaties (Winer, 2002; Stern, 2003; Mahan et al., 2008; Dettmer et al., 2015; Trends, 2015; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie). Zo heeft bijvoorbeeld Iran jarenlang Hezbollah zeshonderd miljoen dollar per jaar geschonken (Mahan et al., 2008).

Ten vierde kunnen terroristische groeperingen ook in het bezit zijn van liefdadigheidsorganisaties waarbij de groepering het geschonken geld aanwendt voor de financiering van haar terroristische activiteiten (Winer, 2002; Stern, 2003; Mahan et al., 2008; de Poot, et al., 2009; Kleemans, persoonlijke communicatie; Rajakumar, persoonlijke communicatie; X, persoonlijke communicatie). Deze liefdadigheidsinstellingen zijn vaak gesitueerd in de Westerse wereld. Ook hier kan al Qaida aangehaald worden (Stern, 2003).

Internet kan een rol spelen bij het verkrijgen van financiën. Zo kan bijvoorbeeld een terroristische groepering trachten gestolen kunst te verkopen via verkoopsites als Ebay of kan het trachten online donaties te verkrijgen (Dettmer et al., 2015; Rajakumar, persoonlijke communicatie).

4.3.3 Fraude en witwassen

Ook terroristische groeperingen wassen hun illegaal bekomen geld wit (Winer, 2002; Mahan et al., 2008; Rajakumar, persoonlijke communicatie). Het witwassen van fondsen gebeurt door cellen die voornamelijk opereren in jurisdicties die op een ruime afstand liggen van waar de politieke basis van de groepering gesitueerd is of waar de groepering aanslagen wenst uit te voeren. De effectiviteit van het witwassen verhoogt door de mogelijkheid fondsen te verbergen, te investeren of te transporteren via internationale financiële instellingen (Winer, 2002). Hierbij spelen belastingparadijzen zeker een rol (Pauwels, persoonlijke communicatie; X, persoonlijke communicatie). IS wast haar fondsen wit via *trade-based* witwassen. Een voorbeeld hiervan wordt aangehaald onder 5.3 ‘het samenkomen/samenwerken van georganiseerde misdaad en terrorisme’ (Dettmer et al., 2015).

Verder kan een terroristische groepering zich ook schuldig maken aan fraude (Rajakumar, persoonlijke communicatie).

5. Een vergelijking tussen georganiseerde misdaad en terrorisme

In dit hoofdstuk wordt een vergelijking gemaakt tussen georganiseerde criminaliteit, besproken in hoofdstuk twee, en terrorisme, besproken in hoofdstuk drie. Om dit hoofdstuk leesbaar te houden, wordt bronvermelding enkel gebruikt bij de introductie van nieuwe bronnen of nieuwe informatie van een bestaande bron die nog niet voorkwam in hoofdstuk twee of drie.

Een trend die de laatste jaren voorkomt is het samen vloeien van georganiseerde criminaliteit met terrorisme. Dit samenvloeien wordt in de beperkte literatuur *narco-terrorism* genoemd (Schmid, 2011). Volgens Farcy (persoonlijke communicatie) bestaat er dan ook een soort kruisbestuiving tussen beide criminaliteitsfenomenen waarbij een terroristische groepering enkel goed functioneert wanneer ze banden heeft met criminele samenwerkingsverbanden (Dupuis, 2010; Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie). Evenwel is het ene criminele samenwerkingsverband het andere niet en is de ene terroristische groepering de andere niet (Schmid, persoonlijke communicatie). Een terroristische groepering hoeft, afhankelijk van haar gedachtegang, niet samen te werken met een criminele organisatie. Zo zal een politiek-geïnspireerde terroristische groepering twijfelen om samenwerking aan te gaan met georganiseerde criminaliteit, wanneer deze samenwerking net een mogelijke bedreiging kan vormen voor het verdere bestaan van de groepering (Schmid, 2011).

5.1 Op het vlak van organisatie

In eerste instantie is het duidelijk dat beide criminele samenwerkingsverbanden nationaal kunnen bestaan, maar evenwel ook internationaal. Daarnaast kunnen beide criminaliteitsfenomenen samenwerking hebben met gelijke organisaties, waarbij ook deze samenwerking zich internationaal kan strekken. Bij deze samenwerking speelt vertrouwen een belangrijke rol. Een bepaalde graad van vertrouwen houdt het netwerk bij elkaar (Tucker, 2008). Dit vertrouwen wordt aangevuld met een gemeenschapsgevoel, waardoor een wij-zij-verhaal ontstaat. Verder spelen familie en sociale omgeving bij beiden een rol. Aansluitend berust rekrutering op zelfselectie. Evenwel zal de reden om toe te treden verschillen. Bij een crimineel samenwerkingsverband zal het winstmotief de leidraad zijn, terwijl bij een terroristische groepering een ideologie of buitenstaandersgevoel het motief is.

We zien dat zowel georganiseerde criminele samenwerkingsverbanden als terroristische groeperingen organisatiegewijs aan het evolueren zijn naar een netwerkstructuur waarbij de organisatie gedefinieerd kan worden als *netwar*. Een netwerk heeft het voordeel zich gemakkelijker te kunnen organiseren in multi-organisatorische netwerken ten opzichte van de traditionele, hiërarchische overheidsactoren. Dit is voornamelijk het geval wanneer de criminele groepering een *all-channel* netwerk heeft, waarbij elk knooppunt verbonden is met een ander knooppunt. Volgens Arquilla et al. (2001a) levert dit macht op en betekent dit vervolgens dat wie zich houdt aan de netwerkvorm voordeel verkrijgt boven de organisatie die zich enkel met hiërarchie bezig houdt (Arquilla et al., 2001a). Echter vinden we hier vaak wel nog een kern van autoriteit terug om sturing te geven aan het netwerk. Verder kan het netwerk bij beide criminaliteitsfenomenen compartimenteren in kleinere cellen, waardoor het beter bestand is tegen vernieling van het gehele netwerk en waarbij herstelling van het vernielde deel gemakkelijker is. Dit compartimenteren maakt de bestrijding moeilijker.

Beide criminaliteitsfenomenen maken zich ook schuldig aan corruptie. Ze gebruiken hiervoor dezelfde werkwijzen en soms ook dezelfde soort corruptieve contacten in zowel overheden als in het private zakenleven. Echter hoeft de insteek van corruptie niet hetzelfde te zijn. Bij georganiseerde criminaliteit zal de insteek financieel zijn of gebaseerd zijn op geweld. Bij terrorisme kan de insteek ook financieel zijn, maar kan het ook ideologisch zijn.

Een aantal georganiseerde criminele netwerken gebruiken tactieken die gebruikt worden binnen het terrorisme (Gupta,, Horgan & Schmid, 2009; Schmid, 2011). Terroristische groeperingen en criminele samenwerkingsverbanden gebruiken dan ook vaak dezelfde contrastrategieën gaande van encryptieprogramma's en valse identiteiten tot het gebruik van codetaal en *prepaid-gsm*'s. Verder gebruiken beide criminaliteitsfenomenen veelvuldig internet en media voor tal van redenen en speelt dit meer en meer een belangrijke rol. Via internet kan ook samenwerking ontstaan tussen beide criminaliteitsfenomenen.

5.2 Op het vlak van financiering

Opvallend is dat veel terroristische groeperingen gebruik maken van interne vormen van fondsenwerving om hun terroristische groepering te kunnen financieren die in dezelfde lijn liggen als die van criminele organisaties. Denk hier bijvoorbeeld aan de PKK (Schmid, 2011). Beide criminaliteitsfenomenen doen aan symbiotische en parasitaire misdaad. Enkel onderscheidt terrorisme zich op vlak van financiering door het verkrijgen van donaties.

Daarnaast wassen terroristische groeperingen als criminele samenwerkingsverbanden hun geld wit. Dit kan bij beiden gebeuren aan de hand van rechtspersonen zoals vennootschappen (Winer, 2002; Mahan et al., 2008; Kruisbergen et al., 2012; Christensen, 2012). Ook hier gebruiken criminele samenwerkingsverbanden en terroristische groeperingen dezelfde manieren om geld wit te wassen (Kersten, 2002). De jurisdicties die terroristische groeperingen gebruiken om hun geld te verbergen of te investeren worden doorgaans ook gebruikt door criminele samenwerkingsverbanden (Winer, 2002). Alleen is het moeilijk om te achterhalen of het geld bedoeld is voor de financiering van een terroristische groepering of niet. Wanneer het gaat over georganiseerde criminaliteit is de vraag: “Waar komt het geld vandaan?”. Echter ligt die vraag anders bij terrorisme: “Waar gaat het geld naartoe?” (Mahan et al., 2008; X, persoonlijke communicatie). Beide criminaliteitsfenomenen gebruiken ook dezelfde kanalen om geld te verplaatsen naar deze jurisdicties. Dit is vaak fysiek, zoals transportatie per boot en per vliegtuig en dit door het slikken van geld of in een koffer (X, persoonlijke communicatie).

Verder kunnen zowel terroristische groeperingen als criminele samenwerkingsverbanden activiteiten uitvoeren die in de ene jurisdictie legaal zijn en in de andere jurisdictie illegaal (Kruisbergen et al., 2012; Rajakumar, persoonlijke communicatie). Ten slotte maken beide criminaliteitsfenomenen grotendeels gebruik van dezelfde kanalen om aan financiën te komen (Paternotte, persoonlijke communicatie).

5.3 Het samenkomen/samenwerken van georganiseerde misdaad en terrorisme

Georganiseerde criminele groeperingen en terroristische groeperingen kunnen samenwerken en hebben elkaar soms nodig (de Poot et al., 2009; Dettmer et al., 2015; Farcy, persoonlijke communicatie; Kleemans, persoonlijke communicatie; Pauwels, persoonlijke communicatie; Paternotte, persoonlijke communicatie; X, persoonlijke communicatie). Evenwel halen professor Kleemans (persoonlijke communicatie) en Paternotte (persoonlijke communicatie) aan dat het omgekeerde niet zo hoeft te zijn (Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Een crimineel samenwerkingsverband kan zonder samenwerking met een terroristische groepering goed functioneren (Kleemans, persoonlijke communicatie).

Zo kan een groepering niet eeuwig wapendepots veroveren en zal het nood hebben aan voldoende wapens. De voorraad strekt namelijk niet eeuwig en is er dus een constante bevoorrading vereist als je de oorlog wilt winnen. Je hebt als groepering financiële en logistieke middelen nodig (Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie). Wat er zeker toedoet is de schaalgrootte van de terroristische groepering. Hoe groter de schaal, hoe meer nood aan samenwerking (Pauwels, persoonlijke communicatie).

Soms kan een terroristische groepering criminele activiteiten uitbesteden aan een crimineel samenwerkingsverband. Waar terrorisme en georganiseerde criminaliteit samenkomen, kan een belangenvermenging optreden (Dettmer et al., 2015; Farcy, persoonlijke communicatie; Schmid, persoonlijke communicatie). In dit geval bestaat de mogelijkheid bijvoorbeeld dat een terroristische groepering een lid van het crimineel samenwerkingsverband erop wijst dat het zijn religieuze plicht is of dat het hem reinigt van zijn zonden om een wagen vol drugs te vervoeren (de Poot et al., 2009). Een ander voorbeeld waarin belangenvermenging ook optrad is de connectie tussen al Qaida en de georganiseerde diamanthandel in Sierra Leone. De diamanten worden ‘verkocht’ aan de terroristische groepering voor geld of wapens. De terroristische groepering transporteert en verkoopt vervolgens de diamanten naar en aan diamantverwerkingscentra zoals in Antwerpen, waarmee de terroristische groepering hun fondsen hebben witgewassen en waarbij dit geld kan gebruikt worden voor de financiering van hun terroristische activiteiten (Winer, 2002). Dit is een voorbeeld van *trade based money laundering*. Bij *trade based money laundering* ga je dus met zwart geld goederen kopen die je daarna terug doorverkoopt. Het bedrag dat je dan ontvangt is wit geld (Dettmer et al., 2015; X, persoonlijke communicatie). Georganiseerde criminaliteit kan dus voorkomen om ideologische opvattingen te financieren of gewoon om het pure criminele feit. Soms is er dus een mengeling van de twee criminaliteitsfenomenen (Farcy, persoonlijke communicatie).

Het volgen van de werkwijze van criminele samenwerkingsverbanden door terroristische groeperingen is niet verwonderlijk, aangezien geld een belangrijke rol speelt. Beiden zijn *big business* en gaan te werk als echte ondernemingen (Van de Cloot, 2014; Dettmer et al., 2015; Trends, 2015). Dit komt volgens Louise Shelley door een evolutie in terrorisme, waarbij er een daling te zien is in terrorisme gesponsord door staten, waardoor criminaliteit een grotere rol is gaan spelen (Dettmer et al., 2015).

Echter waren er ook andere terroristische organisaties, zoals IRA en PKK, die in het verleden een terroristische organisatie waren, maar tegelijkertijd ook deden aan georganiseerde criminaliteit (Dettmer et al., 2015; Farcy, persoonlijke communicatie; Kleemans, persoonlijke communicatie; Schmid, persoonlijke communicatie; X, persoonlijke communicatie). Zo maakt de PKK zich schuldig aan drugshandel om haar daden te financieren en doet ze aan wapentrafiëk. FARC is intussen ook geëvolueerd naar georganiseerde criminaliteit (Farcy, persoonlijke communicatie).

Ook IS laat deze kans niet liggen en benut haar opportuniteiten (Farcy, persoonlijke communicatie). Zo werd in april 2015 een IS-kamp gevonden in de Mexicaanse staat Chihuahua, acht mijl van de Amerikaanse grens. Het bijzondere aan dit kamp is de samenwerking van IS met criminele organisaties. Inlichtingenbronnen melden dat mensenhandelaars van het Juárezkartel IS-strijders helpt reizen doorheen de woestijn en over de grens. Bijkomend werden de locaties gekozen om de capaciteitstekorten van provinciale en gemeentelijke politie en het hoog aantal *safe-havens* in een gebied dat beheerst wordt door grootschalige drugsmokkel (Terrorismemonitor, 2015c). Verder gebruikt IS ook mensensmokkelaars naar Syrië, aangezien Syrië binnen geraken moeilijker is geworden met al de internationale aandacht (Pauwels, persoonlijke communicatie). Evenwel gebruikt IS ook de omgekeerde richting. Zo verklaart de Libische overheidsadviseur Abdul Basit Haroen dat IS samenwerkt met mensensmokkelaars om terroristen via vluchtelingenboten terug in Europa te krijgen (svg, 2015). Ten slotte was bij de aanslagen op Charlie Hebdo ook sprake van contacten met de wapenhandel (Farcy, persoonlijke communicatie).

6. Aanbevelingen

“We hold to the belief that the man who passes the sentence should swing the sword. If you would take a man’s life, you owe it to him to look into his eyes and hear his final words. [...] A ruler who hides behind paid executioners soon forgets what death is.”

– George R. R. Martin (2011, p14)

Doorheen de aanbevelingen kunnen overlappingen met andere niveaus voorkomen. Elk niveau is uiteindelijk verbonden met elkaar en vragen daarom soms gelijkende maatregelen. Het is dan ook aangeraden alle niveaus in dit hoofdstuk te raadplegen om tot een algemene visie te komen.

6.1 Aanbevelingen op lokaal niveau

Doorheen de interviews zijn enkele kritiepunten naar voren gekomen waaruit aanbevelingen naar lokaal beleid kunnen worden gemaakt.

Ten eerste worden federale politietaken en gemeentelijke administratieve sancties van justitie naar de lokale politiezones geschoven. De lokale politie is de enige die taken niet kan afschuiven. Dit vormt in aanvulling met het huidige besparingsstelsel, zwaardere capaciteitsproblemen inzake personeel en middelen in het lokale korps. Op deze manier wordt je als korps geconfronteerd met de grenzen van je capaciteit en creëert het een spanningsveld door de combinatie met de stijging van criminaliteit, nieuwe criminaliteitsvormen, een verstrenging van de wetgeving en een stijging van mobiliteit. Een vraag dat vervolgens binnen korpsen rijst is hoe je dan tot een kwaliteitsvol, efficiënt en effectief politiebeleid kan komen (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). De capaciteitsproblemen komen ook aan bod binnen de federale politie (Paternotte, persoonlijke communicatie).

