



universität  
wien

# MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Konstruktionen ziviler Sicherheit in der  
Forschungsförderung: ein diskursanalytischer Vergleich  
zwischen der EU, Deutschland und Österreich“

verfasst von / submitted by

Rita Korunka, MA

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of  
Master of Arts (MA)

Wien, 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt /  
degree programme code as it appears on  
the student record sheet:

A 066 824

Studienrichtung lt. Studienblatt /  
degree programme as it appears on  
the student record sheet:

Masterstudium Politikwissenschaft

Betreut von / Supervisor:

Ao. Univ.-Prof. Dr. Otmar Höll

# Inhaltsverzeichnis

<b>I. Abkürzungsverzeichnis .....</b>	<b>3</b>
<b>II. Tabellenverzeichnis .....</b>	<b>3</b>
<b>1 Einleitung .....</b>	<b>4</b>
<b>2 Theoretische Grundlagen .....</b>	<b>9</b>
<b>2.1 EIN ERWEITERTES VERSTÄNDNIS VON SICHERHEIT .....</b>	<b>9</b>
<b>2.2 DIE PARISER SCHULE DER SECURITISATION THEORY.....</b>	<b>14</b>
<b>2.3 DAS VERHÄLTNISS VON SICHERHEITSPOLITIK UND FORSCHUNG .....</b>	<b>19</b>
<b>2.4 ERÖRTERUNG ZENTRALER BEGRIFFE .....</b>	<b>21</b>
2.4.1 RISIKO .....	21
2.4.2 VULNERABILITÄT .....	25
2.4.3 RESILIENZ .....	27
<b>3 Methode .....</b>	<b>34</b>
<b>3.1 KRITISCHE DISKURSANALYSE .....</b>	<b>34</b>
<b>3.2 COMPUTERGESTÜTZTE AUSWERTUNG MIT ATLAS.TI.....</b>	<b>35</b>
<b>4 Empirische Analyse.....</b>	<b>37</b>
<b>4.1 AUSRICHTUNG, BEDROHUNGSBILDER UND ERKLÄRTE ZIELSETZUNGEN DER UNTERSUCHTEN PROGRAMME .....</b>	<b>37</b>
4.1.1 BEDROHUNGSBILDER.....	37
4.1.2 SICHERHEITSBEGRIFF .....	40
4.1.3 REFERENZOBJEKTE .....	41
4.1.4 SICHERHEITSAKTEURE .....	43
4.1.5 FORSCHUNGSBEGRIFF .....	44
4.1.6 STRATEGISCHE ZIELE .....	46
<b>4.2 RESILIENZ .....</b>	<b>48</b>
4.2.1 „LERNENDE SICHERHEIT“: ZYKLISCHE BETRACHTUNGEN VON GEFAHREN UND RISIKEN.....	48
4.2.2 ALLE GEFAHREN – ALLE KOSTEN?.....	50
4.2.3 DIE ROLLE DER BEVÖLKERUNG .....	52
4.2.4 KLIMAWANDEL-ADAPTION.....	54
<b>4.3 TERRORISMUS .....</b>	<b>57</b>
4.3.1 DATENMANAGEMENT, DATA MINING, (TRANSNATIONALER) DATENAUSTAUSCH.....	57
4.3.2 TERROR IM ZUSAMMENHANG MIT ANDEREN DELIKTEN .....	59
4.3.3 „VULNERABLE PERSONEN UND GRUPPEN“: (DE-)RADIKALISIERUNG .....	61
<b>4.4 MIGRATION.....</b>	<b>64</b>
4.4.1 MENSCHLICHE SICHERHEIT .....	64

4.4.2	DIE INSZENIERUNG „ILLEGALER MIGRATION“ ALS SYSTEMISCHE BEDROHUNG.....	66
<b>4.5</b>	<b>GEFÜHLE UND WERTE UND OBJEKTE ALS REFERENZOBJEKTE ZIVILER SICHERHEIT .....</b>	<b>68</b>
4.5.1	„FREIES LEBEN“: (UN)SICHERHEITSEMPFINDEN IM KONTEXT DER LEBENSQUALITÄT .....	68
4.5.2	DER SCHUTZ VON KULTURELLEN WERTEN UND GÜTERN .....	70
<b>4.6</b>	<b>„SICHERHEIT FÜR DIE WIRTSCHAFT“: DIE VERSICHERHEITLICHUNG WIRTSCHAFTLICHEN</b>	
	<b>WOHLSTANDS.....</b>	<b>73</b>
4.6.1	DIE VOLKSWIRTSCHAFT UND UNTERNEHMEN ALS REFERENZOBJEKTE ZIVILER	
	SICHERHEITSFORSCHUNG .....	73
4.6.2	PRIMAT DES FORTSCHRITTS? DIE POSITIONIERUNG TECHNOLOGISCHER RISIKEN ALS CHANCEN	
	ÖKONOMISCHEN WACHSTUMS .....	78
4.6.3	DIGITALE SICHERHEIT .....	81
<b>4.7</b>	<b>TABELLARISCHE ZUSAMMENFASSUNG DER FORSCHUNGSERGEBNISSE .....</b>	<b>84</b>
<b>5</b>	<b>Schlussfolgerungen .....</b>	<b>89</b>
	<b>Literaturverzeichnis .....</b>	<b>93</b>
	<b>Abstracts.....</b>	<b>103</b>

## **I. Abkürzungsverzeichnis**

**BMBF:** Bundesministerium für Bildung und Forschung

**bmbwf:** Bundesministerium für Bildung, Wissenschaft und Forschung

**bmvit:** Bundesministerium für Verkehr, Infrastruktur und Technologie

**ESVP:** Europäische Sicherheits- und Verteidigungspolitik

**EU INTCEN:** European Union Intelligence and Situation Centre

**EUROPOL:** Europäisches Polizeiamt

**FFG:** Forschungsförderungsgesellschaft

**FP7:** 7. Forschungsrahmenprogramm der Europäischen Union

**FRONTEX:** Europäische Agentur für Grenz- und Küstenwache

**GWoT:** Global War on Terror

**IB:** Internationale Beziehungen

**ISS:** International Security Studies

**KDA:** Kritische Diskursanalyse

**OLAF:** Europäisches Amt für Betrugsbekämpfung

**ÖPNV:** Öffentlicher Personennahverkehr

## **II. Tabellenverzeichnis**

Tabelle 1: Vergleichende Darstellung der Forschungsergebnisse..... 84

## 1 Einleitung

Die Geschichte hat uns anhand zahlreicher Beispiele gelehrt, wie das Aufeinandertreffen von Wissenschaft, technologischer Innovation und Politik die Welt nachhaltig verändern kann. Die turbulente Entstehungsgeschichte der Atombombe, der Wettlauf ins All sowie die spieltheoretischen Nuklearstrategien zu Zeiten des Kalten Kriegs sind nur einige Beispiele. Gegenwärtig, im fortgeschrittenen Zeitalter der Digitalisierung, besitzen Data Mining, Spionagesoftwares, Hackerangriffe und biometrische Überwachungsmethoden die größte mediale Anziehungskraft. Im Hintergrund dieser Schlagzeilen vollzieht sich jedoch ein großer Teil dieser Kooperationen zwischen Forschung, Technologie und Politik weit weniger spektakulär und weit weniger geheim. Auf einen dieser halböffentlichen, bürokratisierten Bereiche der Zusammenarbeit von Akteuren aus Wissenschaft, Industrie, Politik und Exekutive wird sich diese Arbeit konzentrieren: *zivile Sicherheit*.

*Zivile Sicherheit* – als dehnbare Begriff für alle nicht-militärischen Maßnahmen im Feld der Sicherheitspolitik – hat in diesem und im vorigen Jahrzehnt sowohl politisch als auch wirtschaftlich an Bedeutung gewonnen. Die Europäische Union und auch einige Mitgliedstaaten unterstützen sowohl öffentliche Bildungs- und Forschungsinstitutionen als auch private Unternehmen, wenn sie auf diesem Gebiet Forschungsprojekte durchführen. Dies geschieht in Form öffentlicher Ausschreibungsverfahren, denen ein oder mehrere Dokumente zu Grunde liegen. In diesen „Sicherheitsforschungsprogrammen“ wird dargelegt, zu welchem Zweck eine bestimmte Technologie entwickelt und/oder aus welchem Grund eine konkrete sozial-/geisteswissenschaftliche Studie in Auftrag gegeben werden soll. Ausführungen dieser Art erläutern die strategischen Ziele öffentlicher Investitionen und dienen als Legitimationsbasis für eine kritische Öffentlichkeit. Sicherheit legitimiert Forschung und Forschung soll laut Auftrag zu einer Verbesserung der Sicherheit beitragen oder Unsicherheit reduzieren.

Was Sicherheit ist (und Gegenstand der Sicherheitspolitik sein soll), ist jedoch seit jeher umkämpft und von unterschiedlichen Einflussfaktoren abhängig. Unterschiedliche Definitionen dessen, was als sicher gilt und was als bedrohlich eingestuft wird, ziehen unterschiedliche politische Maßnahmen nach sich. Das Maß

an Unsicherheit, das unter bestimmten Gesichtspunkten als tolerabel gilt, verlangt nach unterschiedliche Strategien und Akteuren.

Ziel dieser Arbeit soll es daher sein, empirisch zu analysieren und im Rahmen einer kritischen Diskursanalyse herauszuarbeiten, *wie (Un)sicherheit in den ausgewählten Dokumenten zur Sicherheitsforschung konstruiert wird*. Als theoretisches Fundament dienen Konzepte und Begriffe des gegenwärtigen Diskurses im Bereich der sozialkonstruktivistisch-orientierten *International Security Studies* (ISS; siehe dazu z.B.: (Buzan und Hansen 2009). Im theoretischen Teil der Arbeit soll der Stand der Forschung in den ISS und die Entstehung einiger grundlegender Theorien umrissen werden. Ergänzt wird dies durch eine Erörterung der Begriffe *Risiko*, *Vulnerabilität* und *Resilienz*, von denen speziell letzterer im Kontext ziviler Sicherheit sowohl auf Policy-Ebene als auch im akademischen Diskurs im Laufe des letzten Jahrzehnts an Bedeutung gewonnen hat.

Die vergleichende Analyse stützt sich auf zwei nationale Programme und ein supranationales Sicherheitsforschungsprogramm:

- **EU:** *Secure Societies – Protecting freedom and security of Europe and its citizens*
- **Deutschland:** *Forschung für die zivile Sicherheit 2012-2017*
- **Österreich:** *KIRAS (Ausschreibungsphase 2014-2020)*

Im Zentrum der vergleichenden Analyse steht komplementär zur eingangs gestellten übergeordneten Forschungsfrage die Frage nach der Homogenität oder Heterogenität des sicherheitspolitischen Diskurses in diesem Policy-Bereich an der Schnittstelle zwischen Forschungs-, Innovations- und Sicherheitspolitik. Dieses Interesse entstand vor dem Hintergrund zahlreicher Publikationen, die in der boomenden Entwicklung der zivilen Sicherheit sowohl auf politisch-bürokratischer Ebene als auch auf wirtschaftlicher und technologischer Ebene die Logik einer neoliberal-gefärbten Gouvernamentalität sehen, die sich in modernen Technologien der Überwachung und /oder einer Reduktion/Abgabe staatlicher Sicherheitsaufgaben manifestiere (vgl. Joseph 2013a, 2013b, 2016; Chandler und Reid 2016; Bigo und Tsoukala 2008; Aradau 2014). In der empirischen Analyse soll geklärt werden, *ob und inwieweit in die Richtung einer solchen Gouvernamentalität gehende Tendenzen in den Programmen artikuliert werden oder nicht*.

Im theoretischen Teil der Arbeit sollen daher zunächst unterschiedliche Positionen im Feld der ISS vorgestellt und Konzepte erörtert werden, die für den empirischen Teil der Arbeit relevant sind und als Grundlage für die Diskursanalyse dienen (Kapitel 2). In einem Methoden-Kapitel werden danach knapp die methodischen Werkzeuge präsentiert und reflektiert, mithilfe derer die Dokumente analysiert wurden (Kapitel 4).

Der empirische Teil der Arbeit gliedert sich in sechs Kategorien, die sich sowohl im Zuge der Analyse am Text als auch im Hintergrund der angewandten Theorien als für die Beantwortung der Forschungsfrage relevant erwiesen haben. In einem Schlusskapitel werden die wichtigsten Erkenntnisse zusammengeführt und mit dem theoretischen Hintergrund sowie dem Stand der Forschung in Beziehung gesetzt (Kapitel 5). Bevor es zu den analytischen Teilen der Arbeit geht, werden hier die wichtigsten Daten und Fakten der drei ausgewählten Programme kurz zusammengefasst:

***Secure Societies – Protecting freedom and security of Europe and its citizens:***

Secure Societies ist ein Teilprogramm von Horizon 2020 (deutsch: *Horizont 2020*), dem 8. Forschungsrahmenprogramm der Europäischen Union, das von der Europäischen Kommission ausgeschrieben wird. Horizon 2020 folgt mit einer geplanten Laufzeit von 2014 bis 2020 dem 7. Forschungsrahmenprogramm der EU nach mit der strukturellen Neuerung, dass die zuvor getrennten Bereiche Forschung und Innovation erstmals gebündelt wurden (BMBF 2016f). Diese Zusammenlegung erfolgte im Zuge der Umsetzung der *Innovationsunion*, einer von sieben Teilinitiativen der Europa-2020-Strategie. Ziel der Europa-2020-Strategie ist die Förderung des wirtschaftlichen Wachstums und der Beschäftigung im Laufe des Jahrzehnts (Europäische Kommission 2016).

Durch die Innovationsunion sollen auf lange Sicht „alle politischen Instrumente, Maßnahmen und die Finanzmittel von vornherein auf ihren Beitrag zur Innovation ausgelegt“ und damit die globale Wettbewerbsfähigkeit des Wirtschaftsstandorts Europa gesteigert werden (BMBF 2017c). Dazu soll mit dem Forschungs- und Innovationsprogramm Horizon 2020 ein Beitrag geleistet werden „as means to drive economic growth and create jobs“ (Europäische Kommission 2018b). Eine der Zielvorgaben der Europa 2020-Strategie ist es, 3% des EU-BIPs in Forschung und Entwicklung zu investieren (Europäische Kommission 2016). Diese Vorgabe wurde

bei der Aushandlung des Budgets für Horizon 2020 nicht erreicht, es beläuft sich bei einer jährlichen Inflationsanpassung von 2% auf etwa 75 Milliarden Euro pro Jahr (Europäische Kommission 2013). Davon entfallen etwa 29,7 Milliarden Euro auf den Themenbereich *Societal Challenges*, wo das Sicherheitsforschungsprogramm *Secure Societies* als einer von sieben Forschungsschwerpunkten angesiedelt ist. Vom Gesamtbudget entfallen 2,2% (hochgerechnet etwa 1,7 Milliarden Euro auf die Forschung für die zivile Sicherheit (ebda.). Zivile Sicherheit ist auf europäischer Ebene zum zweiten Mal nach dem „Security Theme“ des 7. Forschungsrahmenprogramms (2007-2013) als eigene Themenkategorie vertreten (Europäische Kommission 2015a).

*Secure Societies* orientiert sich neben der Europa-2020-Strategie inhaltlich an der Umsetzung des *Aktionsplans für eine innovative und wettbewerbsfähige Sicherheitsindustrie*, der *Strategie für die Sicherheit der Europäischen Union* sowie der *Cybersicherheitsstrategie der Europäischen Union* (Europäische Kommission 2018b). Als Expert\*innengruppe in beratender Funktion fungiert die *Protection And Security Advisory Group* (PASAG)<sup>1</sup>, die sich aus nationalen Expert\*innen aus unterschiedlichen Stakeholder-Bereichen zusammensetzt und bei der Erarbeitung der alle zwei Jahre beschlossenen „Work Programmes“ assistiert, die anschließend im Komitologie-Verfahren beschlossen werden (Europäische Kommission 2018a). Als primäre Ziele des Programms werden (1) die gesellschaftliche Resilienz gegenüber Natur- und vom Menschen verursachten Katastrophen, (2) der Kampf gegen Kriminalität und Terrorismus, (3) die Verbesserung der Grenzsicherheit an den europäischen Außengrenzen und (4) die Verbesserung der Cybersicherheit angeführt genannt (Europäische Kommission 2018b).

---

<sup>1</sup> Die Kommission gründete im Jahr 2005 den Europäischen Beirat für Sicherheitsforschung (engl.: *European Security Research Advisory Board — ESRAB*), der die Erarbeitung eines Europäischen Sicherheitsforschungsprogramm hätte vorbereiten sollen (vgl. Europäische Kommission 2005: 1). Ein solches Programm kam in eigenständiger Form nicht zustande, der ESRAB Report diente jedoch als inhaltliche Leitlinie für das „Security Theme“ des 7. Forschungsrahmenprogramms (vgl. Europäische Kommission 2012: 7). ESRAB wurde 2006 aufgelöst.

**Forschung für die zivile Sicherheit 2012-2017:** nennt sich das zweite nationale Sicherheitsforschungsprogramm der deutschen Bundesregierung. Es ist die Fortsetzung von *Forschung für die zivile Sicherheit*, das 2007 vom Bundesministerium für Bildung und Forschung lanciert wurde. 2014 wurde das Programm in die ressortübergreifende „Hightech-Strategie – Innovationen für Deutschland“ integriert, wo unter dem Motto „Wohlstand, Wachstum, Lebensqualität“ die zivile Sicherheit einen von sechs Forschungsschwerpunkten darstellt (BMBF 2016e). Das erklärte Ziel des Programms ist es, „durch die Entwicklung innovativer Lösungen die zivile Sicherheit der Bevölkerung zu erhöhen und dabei die Balance zwischen Sicherheit und Freiheit zu wahren“ (BMBF 2018). Für den Bereich zivile Sicherheit wurden seit dem Jahr 2007 rund 540 Millionen Euro an Fördermitteln vom Bundesministerium für Bildung und Forschung im Rahmen der Projektausschreibungen zur Verfügung gestellt (Stand: Juli 2017).

**KIRAS (Ausschreibungszeitraum 2014-2020):** KIRAS ist das österreichische Programm zur Förderung der nationalen Sicherheitsforschung des Bundesministeriums für Verkehr, Innovation und Technologie (bmvit). Es wurde im Jahr 2005 als europaweit erstes nationales Forschungsprogramm im Bereich Sicherheit gegründet, das Programm-Management obliegt der Österreichischen Forschungsgesellschaft (FFG). Nach der ersten Programmphase 2005-2013 startete 2014 die zweite Programmphase, deren Laufzeit aktuell bis 2020 angesetzt ist (vgl. bmvit 2015a, 2017b). Schwerpunkt von KIRAS (von griechisch „kirkos“ [Ring] und „asphaleia“ [Sicherheit], siehe bmvit 2018) ist der Schutz kritischer Infrastrukturen, übergeordnete Ziele des Programms sind (1) „die Erhöhung der Sicherheit und des Sicherheitsbewusstseins der Bürgerinnen und Bürger“, (2) „Generierung sicherheitspolitisch erforderlichen Wissens“, (3) die „Erzielung von Wissens-, Verfahrens- und Technologiesprüngen“, (4) das „Wachstum der heimischen Sicherheitswirtschaft“ und (5) der „Auf- und Ausbau von Exzellenz im Bereich der Sicherheitsforschung“ (bmvit 2015: 8). Laut Bundesministerium für Verkehr, Innovation und Technologie sind seit 2006 insgesamt 71 Millionen Euro an Förderungen im Rahmen von KIRAS bewilligten worden (Stand 2017; vgl. bmvit 2017b).

## 2 Theoretische Grundlagen

### 2.1 Ein erweitertes Verständnis von Sicherheit

In diesem Kapitel soll in drei Abschnitten das theoretische Fundament skizziert werden, auf das sich das Forschungsdesign stützt. Konkret geht es um eine theoretische Perspektive auf das Thema Sicherheit, die die Frage, wie Sicherheit und Unsicherheit(en) diskursiv hergestellt werden, erlaubt. Einer Perspektive, die geprägt von Vertreter\*innen sozialkonstruktivistischer bis poststrukturalistischer Strömungen, eng mit der europäischen Etablierung der ISS als eigenständige Subdisziplin der Internationalen Beziehungen (IB) verbunden ist (vgl. Buzan und Hansen 2009: 37, 42). Dahin soll in diesem Unterkapitel in groben Zügen geführt werden, ohne die Genese der ISS im Detail rekapitulieren zu können.

Der Begriff „Sicherheit“ war im US-amerikanisch geprägten Mainstream der Internationalen Beziehungen über Jahrzehnte hinweg eng mit den Begriffen „Staat“ und „Militär“ verbunden. Während der Jahrzehnte des Kalten Kriegs überwog ein durch Realismus und später Neorealismus geprägtes Weltbild, in dessen Zentrum Staaten samt ihrer militärischen Kapazitäten als Hauptakteure in einem vernommenen Zustand internationaler Anarchie im Vordergrund standen (vgl. Daase 2010, Filzmaier et al. 2006: 54). Von den 1940er-Jahren bis in die späten 1980er-Jahren kreiste das Interesse der sicherheitspolitischen Analysen daher auch maßgeblich um militärische/kriegerische Angelegenheiten (auch bekannt als *Strategic Studies*, vgl. Wæver 2015: 76).

Bereits in den Jahren, die zum Zerfall der bipolaren Weltordnung führten, aber insbesondere nach ihrem Ende wurde diese zuvor dominante Wahrnehmung des globalen Systems und damit einhergehend auch jene von Sicherheit und Bedrohung herausgefordert (vgl. Höll 2007: 413f.). Aus unterschiedlichen institutionellen, ideologischen und/oder akademischen Anreizen entwickelte sich ein „widening and deepening“ des Verständnisses von Sicherheit (Buzan und Hansen 2009: 187). „Widening“ bezieht sich dabei darauf, dass nicht nur der militärische Sektor, sondern – je nach Auffassung beliebig oder begrenzt viele – weitere politische Bereiche als

für die nationale (und ja nach Problemlage internationale) Sicherheit relevant analysiert werden können: „[T]hus bringing in a wider agenda around economic, environmental, societal and regional security“ (ebda.:189). „Deepening“ bezieht sich indes auf das in seiner Sicherheit bedrohte Referenzobjekt: Je nach Forschungsinteresse sollten nicht nur der Staat, sondern andere Entitäten wie die „Gesellschaft“, die „Gemeinschaft“, das „Individuum“ als Referenzobjekte erkennbar gemacht und zum Gegenstand der Analyse gemacht werden können (vgl. ebda.: 189).

Auf diese Weise wurde es unter anderem möglich, den Staat analytisch von dessen Bürger\*innen zu trennen. Und internationale Konflikte zu analysieren, in denen der Staat selbst eine Bedrohung für Menschen innerhalb seines geographischen Territoriums darstellt, wie dies beispielsweise in den bewaffneten Konflikten am Balkan der Fall war (vg. ebda.: 213). Auch auf politisch-institutioneller Seite wurde der Versuch eines „widening“ unternommen, jedoch ohne den Staat als Souverän in der Internationalen Staatengemeinschaft gleichsam in Frage zu stellen. Ein Beispiel ist das im Rahmen der Palme-Kommission erstmals präsentierte Konzept der *Gemeinsamen Sicherheit* (engl.: *Common Security*). Es ist in diesem Zusammenhang insofern von Bedeutung, als es die internationale Sicherheit nicht vornehmlich durch verfeindete Staaten bedroht sieht, sondern soziale Ungleichheit, Umweltverschmutzung, atomarer Krieg und hohe militärische Ausgaben als globale Probleme in den Blick genommen werden, die alle Staaten betreffen und an deren Lösung dementsprechend alle interessiert sein sollten (vgl. ebda.: 137, 205). Laut Höll (2007) habe das Ende des Kalten Kriegs zu einem wachsenden Bewusstsein für die weltweite Interdependenz im Falle lokaler Krisenherde und Konfliktsituationen geführt (vgl. 414). Diese gegenseitige Abhängigkeit komme besonders im ökonomischen Sektor zum Tragen: „[A]lmost all countries and all their sub-systems are torn together, interfere and relate to one another, at a certain level, being even more dependent on one another than before, especially, but not exclusively, on the economic level“ (ebda.: 415). Die erhöhte Interdependenz in dieser „new, comprehensive global [...] socio-political entity“ (ebda.: 414) habe eine neue, verstärkte Verwundbarkeit zur Folge, die sich vor allem auf die Handlungsmacht von Nationalstaaten auswirke: „[I]nterdependence means also: more vulnerability, for rich and poor, small and big states, also for societies, even for the individuals at

economic, societal and political levels“ (ebda.). Dadurch hätten sich konkrete Probleme (Höll nennt sie „interdependence-problems“) entwickelt...