Ten tweede is er veel te weinig tijd die politiekorpsen aan hun prioriteiten kunnen besteden. Binnen de zonale veiligheidsraad heeft iedereen zijn eigen ideeën waaruit prioriteiten voor de politiezone volgen. Echter neemt je basispolitiezorg al vijftien procent van je capaciteit in, waardoor je amper nog vijf procent van je capaciteit kan gebruiken voor je prioriteiten. Hierdoor moet je binnen de aangereikte prioriteiten nogmaals prioriteren (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie).

De taken dienen mogelijks afgeslankt te worden en er dient gekeken te worden wat er van belang is voor de bevolking (Pieteraerens, persoonlijke communicatie). Deze kritiek komt ook naar boven binnen de Federale Politie. Door de besparingen dienen er continu keuzes te worden gemaakt (X, persoonlijke communicatie).

Ten derde kunnen wijkagenten trachten radicalisme te signaleren binnen de wijken. Hierbij kunnen ze een nauw contact hebben met imams en met personen die een hoog aanzien hebben binnen de allochtone gemeenschap. De vraag stelt zich in hoeverre dit daadwerkelijk effect heeft door het capaciteitsprobleem. Zo beschikt bijvoorbeeld Temse over één wijkagent per vierduizend inwoners. Echter ligt een goede wijkwerking rond de één wijkagent per tweeduizendvijfhonderd inwoners volgens korpschef Pieteraerens (persoonlijke communicatie). Focussen Belgische politiezones zich nog teveel op “brandweer-politie”? Het aantal agenten binnen interventie ligt beduidend hoger dan bij de wijkpolitie (Pieteraerens, persoonlijke communicatie). Hier dient wel een kanttekening gemaakt te worden. Wijkagenten zijn essentieel, maar zijn niet de enige schakel die radicalisme signaleren en voorkomen. Radicalisme wordt door de hele politieorganisatie voorkomen. Zo kan bijvoorbeeld een interventieploeg bij een oproep informatie vergaren rond radicalisme (Lacaeyse, persoonlijke communicatie).

Ten vierde dienen de regering en het politieorgaan te overwegen of een aanpassing van de structurele visie op de organisatie van de politie een oplossing biedt, aangezien er momenteel geen nationaal beleid is. Het lokale luik vraagt om de verschillende normen te herbekijken en te beslissen welke richting de politie uit moet (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). De lokale en federale politie werken niet proactief, maar eerder reactief, waardoor de politie altijd achter het net vist (Lacaeyse, persoonlijke communicatie; Paternotte, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie).

Ten vijfde komt de kritiek uit het lokale luik naar boven dat lokale politiezones onvoldoende inspraak hadden in de maatregelen die het Coördinatieorgaan voor de Dreigingsanalyse (OCAD) nam rond de terreurdreiging. Verder dient een politiekorps niet herleid te worden tot een bunker. Personeel heeft recht op veiligheid, maar een politiekorps blijft nog steeds een openbare dienst (Pieteraerens, persoonlijke communicatie).

Het lokale luik geeft daarnaast aan dat het onvoldoende ingelicht is over de terreurdreiging en waarom men juist voldoende alert dient te zijn. Niemand kan de politie vertellen op basis van welke objectieve en concrete informatie het dreigingsniveau is gebaseerd. Echter kan het OCAD dit niet vertellen, aangezien het haar informatie niet is. Het OCAD vergaart de inlichtingen niet zelf, maar krijgt het van onder andere de Staatsveiligheid en ADIV. Het kan goed zijn dat deze informatie enkel een indicatie gaf van het bestaan van een potentiële dreiging. Deze wens binnen de politie is begrijpelijk, ook al begrijpen ze zelf dat er steeds een kans op lekken bestaat (Lacaeyse, persoonlijke communicatie).

Ten zesde vormt beroepsgeheim bij hulpverlening een probleem inzake de strijd tegen georganiseerde criminaliteit en terrorisme. Dit beroepsgeheim is begrijpelijk aangezien het gaat om een vertrouwensrelatie tussen hulpverlener en patiënt. Doch is dit beroepsgeheim niet compatibel met politie, aangezien informatie niet wordt gedeeld met politie (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). Het probleem reikt echter wel verder dan de hulpverlening, maar omvat onder andere ook CAW, scholen, CLB en jeugthuizen. De vraag is of bijvoorbeeld een school een signaalfunctie heeft en hierrond informatie moet delen met politie. Je hebt dan een vertrouwensrelatie versus signalisatie (Lacaeyse, persoonlijke communicatie).

Ten zevende is er meer nood aan samenwerking, ook met de federale politie (Pieteraerens, persoonlijke communicatie). Criminaliteitsfenomenen zoals georganiseerde criminaliteit spelen zich deels bovenlokaal af. Doch zien we lokaal enkel maar puzzelstukjes (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). Desalniettemin bezitten we in België wel een uniek samenwerkingsinitiatief: namelijk de nationale gegevensdatabank. Het probleem is wel dat iedereen op zijn informatie blijft zitten (Lacaeyse, persoonlijke communicatie).

Ten achtste dient de politie georganiseerde criminaliteit in eerste instantie in kaart te brengen. Een bevolkingsbevraging zoals de veiligheidsmonitor is hierbij een goede manier om zicht te krijgen op wat de bevolking als problemen ervaart. Hieruit kan je een beleid uittekenen (Pieteraerens, persoonlijke communicatie). Verder kan een buurtinformatienetwerk een schat aan informatie opleveren. De succesformule van het buurtinformatienetwerk vertaalt zich wel enkel in wijken waar een grote sociale cohesie aanwezig is (Lacaeyse, persoonlijke communicatie).

Daarnaast vormen ANPR-camera's een grote hulp bij het in kaart brengen van grote verkeersstromen (Lacaeyse, persoonlijke communicatie; Pieteraerens, persoonlijke communicatie). Bijkomend geeft korpschef Lacaeyse (persoonlijke communicatie) aan dat de lokale politie weinig zicht heeft op de rekrutering bij georganiseerde criminaliteit. Dit dient volgens hem op federaal niveau te worden aangepakt, maar dit gebeurt niet mede door het capaciteitsprobleem bij de federale politie. De politie vist altijd een achter het net. De reactie op de criminaliteit is er pas bij een nefaste aanwezigheid van het probleem volgens Lacaeyse (Lacaeyse, persoonlijke communicatie).

Ten negende dient ingezet te worden op de actoren in de lokale omgeving zoals ouders, school en *peergroup* om radicalisering aan te pakken op lokaal niveau. Het lokale niveau is een belangrijk niveau, aangezien radicalisering op het lokaal niveau begint, ondanks het internationale aspect van terrorisme. Bij deze radicaliseringspreventie dienen geen losse structuren opgebouwd te worden naast de bestaande preventiekanalen, maar juist binnen deze bestaande preventiekanalen (Pauwels, persoonlijke communicatie).

6.2 Aanbevelingen op nationaal niveau

Criminele samenwerkingsverbanden bezitten een kwetsbare positie doordat ze opereren in een reguliere omgeving. Echter raken daders voorbij het autoritaire toezicht. Voor dit ontbrekende en falende autoritaire toezicht zijn volgens Kruisbergen et al. (2012) drie oorzaken te vinden, waarvan twee toepasbaar zijn op het nationale niveau. Ten eerste opereren criminele samenwerkingsverbanden in een sterk afgeschermd omgeving, aansluitend met een hoge sociale cohesie, een reputatiesysteem en een code van zwijgzaamheid. Ten tweede kan het toezicht ontbreken of functioneert het niet naar behoren (Kruisbergen et al., 2012). Dit is mogelijk een indicator die het belang van de aanwezigheid van politie in het straatbeeld aantoont.

Daarnaast is er nood aan een aanpassing van politietechnieken. In enkele interviews kwam de nood aan burgerinfiltranten, zoals fiscalisten en boekhouders, naar boven. De wet laat dit momenteel niet toe, terwijl in buurlanden als Duitsland dit wel mogelijk is (Paternotte, persoonlijke communicatie; X, persoonlijke communicatie).

In deze geglobaliseerde wereld waarin ook criminaliteit geglobaliseerd is, kijken we in België in verband met georganiseerde criminaliteit door een sleutelgat. Dit sleutelgat vernauwt door besparingen en doordat we zaken door andere landen laten onderzoeken, waardoor onze kennis niet toeneemt en ons sleutelgat klein blijft (X, persoonlijke communicatie). Aansluitend worden terrorisme en georganiseerde criminaliteit in de praktijk weinig aan elkaar gelinkt. Er is weinig kruisbestuiving bij het operationele luik van de politie inzake deze twee criminaliteitsfenomenen. Met andere woorden doet de politie aan hokjesdenken. Echter weet je bij witwassen niet of het geld dient voor de financiering van een terroristische groepering of niet. Pas bij het onderzoek kan er mogelijk een hint naar voren komen waarbij je weet in welke categorie je bezig bent (Farcy, persoonlijke communicatie; X, persoonlijke communicatie). In Bergen is er echter een uniek initiatief binnen de Federale Gerechtelijke Politie (FGP), namelijk de Cel Organised Crime – Terrorism (COT). Het tracht linken te leggen tussen georganiseerde criminaliteit en terrorisme. Bergen heeft dan ook last van zowel georganiseerde criminaliteit (motorbendes, Albanese maffia en fiscale fraude) en van terrorisme (Grijze Wolven en PKK) (Farcy, persoonlijke communicatie).

Meerdere oprichtingen van gezamenlijke afdelingen COT's kunnen de informatieverwerking beter doen lopen en de kennis vergroten over zowel de samenhang van de twee criminaliteitsfenomenen als van elk criminaliteitsfenomeen individueel (Dupuis, 2010; Farcy, persoonlijke communicatie). Paternotte (persoonlijke communicatie) deelt deze mening niet, aangezien georganiseerde criminaliteit illegale vermogensvoordelen beoogt en terrorisme invloed op een bepaald territorium beoogt (Paternotte, persoonlijke communicatie). Evenwel haalde we al aan dat Louis Shelley (2015) een evolutie ziet in terrorisme waarbij terroristische groeperingen zich ook op winst gaat focussen (Dettmer et al., 2015). Door het toenemende winst oogmerk worden georganiseerde criminaliteit en terrorisme op het gebied van doelstelling gelijkwaardiger en kan het hierdoor mogelijk een deur openen richting de oprichting van COT's.

De COT is dadergericht, waardoor het individugericht te werk kan gaan. Dit terwijl andere initiatieven voornamelijk fenomeengericht te werk gaan en de magistratuur zaakgericht te werk gaat. Er wordt dus teveel op fenomenen gewerkt en te weinig op dadergroepen (Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie).

Inzake de benadering dient evenwel opgelet te worden. Wanneer enkel dadergericht wordt gewerkt, worden activiteiten op één hoop gegooid. Echter is een crimineel samenwerkingsverband vaak polycrimineel en dus bezig met meerdere activiteiten. De aanpak dient dus een combinatie te zijn van fenomeengericht en dadergericht werken (Kleemans, persoonlijke communicatie).

Verder haalt Farcy (persoonlijke communicatie) aan dat hun diagnose opgenomen is als *best practice* binnen de federale politie. Terwijl Belgische politiediensten hun diagnose rond georganiseerde criminaliteit stellen aan de hand van de beeldvorming in Vlaanderen, vertrekt Bergen vanuit een arrondissementele diagnose van criminaliteit gebaseerd op drie elementen. Ten eerste kijk je naar het statistisch fenomeen. Ten tweede kijk je naar het milieu waar de dadergroep gezeteld is. Ten derde kijk je naar de criminele territoria bestaande uit drie delen: (A) het jachtterrein (de plaats van de feiten), (B) de verblijfplaats (van de crimineel of organisatie) en (C) de *lieu de plaisir* (de ontmoetingsplaats zoals een bar, stripclub of café). De combinatie van deze elementen leiden tot een diagnose waarbij je een specifiek beeld krijgt van je zone (Farcy, 2015; Farcy, persoonlijke communicatie). Vervolgens is een andere goede manier van werken het gebruik van een risicoanalyse (*threat assessment*). Hierbij kijk je naar wat een criminele organisatie wilt bereiken en wat ze kan bereiken. Je kijkt hierbij naar de capaciteit: wat zijn hun middelen, hun kennis en expertise? Verder wordt er ook gekeken naar de impact die ze kunnen hebben (Paternotte, persoonlijke communicatie).

Om crimineel gedrag te voorkomen dienen alle actoren die mogelijks een rol spelen, betrokken te worden. Dit zou kunnen gebeuren aan de hand van een programmawerking zoals beschreven in artikel 95 'et tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus'³ (Paternotte, persoonlijke communicatie).

Vervolgens zouden nationale overheidsdiensten zoals politie en douane meer moeten samenwerken om tot meer kennis te komen. Toegang tot elkaars databanken zou hierbij een pluspunt vormen. Op financieel crimineel vlak zouden meerdere ondersteuningscellen een oplossing kunnen bieden. In deze ondersteuningscellen zitten één politieambtenaar en twee fiscalisten. Elke vennootschap dient een btw-aangifte te doen, waarbij de ondersteuningscellen deze btw-aangiftes controleren (X, persoonlijke communicatie).

³ Art. 95. Wet tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Van 7 december 1998.

Zoals uit deze masterproef blijkt, bestaat corruptie in relatie tot terrorisme en georganiseerde criminaliteit nog steeds (Williams, 2001; Zanini et al., 2001; Boerman et al., 2012; Kruisbergen et al., 2012; Ruggiero & Gounev, 2012; Dettmer et al., 2015; Trends, 2015; Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie; Pauwels, persoonlijke communicatie; Rajakumar, persoonlijke communicatie; X, persoonlijke communicatie). De strijd hiertegen mag niet opgegeven worden door nationale overheden en de Europese Unie. De relatie tussen een crimineel netwerk en haar corruptieve contacten doorbreken, biedt kansen om het netwerk los te maken van haar ondersteunende structuren (Williams, 2001). Verder wordt corruptie voornamelijk gelinkt aan overheidsdiensten. Doch komt corruptie ook voor binnen de private zakenwereld (Ruggiero et al., 2012; Kleemans, persoonlijke communicatie). Ten slotte mag een corruptief contact niet steeds gepercipieerd worden als lid van een criminele organisatie. Het is goed mogelijk dat het corruptief contact net een slachtoffer is van corruptie omwille van bedreigingen naar zijn persoon toe of naar zijn gezin of familie toe (Ruggiero et al., 2012). Dit is een punt waar zeker rekening mee dient gehouden te worden bij de aanpak van corruptie.

Daarnaast haalden we aan dat corruptie binnen de Belgische douane niet vaak voorkomt, juist omdat de hoeveelheid goederen die dagelijks passeren doorheen de Antwerpse haven onmogelijk allemaal gecontroleerd kan worden (Bezlov et al., 2012). De besparingen die de douane treffen, maken de Antwerpse haven een gemakkelijk doelwit voor de invoer van illegale goederen. Wanneer essentiële zaken als containerscanners het begeven en de douane geen geld heeft om dit te laten repareren, dient de regering op te treden (Bergmans, 2015). Er dient dus meer gedaan te worden in een context waar minder middelen ter beschikking zijn (Paternotte, persoonlijke communicatie; Pauwels, persoonlijke communicatie).

De nationale gegevensdatabank bevat enkel gerechtelijke informatie (Laceyse, persoonlijke communicatie). Bestuurlijke informatie is van preventieve aard, gerechtelijke informatie van repressieve aard (Lokale politie – KASTZE, 2015). In verband met bestuurlijke informatie met betrekking tot terrorisme en radicalisme bestaat er geen databank. Dit komt, omdat artikel 44 van de ‘Wet op het Politieambt’⁴ is opgeheven door een nieuwe wet die in werking trad op zeven april 2014⁵ (Lacaeyse, persoonlijke communicatie).

⁴ Art. 44/1 tot art. 44/11. Wet op het politieambt. Van 5 augustus 1992.

⁵ Wet betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering. Van 18 maart 2014.

Momenteel is er dus geen databank die bestuurlijke informatie op een wettelijke en gestructureerde manier verzameld. Dit leidt tot sluikdatabanken, maar die kan je niet exploiteren. Politie is hier dus deels (noodgedwongen) illegaal aan het handelen (Lacaeyse, persoonlijke communicatie).