„...that cannot be solved by single states alone like that of ecological pollution, migration, terrorism, proliferation of weapons of mass destruction, trafficking people and other forms of trans-national organized crime and – last but not least – epidemics, diseases, and natural catastrophes“ (Höll 2007: 418)

Laut Buzan/Hansen sei es die Palme-Kommission gewesen, die die Samen für ein Verständnis individueller Sicherheit gesät hat, das etwa zehn Jahre später durch UNDP's Agenda der *menschlichen Sicherheit* (engl.: *human security*) international bekannt wurde, da es dem Individuum zumindest theoretisch als zu schützendem Referenzobjekt Priorität gegenüber dem Staat verschaffte:

„This implied a radical widening of the types of threats to and sectors to which security was applicable to food, health, the environment, population growth, disparities in economic opportunities, migration, drug trafficking and terrorism.“ (Buzan/Hansen 2009: 203)

Auf akademischer Seite gewannen Autor\*innen an Einfluss, die sich dem diskursiven Element von Sicherheit widmeten. Die Sicherheit nicht als objektiv zu erreichenden Zustand verstanden, sondern als diskursive Praxis und Performativität mit entsprechenden Konsequenzen. Die bekannteste dieser diskursive (Filzmaier et al. 2006)n Schulen ist die *Kopenhagener Schule* mit der Theorie der *Versicherheitlichung*. Unter *Versicherheitlichung* wird der Prozess verstanden, indem zunächst ein zuvor beliebiges politisches Problem durch einen strategischen Akteur zu einer existenziellen Bedrohung stilisiert wird. Durch diese Inszenierung kann der Akteur zu Maßnahmen greifen, für die die verfassungsrechtlich festgelegten „normalen“ Verfahren politischer Legitimierung ausgesetzt sind (Buzan et al. 1998).

Durch diese Spezifikation grenzen die Autoren den Prozess der *Versicherheitlichung* von jenem der Politisierung ab, bei dem eine Thematik lediglich zu einem Thema öffentlicher, politischer Debatte erhoben wird. „In this context, security is about survival“ (ebda.: 21), schreiben Buzan et al., stellen jedoch klar, dass es sich dabei nicht um menschliches, physisches Überleben handeln muss. Ausschlaggebend ist die Artikulation einer existenziellen Bedrohung in Bezug auf ein Referenzobjekt (vgl. ebda.: 24). So könne beispielsweise die „Identität“ einer Nation oder einer substaatlichen Kollektivität als existenziell bedrohtes Referenzobjekt konstruiert werden – oder nicht – mit unterschiedlichen Konsequenzen: „Thus, whether migrants

or rival identities are securitized depends upon whether the holders of the collective identity take a relatively closed-minded view of their identity or a relatively open-minded view of how their identity is constituted“ (ebda.: 23). Der Prozess der Versicherheitlichung sei jedoch nur dann erfolgreich und abgeschlossen, wenn der *securitization move* eines Akteurs, also der Sprechakt der Versicherheitlichung, von einem nicht näher definierten öffentlichen Publikum („audience“) akzeptiert wird:

„In security discourse, an issue is dramatized and presented as an issue of supreme priority; thus, by labeling it as security, an agent claims a need for a right to treat it by extraordinary means. For the analyst to grasp this act, the task is not to assess some objective threats that “really” endanger some object to be defended or secured; rather, it is to understand the *processes of constructing a shared understanding of what is to be considered and collectively responded to as a threat.*“ (Buzan et al. 1998)

Die Autoren fügen erklärend hinzu, dass es zwischen dem Akteur und der Legitimation verschaffenden „audience“ um eine „civilized, dominance-free discussion“ handeln muss (ebda.: 25): „[I]t only means that an order always rests on coercion as well as consent.“ (ebda.: 25). Theoretisch könnte jeder und jede ein Thema versicherheitlichen. In der Praxis sei es jedoch so, dass die Kräfte ungleich verteilt seien, dass es Akteure gibt, denen mehr Vertrauen geschenkt wird, wenn sie über Sicherheit sprechen als anderen (ebda.: 31). Diese asymmetrische Verteilung an sozialem und oft auch finanziellem Kapital in einem Tätigkeitsfeld werden von den Autoren als *facilitating conditions* bezeichnet. Die (Definitions)macht über Sicherheit und Unsicherheit sei aber niemals absolut zu fassen, sondern müsse immer relational zu den anderen Akteuren im Feld gesehen werden: „The field ist structured or biased, but no one exclusively „holds“ the power of securitization. (ebda.: 31).

2009 erweiterten Buzan/Waever die Theorie der Versicherheitlichung um das Konzept der *macrosecuritisation*. Damit versuchten die Autoren den Prozess konzeptionell zu erfassen, in dem es einem strategischen Akteur gelingt, eine „security constellation“ zu schaffen, durch die regionale und nationale *securitisations* durch eine globale *macrosecuritisation* kanalisiert und aneinandergeschaltet werden (Buzan und Wæver 2009). Ein Beispiel in einer zeitweise gelungenen Makro-Versicherheitlichung nennen die Autoren den „Global War on Terror“ (GWOt) der Bush- und Blair-Regierungen (ebda.: 254). Anders als Versicherheitlichungen auf der Ebene von Staaten und Kollektivitäten vergleichbarer Größe, seien *macrosecuritisations* aufgrund der globalen Reichweite und der Subsumierung

zahlreicher „middle-level securitisations“ immer umkämpft und fragiler (ebda.: 257). Ihr Gelingen hänge von der erfolgreichen Etablierung eines Diskurses ab, der sich auf „Universalismen“ stützt, die mit nationalen Interessen Beteiligter einerseits nicht im Widerspruch stehen und andererseits Anknüpfungspunkte an nationale Interessen ermöglichen: „The ability to generate a successful macrosecuritisation depends not just on power, but on the construction of higher level referent objects capable of appealing the identity politics of a range of actors within the system“ (ebda.: 268).

Terrorismus sei im Zuge dieser Makro-Versicherheitlichung zu einem „watch word“ geworden, das Buzan/Waever mit einer institutionalisierten Versicherunglichung, wie sie zuvor skizziert wurde, gleichsetzen. Versicherunglichungen müssten nämlich nicht immer „ad-hoc“ geschehen, sondern könnten sich auch über einen längeren Zeitraum „normalisieren“: „If a given type of threat is persistent and recurrent, it is no surprise to find that the response and sense of urgency become institutionalized“ (Buzan et al. 1998). Die Strahlkraft einer definierten Bedrohung geht dann über sich hinaus und hat das Potenzial, zuvor unverwandte Themen durch bestimmte Artikulationen diskursiv an sich zu binden: „[S]o by linking any specific issue (uncontrolled financial flows, religious radicalisation) to terrorism, they become immediately security issues“ (Buzan und Wæver 2009).

Ungeachtet ihrer eigentlichen Interessen sei es den USA gelungen, durch das universalistische Framing der „westlichen Zivilisation“ Demokratie, Menschenrechte und den freien Markt als globale Referenzobjekte zu etablieren, die es vor der Bedrohung des islamistischen Terrors zu schützen gelte. Umgekehrt sei der durch den Westen bedrohte Islam das universelle Referenzobjekt von Al-Qaeda, mithilfe dessen sie als transnationaler Akteur auf „lower level securitisations“ Einfluss nehmen können (ebda.: 268f). Laut Buzan/Waever sei es unerheblich, ob beteiligte Akteure sich der Tatsache bewusst seien, dass sie Teil der größeren Struktur einer Makrosecuritisation sind, wichtig sei lediglich der Zusammenhalt dieser interdependenten Versicherunglichungen in einer globalen Sicherheitskonstellation (vg. ebda.: 268). An dem Erfolg der von der Bush-Regierung inszenierten Macrosecuritisation zweifeln die Autoren 2009 bereits: Einerseits würde der Terrorismus als Bedrohung in den USA an Legitimität einbüßen (vgl. ebda.: 274), andererseits seien die dahinterliegenden Interessen der USA auf längere Sicht zu durchschaubar (vgl. ebda.: 274).

Die Theorie der *Versicherheitlichung* wurde ganz besonders von poststrukturalistisch-inspirierten Denker\*innen kritisiert und weiterentwickelt, denen Buzan et al.s Theorie zu rationalistisch geprägt erschien. Während die Gründer der Kopenhagener Schule in ihrer Konzeption von Sicherheit daran interessiert sind, den Prozess freizulegen und nachzuzeichnen, in denen sich eine Thematik in ein Problem der öffentlichen Sicherheit verwandelt, so geht es bei den Poststrukturalist\*innen stärker darum, dahinterliegenden Macht-Wissen-Komplexe von Versicherheitlichungen auf den Grund zu gehen. Im Zentrum poststrukturalistischer Analysen steht die Versicherheitlichung als gouvernementale Technik der Subjektivierung: „Security politics, argued Poststructuralism, was fundamentally about the construction of a radically different, inferior and threatening Other, but also, since identity is always relational, about the Self“ (Buzan/Hansen: 143).

## **2.2 Die Pariser Schule der Securitisation Theory**

Die sogenannte „Pariser Schule“ oder in der Selbstbezeichnung „PARIS School of Liberty and Security“ verbindet die Perspektive der im vorangegangenen Kapitel skizzierten Kopenhagener Schule mit Theorien und Forschungsmethoden aus der (politischen) Soziologie und der Kriminologie (vgl. Bigo 2016). Innere und äußere Sicherheit sind in der Vorstellung der Vertreter\*innen der Pariser Schule keine Sphären, die sich separat zu analysieren sind, sondern transnationale Felder politischer, bürokratischer und technologischer Praxis, die wie ein Möbiusband miteinander verbunden sind (vgl. Bigo und Tsoukala 2008: 5, Bigo 2016: 1083).

Begründer und gleichzeitig der bekanntester Vertreter der Pariser Schule ist Didier Bigo, dessen Forschung sich auf die Praktiken und Beziehungen von transnationalen Sicherheitsakteuren innerhalb Europas konzentriert. Bigo entgegnet der Vorstellung eines strategischen Akteurs, der sich für das Gelingen des Sprechakts der Versicherheitlichung verantwortlich zeichnet, die alltäglichen bürokratischen Routinen der „professionals of (in)security“ (Bigo und Tsoukala 2008). Bigos theoretisches Fundament hierfür ist die Feldtheorie Bourdieus, mithilfe derer er darzulegen versucht, wie alltägliche Macht- und Deutungskämpfe um das zu verteilende Kapital innerhalb eines sozialen Raums Diskurs und Praxis zu einem gegebenen Zeitpunkt prägen und strukturieren können (vgl. Bigo et al. 2007: 9). Praktiken, die sich fernab

einer politischen Bühne abspielen, weshalb Bigo/Tsoukala den Sprechakt gegenüber einer öffentlichen „audience“ für den Prozess der Versicherheitlichung nicht als ausschlaggebend erachten: „The (in)securitization process is then a social and political construction related to speech acts, but these speech acts are not decisive“ (Bigo/Tsoukala 2008: 4).

Die Vertreter\*innen der Pariser Schule teilen die Auffassung zahlreicher anderer Autor\*innen, wonach die politischen Nachwehen von 9/11 auch in Europa zu einem Ungleichgewicht zwischen „Freiheit und Sicherheit“ zugunsten von Überwachungs- und Profilingmethoden und zulasten der Bürger\*innenrechte geführt haben (Bigo et al. 2007).

Ein „Feld“ konstituiert sich nach der Theorie Bourdieus aus den Kämpfen der in formell teils unterschiedlichen Sektoren und Ebenen angesiedelten Akteuren: „The notion of field can [...] be said to refer to a social space structured by struggles over a specific capital determining part of what is at stake in these struggles“ (ebda.: 9). Gekämpft wird um „Kapital“, soziale, kulturelle, wissenschaftliche, materielle Ressourcen, die die Machtverhältnisse innerhalb des Felds verschieben. Einfluss und Macht muss nach der „Logik des Felds“ immer relational und relativ gesehen werden – des einen (Zu)Gewinn ist des anderen Verlust. Die „stakes“ im Falle des „field of the professionals of security“ seien die „struggles over material or human resources“ sowie „rivalries over the legitimate systems of classification of threats“ (ebda.: 37).

Im Zuge der Feld-immanenten Auseinandersetzungen innerhalb der europäischen Sicherheits- und Justizagenturen – in der Studie werden EUROPOL, EUROJUST, FRONTEX, OLAF und INTCEN (damals SITCEN) beleuchtet – hätten sich mehrere Pole herausgebildet, an deren Enden einander entgegengesetzte Auffassungen stehen:

1. *Modernisierer\*innen/Traditionalist\*innen*: Die erste Konfrontationslinie verlaufe zwischen „Modernisierer\*innen“ und „Traditionalist\*innen“ (ebda.: 31). Während erstere eine für stärkere Harmonisierung innerhalb der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) und für eine Aufweichung der „internal/external distinction“ stünden, wären zweitere stärker national

orientiert und hätten größere Vorbehalte gegenüber einer zunehmend entgrenzten Sicherheitslogik (vgl. ebda.).

2. *Individuelle/Kollektive Sicherheit*: Eine weitere Demarkationslinie im Feld der europäischen Sicherheitsexpert\*innen sei eine personalisierte, auf einzelne Individuen oder eine depersonalisierte, auf Gruppen/Kollektive, abzielende Exekutivarbeit (ebda.: 31).
3. *Proaktive Sicherheit/Strafverfolgung*: Als dritte Konfliktlinie nennen Bigo et al. die Priorisierung des präventiven/proaktiven „monitoring of the future“ gegenüber einer traditionellen Logik der Strafverfolgung samt Unschuldsvermutung nach einer begangenen Tat (ebda.: 31f.)

Die Vertiefung transatlantischer Beziehungen nach 9/11 habe dazu geführt, dass sich eine von den Autoren als „intelligence rationale“ bezeichnete Sicherheitslogik gegenüber anderen, traditionellen Sicherheitskonzepten durchzusetzen begonnen habe (ebda.: 25). Dahingehende Tendenzen seien insbesondere bei FRONTEX, EUROPOL sowie INTCEN zu vernehmen, während in den verbleibenden Agenturen (EUROJUST, OLAF) die Widerstände größer seien bzw. ein dahingehendes Interesse nicht so stark vorhanden sei (vgl. ebda: 46).

Diese „Geheimdienst-Rationalität“ kennzeichnet laut den Autoren eine aus den USA bekannte antizipativen/proaktiven Form der Exekutivarbeit, die auf großangelegten Profiling aufgebaut ist (ebda.: 37). Mit ihr halte ein „technologischer Imperativ“ in das Feld der europäischen Sicherheitsakteure ein, dessen oberste Maxime die Akkumulation, Abrufbarkeit und Vernetzung möglichst großer Datenmengen von Seiten europäischer Institutionen sei (vgl. ebda.: 44). Hinzukommt die in den Vereinigten Staaten praktizierte „Automatisierung“ des Screenings dieser Daten mit entsprechender Software, gegen die es jedoch zum Teil aus Gründen der Existenzsicherung auch innerhalb der Behörden, die mit dem „intelligence rationale“ sympathisieren, noch Vorbehalte gebe (als Beispiel wird EUROPOL genannt, vgl. ebda.: 46).

In *Terror, Insecurity and Liberty – Illiberal practices of liberal regimes after 9/11* kombinieren Anastasia Tsoukalla und Didier Bigo (2008) die Analyse des Felds der Sicherheitsakteure mit Foucaults Theorien zur Gouvernementalität. Auf diese Weise

erfolgt eine noch stärkere Zuspitzung in Richtung Überwachung, Migration und einer Logik des Marktes (Bigo und Tsoukala 2008: 3). 9/11 und die politischen Entwicklungen im Anschluss habe einer Gruppe von Akteuren zu einem Machtzuwachs verholfen, deren Zuständigkeiten zuvor eher in der Peripherie der europäischen Sicherheitsarchitektur angesiedelt gewesen seien (Bigo 2008: 16). Am Wirken sei ein neues „transnational regime of truth“ (ebda.: 13), einer bewusst transnationalisierten Sicht auf Sicherheit und Bedrohung als Folge eines neuen Macht-Wissen-Komplexes sogenannter “transnational guilds“ (ebda.: 15). Die Folge sei eine

„[...] practical redefinition of systems of knowledge and know-how that connect the public and private security agencies who claim to possess a ‘truth’ founded on numerical data and statistics, technologies of biometrics and sociological profiles of potential dangerous behaviour, applied to the cases of persons who themselves feel the effects of the (in)securitization, living in a state of unease. Such professional managers of unease then claim, through the ‘authority of the statistics’, that they have the capacity to class and prioritize the threats, to determine what exactly constitutes security.“ (ebda.: 12)

Auf nationaler Ebene würden sich diese privaten und öffentlichen “professional managers of unease” (ebda.: 46) durch strategische Allianzen in internen Deutungskämpfen angesichts des neu erworbenen symbolischen Kapitals durch die Bedrohung des Terrorismus durchsetzen:

Within the production of this regime of truth and the battle to establish the ‘legitimate’ causes of fear, of unease, of doubt and uncertainty, the (in)security professionals have the strategy to overstep national boundaries and form corporatist professional alliances to reinforce the credibility of their assertions and to win the internal struggles in their respective national fields (Bigo 2008: 12-13)

Der Schutz des individuellen Lebens verliere in dieser soziotechnologischen Neukonfiguration an Bedeutung:

“Security is then, conceptually, reduced to technologies of surveillance, extraction of information, coercion acting against societal and state vulnerabilities, in brief to a kind of generalized ‘survival’ against threats coming from different sectors, but security is disconnected from human, legal and social guarantees and protection of individuals.“ (ebda.: 13)

Auch die spezialisierte Betrachtung unterschiedlicher Formen des Verbrechens ist nicht mehr von Belang. An ihre Stelle tritt das von Bigo mehrfach thematisierte “semantische Kontinuum“ (siehe dazu auch Bigo 2013) einer Vielzahl heterogener

Delikte unterschiedlicher Schwere (von Terrorismus, Drogenschmuggel über Migration), die Exekutivbeamt\*innen mit unterschiedlichen Zuständigkeiten einen Nutzen verschaffen.

“We can thus take account of all the intermediary agencies such as police with military status, border guards, customs agents, or immigration agents, to better understand the links these agents establish among themselves and how the effects of their positions have implications on their respective narratives. Furthermore, breaking down this dichotomy allows us to understand how a semantic continuum is constructed, with the struggle against terrorism at one end and the reception of refugees at the other.” (Bigo 2008: 16)

Das relationale Zusammenspiel zwischen den institutionalisierten „bureaucratic decisions of everyday politics, with Weberian routines of rationalization“ (Bigo und Tsoukalla 2008: 5) und den Entscheidungen politischer Entscheidungsträger nach 9/11 bezeichnen Bigo und Tsoukalla in Anlehnung an Foucaults Dispositiv-Theorie als „ban-opticon dispositif“:

„This ban-opticon is deployed at a level that supersedes the nation-state and forces governments to strengthen their collaboration in more or less globalized spaces, both physical and virtual, sometimes global or Westernized, and still more frequently Europeanized. The effects of power and resistance are thus no longer contained by the political matrix of the relation between state and society.” (Bigo 2008: 32)

Jef Huysmans greift in *The Politics of Insecurity. Fear, Migration and Asylum* Bigos Analysen des semantischen Kontinuums auf, um sich explizit dem Thema Migration und Asyl im Kontext des prozessualen „framings of insecurity“ (Huysmans 2006: 15f.), wie Huysmans es bezeichnet, zu widmen. Huysmans vertritt die Ansicht, dass die zunehmende Technologisierung des europäischen Grenzschutzes dazu beigetragen habe, dass Migrant\*innen und Asylsuchende als „Unsicherheit“ (=Bedrohung) neben traditionelleren Delikten wie Terrorismus, Schmuggel und organisierter Kriminalität im Allgemeinen konstruiert wurden (Huysmans 2006: 4).

Im empirischen Teil wird zu untersuchen sein, ob und inwieweit die von Bigo, Tsoukala et al. beobachteten Tendenzen des *intelligence-led policing* (Überwachungstechnologien, Data-Mining, Profiling, Prävention) in den Forschungsvorhaben priorisiert werden oder ob andere Framings ziviler Sicherheit den Diskurs stärker prägen. Ein zweiter relevanter Aspekt bei der Analyse zweier nationaler und eines supranationalen Programms ist die Frage, inwieweit dort eine „transnationalisierte“ Logik von Sicherheit mit ihren entsprechenden Attributen Raum

gegeben wird oder gegenteilige Auffassungen vorherrschen. Bigo macht in seinen Analysen darauf aufmerksam, wie das komplexe Zusammenspiel unterschiedlicher Kapitalformen zu „Machteffekten“ führen können, die nicht zwingend von der Politik ausgehen müssen. Im Folgekapitel soll daher in einem weiteren Unterkapitel etwas konkreter auf das Verhältnis zwischen Sicherheitspolitik, Expertise, Forschung und Wissenschaft eingegangen werden.

### **2.3 Das Verhältnis von Sicherheitspolitik und Forschung**

Die Produktion von Wissen im Kontext von Sicherheit bzw. für die Umsetzung konkreter sicherheitspolitischer Maßnahmen ist ein Gebiet, mit dem sich in den letzten Jahren immer mehr Autor\*innen aus den Bereichen Internationale Beziehungen, der Science & Technology Studies (STS), der Wissenschaftssoziologie oder der Politischen Soziologie auseinandergesetzt haben. Gleichzeitig erschienen auf dem Gebiet der Wissenschaftstheorie in vergangenen zwei Jahrzehnten zahlreiche Arbeiten, in denen über paradigmatische Veränderungen in der Praxis der wissenschaftlichen Produktion von Wissen und neuen Formen der Expertise reflektiert wurde (*siehe dazu* u.a.: (Gibbons 1995; Collins und Evans 2002).

Trine Villumsen Berling und Christian Bueger (2015) haben sich in *Security Expertise. Practice, Power, Responsibility* gezielt mit der Frage auseinandergesetzt, in welchen Settings Wissensproduktion und Sicherheitspolitik einander wechselseitig konstituieren (vgl. Villumsen Berling und Bueger 2015: 4). Im Fokus steht dabei die unter anderem die legitimierende Funktion von Expert\*innen, die in der „modernen“, problem- und anwendungsorientierten Forschung eine heterogene Gruppe mit unterschiedlichen Qualifikationen und/oder Erfahrungswerten darstellen: „[T]he study of expertise promises to bring to the fore issues of the authority of expert voices in making security and the general trust in knowledge which underpins the authority of expertise in modern society“ (ebda.: 5).

Eine der wichtigsten Erkenntnisse aus den STS für die Policy-Analyse ist laut Robert Evans die Enthüllung von Praktiken, in denen vorgeblich neutraler, objektiver Expert\*innenrat von Wertvorstellungen und Vorannahmen geleitet ist, die eigentlich der Gegenstand öffentlicher Debatte sein sollten (vgl. Evans 2015: 23). Mit der depolitisierenden Funktion und anderen möglichen Machteffekten wissenschaftlicher

Settings hat sich Villumsen Berling (2011) in *Science and securitization: Objectivation, the authority of the speaker and mobilization of scientific facts* auseinandergesetzt und zwar im Kontext der Securitisation Theory. Dabei begreift sie Wissenschaft als einen Mechanismus, der sowohl in die innere Dimension der Versicherheitlichung (der Sprechakt) als auch in deren äußere Dimension (der Kontext der Versicherheitlichung) eingreift (vgl. (vgl. Villumsen Berling 2011: 387). Wie auch Bigo nimmt Berling die Bourdieusche Feldtheorie als theoretische Grundlage (vgl. ebda.: 386).