Net als aangehaald bij de lokale politie, kampt ook de federale politie met een capaciteitsprobleem en is er een gebrek aan een structurele visie. Zo kwam naar voren uit een interview dat er vroeger een *Terrorist Finance Unit* was binnen de Directie Economische en Financiële Criminaliteit (DJF). Deze *Unit* screende onder andere VZW's. Nu is deze Unit verhuisd naar de Directie van de Bestrijding van de Criminaliteit tegen Personen (DJP). Echter werkt momenteel niemand meer rond de financiering van terrorisme binnen de Directie van de bestrijding van Serious and Organised Crime (DJSOC) van de FGP (X, persoonlijke communicatie).

Verder ligt de focus van het onderzoek binnen de FGP verkeerd. Financieel gedreven onderzoek wordt niet gedaan. De focus ligt eerder op bijvoorbeeld drugs dan op het geld en dit zou volgens de respondent ook blijken uit een rapport van de CFI. Op deze manier kom je tot een ander beeld van de organisatie. Echter, wie financieel speurt begint bovenaan de organisatie, namelijk bij wie het geld beheert. Wie langs drugszijde speurt begint beneden, waardoor een grotere kans op vastlopen bestaat. Wanneer je kijkt naar de Verenigde Staten, merk je op dat de *Drug Enforcement Administration* wel focust op de geldstromen. Er is dus nood aan financiële speurders (X, persoonlijke communicatie). Ook Paternotte (persoonlijke communicatie) haalt aan dat er teveel op feiten wordt gewerkt, maar te weinig op financiële stromingen. Zo weet men vaak niet wat er achteraf met het bekomen geld gebeurt. Verder zijn inbeslagname en verbeurdverklaring in België laag (Paternotte, persoonlijke communicatie). Daarnaast zou er gescreend moeten worden waar onze benzine vandaan komt, zodat we onbewust groeperingen als IS niet mee financieren. Daar heb je onderzoekers voor nodig die voldoende vaardigheden hebben, waarbij ze dienen te weten wat een vennootschap is en wat het inhoudt. Zowel een anonieme respondent (persoonlijke communicatie) als Paternotte (persoonlijke communicatie) stellen zich hier de vraag of onderzoekers wel over voldoende kennis en vaardigheden beschikken (Paternotte, persoonlijke communicatie; X, persoonlijke communicatie).

De Europese Unie was geschrokken dat Syriëstrijders uit Europa doorgaans deel uitmaken van niet een eerste, maar juist van de tweede en derde generatie moslims binnen de Europese Unie, en dus binnen de Europese Unie geboren en opgegroeid zijn. Deze personen zijn groot gebracht met de Europese waarden en normen, maar opteren toch op een bepaald moment in hun leven om te strijden voor IS. De Europese Unie heeft hier een *wake up call* gehad en kwam tot het besef dat het niet meer het veilige front Europa is (Pauwels, persoonlijke communicatie). Naast onderdrukking en sociaaleconomische status kan een mogelijke oorzaak, zoals aangehaald bij 4.2.1 ‘rekrutering’, racisme zijn. Wanneer blijkt dat racisme een oorzaak kan zijn van moslimradicalisatie, dient gekeken te worden in eigen boezem en dient onderzocht te worden waar de mogelijke oplossing ligt in de maatschappij (Horgan 2005; Wright-Neville, 2010; Pauwels, Persoonlijke communicatie). Terrorisme mag nooit los gezien worden van de maatschappij, aangezien terrorisme zich situeert in de maatschappij (Bjørge, 2002; Horgan, 2005). Het is dus een gedeelde verantwoordelijkheid.

Racisme komt nog vaak voor in onze maatschappij, zowel in het privéleven als in de zakenwereld. Wanneer uitzendkantoren jobs gaan toekennen op basis van huidskleur en hoe buitenlands een naam klinkt, weet je dat je maatschappij met een groot probleem kampt (BBC, 2004; Volt, 2010). Volgens een undercover-reportage van het televisieprogramma Volt gaat het in België om zes op de acht interimkantoren die zich schuldig maken aan racisme ondanks charters om niet te discrimineren (Volt, 2010). Door de directeur van het Centrum voor Gelijke Kansen en Racismebestrijding, Jozef De Witte, werd tevens bevestigd dat de uitzendsector met een essentieel probleem zit op dit vlak (Deredactie.be, 2010). In een onderzoek van Nele Spaas (2015) voor het Minderhedenforum komen gelijkende resultaten naar voren. Uit haar onderzoek blijkt dat amper één op drie dienstencheques-ondernemingen weigerde te discrimineren op basis van etnische origine en dat drieënzestig procent van de dienstencheques-ondernemingen discrimineerde (Spaas, 2015). Raciale discriminatie kan leiden tot een tot het gevoel een buitenstaander te zijn, wat op zijn beurt kan leiden tot radicalisering (Wieviorka, 2004; Wright-Neville, 2010). Ook ex-politicus Selahattin Koçak haalt aan dat hij als moslim niet het gevoel heeft gelijkwaardig behandeld te worden met autochtone Belgen, wat vervolgens leidt tot een afkeer van alles wat Europees is, en dus tot een gevoel van ongenoegen (Cobbaert, 2015a). Bij preventie van terrorisme dient men federaal ook met dit aspect rekening te houden. Dit kan gebeuren aan de hand van campagnes en door meer verschillende etniciteiten positief in beeld te brengen zoals door het presenteren van een televisieprogramma (Wright-Neville, 2010; Cobbaert, 2015a).

Echter, wanneer een Vlaamse minister voor Gelijke Kansen het niet pikt dat er een debat ontstaat waarin racisme en radicalisering samen worden vermengd, kan er misschien gesteld worden dat de politiek hier nog niet voor open staat (Cobbaert, 2015b).

Zoals eerder aangehaald is racisme niet het enige mogelijke ontstekingsmechanisme. Er zijn ook andere ontstekingsmechanismen zoals sociaal economische status of elementen waardoor je als individu maatschappelijke druk voelt, waardoor een haat tegen onze maatschappij ontstaat (Wright-Neville, 2010; Alde'emeh, 2014; Pauwels, persoonlijke communicatie).

Het opleggen van een gevangenisstraf aan terugkerende strijders is een delicaat onderwerp. Uit een onderzoek van Post et al. (2010) onder vijftig terroristen kwam naar voren dat gevangenisstraf een negatieve impact heeft op de gevangengenomen terrorist, voornamelijk bij religieus-geïnspireerde terroristen. Het versterkte hun groepsidentiteit met de groepering, wat een belangrijk element vormt in hun persoonlijke identiteit. De gevangengenomen terroristen leerden in de gevangenis meer over hun groepering, voelden zich hechter met hun groepering en kregen meer sympathie met in hun ogen 'het goede doel' na te streven. Er is wel sprake van een verschil tussen seculiere terroristen en religieus-geïnspireerde terroristen. Deze ervaring binnen gevangenschap was hoger bij religieus-geïnspireerde terroristen (zevenenzeventig procent) dan dat van seculiere terroristen (vierenvijftig procent). Dertig procent van de respondenten had meermaals in de gevangenis gezeten. Maar een klein aantal respondenten gaven aan geen contact meer te hebben gehad met hun groepering na hun gevangenschap. Tweeënzestig procent van de seculiere respondenten en vierentachtig procent van de religieus-geïnspireerde respondenten in het onderzoek waren na hun gevangenschap dan ook terug actief in hun gevangenschap (Post et al., 2010). Verder zien bijvoorbeeld jihadisten opsluiting als onderdeel van het martelaarschap (de Poot et al., 2009). Deze cijfers maken duidelijk dat over de rol van gevangenis diep moet worden nagedacht. De haat tegenover de maatschappij die het lid van een groepering in eerste instantie had, kan door opsluiting weer opflakkeren (Alde'emeh, 2014). Er dient wel een verschil gemaakt te worden tussen personen die mensen hebben omgebracht en personen die dit niet hebben gedaan. Moord blijft moord, ongeacht wat het doel is (Onwudiwe, 2001).

Wanneer een persoon die lid is van een terroristische groepering wenst terug te keren naar België, dient daar accuraat en deradicaliserend mee te worden omgegaan (Pauwels, persoonlijke communicatie). De maatschappij dient hierbij de vraag te stellen waarom deze *foreign fighter* is teruggekeerd naar België (Pieteraerens, persoonlijke communicatie).

Van de tweehonderddrieënzestig vertrokken Belgen zijn er honderdtweëntwintig teruggekeerd naar België (nadb, 2015). Deradicalisatie is het verlaten van sociale normen, waarden en attitudes van de terroristische groepering (Horgan, J., 2009). Als voorbeeld kunnen we Denemarken nemen. In Denemarken begeleiden politieambtenaren en buurtwerkers teruggekeerde jongeren uit Syrië om terug naar school te gaan, om op deze manier aan te tonen dat ze deel kunnen uitmaken van de samenleving op voorwaarde dat men geen misdaden heeft begaan in Syrië. Wanneer deze laatste voorwaarde niet is vervuld, wordt de teruggekeerde Syriëstrijder vervolgd. De begeleiding door een mentor kan jarenlang duren waarbij aandacht wordt besteed aan werk en educatie. In Denemarken tracht men dus een afweging te maken tussen hulpverlening en veiligheid (Deredactie.be, 2015a). Deze hulpverlening is ook nodig, aangezien deze ex-terroristen trots zijn op wat ze deden omdat ze in hun ogen in oorlog waren of hun geloof verdedigden (Post et al., 2010). Echter zal de ex-terrorist een reden hebben, waardoor hij de groepering wenst te verlaten. Dit kan bijvoorbeeld het besef zijn dat de groep waar hij zichzelf mee identificeert toch geen oplossing is voor het probleem dat de groepering benadert. De stap naar het verlaten van een groep is geen gemakkelijke stap (Horgan, 2005).

In België komt deradicalisatie nog niet voor, maar de hedendaagse belangstelling aan het fenomeen van Syriëstrijders lokt wel bevolkingsinitiatieven uit in onder andere Antwerpen. Zo zijn er imams die in scholen gaan spreken over radicalisme en extremisme en zijn er Vlaamse moslims die zoekende jongeren trachten op andere gedachten te brengen. Deze Vlaamse moslims zijn psychosociale begeleiders die trachten te vertrekken vanuit de persoon. Ze hekelen dat onze maatschappij eerder vertrekt vanuit een veiligheidsbenadering en niet vanuit een individuele benadering (Deredactie.be, 2015c). Ook politici nemen aan dat preventie een vereiste is in de strijd tegen radicalisering. Zo wenst de Vlaamse minister van Gelijke kansen, Liesbeth Homans, dat er een opleiding moet komen voor eerstelijns werkers, zoals straatwerkers en leerkrachten, om signalen van radicalisering sneller en beter op te pikken (Cobbaert, 2015). Ook Bjørgo (2002) haalt het belang van opleiding in preventie aan (Bjørgo, 2002).

Professor Pauwels raadt aan dat België en de Europese Unie een goed sociaal beleid uitwerken inzake deradicalisering waarbij ze gebruikmaken van exit-bewegingen (Pauwels, persoonlijke communicatie). Deze exit-bewegingen hebben reeds goede resultaten geboekt in Noorwegen, Zweden en Duitsland (Bjørgo, 2002).

Dit initiatief is afkomstig uit Noorwegen in de jaren negentig na problemen met extreemrechts. Het doel van de bewegingen is leden van extreemrechtse organisaties begeleiden bij het deradicaliseren wanneer ze uit een groepering stappen (Bjørge, 2002; Pauwels, persoonlijke communicatie).

Uit deze deradicalisatie kunnen initiatieven opkomen zoals de Noorse JustUnity, waarbij individuen die gederadicaliseerd zijn op scholen gaan spreken (JustUnity, 2015; Pauwels, persoonlijke communicatie). Deze personen geven dan bijvoorbeeld aan jongeren de redenen waarom ze net uit de groepering zijn gestapt. Op deze manier zet je tegelijkertijd in op preventie en bestrijd je propaganda. Deze initiatieven kunnen dus gelden als *resilience-training*. Hedendaags is school als preventiemiddel onderbenut. De *foreign fighters* die terugkeren hebben lokaal *street credibility*, waardoor jongeren eerder naar hen gaan luisteren (Pauwels, persoonlijke communicatie).

Evenwel dient hier aangehaald te worden dat deradicalisatie niet kan bereikt worden door het omgekeerde te doen van hoe de geradicaliseerde is geradicaliseerd. Deradicalisering dient daarnaast steeds zoveel mogelijk aangepast te worden aan het individu en de rol die hij opnam binnen het terroristisch netwerk (Moghaddam, 2009). Bijkomend dient de moslingemeenschap betrokken te worden bij moslimterrorisme. Want hoe kan je mensen iets afraden te doen als je de godsdienst niet kent (Pauwels, persoonlijke communicatie)? Verder dient rond de signalering van radicalisme, de families van de gerekruteerde op te worden gevolgd. Families zijn vaak het grootste slachtoffer van de radicalisering (Pieteraerens, persoonlijke communicatie). Zo komen families bijvoorbeeld ook aan bod bij JustUnity (JustUnity, 2015).

6.3 Aanbevelingen op Europees niveau

Daarnt haalden we al twee oorzaken aan in 6.2 “aanbevelingen op nationaal niveau” over hoe criminele samenwerkingsverbanden toezicht te omzeilen. Een derde oorzaak van hoe criminele samenwerkingsverbanden toezicht omzeilen, is doordat het toezicht soms (al dan niet bewust) beperkt wordt gehouden door concurrerende belangen. Zo wordt in belastingparadijzen toezicht bewust beperkt gehouden omwille van economische motieven (Kruisbergen et al., 2012).

Wat contant geld betreft gaan we de goede richting uit. Een probleem schuilt in de mogelijkheden die het bedrijfsleven biedt. Zaken als anonimiteit, op nummer bankieren en belastingconstructies worden ook door georganiseerde criminaliteit gebruikt. Deze hiaten dienen gedicht te worden, ondanks dat criminaliteitspreventie soms op gespannen voet staat met economische belangen (Kleemans, persoonlijke communicatie). Het bankgeheim en een gunstig fiscaal regime bieden een concurrentievoordeel wanneer het gaat om buitenlandse vermogende partijen aan te trekken (Kruisbergen et al., 2012). Banken zoals HSBC trekken door middel van het bankgeheim criminele samenwerkingsverbanden en terroristische groeperingen aan en maken zich hierdoor medeschuldig aan georganiseerde fiscale fraude en witwassen (Winer, 2002; Eeckhaut, 2014). Verder helpen belastingparadijzen onrechtstreeks corruptie. In een aantal Europese lidstaten wordt de activa van openbare ambtenaren onder de loep genomen om aanwijzingen van corruptie te vinden. Deze praktijk blijkt ineffectief door het bestaan van belastingparadijzen (Bezlov et al., 2012). Doordat financiële stromingen geglobaliseerd zijn, zou het opheffen van het bankgeheim wereldwijd een oplossing kunnen bieden. Momenteel is het verbeteren van Europese samenwerking tussen banken en overheden en het verbieden van het bankgeheim binnen de Europese Unie een eerste stap.

Het bestrijden van de bronnen aan financiering voor terroristische groeperingen wordt door experts wereldwijd erkend als één van de belangrijkste counterstrategieën die een overheid kan uitvoeren (Schmid, 2011). Verder dient de strijd tegen de financiering van terrorisme en georganiseerde criminaliteit op internationaal niveau te gebeuren (Winer, 2002; Mahan et al., 2008). Toch merkten we al eerder op dat amper één procent van het geld dat wit wordt gewassen, en mogelijk ook leidt tot de financiering van terrorisme, wordt opgemerkt (Farcy, 2015; Farcy, persoonlijke communicatie). Een aanvullende stap, naast het opheffen van het bankgeheim en dus gaan naar meer transparantie, is banken verplichten om anti-witwasmaatregelen te nemen. Wanneer ze deze nemen, zouden overheden mogelijk (tijdelijke) beloningen kunnen geven aan de bank. Dit vereist dan ook voldoende toezicht op het internationaal geldverkeer. Dit toezicht dient internationaal te zijn doordat financiële geldstromingen over jurisdicties en grenzen heen gaan (Winer, 2002). Het herbekijken van de huidige opties en regelgeving op Europees niveau wordt dan ook sterk aangeraden. Verder is de oprichting van een Europese *Financial Intelligence Unit* (FIU) een goede zaak (Paternotte, persoonlijke communicatie; X, persoonlijke communicatie). Samenwerking tussen nationale FIU's loopt niet altijd even vlot (Freeland, 2002).