In ihrer theoretischen Analyse zeigt Berling anhand von Beispielen vier Arten auf, in denen die Wissenschaft als „strategische“ Waffen im Prozess der Versicherheitlichung eingesetzt werden können:

*Mobilisierung wissenschaftlicher Erzeugnisse:* Wissenschaftliche Fakten (Modelle, quantitative Analysen, seltener: Theorien) sind „Asse“, die in einer politischen Kontroverse die Legitimität eines Vorhabens zumindest temporär untermauern können. Sie schaffen eine Aura komplexer wissenschaftlicher Zusammenhänge, die nicht von Interessen geleitet sind und nur durch ein „Kontern“ mit wissenschaftlicher Gegen-Evidenz wirksam dekonstruiert werden können (vgl. ebda.: 386, 393).

*Objektivierung/„Non-Politisierung“:* Wissenschaft könne als eine Methode des „Silencing“ dienen, indem ein politisches Thema mit dem Schleier der Wissenschaft umhüllt wird, „normalisiert“ wird und auf diese Weise aus der Sphäre der politischen Auseinandersetzung entfernt wird: „The non-politicized has no language; it is ‚what we know without knowing that we know it‘ – what Bourdieu referred to as *doxic practice*.“ (ebda.: 391).

*Die Autorität des Sprechers:* Die Zirkulation von Wissen zwischen Politik und dem „Laboratorium“ könne auch Wissenschaftler\*innen und Forscher\*innen innerhalb ihres „Settings“ zu einem Zuwachs an Autorität verhelfen. Als Beispiel nennt Berling Clintons Propagierung der „democratic peace theory“ im Präsidentschaftswahlkampf 1992, in Folge dessen Anhänger\*innen dieser Theorie sowohl auf akademischer als auch in der Grauzone zwischen Wissenschaft und politischer Praxis deutlich an Einfluss gewinnen konnten (vgl. ebda.: 292).

Das grundlegende Erkenntnisinteresse in den sozialkonstruktivistisch orientierten STS ist die Frage nach dem (sozialen, historischen, kulturellen, politischen, ökonomischen) Kontext, in dem Wissensproduktion stattfindet (vgl. Evans 2015: 2, 5, 20). Robert Evans betrachtet Expertise in diesem Kontext als eine relationale Praxis, in der der Experte oder die Expertin die Rolle eines „quasi-political actor“ (ebda.: 22) innehat. In dieser Funktion liege es im eigenen Interesse des Experten oder der Expertin, ein soziales Netzwerk zu schaffen und zu erhalten, in dem das eigene Fachwissen von Relevanz ist (vgl. ebda.). Dazu gehöre unter anderem auch die „entrepreneurial practice of aligning technical possibilities with social needs in order to create a new socio-technical network in which both artefacts and humans play their part (ebda.: 23).

## **2.4 Erörterung zentraler Begriffe**

### **2.4.1 Risiko**

Die Begriffe „Risiko“ und „Sicherheit“ werden oft zusammen oder als zusammengesetzter Begriff („Sicherheitsrisiko“) erwähnt. Der Duden definiert „Risiko“ *„als möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind; mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis“* (Duden Online o. J.). Das Merriam Webster Online Dictionary bezeichnet „risk“ zum einen als die Wahrscheinlichkeit eines Verlustes oder einer Verletzung (*possibility of loss or injury*), zum anderen aber auch ein Subjekt oder Objekt, von dem eine Gefahr ausgeht (*someone or something that creates or suggests a hazard possibility of loss or injury* (Merriam-Webster Online o. J.).

Anders als die Begriffe „Gefahr“ und „Unsicherheit“ wird Risiko jedoch im Alltagsgebrauch nicht rein negativ assoziiert, sondern auch mit der Chance auf Gewinn in Verbindung gebracht. Das bezieht sich vor allem auf finanzielle Gewinne/Renditen privater oder unternehmerischer Natur („high risk investments“, Glücksspiel mit hohen Einsätzen), doch auch in Bezug auf immaterielle Werte wird auf das Chancen-Risiken-Narrativ zurückgegriffen, wie zum Beispiel in der Redewendung wie „Wer nicht wagt, der nicht gewinnt!“. In der Sozialwissenschaft wird bei dem Begriff „Risiko“ häufig auf die Theorien von Beck, Luhmann und

Giddens verwiesen (siehe dazu z.B. Aradau und van Munster 2007; Daase 2002). Becks gesellschaftstheoretisches Konzept der „Risikogesellschaft“ (Beck 1986), das er später zur „Weltrisikogesellschaft“ erweiterte (Beck 2007), hat in den theoretischen Analysen zu den sicherheitspolitischen Entwicklungen nach 9/11 große Resonanz gefunden (vgl. Aradau und van Munster 2007; Kühn 2017). Aus der Konjunktur des Risikobegriffs entwickelten sich Studiengänge, die sich allein mit der Definition, dem Assessment und Management von Sicherheitsrisiken auseinandersetzen.

Becks ursprüngliches Konzept der „Risikogesellschaft“ gründet sich auf dessen Annahme, dass die Menschheit im Zeitalter des Risikos ihre Risiken selbst produziert. Ursache ist die Produktion neuer Technologien, die kontinuierlich neue Risiken hervorbrächten (er erklärt das anhand der Ereignisse in Tschernobyl). Einerseits könnten Technologien von Nutzen sein, um Risiken einzudämmen und zu beherrschen, gleichzeitig würden sie riskante „Nebeneffekte“ produzieren, die nicht immer schon im Vorfeld absehbar seien (*reflexive Modernisierung*, Dialektik der Moderne (vgl. Beck 2007, vgl. Kühn 2017: 27ff). Glaubt man Becks Darstellung der Moderne, so zieht das einschlägige Konsequenzen für die Politik nach sich. Christopher Daase (2002) kommt in *Internationale Risikopolitik* zu dem Schluss, dass die Politik, wenn sie mit Risiken konfrontiert wird, eine „doppelte Ungewissheit“ auf sich nehmen muss:

„Politik ist demnach nicht nur deswegen ungewiss, weil die externen Risiken und Gefahren unbestimmt sind, sondern auch, weil die Handlungsalternativen, die im Umgang mit diesen Risiken gewählt werden können, unklar sind und ihr Erfolg keineswegs gesichert ist. Luhmann spricht deshalb von der „mehrfachen Kontingenz“ des Risikos. Diese doppelte Ungewissheit der Politik (riskante Ereignisse und riskante Strategien) ist die allgegenwärtige und unaufhebbare Bedingung jeder Politik.“ (Daase 2002: 12)

Im Unterschied zu Beck, der hier keine scharfe Trennung vollzieht, definiert Daase den Begriff „Risiko“ in Abgrenzung zum Begriff der „Bedrohung“ (ebda.: 12ff.). Nach Daase lassen sich Bedrohungen durch ein Dreieck identifizierbarer Parameter charakterisieren – einem *Akteur*, einer *Intention* und das *militärisches Potenzial* eines Angreifers). Fehlt eine oder mehrere dieser Komponenten oder ist nicht zuordenbar, zerfällt dieses Dreieck und der Faktor *Ungewissheit* (entspricht ungefähr dem englischen *uncertainty*) kommt ins Spiel. Daraus ergibt sich nach Daases Konzeption das trennende Moment zwischen beiden Begriffen:

„Was Sicherheitsrisiken von Sicherheitsbedrohungen unterscheidet, ist demnach die Erwartungsgewissheit, die verloren geht, wenn mindestens eine Größe der klassischen Sicherheitskalkulationen – Akteur, Intention, Potenzial – zur Unbekannten wird. Die Folge ist, dass aus dem Bedrohungsdreieck eine Vielzahl von Risikofaktoren werden und sich die Zahl möglicher Gefahren potenziert. Denn für Risiken ist die Unterscheidung zwischen Wirklichkeit und Möglichkeit zentral.“ (Daase 2002: 16)

Als urtypisches Beispiel eines solchen Risikos nennt Daase den islamistisch motivierten Terrorismus und die politischen Entscheidungen, die diesem Risiko gefolgt sind. Daase spricht von 9/11 als paradigmatischem Wendepunkt in der amerikanischen Sicherheitspolitik, am dem sich die USA dafür entschieden, Terrorismus nicht als Kriminaldelikt, sondern als Kriegshandlung einzuordnen. Dies habe nicht nur die bekannten außenpolitischen Entscheidungen der Bush-Regierung nach sich gezogen, sondern auch im Bereich der Inneren Sicherheit dem Wechsel von einer *reaktiven Bedrohungspolitik* zu einer – zunehmend entgrenzten – *proaktiven Risikopolitik* den Weg geebnet (vgl. ebda.: 137).

Aradau/van Munster wie auch Kühn begegnen den Entwicklungen, die Daase in Bezug auf die Internationalen Beziehungen beschreibt, aus einer Foucaultschen Perspektive mit dem Begriff des „Risikodispositivs“, (vgl. Aradau und van Munster 2007, Kühn 2017: 152). Durch den GWoT habe sich ein „dispositif of precautionary risk“ (Aradau und van Munster 2007: 91) durchgesetzt, das all jene Praktiken und Technologien unter sich vereine, die auf jeglich erdenkliche Art und Weise in Hinblick auf die Zukunft präventiv nützlich *sein könnten*: „What is new is not so much the advent of risk society as the emergence of a precautionary element that has given birth to new configurations of risk that require that the catastrophic prospects of the future be avoided at all costs“ (Aradau und van Munster 2007). Die Folge sei ein „insatiable quest for knowledge: profiling populations, surveillance, intelligence, knowledge about catastrophic management, prevention etc“ (ebda.: 91).

Während die „klassische“ Form der Risikokalkulation auf der Verarbeitung von Wissen aus der Vergangenheit basiert habe, so würde die neue Risiko-Konfiguration von der Bedingung des Unwissens und der Unvorhersehbarkeit leben. Der „neue“ Dispositif des „precautionary risk“ würde als „logischer Konnektor“ für eine Anzahl heterogener Maßnahmen fungieren, die dadurch aufgewertet würden: „As the underestimation of intelligence and knowledge is considered irresponsible from the viewpoint of precautionary risk, the scope and field of intelligence needs to be

enlarged accordingly“ (ebda.: 104). Aradau/van Munster nehmen Bezug auf Bigos “managers of unease”, die als Profiteure aus dieser Gouvernamentalität „at the limit of knowledge“ hervorgehen würden (ebda.: 105).

Zu einem späteren Zeitpunkt entwickeln Aradau und van Munster (2013) ihr Konzept weiter und ersetzen den Begriff des Risikos durch jenen der Katastrophe. In *Politics of Catastrophe: Genealogies of the Unknown* beschäftigen sich die Autor\*innen erneut mit der Gouvernamentalität des Zukünftigen, gelangen jedoch zu der Erkenntnis, dass die Grammatik des „precautionary risk“ einer Grammatik der „politics of catastrophe“ gewichen sei (Aradau und van Munster 2013: 3). Die „language of catastrophe“ (ebda.: 4) habe zu einer „proliferation of expert knowledge“ (ebda.: 7) geführt, welches sich hauptsächlich mit der Imaginierung von Worst-Case-Szenarien befaße. Dabei reiche das Spektrum von „natural or manmade disasters“, deren Framing als „katastrophal“ das entscheidende Kriterium und der gemeinsame Nenner sei (ebda.: 13). Der Diskurs des Katastrophalen lebe aus der Sicht von Aradau/Munster von einem Paradox: Davon, eine Zukunft zu regieren, die als unvorhersehbar konstruiert wird, von der jedoch gleichzeitig angenommen wird, dass sie in noch unbekannter Weise katastrophal und in einem gewissen Maß unregierbar sein muss. [I]f risk and probability introduce an array of finite possibilities for the future, catastrophe challenges the limits of possibility (ebda.: 10). Die Autor\*innen sprechen von „new styles of scientific reasoning“ (ebda.: 14), die sich der Imagination als Methode bedienen und gleichzeitig das „break-down of modern risk-management“ (ebda.: 11) markieren.