Evenwel vindt witwassen op internationaal niveau plaats. Er is wel een verplichting tot samenwerking, maar de communicatie is beperkt. Vertrouwen vormt hier een grens en soms is dit ook de taalbarrière (Freeland, 2002; X, persoonlijke communicatie). Initiatieven zoals ‘De Egmont Groep’ proberen hier een mouw aan te passen. ‘De Egmont Groep’ is een informeel netwerk bestaande uit FIU’s om internationale samenwerking te stimuleren (The Egmont Group, 2015).

Door het toegenomen belang aan internet vormen cyberaanvallen een meer voorkomende werkwijze van terroristische groeperingen (Knack, 2015; Terrorismemonitor, 2015a; Terrorismemonitor, 2015b; Terrorismemonitor, 2015c; Farcy, persoonlijke communicatie). Overheidsinfrastructuur dient dan ook voldoende beveiligd te worden om cyberaanvallen te vermoeilijken en te weerstaan. Hoe zwakker de infrastructuur, hoe meer aantrekkelijk het wordt voor terroristen om aan te vallen (Zanini et al, 2001). Verder is propagandavoering via het internet aan een opmars bezig, waarbij ook de Europese Unie meer gaat moeten nadenken over preventiemaatregelen die betrekking hebben op de invloed van internet (Zanini et al., 2001; Marsden et al., 2011; Knack, 2015; Pauwels, persoonlijke communicatie). In eerste instantie moeten we leren omgaan met de snelheid en impact die het internet heeft en moeten we hier sneller op kunnen reageren (Farcy, persoonlijke communicatie; Pauwels, persoonlijke communicatie). Tegenstanders gebruiken meer en meer perceptie-management en operaties die rond informatie draaien. Deze mediagerichte maatregelen dienen om mensen aan te trekken, (rekrutering) of mensen te desoriënteren (angst aanjagen). Hierbij tracht de tegenstander de algemene perceptie in de negatieve zin te veranderen rond hoe veilig de maatschappij is. Het psychologisch verstoren kan een even belangrijk doel worden als fysieke vernietiging (Arquilla et al., 2001a). De oprichting van het Europese antipropagandabureau, wat een tegenkanaal zoekt te worden voor de propaganda die verspreid wordt via sociale media, is alvast een eerste stap in de juiste richting (De Greef, 2015). Kortom, dient de Europese Unie voldoende aandacht te besteden aan het gebruik van internet door de tegenstander.

Al in 2001 haalde de Verenigde Staten van Amerika aan dat er nood is aan een wetgeving rond internetcriminaliteit, waarbij deze wetgeving de opsporing en vervolging in goede banen leidt, ongeacht het internationale karakter van het misdrijf (Dennings, 2001). Ook andere literatuur haalt de noodzaak aan een voorzichtig juridisch omliggende wetgeving rond internetgebruik uit te werken (Weimann, 2006).

Echter halen meerdere respondenten aan dat nieuwe technologie zoals Whatsapp, Skype, Voice over IP en anonieme browsers als Tor nog niet wettelijk geregeld zijn in België, laat staan internationaal (Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie; Pauwels, persoonlijke communicatie; X, persoonlijke communicatie). Elk land vult hier zelf de regelgeving in (X, persoonlijke communicatie). Professor Pauwels stelt hierbij de vraag of de juridische voorwaarden van telefoontap niet kunnen verbonden worden aan het internet. Hier dienen België en de internationale gemeenschap snel een oplossing voor te bieden, want we wissen nu al achter het net en een maatschappij mag toch niet achterblijven (Pauwels, persoonlijke communicatie; X, persoonlijke communicatie)? Aanvullend haalt een respondent (persoonlijke communicatie) hier aan dat Europa niet aanwezig is in het debat rond de juridische gevolgen van het afschaffen van *roaming* binnen de Europese Unie. Zal bijvoorbeeld Vodafone dezelfde diensten kunnen leveren aan politiediensten in België? En kan de wetgeving niet aangepast worden dat er een meldingsplicht komt bij telecomoperatoren, aangezien politie nu dient te betalen voor telefoontap (X, persoonlijke communicatie)?

Vervolgens is het van belang dat de overheidsorganisatie en –structuur mee evolueert. Overheden dienen na te denken met wat voor organisatie ze netwerken dient te bestrijden, in plaats van vast te houden aan een hiërarchische orde met verticale relaties. Door het dynamische en losse aspect van terrorisme dienen (internationale) initiatieven zich meer flexibel op te stellen in hun aanpak om zo bureaucratische grenzen te overstijgen (Williams, 2001; Zanini et al., 2001; Marsden et al., 2011). Echter dient hier aangeduid te worden dat niet iedereen deze mening deelt. Zo stelt Tucker (2008) dat hiërarchische organisaties op lange termijn het meest bruikbaar blijven in de strijd tegen netwerken. Dit stelt hij, omdat hiërarchische organisaties goed zijn in veiligheid, handig zijn om strategische richting te geven en vasthangen aan legale en strategische beperkingen (Tucker, 2008). Echter dient een middenweg gekozen te worden, waarbij het flexibele aspect van netwerken kan gecombineerd worden met de veiligheid en het geven van strategische richting van hiërarchische organisaties. Belgische politie heeft een eerste stap genomen in dit proces door te evolueren naar het tweeluik lokale en federale politie die horizontaal samenwerken, maar waarbij nog steeds een kleine kern de hoofdrichtlijnen aangeeft. Echter blijft structurele evolutie een *must*. Vooralsnog dient men ook op te letten op managerialisme. Een overheidsdienst dient op te letten dat het voeling behoudt met het operationele luik (X, persoonlijke communicatie).

Tijdens deze structuurherziening dient ook nagedacht te worden over methoden om internationale en Europese samenwerking te verbeteren, zowel rond georganiseerde criminaliteit als rond terrorisme (Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie; Pauwels, persoonlijke communicatie; X, persoonlijke communicatie). De huidige gecentraliseerde organisaties zijn gekend omwille van hun samenwerkingsproblemen met andere organisaties (Tucker, 2008). Één respondent (persoonlijke communicatie) haalde zelfs aan dat deze internationale factor onze grootste structurele zwakte is (X, persoonlijke communicatie). Terrorismen is niet het probleem van één land en heeft ook niet enkel invloed op één land. Echter is om terrorisme te bestrijden internationale samenwerking een noodzaak (Weimann, 2006). Zaken als proactieve recherche of grensoverschrijdend politieoptreden komen internationaal onvoldoende aan bod (Lacaeyse, persoonlijke communicatie). Wederom komt ook hier het vertrouwensprobleem tussen landen aan bod (Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie; X, persoonlijke communicatie). Gegevensuitwisseling dient dus verbeterd te worden (Kleemans, persoonlijke communicatie). Daarnaast dienen EU-instrumenten geharmoniseerd te worden om tot een efficiënter beleid te komen (Paternotte, persoonlijke communicatie). Om nationale en bureaucratische grenzen te overstijgen, wordt in de literatuur *Join Task Forces* aangeraden (Williams, 2001). Dit bestaat binnen de Europese Unie al onder de benaming *Joint Investigation Teams* (JIT's). JIT's zijn onderzoeksteams die voor een bepaalde tijd worden opgericht voor een bepaald doel (Europol, 2015; Paternotte, persoonlijke communicatie).

De Europese Unie zou burgerinitiatieven kunnen steunen in hun strijd tegen terrorisme en georganiseerde criminaliteit, wanneer deze burgerinitiatieven getuigen van een grote mate aan expertise. Dit helpt de Europese Unie in haar strijd, kost geen middelen of capaciteit en tracht vuur met vuur te bestrijden. Een goed voorbeeld van een dergelijk burgerinitiatief is de hackersbeweging Anonymous. Deze organisatie, die trouwens ook geclassificeerd kan worden als een *leaderless network*, bestaat uit hack-experten die vrijwillig via hacking de wereld wat beter proberen te maken. Anonymous tracht de propagandamachine van IS te verzwakken door haar Twitter-accounts te hacken (Parkinson, 2015). Op dergelijke manier bestrijd je vuur met vuur.

Verder dient de Europese Unie goed na te denken over hoe het wenst terrorisme te bestrijden en hoe het wenst om te gaan met terugkerende strijders. Elke stap kan later gevolgen hebben. De Europese Unie dient op te letten dat het niet in de valkuilen van het verleden stapt (Pauwels, persoonlijke communicatie).

Zo haalt Nesser (2006) aan dat de invasie in Irak door Westerse troepen een ‘*spillover effect*’ had op het jihadisme in West-Europa. Terroristische groeperingen die de ideologie van al Qaida deelden, stuurden net meer *foreign fighters* naar Irak om mee te vechten tegen het Westen (Nesser, 2006; Mahan et al., 2008; Pauwels, persoonlijke communicatie). Desalniettemin wil je niet dat de volgende generatie de schuld op het Westen steekt, omdat die een land is binnengevallen en hierbij een nieuwe jihad achterlaat (Pauwels, persoonlijke communicatie). Vroeger stond georganiseerde criminaliteit centraal en toen hebben de regeringen bepaalde zaken niet aangepakt. Nu staat terrorisme centraal en komen dezelfde vragen terug naar boven. Evenwel zijn maatregelen bij terrorisme snel extreem en moet er opgelet worden dat het doel niet voorbij wordt geschoten (Kleemans, persoonlijke communicatie). Louise Shelley stelt voor om terrorisme te bestrijden met een variëteit aan wettelijke maatregelen in plaats van enkel te focussen op strafrecht, omdat terroristische groeperingen geëvolueerd zijn naar bedrijven (Dettmer et al., 2015). Verder is het aangeraden om de buitengrenzen goed te bewaken en *best practices* te verzamelen. Er is dus nood aan een holistisch beleid waarbij secundaire preventie, tertiaire preventie, afwering via intelligence en repressie (echter niet los van begeleiding) elk hun rol spelen (Pauwels, persoonlijke communicatie).

In dit bestrijden dient ook steeds rekening gehouden te worden met de juridische context zoals fundamentele mensenrechten. Terrorisme is geen excuus om deze vrijheden op te geven. Verder raadt professor Pauwels aan dat islamitische landen dienen op te treden tegen terrorisme als symbolische reactie (Pauwels, persoonlijke communicatie).

Ten slotte dient de Europese Unie aandacht te besteden aan deradicalisering (zoals besproken in de aanbevelingen voor het nationale niveau) en aan *homegrown terrorism* (Pauwels, persoonlijke communicatie). Dit laatste vormt een groot gevaar doordat het een goedkope manier is om aanslagen te plegen en waarbij je de benodigde informatie, zoals hoe je een bom moet maken, via het internet kan vinden (Zanini et al., 2001; Crenshaw, 2008; Mullins, 2009; Marsden et al., 2011; Stenersen, 2013; Burke, 2015; Dunham et al., 2015; Pauwels, persoonlijke communicatie).

6.4 Aanbevelingen op academisch niveau

Onderzoek door academici beïnvloedt deels beleid, publieke opinie en publieke perceptie over tal van zaken, waaronder corruptie. Sinds midden jaren negentig is de publieke perceptie over corruptie gevormd door de *Corruption Perceptions Index* (CPI) van *Transparency International*. De bevindingen uit de CPI hebben een grote globale invloed, aangezien ze wereldwijd wordt gebruikt voor *credit ratings*. Maar de CPI houdt er een scheve redenering op na, waarbij maar één zijde van het verhaal wordt verteld. De helft van de landen die in 2009 werden beoordeeld als minst corrupt, blijken fiscaal-juridisch afgeschermdde jurisdicties te zijn. Denk hierbij aan Zwitserland, Luxemburg en Hong Kong. Zo wordt bijvoorbeeld Zwitserland binnen Europa niet geranked als één van de meest corrupte landen, ook al moedigt het land daders aan om daar hun *dirty money* veilig te plaatsen. Daarnaast is geen enkel Afrikaans land geranked als minst corrupt. Maar wanneer we dan kijken naar het minst corrupte land in Afrika volgens de CPI, namelijk Botswana, zien we dat dit land veel eigenschappen heeft van een fiscaal-juridisch afgeschermdde jurisdictie. Met andere woorden wordt volgens Christensen (2012) te weinig rekening gehouden in de CPI met corruptie in banken gelegen in fiscaal-juridisch afgeschermdde jurisdicties die omwille van het bankgeheim gemakkelijker samen kunnen werken met criminele samenwerkingsverbanden en terroristische groeperingen (Christensen, 2012). Onderzoek dient dan ook voortdurend geëvalueerd te worden om steeds betere en betrouwbaardere onderzoeken te publiceren. Hoe betrouwbaarder het onderzoek, hoe beter dit zal leiden tot politieke maatregelen, aangezien de politieke wereld haar beleidskeuzes mede baseert op onderzoek.

Netwerkanalyse komt als techniek vaker voor (Kleemans, persoonlijke communicatie). Nu focussen studies op de groepsverdeling binnen de netwerken. De vraag is of we ons niet beter zouden focussen op de concrete en specifieke gebeurtenissen, diens specifieke opvolging van gebeurtenissen en diens specifieke omgevingsfactoren waar georganiseerde criminaliteit zich afspeelt. Zo beschrijft Felson (2006) een interview waarin een commissaris hem vertelde dat ze een leider van een drugsbende hadden gearresteerd. Een week na de arrestatie was deze zogenaamde leider drugs aan het verkopen op straat. De persoon die de vracht aan drugs ontving was voor een week of twee de ‘grote vangst’ van dienst, waarna hij terug ‘kleine vangst’ werd. Zelfs diens netwerk veranderde om de week, aangezien hij elke week van mededaders veranderde. De gebeurtenissen, diens opvolging en de omgevingsfactoren kunnen mogelijk de structuur bepalen waarin sociale groepen hun netwerken vormen (Felson, 2006).

Evenwel haalt professor Kleemans (persoonlijke communicatie) aan dat naast het aantal contacten nu soms wel aandacht wordt besteed aan de inhoud van de contacten. Hierdoor komt de vraag hoe belangrijk iemand is in een netwerk meer naar voor (Kleemans, persoonlijke communicatie).

Marsden en Schmid (2011) halen aan dat veel experten en auteurs gespecialiseerd in criminele organisaties en terroristische groeperingen kritiekloos de netwerkstructuren omarmen. Maar terzelfdertijd bestaan er verschillende soorten definities voor ‘netwerk’ en worden deze door elkaar toegepast. Het is daarnaast in organisatorische termen onduidelijk wat er valt onder een efficiënt en functioneel netwerk bij een entiteit die werkzaam is in de onderwereld (Marsden et al., 2011). Er is nood aan meer onderzoek naar terroristische netwerkstructuren. Een systematische analyse van terroristische groeperingsstructuren kan leiden tot het beter begrijpen van de psychologie van radicalisering en van het groepsgedrag. Dit kan ten slotte leiden tot betere counterstrategies (Mullins, 2009). Zo heeft een overheid aan de hand van het netwerkstructuur een indruk wat de zwaktes en sterktes zijn van de groepering. Zo schreven bijvoorbeeld Aquilla et al. (2001b) dat wanneer al Qaida een *hubnetwerk* had, er een kans bestond dat de dood van Osama bin Laden het einde zou betekenen voor het terroristisch netwerk. Echter, wanneer al Qaida een *all channel-netwerk* zou hebben gehad, zou de dood van Osama bin Laden niet het einde hoeven te betekenen voor al Qaida (Aquilla et al., 2001b; Pauwels, persoonlijke communicatie).

Onderzoek naar terrorisme is een steeds evoluerend continuüm waarbij de rol van kennis over de interne dynamiek van groeperingen steeds toeneemt (Marsden et al., 2011). Echter is terrorisme een onderwerp waar veel over is geschreven op basis van weinig onderzoek (Horgan, 2005). Er is bijgevolg nood aan meer kennis inzake terrorisme via gefundeerd onderzoek en effectiviteitsonderzoeken. We weten nog niet veel over wat er werkt, hoe aan deradicalisering dient te worden gedaan, wanneer en waarom individuen stoppen met radicalisering en wat de *best practices* zijn. We kunnen hierbij ook veel leren uit etiologisch onderzoek, maar met betrekking tot radicalisering is er nog niet veel onderzoek gevoerd (Pauwels, persoonlijke communicatie). Momenteel neemt België initiatieven in alle richtingen voor de bestrijding van terrorisme. Evenwel dient ook onderzoek gevoerd te worden naar het verband tussen georganiseerde criminaliteit en terrorisme (Paternotte, persoonlijke communicatie). Deze link wordt namelijk niet vaak gelegd in onderzoek (Dettmer et al., 2015). Om *evidence-based* te kunnen werken dien je kennis te bezitten (Pauwels, persoonlijke communicatie).

Bijkomend dient kennis uit de verschillende landen meer actief gedeeld te worden. Daarnaast is er binnen België geen geld voor onderzoek. Terrorisme vormt een bijkomend probleem waar minder geld voor voorradig is (Pauwels, persoonlijke communicatie).

Verder viel tijdens het schrijven van deze scriptie op dat het begrip ‘geweld’ in terroristisch onderzoek enkel wordt aangehaald wanneer het gaat over aanslagen, maar nergens wordt aangehaald wanneer het wordt gebruikt als afschermingsmethode. Hier wilt deze scriptie aan toevoegen dat intimidatie en bedreiging met geweld kan voorkomen als afschermingsmethode, waarmee het tracht overheden te doen stoppen met bestrijding van terrorisme, aan de hand van dreigementen tot aanslagen of andere criminele feiten. Zo gebruikt bijvoorbeeld IS deze tactiek. IS dreigde ermee om hun Britse gijzelaar te onthoofden als het Westen niet stopte met hun operaties tegen IS (Duffin et al., 2014).

Vervolgens is er nood aan onderzoek naar deradicalisatie en naar het uit de terroristische groepering stappen van de ex-terrorist. Onderzoek lag tot nu voornamelijk op de betrokkenheid van een individu en rekrutering. De gedachte onder onderzoekers leeft dat de terrorist en de groepering niet meer relevant zijn bij het uitdoven of verlaten van de groepering. Dit geeft de richting aan die het onderzoek naar terrorisme uitgaat. Dit werd zowel aangehaald door de literatuur als door Professor Pauwels (Horgan, 2005; Pauwels, persoonlijke communicatie).

Ten slotte dient academisch onderzoek meer toegang te krijgen tot casusmateriaal. In landen als Nederland is dit mogelijk, maar in heel wat landen is dit onmogelijk. Zo dient er bijvoorbeeld een betere samenwerking te ontstaan met politie om toegang te krijgen tot hun gegevens (Kleemans, persoonlijke communicatie; Paternotte, persoonlijke communicatie). Zoals eerder gezegd helpt goed academisch onderzoek een goed beleid uit te tekenen. Maar om tot goed academisch onderzoek te komen is wel nieuw materiaal noodzakelijk. Nu draait academisch onderzoek te vaak rond hetzelfde oude materiaal. Indien het mogelijk is, zou dit Europees dienen te worden geregeld (Kleemans, persoonlijke communicatie).

6.5 Aanbevelingen op inlichtingenniveau

Doordat het gebruik van internet binnen het criminele milieu aan een grote opmars bezig is, is het aangeraden dat inlichtingendiensten het gebruik van internet bij terroristische groeperingen monitort om een beeld te vormen rond de organisationele en offensieve capaciteiten en te zoeken naar hun elektronische zwaktes. Bijkomend is het ook aangeraden om de informatiestromen tussen schakels binnen een terroristische groeperingen of tussen cellen in het vizier te nemen. Ook inlichtingen voor terroristische cellen zijn van noemenswaardig belang (Zanini et al., 2001). Dit is geen simpele opdracht door het gebruik van prepaid-gsm's, doorgeefgsm's, anonieme webbrowsers, encryptieprogramma's en wettelijk ongeregelde elektronische correspondentiemiddelen zoals Voice over IP, Skype en Whatsapp (Zanini et al., 2001; Arquilla et al., 2001b; Stern, 2003; de Poot et al., 2009; Schmid, 2011; Klausen, 2015; Farcy, persoonlijke communicatie; Paternotte, persoonlijke communicatie; Pauwels, persoonlijke communicatie; X, persoonlijke communicatie).

Verder dient een inlichtingendienst te evolueren doorheen de tijd. Hier is echter niets nieuws aan, aangezien inlichtingendiensten zich altijd al hebben moeten aanpassen aan doelwitten, het veranderen van de operationele omgeving en het veranderen van de vraag voor extern toezicht (Wilson, 2008). Inlichtingendiensten zullen wel meer rekening dienen te houden met de opkomst van *homegrown terrorism*, waarbij aanslagen 'thuis' worden beoogd, waarbij amper één persoon noodzakelijk is om de aanslag te plegen (Dunham et al., 2015; Pauwels, persoonlijke communicatie).

Ten slotte blijft internationale samenwerking de sleutel tot betere resultaten (Tucker, 2008). Inlichtingenwerving en het delen van informatie tussen landen zijn twee belangrijke counterstrategieën in de strijd tegen terrorisme (Schmid, 2011; X, persoonlijke communicatie). Veel inlichtingendiensten delen niet graag inlichtingen met andere inlichtingendiensten wanneer het niet op basis van een bilateraal akkoord gebeurt. Maar wanneer inlichtingen over globalisatie gaat, dient de vraag gesteld te worden hoe geheim de informatie is versus de resultaten het kan bekomen door te delen met andere inlichtingendiensten. Als we effectief wensen om te gaan met de oude vormen van terrorisme, die nog steeds bestaan ongeacht het bestaan van nieuwe vormen, dienen we deze goed te begrijpen, zodat we op een meer gesofisticeerde manier kunnen strijden tegen de nieuwe vormen (Aldrich, 2008). Zoals eerder gesteld is internationale samenwerking een *must* om terrorisme te bestrijden (Weimann, 2006).

7. Concluderend kader

In deze masterproef hebben we twee criminaliteitsfenomenen, namelijk georganiseerde criminaliteit en terrorisme, apart bekeken en daarna met elkaar vergeleken om te zien waar de twee overeenstemmen en juist verschillen. Uit deze individuele criminaliteitsfenomenen en de vergelijking ertussen, hebben we aanbevelingen getrokken naar lokaal, federaal, Europees, academisch en inlichtingenniveau.

In het begin van elk individueel luik bleek al snel dat zowel terrorisme als georganiseerde criminaliteit zich niet laten vatten in één universele definitie. Een gebrek aan universele definities bemoeilijkt de bestrijding van beide criminaliteitsfenomenen. Hoe kan je een complex, voortdurend evoluerend fenomeen vatten in één universele definitie? Dit zal niet gaan en zal steeds een evolutie in definiëring vragen.

Uit deze scriptie komt naar voren dat terroristische groeperingen en criminele samenwerkingsverbanden veel aspecten gemeen hebben, maar toch ook op heel wat vlakken verschillen. Echter mag nooit uit het oog verloren worden dat elke terroristische groepering en crimineel samenwerkingsverband uniek is in al haar aspecten. Met zekerheid kan wel gezegd worden dat er een verband bestaat tussen de twee criminaliteitsfenomenen, waarbij belangenvermenging kan optreden. Terroristische groeperingen hebben financiële en materiële middelen nodig om hun strijd te kunnen voeren. Dit kan niet bereikt worden met ideologie alleen en leidt bijgevolg tot de trend dat terrorisme naast een ideologisch motief ook een winstmotief heeft. Hierdoor is het ook duidelijk dat terrorisme vaak nood heeft aan samenwerking met georganiseerde criminaliteit. Omgekeerd hoeft dit verband dan weer niet te bestaan. De FGP van Bergen probeert als uniek initiatief in België georganiseerde misdaad en terrorisme aan elkaar te koppelen in de COT waar dadergericht wordt gewerkt. Uitbreiding van de COT's lijkt dan ook een goede zaak, maar mag het hele model niet vervangen. Er dient steeds een middenweg gevonden te worden tussen fenomeengericht werken en dadergericht werken. Evenwel bevorderen COT's wel de samenwerking tussen politiediensten.

Jongere terroristische groeperingen zoals IS verschillen niet zo zeer van andere terroristische organisaties. IS gebruikt dezelfde netwerkvormen, dezelfde financieringswijzen en dezelfde kanalen. Evenwel valt het op dat internet en media grote rollen spelen binnen IS, in vergelijking met andere terroristische groeperingen.

IS gebruikt professioneel videomateriaal om potentiële leden te werven en mensen af te schrikken via lugubere beelden, hackt ze vaak bezochte sociaalnetwerksites om pro-terroristische slogans te posten, heeft het een eigen televisiezender en verspreidt het online magazines. Daarnaast is IS polycrimineel, een trend dat de laatste jaren meer voorkomt. Het houdt zich bezig met een grote verscheidenheid aan activiteiten, waaronder het verkopen van olie, het smokkelen van pornografie en kidnapping. Verder zet het ook meer dan ooit in op *homgrown terrorism*.

De impact die opkomende technologieën hebben zoals sociale media en internet zijn enorm, zowel voor terrorisme als voor georganiseerde criminaliteit. Media helpt onder andere bij het verspreiden van propaganda, het verspreiden van geruchten en het vinden van klanten. Internet helpt onder andere bij het verspreiden van kennis, het rekruteren van nieuwe leden, het verwerven van fondsen en het veroorzaken van schade. Bovenal is het een toegankelijk en goedkoop hulpmiddel. Dit hulpmiddel wordt meer en meer gebruikt. Hierdoor wordt het moeilijker om terrorisme en georganiseerde misdaad te bestrijden, want internet en media vergroten de speelruimte voor criminelen. Echter zijn elektronische correspondentiemiddelen zoals Whatsapp en Viber niet wettelijk geregeld en vissen politie en inlichtingendiensten daardoor achter het net. Hier dringt nationale en Europese wetgeving zich dan ook op.

Aansluitend aan het internet, kwam deze scriptie tot de vaststelling dat door middel van internet *homegrown terrorism* een realistische dreiging vormt binnen de Europese Unie. Internet maakt het makkelijk voor potentiële terroristen om *know-how* te bemachtigen zodat hij/zij weet hoe hij/zij een aanslag kan plegen. Terroristische groeperingen zoals IS en al Shabaab proberen hiertoe mensen aan te zetten om in het land waar het potentiële lid woont, aanslagen te plegen. Doorheen de aanbevelingen raden we zowel inlichtingendiensten als overheden aan om hier voldoende aandacht aan te besteden.

In de aanbevelingen rondom het academisch luik blijkt al snel dat er nood is aan meer onderzoek. Georganiseerde criminaliteit is op een grote variëteit aan aspecten uitgebreid beschreven. Doch viel doorheen deze scriptie op dat dit bij terrorisme niet steeds het geval is. Zo wordt geweld nooit gekoppeld aan afschermingsmethoden, waardoor deze scriptie zoekt bij te dragen aan de literatuur. Verder blijkt ook dat literatuur rond terrorisme gebaseerd is op weinig onderzoek. Er is dan ook nood aan een gefundeerd onderzoek zodat we te weten komen waarom individuen een terroristische groepering verlaten, hoe aan deradicalisatie dient te worden gedaan en wat de *best practices* zijn om terrorisme te bestrijden.

De aanbevelingen begonnen met een citaat van George R. R. Martin (2011) waarmee we duidelijk proberen te maken dat beleidsmakers een enorme impact hebben met de keuzes die ze maken op het vlak van georganiseerde criminaliteit en terrorisme. Dit mogen beleidsmakers nooit uit het oog verliezen. Zo staat het zwaard in het citaat voor de macht en de impact die beleidsmakers hebben. Met dit zwaard dienen ze zelf de straf of gevolgen te bepalen voor bijvoorbeeld Syriëstrijders die terugkeren. Een beleidsmaker dient zich niet te verbergen achter personeel dat het vuile werk voor hem opknapt (lees: justitie en penitentiaire inrichtingen), maar dient mee te denken over preventieve, deradicaliserende en repressieve mogelijkheden en keuzes in samenspraak met academici, experts en indien mogelijk ex-Syriëstrijders, met als doel preventief jongeren te weerhouden te gaan strijden en terugkeerders te deradicaliseren zodat ze geen gevaar (meer) vormen voor onze maatschappij.

Dit moet blijken uit de aanbevelingen die we gaven rond gevangenisstraf, deradicaliserende en preventieve initiatieven. In eerste instantie is het van belang dat de maatschappij in eigen boezem kijkt wat er fout loopt binnen de maatschappij, vooraleer ze kijkt naar terrorisme. Hierbij dient aandacht besteed te worden aan racisme, sociaaleconomische status en werkgelegenheid. Verder dient een maatschappij zowel in te zetten op secundaire preventie, tertiaire preventie, afwering via intelligence en repressie verbonden aan begeleiding. In deze scriptie prijzen we de burgerinitiatieven inzake preventie en deradicalisatie aan, maar dient ook de overheid, zowel Europees als nationaal, hierin actief te zijn. In de thesis raden we dan ook JustUnity aan voor het preventionele luik en exit-bewegingen aan voor het deradicaliserende luik.

8. Bibliografie

8.1 Boeken

BOERMAN, F., GRAPENDAAL, M. & MOOIJ, A. (2008). *Nationaal dreigingsbeeld 2008: Georganiseerde criminaliteit*. Zoetermeer, Dienst IPOL, 261p.

BOERMAN, F., GRAPENDAAL, M., NIEUWENHUIS, F. & STOFFERS, E. (2012). *Nationaal Dreigingsbeeld 2012: Georganiseerde criminaliteit*. Zoetermeer, Dienst IPOL, 284p.

DECORTE, T., TIEBERGHIEN, J. & PETINTSEVA, O. (2014). *Methoden van onderzoek: ontwerp en dataverzameling – Een handleiding*. Gent, Academia Press, 265p.

DE POOT, C. J., SONNENSCHIN, A., SOUDIJN, M. R. J., BIJEN, J. G. M. & VERKUYLEN, M. W. (2009). *Jihadistisch terrorisme in Nederland: Een beschrijving op basis van afgesloten opsporingsonderzoeken*. Meppel, Boom Juridische Uitgevers, 185p.

FIJNAUT, C., BOVENKERK, F., BRUINSMA, G., & VAN DE BUNT, H. (1996). *Parlementaire Enquêtecommissie Opsporingsmethoden (PEO), Inzake opsporing: Enquête opsporingsmethoden*. Den Haag, Sdu Uitgevers, 484p.

FINCKENAUER, J. O. (2007). *Mafia and organised crime: A beginner's guide*. Londen, Oneworld Publications, 232p.

GAMBETTA, D. (1996). *The Sicilian mafia: The business of private protection*. Cambridge Massachusetts, Harvard University Press, 335p.

HORGAN, J. (2005). *The psychology of terrorism*. Oxon, Routledge, 199p.

KENNEY, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. University Park, The Pennsylvania State University, 293p.

KLEEMANS, E.R., VAN DEN BERG, E. A. I. M., VAN DE BUNT, H. G. & BROUWERS, M. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*. Den Haag, WODC, 177p.

KRUISBERGEN, E.W., VAN DE BUNT, H.G., KLEEMANS, E.R., KOUWENBERG, R.F., HUISMAN, K., MEERTS, C.A. & DE JONG, D. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de monitor Georganiseerde Criminaliteit*. Den Haag, WODC, 377p.

MAHAN, S. & GRISET, P. L. (2008). *Terrorism in perspective*. Thousand Oaks, Sage Publications Inc., 425p.

MARTIN, G. R. R. (2011). *A Game of Thrones*. Londen, Harper Voyager, 801p.

NAYLOR, R.T. (2002). *Wages of crime: Black markets, illegal finance, and the underworld economy*. Ithaca New York, Cornell University Press, 336p.

ONWUDIWE, I. D. (2001). *The globalization of terrorism*. Hampshire, Ashgate Publishing Limited, 171p.

VAN GESTEL, B. (2014). *Facilitering van mobiele bendes*. Den Haag, Wetenschappelijk Onderzoek- en Documentatiecentrum, Ministerie van Veiligheid en Justitie, 69p.

VERSCHUREN, P. & DOOREWAARD, H. (2007). *Het ontwerpen van een onderzoek*. Den Haag, Lemma, 327p.

WEIMANN, G. (2006). *Terror on the internet: The new arena, the new challenges*. Washington, United States Institute of Peace, 309p.