Beck nimmt in der *Weltrisikogesellschaft* eine ähnliche Analyse vor (Beck 2007). Er argumentiert, dass in der *Weltrisikogesellschaft* Risiko als objektive Größe und die Wahrnehmung von Risiko als Konstruktion zunehmend eins werden und die „Inszenierung der Katastrophe“ das politische Denken und Handeln bestimme (vgl. ebda: 13ff.). Dies führt Beck auf die Beschaffenheit der terroristischen Bedrohung zurück, wo im Vergleich zu den vom ihm als systemisch bezeichneten ökologischen und ökonomischen Risiken „Zufall durch Absicht ersetzt wird“ (ebda.: 38). Diese „Absicht“ werde in unendlich vielen imaginierte Szenarien der Katastrophe antizipiert. Das daraus folgende, von unendlich vielen Möglichkeiten ausgehende „Denken bislang undenkbar Gefahren“ gefährde laut Beck in letzter Konsequenz „Freiheit und Demokratie“ (ebda.: 39).

## 2.4.2 Vulnerabilität

Vulnerabilität (englisch: *vulnerability*) wird in den Internationalen Beziehungen häufig im Kontext von Resilienz thematisiert (siehe folgendes Unterkapitel). Während in den letzten Jahren eine beträchtliche Menge an Literatur erschienen ist, in der über die Bedeutung(en) von Resilienz im Sicherheitsdiskurs debattiert worden ist, so wurde dem Begriff Vulnerabilität isoliert weniger Beachtung geschenkt. Allenfalls im Kontext der Internationalen Entwicklung ist Vulnerabilität schon länger ein Begriff. Um ein klareres Verständnis dessen zu bekommen, was Vulnerabilität im Kontext ziviler Sicherheit bedeuten kann, soll zunächst in andere Disziplinen bzw. praktische Anwendungsbereiche geblickt werden. Abschließend wird eine kritische Lesart des Vulnerabilitätsdiskurses vorgestellt (Chandler und Reid 2016).

Die *Encyclopedia of Global Warming and Climate Change* definiert Vulnerabilität als “degree of fragility of a person, group, community, or area toward defined hazards” (Yenneti 2012). Vulnerabilität ist demnach ein Maß für die Fragilität gegenüber definierten Gefahren. Darüber hinaus beinhaltet das Konzept zusätzlich jedoch “the idea of response and coping, since it is determined by the potential of a community to react and withstand a disaster. The vulnerability of an area varies both at the geographical and social level” (ebda.). Vulnerabilität habe eine *ökonomische*, eine *soziale* und eine *ökologische* Dimension (ebda.: 1445), durch die sich die Gesamtvulnerabilität eines Ökosystems ergebe („Multihazard Vulnerability“, ebda.: 1447). Risiko wird durch eine Formel definiert, in der das Produkt der Vulnerabilität multipliziert mit der Eintrittswahrscheinlichkeit eines katastrophalen Ereignisses das Risiko ergibt (ebda. 1444). Resilienz und Vulnerabilität stünden laut dieser Definition in einem dialektischen Verhältnis zueinander (ebda.: 1447). Während die Referenzgröße von Vulnerabilität die Fähigkeit zu Widerstand oder Adaption sei, so beziehe sich Resilienz auf das Maß an Beständigkeit und Nachhaltigkeit eines Ökosystems (vgl. ebda.: 1447). Werde die Vulnerabilität gesenkt, so steige auch die Resilienz eines sozioökologischen Systems:

„Vulnerability points to the need for systems to change. When these changes include preparedness, recovery, and mitigation, geared to alleviate the effect of specific hazards, resilience increases, which in turn results in the reduction of vulnerability” (ebda.: 1448).

Der Autor hebt die Wichtigkeit dieser Beziehung in Bezug auf die *menschliche Sicherheit* hervor: "This relationship is important for the development of resilient socioecological systems, as well as for the promotion of human security" (ebda. S.1448).

In der *Encyclopedia of Crisis Management* wird Vulnerabilität als „the potential for harm incurred by a person, asset, activity, or assemblage of items that is at risk“ definiert (Alexander 2013: 1011). Stärker als in der auf den Klimawandel bezogenen Definition wird die auf die durch menschliches Handeln verursachte Komponente von Vulnerabilität hingewiesen: "As [disaster] is mainly the result of social, economic, political and cultural factors in decision-making, vulnerability is constructed socially." (ebda.). Auch in dieser Definition wird die Multidimensionalität von Vulnerabilität betont, die „menschengemachte“ Komponente jedoch zur fundamentalen Ursache erklärt: „In synthesis, the vulnerability approach begins with the principle, that people, not physical forces, are the most fundamental cause of risk and disasters“ (ebda.). Vulnerabilität müsse sowohl als Phänomen als auch als „set of dynamic processes“ verstanden werden. Interessant ist die Sichtweise des Autors, dass die „interconnectedness in world commerce“ eine „major source of vulnerability“ darstelle (ebda.:1022).

David Chandler hat die Operationalisierung von Vulnerabilität in Kriseninterventionsprogrammen der UN analysiert (2016). Chandler vertritt die Auffassung, dass der „gaze of neoliberalism“ Vulnerabilität lediglich auf der Ebene verletzlicher Subjekte und Gemeinschaften ansiedle und auf diese Weise die zuvor erwähnten strukturelle Faktoren gezielt ausblende (Chandler 2016: 123): "The vast structural inequalities across continents, regions, states, and societies become reinscribed as evidence of the distinctiveness of the differences of subjective adaptive capacities and capabilities" (ebda.: 124). Diese Technik der Subjektivierung führe dazu, dass das „vulnerable Subjekt“ ins Zentrum des politischen Interesses rücke, das für die globalen Probleme und Konflikte ursächlich sei und nicht umgekehrt:

„Rather than social and economic relations producing vulnerable and marginalized subjects, neoliberal discourse inverses previous understandings to posit social and economic problems as symptoms or consequences of poor informational choices by vulnerable subjects“ (ebda.: 124).

Für den empirischen Teil der Arbeit wird relevant sein, in welchen Zusammenhängen Vulnerabilität inhaltlich in Erscheinung tritt und mit welchen Forschungszielen die verwendete Definition des Konzepts verknüpft ist.

### **2.4.3 Resilienz**

„Not only is resilience a shallow concept, it is also a shifting concept“ ( Joseph 2013a: 51). Der Begriff Resilienz hat in den Internationalen Beziehungen nach dem ersten Jahrzehnt der 2000er-Jahre wachsende Verbreitung gefunden. Seither ist eine beträchtliche Menge teils auch empirisch fundierter Forschungsliteratur zu dem Konzept erschienen, anhand derer in den folgenden Absätzen Resilienz als sicherheitspolitische Zielgröße – und politische Praxis – diskutiert werden soll.

Was Resilienz im Kontext von Sicherheit bedeutet und wie das Konzept den sicherheitspolitischen Diskurs prägt und transformiert, darüber wird seit jeher kontrovers diskutiert. Kritiker\*innen und Befürworter\*innen des Konzepts stimmen in ihren Analysen weitgehend überein, dass Resilienz eine Welt und Gesellschaften voraussetzt, die „komplex“, d.h. global vernetzt und interdependent sind (Aradau 2014; Fjäder 2014; Joseph 2016). Diese Komplexität rufe kontinuierlich neue, unvorhersehbare Unsicherheiten hervor, auf die nur mit Maßnahmen reagiert werden könne, die alle Unsicherheiten, die eine Gesellschaft potenziell betreffen können, in ihrer Gesamtheit in den Blick nehmen („all-hazards approach“; vgl. Fjäder 2014: 128, Chandler/Coaffee 2014: 8, Rogers 2015: 27). Dem Zeitalter der Komplexität wird aufgrund dieser „Ausgangssituation“ ein erhöhtes Maß an Unsicherheit zugeschrieben, mit dem es sich – auf unterschiedlichen Ebenen und mit innovativen Maßnahmen und Herangehensweisen – zu arrangieren gelte. So schreibt Aradau: „Resilience is [...] a proactive response to a world that is ‘complex, unstable, unknowable, unpredictable’. The problematisation that calls for resilience is that of ‘un-ness’: unexpected, unknowable, unpredictable, unmanageable events“ (Aradau 2014: 78).

Resilienz strebt aufgrund dieser Art der Problematisierung im Gegensatz zu Sicherheit nicht in Richtung eines zu erreichenden Idealzustandes („Sicher Sein“), sondern orientiert sich aufgrund einer „new awareness of insecurity or contingency“ (Chandler und Coaffee 2017: 4) stärker an den Handlungsmöglichkeiten, die sich in

einer unsicheren – und auch letztlich niemals komplett zu sichernden – Umgebung eröffnen: „We suggest that the world of resilience is one with less confidence in the power of securing agency and the capacity of knowledge and generalisation“ (ebda.: 4). Kern des Resilienz-Konzepts sei die Annahme, dass Katastrophen aufgrund der unübersichtlichen Bedrohungslage heute nicht mehr zur Gänze verhindert werden können, und deshalb verstärkt die Eindämmung katastrophaler Ereignisse sowie die Anpassung nach dem Eintreten einer Katastrophe in den Vordergrund rücken sollten (vgl. ebda.: 79).

Chandler & Coaffee (2014: 5) machen im Resilienz-Diskurs der vergangenen Jahre mindestens drei unterschiedliche Framings von Resilienz aus:

1. *Homöostatische* – am Gleichgewicht orientierte – Resilienz orientiert sich am Status Quo, der nach einem unerwarteten Schock so schnell wie möglich wieder erreicht werden soll (vgl. ebda.: 5). Es ist die Resilienz des „bouncing back“, deren Hauptziel es ist, das gedehnte Band wieder in seinen Urzustand zu bringen. Homöostatische Resilienz schließt jedoch nach Chandler/Coaffee nicht aus, sich in der Gegenwart auf zukünftige Schocks oder Krisen einzustellen/vorzubereiten: “These changes are geared less towards preventing risks, threats or problems from taking place (pre-resilience views of security) and more often towards addressing or responding to them and recovering with the minimum of disruption” (ebda.: 5). Bei diesem Verständnis von Resilienz würden neue Technologien eine unterstützende Rolle einnehmen oder als solche propagiert werden, die Autoren nennen “Big Data, digital sensing, machine-learning and the Internet of Things” (ebda.: 5). Chandler/Coaffee sehen in diesem Zugang die „first generation of resilience thinking“ (ebda.: 5).
2. Die „zweite“ Generation beschäftige sich weniger mit der Rückkehr zu einem Gleichgewicht aus der Vergangenheit als mit dem Thema Wachstum und Entwicklung im Angesicht von kontinuierlicher Veränderung. Diese Sichtweise wird als *autopoetisch* – selbsterhaltend – bezeichnet: „Resilience is longer about returning to the equilibrium or maintaining the status quo, but is seen to be a process of ongoing self-transformation that can be likened to ‘bouncing forward’” (ebda.: 5). Diese Idee von Resilienz verändere die Beziehung

zwischen dem Souverän, der Außenwelt und den Individuen. Autopoietische Resilienz konzentriert sich auf Reflexion, Lernfähigkeit und „self awareness“ – es wird hierbei davon ausgegangen, dass Systeme aus Krisen und Erschütterungen gestärkt hervorgehen können (ebda.: 6). Herkömmliche Problemlösungsansätze werden hier herausgefordert und – sofern möglich – durch nachhaltigere ersetzt, die darauf ausgerichtet sind, selbst keine neuen Probleme/Schäden zu erzeugen (ebda.: 6).

3. Eine dritte Form von Resilienz-Denken verorten Chandler/Coaffee in Zugängen, die ausschließlich auf der Community-Ebene praktiziert werden und von Beginn an ziviles Engagement voraussetzen. Resilienz werde hier als fortlaufender Prozess gesehen, in denen Probleme als Chancen und Möglichkeiten der Ermächtigung gerahmt werden (vgl. ebda.: 6).