WRIGHT-NEVILLE, D. (2010). *Dictionary of terrorism*. Cambridge, Polity Press, 221p.

STERN, J. (2003). *Terror in the name of God: Why religious militants kill*. New York, HarperCollins Publishers, 400p.

ZAITCH, D. (2002). *Trafficking cocaine: Colombian drug entrepreneurs in the Netherlands*. Den Haag, Kluwer Law International, 335p.

8.2 Bijdragen in verzamelwerken

ALDRICH, J. A. (2008). “Setting priorities in a world of changing threats”, in TSANG, S. (Ed.). *Intelligence and human rights in the era of global terrorism*, 158-170.

ARQUILLA, J. & RONFELDT, D. (2001a). “The advent of netwar (revisited)”, in ARQUILLA, J. & RONFELDT, D. (eds.). *Networks and netwars: The future of terror, crime, and militancy*, 1-25.

ARQUILLA, J. & RONFELDT, D. (2001b). “Afterword (September 2001): The sharpening fight for the future”, in ARQUILLA, J. & RONFELDT, D. (eds.). *Networks and netwars: The future of terror, crime, and militancy*, 363-371.

BEYENS, K. & TOURNEL, H. (2010). “Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview”, in DECORTE, T. & ZAITCH, D. (red.). *Kwalitatieve methoden en technieken in de criminologie*. Leuven/ Den Haag, Acco, 199-232.

BEZLOV, T. & GOUNEV, P. (2012). “Organised crime, corruption and public bodies”, in GOUNEV, P. & RUGGIERO, V. (Eds.). *Corruption and organized crime in Europe: Illegal partnerships*. Oxon/New York, Routledge, 32-54.

CRENSHAW, M. (1998). “The logic of terrorism: Terrorist behavior as a product of strategic choice”, in REICH, W. (Ed.). *Origins of terrorism: Psychologies, ideologies, theologies, states of mind*. Washington DC, Woodrow Wilson Center Press, 7-24.

DENNING, D. E. (2001). “Activism, Hactivism, and cyberterrorism: The internet as a tool for influencing foreign policy”, in ARQUILLA, J. & RONFELDT, D. (eds.). *Networks and netwars: The future of terror, crime, and militancy*, 239-288.

FLICK, U. (2010). “Kwalitatief online-onderzoek: gebruik van het internet”, in DECORTE, T. & ZAITCH, D. (red.). *Kwalitatieve methoden en technieken in de criminologie*. Leuven/ Den Haag, Acco, 415-439.

FREELAND, C. (2002). "How can sound customer due diligence rules help prevent the misuse of financial institutions in the financing of terrorism?" in PIETH, M. (Ed.). *Financing terrorism*, 41-48.

GOUNEV, P. (2012). "Organised crime, corruption and the private sector", in GOUNEV, P. & RUGGIERO, V. (Eds.). *Corruption and organized crime in Europe: Illegal partnerships*. Oxon/New York, Routledge, 55-68.

GUPTA, D. K., HORGAN, J. & SCHMID, A. P. (2009). "Terrorism and organized crime: A theoretical perspective", in CANTER, D. (ed.). *The faces of terrorism: Multidisciplinary perspectives*. Oxford/Malden, Wiley-Blackwell, 123-136.

HORGAN, J. (2009). "Disengaging from terrorism", in CANTER, D. (ed.). *The faces of terrorism: Multidisciplinary perspectives*. Oxford/Malden, Wiley-Blackwell, 257-276.

KERSTEN, A. (2002). "Financing of terrorism – a predicate offence to money laundering?" in PIETH, M. (Ed.). *Financing terrorism*, 49-56.

LEYS, M., ZAITCH, D. & DECORTE, T. (2010). "De gevalstudie", in DECORTE, T. & ZAITCH, D. (red.). *Kwalitatieve methoden en technieken in de criminologie*. Leuven/ Den Haag, Acco, 174-197.

MAESSCHALCK, J. (2010). "Methodologische kwaliteit in het kwalitatief criminologisch onderzoek", in DECORTE, T. & ZAITCH, D. (red.). *Kwalitatieve methoden en technieken in de criminologie*. Leuven/ Den Haag, Acco, 119-145.

MARSDEN, S. V. & SCHMID, A. P. (2011). "Typologies of terrorism and political violence", in SCHMID, A. P. (ed.). *The Routledge Handbook of Terrorism Research*. Oxon, Routledge, 158-200.

MOGHADDAM, F. M. (2009). "De-radicalization and the staircase from terrorism", in CANTER, D. (ed.). *The faces of terrorism: Multidisciplinary perspectives*. Oxford/Malden, Wiley-Blackwell, 277-292.

MONGE, P. & FULK, J. (1999). "Communication technology for global network organizations", in DESANCTIS, G. & FULK, J. (eds.). *Shaping organizational form: communication, connection and community*. Thousand Oaks, Sage, 71-100.

MORTELMANS, D. (2010). "Het kwalitatief onderzoeksdesign", in DECORTE, T. & ZAITCH, D. (red.). *Kwalitatieve methoden en technieken in de criminologie*. Leuven/ Den Haag, Acco, 75-118.

MULLINS, S. (2009). "Terrorist networks and small group psychology", in CANTER, D. (ed.). *The faces of terrorism: Multidisciplinary perspectives*. Oxford/Malden, Wiley-Blackwell, 137-150.

O'GORMAN, A. & VANDER LAENEN, F. (2010). "ethische aspecten van het kwalitatief onderzoek", in DECORTE, T. & ZAITCH, D. (red.). *Kwalitatieve methoden en technieken in de criminologie*. Leuven/ Den Haag, Acco, 531-557.

REICH, W. (1998). "Understanding terrorist behaviour: The limits and opportunities of psychological inquiry", in REICH, W. (ed.). *Origins of terrorism: psychologies, ideologies, theologies, states of mind*. Washington DC, Woodrow Wilson Center Press, 261-279.

RUGGIERO, V. & GOUNEV, P. (2012). "Corruption and the disappearance of the victim", in GOUNEV, P. & RUGGIERO, V. (Eds.). *Corruption and organized crime in Europe: Illegal partnerships*. Oxon/New York, Routledge, 15-31.

SCHMID, A. P. (2011). "Introduction", in SCHMID, A. P. (ed.). *The Routledge Handbook of Terrorism Research*. Oxon, Routledge, 1-37.

WILLIAMS, P. (2001). "Transnational criminal networks", in ARQUILLA, J. & RONFELDT, D. (eds.). *Networks and netwars: The future of terror, crime, and militancy*, 61-97.

WILSON, P. (2008). "Preparing to meet new challenges", in TSANG, S. (Ed.). *Intelligence and human rights in the era of global terrorism*, 111-120.

WINER, J. M. (2002). "Globalization, terrorist finance, and global conflict – time for a white list?", in PIETH, M. (Ed.). *Financing terrorism*, 5-40.

ZANINI, M. & EDWARDS, S. J. A. (2001). "The networking of terror in the information age", in ARQUILLA, J. & RONFELDT, D. (eds.). *Networks and netwars: The future of terror, crime, and militancy*, 29-60.

8.3 Tijdschriften

ANDREAS, P. & WALLMAN, J. (2009). "Illicit markets and violence: What is the relationship?", *Crime, Law and Social Change*, volume 52, nummer 3, 225-229.

BARBER, B. R. (1992). "Jihad vs. Mcworld", *Atlantic Monthly*, volume 269, nummer 3, 53-65.

CHRISTENSEN, J. (2012). "The hidden trillions: Secrecy, corruption, and the offshore interface", *Crime, Law and Social Change*, volume 57, nummer 3, 235-343.

CRELINSTEN, R. (2014). "Perspectives on counterterrorism: From stovepipes to a comprehensive approach", *Perspectives on terrorism: a journal of the terrorism research initiative*, volume 8, nummer 1, 2-15.

DUPUIS, B. (2010). "Bestrijding van georganiseerde misdaad door FGP Bergen", *Infoevue – Tijdschrift van de geïntegreerde politie*, volume 11, nummer 1, 24-27.

FARCY, F. (2015). "Renseignement criminel et lutte contre la criminalité organisée en Belgique", *Revue Française de Criminologie et de Droit Pénal*, nummer 4, 3-40.

FINCKENAUER, J. O. (2005). "Problems of definition: What is organized crime?", *Trends in Organized Crime*, volume 8, nummer 3, 63-83.

GARTENSTEIN-ROSS, D. (2009). "The strategic challenge of Somalia's Al-Shabaab – Dimensions of Jihad", *Middle East Quarterly*, volume 16, nummer 4, 25-36.

HAGAN, F. E. (2006). “*Organized crime and "organized crime": Indeterminate problems of definition*”, *Trends in Organized Crime*, volume 9, nummer 4, 127-137.

HEGGHAMMER, T. (2010). “*The rise of Muslim foreign fighters – Islam and the globalization of Jihad*”, *International Security*, volume 35, nummer 3, 53-94.

HELDENS, J. & REYSOO, F. (2005). “*De kunst van het interviewen: reflecties op het interview met een guide*”, *KWALON*, volume 10, nummer 3, 106-121.

HOLTMANN, P. (2014). “*Terrorism and Jihad: Differences and similarities*”, *Perspectives on terrorism: a journal of the terrorism research initiative*, volume 8, nummer 3, 140-143.

KEATINGE, T. (2014). “*The importance of financing in enabling and sustaining the conflict in Syria (and beyond)*”, *Perspectives on terrorism*, volume 8, nummer 4, 53-61.

KLAUSEN, J. (2015). “*Tweeting the jihad: Social media networks of Western foreign fighters in Syria and Iraq*”, *Studies in Conflict & Terrorism*, volume 38, nummer 1, 1-22.

KOOMEN, W. & VAN DER PLIGT, J. (2009). “*Achtergronden en determinanten van radicalisering en terrorisme*”, *Tijdschrift voor Criminologie*, volume 51, nummer 4, 345-359.

LEVITT, M. (2013). “*Hezbollah’s organized criminal enterprises in Europe, Perspectives on terrorism*, volume 7, nummer 4, 27-40.

NESSER, P. (2006). “*Jihadism in Western Europe after the invasion of Iraq: Tracing motivational influences from the Iraq war on jihadist terrorism in Western Europe*”, *Studies in conflict and terrorism*, volume 29, nummer 4, 323-342.

POST, J., SPRINZAK, E. & DENNY, L. (2010). “*The terrorist in their own words: interviews with 35 incarcerated Middle Eastern terrorists*”, *Terrorism and Political Violence*, volume 15, nummer 1, 171-184.

RAPOPORT, D. C. (2002). “*The four waves of rebel terror and september 11*”, *Anthropoetics*, volume 8, nummer 1, <http://www.anthropoetics.ucla.edu/ap0801/terror.htm>.

SCHMID, A. P. (2012). "The revised academic consensus definition of terrorism", *Perspectives on terrorism: a journal of the terrorism research initiative*, volume 6, nummer 2, 158-159.

SIEGEL, D. (2014). "Mobiel banditisme uit Oost- en Centraal-Europa", *het Tijdschrift voor de Politie*, volume 76, nummer 4/5, 29-31.

SINAI, J. (2008). "How to define terrorism", *Perspectives on terrorism: a journal of the terrorism research initiative*, volume 2, nummer 4, 9-11.

STENERSEN, A. (2013). "'Bomb-making for beginners': Inside al Al-Qaeda e-learning", *Perspectives on terrorism*, volume 7, nummer 1, 25-37.

TILLY, C. (2005). "Terror as strategy and relational process", *International Journal of Comparative Sociology*, volume 46, nummer 1-2, 11-32.

TUCKER, D. (2008). "Terrorism, networks and strategy: Why the conventional wisdom is wrong", *Homeland Security Affairs*, volume 4, nummer 2, <https://www.hsaj.org/articles/122>.

VAN DAELE, S. & VANDER BEKEN, T. (2010). "Migratie en mobiele daders – Heling bij rondtrekkende dadergroepen", *Tijdschrift voor Criminologie*, volume 52, nummer 2, 170-185.

WIEVIORKA, M. (2004). "The making of difference", *International Sociology*, volume 19, nummer 3, 281-297.

8.4 Elektronische bijdragen

BAJEKAL, N. (2014). Time (Elektronische versie). *More foreign fighters are going to Iraq and Syria than ever before, UN says*. Geconsulteerd op 14 december 2014, <http://time.com/3550713/isl-isis-iraq-syria-un/>.

BBC. (2004). *Five live survey suggests ethnic minority applicants still discriminated against in UK job market*. Geconsulteerd op 4 mei 2015, http://www.bbc.co.uk/pressoffice/pressreleases/stories/2004/07_july/12/minorities_survey.shtml.

BELGA. (2014). De Tijd (Elektronische versie). *Meer dan 300 Belgische Syrië-strijders*. Geconsulteerd op 15 december 2014, http://www.tijd.be/politiek_economie/belgie_algemeen/Meer_dan_300_Belgische_Syrie_strijders.9543169-4002.art.

BELGA & RR. (2014). Knack (Elektronische versie). *Whatelet: ruim 300 Belgische Syriëstrijders*. Geconsulteerd op 15 december 2014, <http://www.knack.be/nieuws/belgie/wathelet-ruim-300-belgische-syriestrijders/article-normal-299201.html>.

BERGMANS, E. (2015). De Standaard (Elektronische versie). *'In de Antwerpse haven is het vijf na twaalf': Schade aan scanner zou oplopen tot meer dan 800.000 euro*. Geconsulteerd op 10 mei 2015, http://www.standaard.be/cnt/dmf20150216_01532628.

BJØRGO, T. (2002). *Exit neo-nazism: Reducing recruitment and promoting disengagement from racist groups*. Geconsulteerd op 17 mei 2015, [http://freilich.anu.edu.au/sites/default/files/Bjorgo%20\(2002\).pdf](http://freilich.anu.edu.au/sites/default/files/Bjorgo%20(2002).pdf).

BOFFEY, D. (2015). The Guardian (Elektronische versie). *Boko Haram declares allegiance to Islamic State: Video Purportedly by leader of Nigeria group posted after female Islamists suicide bombers kill at least 50 in coordinated attacks in Maiduguri*. Geconsulteerd op 14 mei 2015, <http://www.theguardian.com/world/2015/mar/07/boko-haram-suicide-bombers-50-dead-maiduguri>.

BORGER, J. (2015). The Guardian (Elektronische versie). *Paris gunman Amedy Coulibaly declared allegiance to Isis*. Geconsulteerd op 1 mei 2015, <http://www.theguardian.com/world/2015/jan/11/paris-gunman-amedy-coulibaly-allegiance-isis>.

BURKE, J. (2015). The Guardian (Elektronische versie). *The road that led from tough Paris estate to radical Yemen training*. Geconsulteerd op 5 mei 2015, <http://www.theguardian.com/world/2015/jan/10/charlie-hebdo-paris-attack-yemen-connection>.

BVB. (2014). De Standaard (Elektronische versie). *Witte Huis bevestigt echtheid IS-onthoofdingsvideo*. Geconsulteerd op 19 november 2014, http://www.standaard.be/cnt/dmf20141117_01379526.

BVB & EVG. (2014). *2013 zwart jaar voor terrorisme*. Geconsulteerd op 14 december 2014, http://www.standaard.be/cnt/dmf20141118_01381974.

COBBAERT, P. (2015a). Knack (Elektronische versie). *Selahattin Koçak: 'Moslims worden anders behandeld'*. Geconsulteerd op 4 mei 2015, <http://www.knack.be/nieuws/belgie/selahattin-kocak-moslims-woorden-anders-behandeld/article-normal-526315.html>.

COBBAERT, P. (2015b). Knack (Elektronische versie). *Homans: 'Migranten krijgen hier wel degelijk kansen, ze moeten ze ook willen grijpen'*. Geconsulteerd op 4 mei 2015, <http://www.knack.be/nieuws/belgie/homans-migranten-krijgen-hier-wel-degelijk-kansen-ze-moeten-ze-ook-willen-grijpen/article-normal-528025.html>.

COOLSAET, R. (2014). *Tweeënhalf jaar moslimterreur: 393 aanslagen, 7.085 doden, 10.132 gewonden. Hoe succesvol is de wereldterrorist? Hieronder een overzicht van moslimterroristische aanslagen van dag tot dag*. Geconsulteerd op 6 december 2014, http://www.rikcoolsaet.be/files/comments/2004-04-16_RikCoolsaet.pdf.

De Greef. (2015). *Europa krijgt antipropagandabureau*. Geconsulteerd op 6 mei 2015, <http://deredactie.be/cm/vrtnieuws/buitenland/1.2244535>.

DEREDACTIE.BE. (2010). *"Klant is koning, maar wet is keizer"*. Geconsulteerd op 5 mei 2015, <http://deredactie.be/cm/vrtnieuws/binnenland/1.864486>.

DEREDACTIE.BE. (2015a). Het Journaal van 29 april 2015. *Waarom is Denemarken gidsland voor aanpak van Syriëstrijders?*. Geconsulteerd op 29 april 2015, <http://deredactie.be/cm/vrtnieuws/videozone/programmas/journaal>.

DEREDACTIE.BE. (2015b). Het Journaal van 30 april 2015. *Politie verijdeld terreuraanslag in Frankfurt*. Geconsulteerd op 30 april 2015,

<http://deredactie.be/cm/vrtnieuws/videozone/programmas/journaal>.

DEREDACTIE.BE. (2015c). Het Journaal van 30 april 2015. *Hoe gaan Belgische moslims om met radicalisering en extremisme?*. Geconsulteerd op 30 april 2015,

<http://deredactie.be/cm/vrtnieuws/videozone/programmas/journaal>.

DETTMER, M. & SCHINDLER, J. (2015). Der Spiegel (Elektronische versie). *Terror expert Louise Shelley: 'Islamic State is a diversified criminal operation'*. Geconsulteerd op 13 mei 2015, <http://www.spiegel.de/international/business/terror-expert-shelley-speaks-of-islamic-state-business-model-a-1011492.html>.

DIENST VOOR HET STRAFRECHTELIJK BELEID. (2015). *Georganiseerde criminaliteit*. Geconsulteerd op 18 februari 2015,

http://www.dsbsp.be/web/index.php?option=com_content&task=view&id=55&Itemid=80&lang=dutch.

DUFFIN, C. & ROSS, T. (2014). The Telegraph (Elektronische versie). *British hostage David Haines beheaded by Islamic State terrorists*. Geconsulteerd op 17 mei 2015,

<http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11094852/British-hostage-David-Haines-beheaded-by-Islamic-State-terrorists.html>.

DUNHAM, W., BEECH, E. & KERRY, F. (2015). *Islamic State calls on backers to kill 100 U.S. military personnel*. Geconsulteerd op 30 april 2015,

<http://www.reuters.com/article/2015/03/21/us-mideast-crisis-threat%20idUSKBN0MH0QQ20150321>.

DURY, F. (2015). Daily Mail (Elektronische versie). *'His heart burned to join his brothers': France's most wanted woman praises Paris deli murderer husband in ISIS magazine as she boasts about how easy it was to flee to Syria*. Geconsulteerd op 1 mei 2015,

<http://www.dailymail.co.uk/news/article-2950446/Amedy-Coulibaly-s-wife-gives-interview-ISIS-magazine.html>.

EECKHAUT, M. (2014). De Standaard (Elektronische versie). *HSBC-bank officieel verdacht van fraude*. Geconsulteerd op 11 maart 2015, http://www.standaard.be/cnt/dmf20141117_01379772.

EUROPA. (2014). *Bestrijding van de georganiseerde misdaad*. Geconsulteerd op 18 december 2014, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/index_nl.htm.

EUROPA. (2015a). *European Police Office – Europol*. Geconsulteerd op 26 februari 2015, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0025_en.htm.

EUROPA. (2015b). *Fight against organised crime: participation in a criminal organisation*. Geconsulteerd op 26 februari 2015, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0011_en.htm.

EUROPA. (2015c). *Fight against terrorism*. Geconsulteerd op 11 mei 2015, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/index_en.htm.

EUROPOL. (2015). *Joint Investigation Teams (JITS)*. Geconsulteerd op 9 mei 2015, <https://www.europol.europa.eu/content/page/joint-investigation-teams-989>.

FELSON, M. (2006). *The ecosystem for organized crime*. Geconsulteerd op 11 maart 2015, http://www.heuni.fi/material/attachments/heuni/papers/6Ktmwqur9/HEUNI_papers_26.pdf.

JALIL, J. (2015). The Times of Israel (Elektronische versie). *Islamic State calls for terror attacks in France, Belgium*. Geconsulteerd op 30 april 2015, <http://www.timesofisrael.com/islamic-state-calls-for-terror-attacks-in-france-belgium/>.

JUSTUNITY. (2015). *Hjem*. Geconsulteerd op 15 mei 2015, <http://www.justunity.no>.

KM. (2015). De Standaard (Elektronische versie). *IS heeft nu ook eigen televisiekanaal*. Geconsulteerd op 5 mei 2015, http://www.standaard.be/cnt/dmf20150427_01651172.

KNACK. (2015). Knack (Elektronische versie). *TV5 Monde gesaboteerd door IS*. Geconsulteerd op 18 april 2015, <http://www.knack.be/nieuws/tv5-monde-gesaboteerd-door-is/video-iwatch-560725.html>.

LÖCKINGER, G. (2005). *Terrorismus, Terrorismusabwehr, Terrorismusbekämpfung*. Ministerie van Defensie. Geconsulteerd op 16 april 2015, http://www.bundesheer.at/pdf_pool/publikationen/05_ttt_01_ttt.pdf.

LOKALE POLITIE – KASTZE. (2015). *Taken van de politie*. Geconsulteerd op 14 mei 2015, <http://www.lokalepolitie.be/5412/de-geintegreerde-politie/152-taken-van-de-politie.html>.

MAEREVOET, E. (2015). *Mensensmokkelaars verkopen hun diensten via sociale media*. Geconsulteerd op 5 mei 2015, <http://deredactie.be/cm/vrtnieuws/buitenland/1.2314020>.

MORENO, C. (2014). The Huffington Post (Elektronische versie). *Benicio Del Toro talks the two sides of Pablo Escobar*. Geconsulteerd op 11 mei 2015, http://www.huffingtonpost.com/2014/10/06/two-sides-pablo-escobar-_n_5940340.html.

NADB. (2015). De Standaard (Elektronische versie). *'Overal waar IS is, zijn er Belgen'*. Geconsulteerd op 15 mei 2015, http://www.standaard.be/cnt/dmf20150515_01682185.

PARKINSON, H. J. (2015). The Guardian (Elektronische versie). *Anonymous target terrorist Twitter accounts after Charlie Hebdo attack*. Geconsulteerd op 1 mei 2015, <http://www.theguardian.com/technology/2015/jan/12/anonymous-target-terrorist-twitter-accounts-charlie-hebdo-attack>.

REULINK, N. & LINDEMAN, L. (2005). *Kwalitatief onderzoek*. Geconsulteerd op 19 december 2014, [http://www.cs.ru.nl/~tomh/onderwijs/om2%20\(2005\)/om2_files/syllabus/kwalitatief.pdf](http://www.cs.ru.nl/~tomh/onderwijs/om2%20(2005)/om2_files/syllabus/kwalitatief.pdf).

ROLLINS, J. W. & ROSEN, L. (2015). *U.S. citizens kidnapped by Islamic State*. Geconsulteerd op 17 mei 2015, <http://www.fas.org/sgp/crs/terror/IN10167.pdf>.

SPAAS, N. (2015). *Dienstencheques: subsidiëren om te discrimineren?*. Geconsulteerd op 5 mei 2015,

<http://www.minderhedenforum.be/download/media/370/rapport-dienstencheques.pdf>.

STOKKING, K. M. (2003). *Kiezen van een onderzoeksstrategie en soorten onderzoek*. Geconsulteerd op 21 december 2014,

<http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CDAQFjAC&url=http%3A%2F%2Fstudion.fss.uu.nl%2FBouwstenenonline%2F2aonderzoeksstrategie.doc&ei=sp-UVN WGAYGp7Abek4DADg&usq=AFQjCNFrFcRq1RTNk7Nb-0t5-PWnEMRs8A&bvm=bv.82001339,d.d2s>.

SVG. (2015). De Standaard (Elektronische versie). *IS-leden 'verstoppert zich tussen bootvluchtelingen'*. Geconsulteerd op 17 mei 2015,

http://www.standaard.be/cnt/dmf20150517_01684563.

SWAINE, J. (2015). The Guardian (Elektronische versie). *Terror threats issued against British, American and Canadian shopping malls*. Geconsulteerd op 17 mei 2015,

<http://www.theguardian.com/world/2015/feb/22/terror-threats-issued-against-british-american-and-canadian-shopping-malls>.

TACK, H. (2014). De Standaard (Elektronische versie). *Opvallend veel Belgische steun voor IS op sociale media*. Geconsulteerd op 14 december 2014,

http://www.standaard.be/cnt/dmf20141128_01401714.

TERRORISMEMONITOR. (2015a). *Update: ISIS hacker valt Nederlandse, Britse en Amerikaanse websites aan*. Geconsulteerd op 18 april 2015, <http://terrorismemmonitor.nl/isis-hacker-valt-nederlandse-britse-en-amerikaanse-websites-aan/>.

TERRORISMEMONITOR. (2015b). *ISIS hackt Twitterpagina populair radiostation in Egypte*. Geconsulteerd op 18 april 2015, <http://terrorismemmonitor.nl/isis-hackt-twitterpagina-populair-radiostation-in-egypte/>.

TERRORISMEMONITOR. (2015c). *ISIS kamp vlakbij Texas gevonden*. Geconsulteerd op 18 april 2015, <http://terrorismemmonitor.nl/isis-kamp-vlakbij-texas-gevonden/>.

THE EGMONT GROUP. (2015). *About*. Geconsulteerd op 15 mei 2015, <http://www.egmontgroup.org/about>.

TOR. (2015). *Tor: Overview*. Geconsulteerd op 17 februari 2015, <https://www.torproject.org/about/overview.html.en>.

TRENDS. (2015). Trends (Elektronische versie). *Waar haalt Islamitische Staat zijn geld vandaan?*. Geconsulteerd op 13 mei 2015, <http://trends.knack.be/economie/finance/waar-haalt-islamitische-staat-zijn-geld-vandaan/article-normal-527115.html>.

VAN DE CLOOT, I. (2014). De Tijd (Elektronische versie). *De economie van de terreur*. Geconsulteerd op 17 mei 2015, http://www.tijd.be/opinie/column/De_economie_van_de_terreur.9537172-2337.art.

VOICES FROM THE BLOGS. (2014). *ISIS: perception on news on-line and social media considering only posts and articles written in Arabic language*. Geconsulteerd op 14 december 2014, http://voicesfromtheblogs.files.wordpress.com/2014/11/isis_on_newssocialmediavoices.pdf.

VOLT. (2010). *Volt undercover in het uitzendbureau*. Geconsulteerd op 5 mei 2015, <http://deredactie.be/cm/vrtnieuws/videozone/archief/programmas/volt/2.12414/2.12417/1.864255>.

WALKER, A. (2012). *What is Boko Haram?*. United States Institute of Peace. Special report 308. Geconsulteerd op 20 november 2014, <http://www.xtome.org/docs/groups/boko-haram/SR308.pdf>.

WB. (2015). Knack (Elektronische versie). *Aanslag op kerken voorkomen in Frankrijk: verdachte opgepakt*. Geconsulteerd op 30 april 2015, <http://www.knack.be/nieuws/wereld/aanslag-op-kerken-voorkomen-in-frankrijk-verdachte-opgepakt/article-normal-564077.html>.

8.5 Papieren mediaberichtgeving

ALDE'EMEH, M. (2014). Knack. Het getuigenis van Michael Delefortrie, teruggekeerde Syriëstrijder: 'Ik ben teruggekomen voor mijn gezin en mijn familie. Dat laat ik niet zomaar schieten'. 24 september 2014, jaargang 44. 34-38.

8.6 Beleidsdocumenten en rapporten

CEL VOOR FINANCIËLE INFORMATIEVERWERKING. (2013). *20 Jaarverslag 2013*. Geconsulteerd op 15 mei 2015,

http://www.ctif-cfi.be/website/images/NL/annual_report/jv2013-03102014.pdf.

DIENST VOOR HET STRAFRECHTELIJK BELEID. (2010). *Jaarrapport 2010: Georganiseerde criminaliteit in België 2007-2009*. Geconsulteerd op 14 maart 2015,

http://www.dsb-spc.be/doc/pdf/RAP_CRIMORG_2007-2009_NL_.pdf.

FEDERALE POLITIE. (2012). *Nationaal Veiligheidsplan 2012-2015*. Geconsulteerd op 19 februari 2015, http://www.polfed-fedpol.be/org/org_pns_nl.php.

RAAD VAN DE EUROPESE UNIE. (2010). *Council conclusions on the fight against crimes committed by mobile (itinerant) criminal groups*. Geconsulteerd op 24 december 2014,

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/118169.pdf.

REGERING. (1996). *Actieplan van de regering tegen de georganiseerde criminaliteit*.

8.7 Juridische bijdragen

EUR-LEX. *Council framework decision on the fight against organised crime*. 2008/831/JHA. Van 24 oktober 2008.

EUR-LEX. *The prevention and control of organised crime: a European Union strategy for the beginning of the new millennium*. OJ C 124. Van 3 mei 2000.

Wet betreffende het politie-informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering. Van 18 maart 2014.

Wet op het politieambt. Art. 44/1 tot art. 44/11. Van 5 augustus 1992.

Wet tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. Art. 95. Van 7 december 1998.

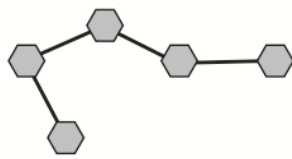
8.8 Persoonlijke communicatie

Naam	Functie	Locatie	Datum
Farcy François	Dirjud FGP Bergen – Doornik / Gewezen Directeur-generaal Federale Gerechtelijke Politie	Bergen	3/04/2015
Kleemans Edward	Hoogleraar Zware Criminaliteit en Rechtshandhaving (VU Amsterdam)	Amsterdam	21/04/2015
Lacaeyse Luk	Korpschef politiezone Erpemere – Lede	Gent	30/03/2015
Paternotte Marc	Diensthoofd Federale Gerechtelijke Politie – DSOC Organised Crime	Brussel	15/04/2015
Pauwels Lieven	Professor Criminal Law and Criminology Department (UGent)	Gent	29/04/2015
Pieteraerens Wim	Korpschef politiezone Kruibeke – Temse	Temse	18/03/2015
Rajakumar Vikram	Senior analyst 'Centre for Political Violence and Terrorism Research' (Singapore)	Elektronische correspondentie	1/04/2015
Schmid Alex	Director, 'Terrorism Research Initiative' (TRI), Editor-in-Chief, 'Perspectives on Terrorism' (PT), Research Fellow, International Centre for Counter-Terrorism - The Hague	Elektronische correspondentie	1/04/2015
X	X	X	X

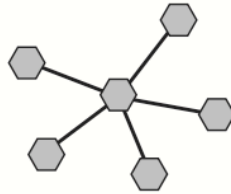
9. Bijlagen

9.1 Figuren

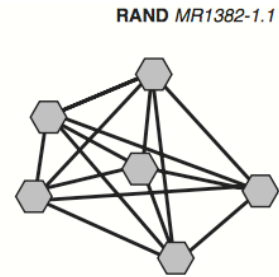
9.1.1 De drie basisvormen van netwerken van J. Arquilla & D. Ronfeldt (2001a)