Kritiker\*innen des Resilienz-Konzepts sehen darin mehrheitlich eine neoliberal-gefärbte Praxis, durch die sich Nationalstaaten einerseits ein Stück weit der Verantwortung entziehen, für die Sicherheit ihrer Bevölkerung zu sorgen und andererseits eine Praxis der Gouvernamentalität etablieren, die es ermöglicht, die Bürger\*innen aus der Distanz in die Pflicht zu nehmen (siehe dazu Aradau 2014; Joseph 2016; Zebrowski 2016).

Der bekannteste Vertreter dieser kritischen Position ist Jonathan Joseph, der den Einzug des Resilienz-Diskurses in Institutionen und Strategie-Papiere der EU analysiert hat (Joseph 2013a, 2013b, 2016). Resilienz sei aus seiner Sicht als politische Idee „very Anglo-Saxon in nature“ (Joseph 2013a: 52) und habe in der Europäischen Union deshalb Anklang gefunden, weil es einer neoliberalen Politikgestaltung zugutekomme: “The ideas play a role in European discourse insofar as they support its neoliberal drive” (ebda.: 52, siehe auch Joseph 2013b.. Anhand empirischer Beispiele aus dem Vereinigten Königreich, der EU und Frankreich stellt er die inhaltliche Bedeutung des Resilienz-Konzepts für politische Belange radikal in Frage und ermahnt dazu, den Vormarsch dieses Konzepts als „paradigm for intervention and problem-solving“ (Joseph 2016: 370) im Bereich der Inneren Sicherheit sowie im Bereich humanitärer Interventionen ausschließlich relational zu betrachten. Für Joseph ist Resilienz als *Governance*-Technik nichts weiter als ein Resultat neoliberaler Regierungspraktiken des angelsächsischen Raums. In diesem

Kontext gelte es die ontologischen Annahmen zu hinterfragen, die als Voraussetzungen für eine praktische Anwendung von Resilienz dienen (vgl. Joseph 2016: 372).

Die Hauptkritik des Autors lautet, dass Resilienz als politisches Konzept ein Bild der Gegenwart zeichnet, indem sich die Menschen den zu Beginn skizzierten strukturellen Gegebenheiten unhinterfragt anpassen müssten: „Rather than being a process that we can control, globalization is seen as something that we have to learn from and adapt to (ebda.: 377). Dahinter stehe eine konservative Ideologie, in der die Verantwortung des Einzelnen im Vordergrund steht und die Möglichkeiten politischer Steuerung globaler Prozesse ablehnend gegenübersteht:

“The conservative ontology behind this (the political acronym is TINA or there is no alternative) is shared with a range of other contemporary social ideas such as reflexive modernity, risk society, network society and information age, all of which posit the idea that we must change our behavior and adapt to things beyond our control.” (Joseph 2013a)

Resilienz würde eine Marktlogik im Sicherheitsdiskurs verankern, die das Funktionieren ökonomischer Abläufe im Falle einer Krise an oberster Stelle platziert und jene Referenzobjekte in den Vordergrund rückt, die in diesem Bereich von Bedeutung sind. Als Beispiel nennt Joseph kritische Infrastrukturen, deren Schutz in den Sicherheitsagenden der vergangenen zwei Jahrzehnte kontinuierlich gewachsen sei (ebda.: 49). Auch Aradau (2014) sieht im Aufkommen von Resilienz eine weitere „instantation of the neoliberal logic of security, with its attendant constitution of vulnerability and abjection“ (Aradau 2014). Sie ist der Ansicht, dass der Resilienz-Diskurs einen Mechanismus darstellt, durch den die epistemologischen Grundlagen von Sicherheitspolitik transformiert würden. Durch die Evokation von Resilienz würden sich alle sicherheitspolitischen Zielsetzungen um das Momentum einer unerwarteten noch nicht bekannten „Überraschung“ zirkulieren, wodurch das Versprechen von Sicherheit ausgesetzt wird:

„Even as security remains desirable, the problematisation of surprising events renders its promise impossible, to be replaced by resilience. Resilience does not promise anything inasmuch as it does not purport to ‚tame‘ contingency but only to live through the surprising and the unexpected.“ (Aradau 2014: 87)

Laut Zebrowski (2016) würde Resilienz auf den ersten Blick eine Verheißung darstellen, durch die das Spannungsverhältnis zwischen Sicherheit und Freiheit

gelöst werde (Zebrowski 2016). Auf den zweiten Blick habe der „shift to resilience-based security policies“ jedoch dazu geführt, dass unter dem Vorwand einer liberalen Kritik eine protektive Form der Risikopolitik zugunsten einer Toleranz von Risiken abgelöst wurde (Zebrowski 2016: 13). Resilienz stelle eine Form neoliberaler Biopolitik dar, die darauf abzielt, Individuen für diese „unsichere“ und „prekäre“ Welt zu „resilienten Subjekten“ auszubilden (vgl. ebda.: 14f). Der „Wert“ von Resilienz sei ein selektiver: „Resilience thus calls on government to create the conditions within which we may be permitted to be ‚free‘“ (ebda: 4).

Fjäder sieht im Resilienz-Diskurs zwar keine neue Form neoliberaler Gouvernementalität/Biopolitik, teilt jedoch die Ansicht, dass eine Verschiebung von „Sicherheit“ zu „Resilienz“ den Staat von seiner traditionellen Sicherheitsaufgabe entbindet (Fjä (Fjäder 2014: 128). Fjäder betrachtet die Erweiterung des „Sicherheits-Portfolios“ um heterogene Formen von Gefahren, Risiken und Bedrohungen nicht als Konsequenz einer resilienzorientierten Sicherheitspolitik, sondern als eine Bedingung, die Resilienz als sicherheitspolitisches Paradigma erst ermöglicht hat:

„The inclusion of a variety of new threats (such as the environmental, the economic and the societal) to the national security agenda, as well as the securitisation of critical infrastructure, has created favourable conditions for a resilience approach to national security“ (ebda.: 128).

Sicherheit habe essenziell präventiv und proaktiv zu sein habe (vgl. ebda.: 122), Resilienz hingegen suggeriere “that preventive measures have not had full effect, and it consequently focuses and minimizing disruption to critical services to the society once an event has nonetheless happened” (ebda.: 123). Resilienz sei eine geeignete Strategie, um “business continuity” im Falle einer Katastrophe sicherzustellen und schützt den Staat vor Versagen, wenn der sich nicht mehr verpflichtet fühlt, das Eintreten eines katastrophalen Ereignis zu verhindern (ebda: 127). Um dies zu legitimieren brauche es laut Fjäder jedoch einen neuen Gesellschaftsvertrag zwischen Bevölkerung und Staat, indem diese Verschiebung festgeschrieben wird:

„The application of resilience in this context, however, requires the nation-state to agree on a new social contract with its citizens, based on a mutual understanding that acknowledges at least a partial shift from prevention of threats to management of the impacts of threats.” (Fjäder 2014: 128)

Pospisil und Gruber (2016) sehen im Resilienzdiskurs – anhand einer empirischen Analyse des Beispiels UK – keinen „roll-back of state policies in the realm of security“ (ebda.: 213). Resilienz wäre im Gegenteil von der „traditionellen“ Form exceptioneller Sicherheitspolitik abhängig, da sie in deren Versagen und Unwirksamkeit ihre Existenzberechtigung findet (vgl. ebda.: 212). Das Aufkommen des „resilience-security-nexus“ (ebda.: 212) stehe für eine partielle Zurückweisung staatlicher Verantwortung in Sicherheitsaufgaben aufgrund der schieren Unmöglichkeit ihrer Erfüllung (ebda.: 213).

Münkler & Wassermann (2012) sehen im Resilienz-Diskurs eine strategische Möglichkeit souveräner Staaten, den Weg einer Sicherheitspolitik zu gehen, in der Unsicherheit aus strategischen Gründen akzeptiert wird. Anders als Fjäder verlangen die Autoren dafür jedoch keinen neuen Gesellschaftsvertrag, da sie die Ansicht vertreten, dass ein gewisses Maß an Unsicherheit im Sinne eines „trade-off“ gegenüber anderen Nachteilen notwendig ist. Laut Münkler und Wassermann ersetzen *Vulnerabilität* und *Resilienz* in der gegenwärtigen Weltordnung die Begriffe *Bedrohung* und *Abschreckung*. Da staatliche Akteure sich ihrer konkreten Bedrohungen nicht mehr gewiss seien, müssten sie sich verstärkt ihrer eigenen Vulnerabilität – also Schwächen und möglichen Angriffspunkte, die unbekannte Täter\*innen ausnützen könnten – zuwenden. Da jedoch das Erreichen einer vollständigen Unverwundbarkeit unrealistisch sei, müsse ein weiteres Augenmerk auf Schadensreduktion und die Bewältigung katastrophaler Ereignisse gelegt werden. Vulnerabilität und Resilienz seien demnach nicht das jeweilige Gegenteil voneinander, sondern bedingen einander wechselseitig: „Resilienz erscheint somit eher als Komplementär- denn als Gegenbegriff zu Vulnerabilität, insofern als gerade verwundbare Systeme wie etwa komplexe Industriegesellschaften darauf angewiesen sind, durch resiliente Strukturen ihre Überlebenschancen in einem Umfeld großer Unsicherheit zu sichern“ (ebda.: 87).

Denn die „bedingungslose Sicherheitsmaximierung“ sei nach Münklers Auffassung aus zwei Gründen nicht erstrebenswert: Zum einen würde sie zu einer „Ressourcenüberforderung“ führen, zum anderen würden überzogene Sicherheitsvorkehrungen die Prosperität der Volkswirtschaft gefährden (ebda.: 90). Zwischen Wohlstand (der hier gleichgesetzt wird mit ökonomischer Prosperität) und Sicherheit müsse eine „Güterabwägung“ getroffen werden, die nach der Meinung der

Autoren zugunsten der Aufrechterhaltung der Wirtschaft ausfallen sollte: „Der Schlüssel besteht im Nachdenken über Unsicherheit“ (ebda.: 91).

Eine weitere affirmative, aber diametral entgegengesetzte Lesart von Resilienz präsentiert Tierney (Tierney 2014). Anders als das Gros der Autoren, die zuvor zitiert wurden, sieht die Autorin im Resilienzdenken keinen strategischen Schritt zur Suspendierung von Verantwortung, sondern eine emanzipative Form sicherheitspolitischen Handelns, dass Bürger\*innen dabei helfen soll, sicherer zu leben. Für Tierney ist Resilienz keine Form der Unsicherheitspolitik, die Verluste und Schäden in Kauf nimmt, sondern eine Form des Sicherheitsdenkens, die beides – die Vorbeugung und den Umgang mit Risiken – verbessern soll:

“Considering risk and resilience in tandem is important. While risks can be reduced – and must be, unless we are willing to tolerate ever-ballooning losses- no society can eliminate risk. Increasing resilience can both contain risk, making disastrous events less likely, and help those who are at risk better cope with crisis when it occurs.” (Tierney 2014: 7)

Resilienz sei eine systemkritische Praxis, systemischen Risiken und Vulnerabilitäten zu begegnen: “because risk and vulnerability are outcomes of the exercise of political and economic power in their various forms, confronting risk also means confronting power” (ebda.: 9).