Chain network

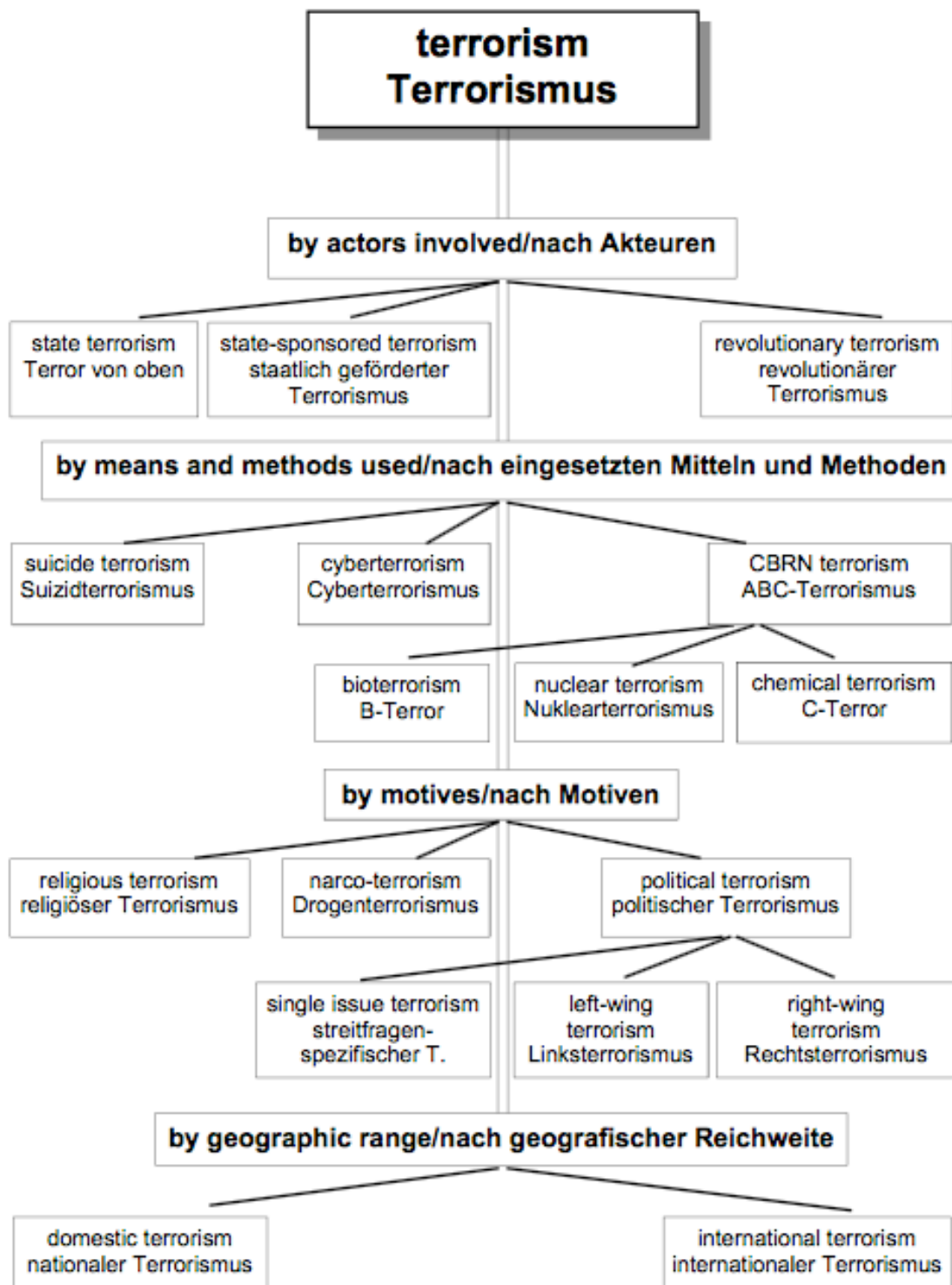


Star or hub network



All-channel network

9.1.2 Boomdiagram van G. Löckinger (2005)



9.2 Interviewvragen inzake het lokale luik

- 1) Krijgen jullie als lokale zone te maken met vormen van georganiseerde misdaad?
 - A) Hoe zit dit dan op het vlak van organisatie: rekrutering, hiërarchie, corruptie...?
 - B) Hoe zit dit dan op het vlak van financiering?
- 2) Wanneer jullie te maken hebben met dergelijk criminaliteitsfenomeen, wat is jullie reactie hierop?
 - A) Is er sprake van voldoende samenwerking, zijn er nadelen?
 - B) Zijn er verschillen bij aanpak tussen georganiseerde criminaliteit en terrorisme?
- 3) Denkt u dat een doorgedreven vorm van community policing zou helpen? (bv: wijkagenten die naar buurtfeesten gaan of iedereen bij naam kennen)
- 4) Zijn jullie als lokale politie voldoende ingelicht rond de terreurdreiging?
- 5) Vindt u dat een betere samenwerking tussen politie en hulpverlening een brug kan vormen naar potentiële daders van georganiseerde criminaliteit en terrorisme?
- 6) Hoe dient een lokaal politiebeleid georganiseerde criminaliteit te voorkomen?
- 7) Hoe dient een lokaal politiebeleid de rekrutering van foreign fighters (zoals Syriëstrijders) te voorkomen?
- 8) Hoe dient een lokaal politiebeleid om te gaan met de terugkeer van foreign fighters? (Wat is de rol van de politie hierin)
- 9) Wat zijn uw aanbevelingen op lokaal beleid?
 - A) Hoe en waar kan het beter?
 - B) Meer nood aan samenwerking en informatie?

9.3 Interviewvragen inzake georganiseerde criminaliteit

Organisatie

- 1) Hoe rekruteren criminele samenwerkingsverbanden nieuwe leden?
 - a) Zijn er bepaalde opvallende oorzaken dat nieuwe leden toetreden tot een crimineel samenwerkingsverband?
 - b) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake rekrutering?
- 2) Hoe ziet het netwerk van een crimineel samenwerkingsverband eruit?
 - a) Maakt het hierbij gebruik van een gemeenschapsgevoel?
 - b) Wat is een gebruikelijke verdeling in functies en jobs binnen een crimineel samenwerkingsverband?
 - c) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake netwerkvorming en functieverdeling?
- 3) Maakt een crimineel samenwerkingsverband gebruik van een hiërarchische orde?
 - a) Hoe ziet deze hiërarchische orde er bijkomend uit?
 - b) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake hiërarchie?
- 4) Vindt er gebruikelijk samenwerking plaats tussen gelijkende criminele organisaties?
 - a) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake samenwerking?
- 5) Maken criminele samenwerkingsverbanden anno 2015 nog steeds gebruik van corruptieve contacten?
 - a) Indien ja, in welke sectoren voornamelijk?
 - b) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake corruptie?
- 6) Maken criminele samenwerkingsverbanden gebruik van rechtspersonen?
 - a) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake rechtspersonen?
- 7) Maken criminele samenwerkingsverbanden gebruik van defensieve contrastrategieën?
 - a) Indien ja, wat voor defensieve contrastrategieën worden er gebruikt?
 - b) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake defensieve contrastrategieën?
- 8) Maken criminele samenwerkingsverbanden gebruik van offensieve contrastrategieën?
 - a) Indien ja, wat voor offensieve contrastrategieën worden er gebruikt?

- b) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake offensieve contrastrategieën?
- 9) Wat voor afschermingsmethoden gebruiken criminele samenwerkingsverbanden? (bv: media, valse identiteit, ICT, geweld)
 - a) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake afschermingsmethoden?

Financiering

- 1) Naylor beweert dat Illegale criminele bedrijven risicominimalisatie nastreven, in plaats van winstmaximalisatie. Bij risicominimalisatie zullen criminele samenwerkingsverbanden proberen aan *outsourcing* te doen, waarbij ze net zo min mogelijk proberen activiteiten in eigen beheer te bezitten. Maar Kruisbergen et al. (2012) spreken deze risicominimalisatie tegen. Zij stellen dat schakels buiten de eigen organisatie kunnen leiden tot risicomaximalisatie, aangezien de scheiding tussen autoriteit en crimineel samenwerkingsverband nooit waterdicht is. Dus doen criminele samenwerkingsverbanden net aan *insourcing*.
 - a) Wat denkt u?
 - b) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake insourcing of outsourcing?
- 2) Wat zijn veel voorkomende manieren van criminele samenwerkingsverbanden om aan winst te geraken?
 - a) Spelen deze manieren zich in de legaliteit of illegaliteit of een zekere schemerzone af?
 - b) Zijn deze vaak marktgeoriënteerd (spelen in op een vraag) of net niet?
 - c) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake financieel gewin?
- 3) Wat zijn vaak voorkomende manieren om het illegaal bekomen geld wit te wassen?
 - a) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake witwassen?
- 4) Vormen zogenaamde belastingsparadijzen een probleem bij de bestrijding van georganiseerde criminaliteit?
 - a) Zijn er verschillen tussen de verscheidene criminaliteitsfenomenen die onder georganiseerde criminaliteit vallen, inzake insourcing of outsourcing?
- 5) Vindt u dat de counterstrategies van de Europese staten en de Europese Unie voldoende zijn als antwoord op de financiering van georganiseerde criminaliteit?

Aanbevelingen

- 1) Wat zijn uw aanbevelingen rond georganiseerde criminaliteit op lokaal niveau?
- 2) Wat zijn uw aanbevelingen rond georganiseerde criminaliteit op federaal niveau?
- 3) Wat zijn uw aanbevelingen rond georganiseerde criminaliteit op Europees niveau?
- 4) Wat zijn uw aanbevelingen rond georganiseerde criminaliteit op academisch niveau?*

**** Enkel voor academici***

Toepassing op beide criminaliteitsfenomenen

- 1) Kan een terroristische groepering functioneren zonder een vorm van georganiseerde criminaliteit?
- 2) Worden verschillende kanalen gebruikt om beide fenomenen op te sporen? Zoja, welke?

9.4 Interviewvragen inzake terrorisme

Organisatie

- 1) Hoe rekruteren terroristische groeperingen nieuwe leden?
 - a) Zijn er bepaalde opvallende oorzaken dat nieuwe leden toetreden tot een terroristische groepering?
 - b) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 2) Hoe ziet het netwerk van een terroristische groepering eruit?
 - a) Maakt het hierbij gebruik van een gemeenschapsgevoel?
 - b) Wat is een gebruikelijke verdeling in functies en jobs binnen een terroristische groepering?
 - c) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 3) Maakt een terroristische groepering gebruik van een hiërarchische orde?
 - a) Hoe ziet deze hiërarchische orde er bijkomend uit?
 - b) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 4) Vindt er gebruikelijk samenwerking plaats tussen gelijkende terroristische groeperingen?
 - a) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 5) Maken terroristische groeperingen anno 2015 gebruik van corruptieve contacten?
 - a) Indien ja, in welke sectoren voornamelijk?
 - b) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 6) Maken terroristische groeperingen gebruik van rechtspersonen?
 - a) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 7) Maken terroristische groeperingen gebruik van defensieve contrastrategieën?
 - a) Indien ja, wat voor defensieve contrastrategieën worden er gebruikt?
 - b) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 8) Maken terroristische groeperingen gebruik van offensieve contrastrategieën?
 - a) Indien ja, wat voor offensieve contrastrategieën worden er gebruikt?

- b) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 9) Wat voor afschermingsmethoden gebruiken terroristische groeperingen? (bv: media, valse identiteit, ICT, geweld)
 - a) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?

Financiering

- 1) Naylor beweert dat Illegale criminele bedrijven risicominimalisatie nastreven, in plaats van winstmaximalisatie. Bij risicominimalisatie zullen criminele samenwerkingsverbanden proberen aan *outsourcing* te doen, waarbij ze net zo min mogelijk proberen activiteiten in eigen beheer te bezitten. Maar Kruisbergen et al. (2012) spreken deze risicominimalisatie tegen. Zij stellen dat schakels buiten de eigen organisatie kunnen leiden tot risicomaximalisatie, aangezien de scheiding tussen autoriteit en crimineel samenwerkingsverband nooit waterdicht is. Dus doen criminele samenwerkingsverbanden net aan *insourcing*.
 - a) Wat denkt u? Is dit ook van toepassing bij terroristische groeperingen?
 - b) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 2) Wat zijn veel voorkomende manieren van terroristische groeperingen om aan winst te geraken?
 - a) Spelen deze manieren zich in de legaliteit of illegaliteit of een zekere schemerzone af?
 - b) Zijn deze vaak marktgeoriënteerd (spelen in op een vraag) of net niet?
 - c) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 3) Wat zijn vaak voorkomende manieren om het illegaal bekomen geld wit te wassen?
 - a) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 4) Vormen zogenaamde belastingsparadijzen een probleem bij de bestrijding van terrorisme?
 - a) Is er een verschil te bemerken in vergelijking met nieuwe groeperingen als Islamitische Staat?
- 5) Vindt u dat de counterstrategies van de Europese staten en de Europese Unie voldoende zijn als antwoord op de financiering van terrorisme?

Aanbevelingen

- 10) Wat zijn uw aanbevelingen rond terrorisme op lokaal niveau?
- 11) Wat zijn uw aanbevelingen rond terrorisme op federaal niveau?
- 12) Wat zijn uw aanbevelingen rond terrorisme op Europees niveau?
- 13) Wat zijn uw aanbevelingen rond terrorisme op academisch niveau?*

**** Enkel voor academici***

Toepassing op beide criminaliteitsfenomenen

- 1) Kan een terroristische groepering functioneren zonder een vorm van georganiseerde criminaliteit?
- 2) Worden verschillende kanalen gebruikt om beide fenomenen op te sporen? Zoja, welke?

9.5 Questionnaire on the funding and organization of terrorism and organized crime

Proem

Dear Sir or Madam

My name is Nicolas Gosselin and I am a Masterstudent Criminology at Ghent University.

I mail you concerning my thesis given your expertise in the subject. My question is if you would be interested in completing the questionnaire that you can find on the second page of the Word-file.

My topic is "A comparative study between organized crime and terrorist groups in terms of organization and financing."

It seeks to gain insight into both the organization (recruitment, hierarchy, networking, the use of corruptive contacts and the use of counter-strategies) as the funding (including bank transactions and the legal and illegal sorts of income) of organized crime and terrorist groups.

What follows are recommendations for local policy, federal policy, European policy and academic level.

I want to emphasize that ANONYMITY is possible if requested. This will be polled later on in the questionnaire. The whole transcription of your mail will NOT be included in the annexes of the thesis.

Are you willing to provide your expertise regarding this topic?

Can you maybe refer me to people whose input is also interesting regarding this topic?

You can mail this file back to my e-mail adress: Nicolas.Gosselin@UGent.be

Thank you and kind regards

Nicolas Gosselin

Masterstudent Criminology

Ghent University

Your name, occupation and Anonymity

Full Name:

Occupation:

I want to emphasize that ANONYMITY is possible if requested.

The whole transcription of your mail will NOT be included in the annexes of the thesis.

Do you want to be anonym in this thesis? YES / NO

The Questions

Please only fill in what you are an expert in. Please don't be afraid to answer extensive.

FINANCING

When it comes to terrorism:

- What are the most used methods for funding and income?
- Are these methods of funding legal, illegal or are they located in a twilight zone?
- Do terrorist groups often use a third party to extent the possibilities of their funding, with or without the knowledge of the third party?
- What are the methods for laundering money when it comes to terrorism?
- Is the response of the European states or the European Union sufficient enough as countermethods for the funding of terrorism?

When it comes to organized crime:

- What are the most used methods for funding and income in the European Union?
- Are these methods of funding legal, illegal or are they located in a twilight zone?
- Does organized crime often use a third party to extent the possibilities of their funding, with or without the knowledge of the third party?
- What are the methods for laundering money when it comes to organized crime?
- Is the response of the European states or the European Union sufficient enough as countermethods for the funding of organized crime?

ORGANIZATION

When it comes to terrorism:

- How does a terrorist network look like? What are the functions within the network?
- Is there a hierarchy within terrorist networks?
- How do terrorist groups recruit members?
- Do terrorist groups use third parties for getting result?
- Is corruption within authoritative personnel an issue when it comes to terrorism?
- Do terrorist groups use counter-strategies to block the pursue of trial? If so, what are they?

When it comes to organized crime:

- How does an organizational crime network look like? What are the functions within the network?
- Is there a hierarchy within organizational crime networks?
- How do organized crime groups recruit members?
- Do organized crime groups use third parties for getting result?
- Is corruption within authoritative personnel an issue when it comes to terrorism?
- Do organized crime groups use counter-strategies to block the pursue of trial? If so, what are they?

REGARDING ORGANIZATION AND FINANCING

When it comes to recommendations:

- What are your recommendations for local and national policy?
- What are your recommendations for European policy?
- What are your recommendations for academic research concerning this subject?

Thank you for reading this file and answering the questions. Your answers will surely help with writing this thesis. If you have any questions or having some tips on literature and/or people who might be interesting to contact, you can e-mail me to this address:

Nicolas.Gosselin@UGent.be

Kind regards

Nicolas Gosselin
Masterstudent Criminology
Ghent University