### 3 Methode

#### 3.1 Kritische Diskursanalyse<sup>2</sup>

Als Methode wurde mit der kritischen Diskursanalyse (abgek.: KDA) nach Jäger (2015) eine Form der Textanalyse gewählt, die einen möglichst „freien“ Weg der Kodierung und Kategorienbildung erlaubt. Jäger orientiert sich bei seiner methodischen „Gebrauchsanweisung“ an der Diskurstheorie Foucaults (ebda.: 18, 76-78) und steht demnach in der Tradition der Auffassung von Diskursen als komplexe „Macht-Wissen-Systeme“ (ebda.: 19) und nicht in der einer (rein) semiotischen Diskurstheorie. Jäger bezeichnet Diskurse als „Flüsse bzw. Abfolgen von oft auch raumübergreifenden sozialen Wissensvorräten durch die Zeit“ (ebda.: 78). Der Autor macht zur Beschaffenheit von Diskursen „einige terminologisch/pragmatische Vorschläge“, die die praktische Umsetzung der Diskursanalyse erleichtern sollen (ebda.: 79):

- *Diskursstränge*: Ein Diskursstrang konstituiert das Sagbare bzw. Unsagbare zu einem bestimmten Thema entweder zu einem gegenwärtigen Zeitpunkt (synchroner Schnitt) oder aus einer historischen Perspektive als „[t]hematisch einheitliche Wissensflüsse durch Zeit und Raum“ (ebda.: 81).
- *Diskurs(strang)verschränkungen*: Diskursstränge sind ein Teil des gesamtgesellschaftlichen Diskurses und ziehen ihre Besonderheit aus der „Verschränkung oder Verzahnung“ mit anderen Diskurssträngen. Ist nun der „zivile Sicherheitsdiskurs“ der Gegenwart und jüngeren Vergangenheit der zur Analyse stehende Diskursstrang, so werde ich mich in der empirischen Analyse auch mit vermuteten oder erwartbaren Diskursstrangverschränkungen, wie sie zumindest aufgrund der Theoriearbeit im Vorfeld „hypothetisch zu unterstellen“ (ebda.: 88) sind, auseinandersetzen.

- *Haupt- und Unterthemen*: „Eine [...] Diskursverschränkung liegt vor, wenn ein Text verschiedene Themen anspricht, aber auch, wenn nur ein Hauptthema angesprochen wird, bei dem aber Bezüge zu anderen Themen vorgenommen werden“ (ebda.: 87). Damit will Jäger zum Ausdruck bringen, dass auch durch die lose Verknotung von Unterthemen eines Diskursstranges (er bezeichnet diese als Diskursfragmente, vgl. ebda.: 80), „besondere Effekte erzeugt werden können“, denen es bei der Analyse „besondere Aufmerksamkeit“ zu erweisen gilt (ebda.: 88).

Mit jener losen Systematik im Hinterkopf wurden die Codes vergeben, aus denen sich im weiteren Folge die repräsentativen empirischen Kategorien gebildet haben, in die sich der empirische Teil gliedert. Der Prozess der Kodierung erfolgte softwaregestützt und soll im nachfolgenden Unterkapitel näher erklärt werden.

### **3.2 Computergestützte Auswertung mit atlas.ti**

Zur Umsetzung des empirischen Teils der Forschung wurde mit der Computer-Assisted Qualitative Data Analysis-Software Atlas.ti gearbeitet. Um den Vergleich zwischen den Texten in Hinblick auf die Forschungsfrage zu erleichtern, wurden die ausgewählten Dokumente in zwei Zyklen kodiert.

Zunächst wurde in einem offenen, an die Grounded Theory angelehnten Kodierungsprozess („Initial Coding“, vgl. Saldaña 2009: 81) die grundlegenden Inhalte der Dokumente erfasst, um deren zentrale Aussagen zu reflektieren und sie mit der Lektüre zum Stand der Forschung in Verbindung zu bringen.

Anschließend wurde – stärker an den ausgewählten theoretischen Konzepten und dem Stand der Forschung orientiert – mit einer Liste vorab festgelegter Codes in die zweite Kodierungsrunde gegangen („Provisional Coding“, vgl. Saldaña 2009: 120). Die Analyse blieb jedoch nicht auf diese fixen, theoriegeleiteten Codes beschränkt, sondern zielte im Gegenteil auf die Erweiterung dieses Korpus ab. Auf Basis dessen

---

<sup>2</sup> Es soll darauf hingewiesen werden, dass sich bei Korunka (2017) im Kapitel „Methode“ ein Abschnitt mit inhaltlichen Überschneidungen zu diesem Unterkapitel zu finden ist.

haben sich die entscheidenden Überkategorien („themes“, vgl. Saldaña 2009: 13) entwickelt und die dazu passenden, repräsentativen Zitate ermittelt.

## 4 Empirische Analyse

### 4.1 Ausrichtung, Bedrohungsbilder und erklärte Zielsetzungen der untersuchten Programme

Als Vorbereitung und Einstieg in die Analyse der empirischen Kategorien soll eine vergleichende Darstellung zunächst einen Überblick über die generelle Ausrichtung und die angestrebte Reichweite der drei Programme bieten. Im Zuge dessen soll erörtert werden, von welcher Bedrohungswirklichkeit ausgegangen wird, wer/was die Referenzobjekte sind, wie Sicherheit definiert/eingegrenzt wird und an welche Akteure/Interessengruppen sich die Programme richten. Darüber hinaus soll das Forschungs- und Technologieverständnis der einzelnen Programme skizziert und die über den Sicherheitsaspekt hinausgehende strategische Zielsetzungen erörtert werden.

#### 4.1.1 *Bedrohungsbilder*

Im deutschen und österreichischen Programm wird das Bild einer Wirklichkeit gezeichnet, deren Bedrohungen und Risiken insbesondere aufgrund ihrer prozessualen Veränderlichkeit unvorhersehbar sind. In beiden finden sich dahingehend Übereinstimmungen, dass sie sich einer Welt mit *vielfältigen* Bedrohungen und Risiken und kontinuierlichen Prozessen des *Wandels* gegenübersehen. Durch die Anrufung des permanenten Wandels wird eine kausale Brücke zu einer permanenten Anpassung in Form von *Innovation* geschlagen, die als logische Antwort auf diese Entwicklung artikuliert wird.

*Österreich:* „Vor dem Hintergrund vielfältiger, sich in stetem Wandel befindlicher Bedrohungslagen für unsere Gesellschaft gilt es, innovative Ansätze für die Begegnung dieser Bedrohungen zu entwickeln.“ (bmvit 2015b: 4)

*Deutschland:* „Wir leben in einer zunehmend vernetzten und komplexen Welt, die im ständigen Wandel ist. Deshalb müssen wir uns Herausforderungen, wie Naturkatastrophen, organisierter Kriminalität oder internationalem Terrorismus stellen.“ (BMBF 2016e: 2)

„Wir werden die zivile Sicherheitsforschung an aktuellen und künftigen Herausforderungen ausrichten und die Entwicklung innovativer Lösungen für den Schutz der Bevölkerung und der kritischen Infrastrukturen fördern.“ (ebda.: 8)

Im europäischen Programm findet sich ein entsprechendes oder ähnliches Narrativ nicht explizit, der Fokus liegt in der Einleitung zu *Secure Societies* auf den spezifischen Risiken, die von den technologischen Fortschritten im Bereich der modernen Informations- und Kommunikationstechnologien ausgehen. Diese werden als treibende Kraft für die „productivity, innovation, commercial exchanges and societal changes“ präsentiert, deren „actual or perceived lack of security“ (Europäische Kommission 2015b: 7) jedoch ein Risiko für die europäische Wirtschaft und Gesellschaft darstellen würde. Der technologische Vorsprung „krimineller Akteure“ wird dabei besonders herausgestellt:

“ICTs boost productivity, innovation, commercial exchanges and societal changes. Hence, the actual or perceived lack of security of digital technologies is putting at risk the European economy and society. Moreover, criminal actors have now widely embraced the new technologies to perpetrate crime.” (ebda.)

Während im österreichischen Programm KIRAS *Vielfalt* und *Wandel* als einzige Attribute des Unbekannten und Unvorhersehbaren ins Feld geführt werden, so wird im deutschen Programm zusätzlich noch der globale Kontext als „Welt“ hervorgehoben, der mit den Adjektiven „vernetzt“ und „komplex“ versehen wird. Während bei KIRAS von „in stetigem Wandel befindlichen Bedrohungslagen für *unsere* [die österreichische] Gesellschaft“ auf das bedrohliche, globale *Andere* allenfalls implizit hingewiesen wird, so wird im deutschen Programm anstelle von Bedrohungslagen der Begriff „Herausforderungen“ gewählt, denen es sich angesichts des Wandels zu stellen gilt. Zugleich werden sowohl in *Sicherheitsforschung 2012-2017* als auch in *Secure Societies* die Globalisierung als grundsätzlich positiv attribuiert, wohingegen im österreichischen Programm KIRAS die Globalisierung oder globale Vernetzungen weder erwähnt noch bewertet werden.

*Deutschland:* „Mit der weiter fortschreitenden Globalisierung von Gesellschaft, Wirtschaft und Politik eröffnen sich für Deutschland neue Chancen. Als weltoffene Gesellschaft und exportorientierte Wirtschaftsnation profitieren wir in hohem Maße von der zunehmenden Vernetzung internationaler Handels-, Reise- und Wissensströme. Dadurch entstehen aber auch neue Verwundbarkeiten. Diese können sich auf die äußere und innere Sicherheit Deutschlands ebenso auswirken wie auf die individuelle Freiheit und Unversehrtheit seiner Bürgerinnen und Bürger.“ (BMBF 2016e)

EU: "Economic growth, together with the opportunities provided by a free and democratic society based on the rule of law, generate prosperity amongst Europe's citizens who benefit from increased mobility across national borders, and from globalized communication and finance infrastructure – but with such opportunities also come risks, as terrorists and criminals seek to pursue destructive and malicious ends." (Europäische Kommission 2017a)

Sowohl die EU als auch Deutschland integrieren eine affirmative Haltung gegenüber der „Globalisierung“ im Sinne transnationaler Mobilität von Personen, Gütern und Dienstleistungen in die Aufzählung der mit ihr einhergehenden Risiken und Bedrohungen. Die „Globalisierung“ wird im Zuge der Artikulation von Chancen und Risiken als Tatsache/Entwicklung charakterisiert, deren ökonomische Vorteile die Sicherheitsrisiken bei Weitem übersteigen. Im deutschen Programm wird diese Position mit der Bezeichnung Deutschlands als „exportorientierte Wirtschaftsnation“ noch stärker verdeutlicht als im Programm der EU. Zusätzlich zur ökonomischen Komponente wird die Globalisierung mit einer „weltoffenen Gesellschaft“ assoziiert und damit ein gesellschaftspolitischer, an die „Menschen“ gerichteter Aspekt hinzuaddiert. Im Programm der EU werden zwar transnationale Mobilität und globalisierte Finanz- und Kommunikationsinfrastrukturen als Grundfeste der „free and democratic EU society“ (Europäische Kommission 2017: 24) charakterisiert, denen die damit einhergehenden inhärenten, grenzüberschreitenden Gefahren gegenübergestellt werden. Die Bejahung der Globalisierung als großem Vorteil für die Gesellschaft wird jedoch weniger stark betont als im deutschen Programm.

In ihrer Aufzählung möglicher Bedrohungslagen, für die die Sicherheitsforschung entwickelt werden soll, sind sich die Programme grundsätzlich ähnlich. Im deutschen Programm lautet der am Anfang jeder Ausschreibung stehende ‚Slogan‘:

„Das Rahmenprogramm der Bundesregierung ‚Forschung für die zivile Sicherheit 2012 bis 2017‘ [...] verfolgt das Ziel, den Schutz der Gesellschaft vor Bedrohungen zu verbessern, die zum Beispiel durch *Katastrophen, Terrorismus, Kriminalität* und *Großschadenslagen* ausgelöst werden.“ (siehe z.B. BMBF 2016a)

In KIRAS werden als „wesentliche Bereiche von Sicherheit bzw. spiegelbildlich Risiko/Bedrohung“ untereinander aufgelistet: „Naturkatastrophen, Infektionskrankheiten, Kriminalität, Terrorismus, sowie Technologie- bzw. Industrieunfälle“ (bmvit 2015a: 7).

In Secure Societies werden „natural and man-made disasters, including extreme weather events, crime and terrorism threats“ (Europäische Kommission 2015b: 9)

genannt. Alle drei Programme stützen sich also auf einen breiten Kanon von heterogenen Bedrohungen, Gefahren und Risiken, wobei die Inklusion von „Kriminalität“ bzw. „crime“ den Interpretationsspielraum, was als Bedrohung für die zivile Sicherheit definiert werden kann, theoretisch ad infinitum erweitert (mehr dazu in den Folgekapiteln).

#### **4.1.2 Sicherheitsbegriff**

Alle drei Programme stützen sich auf einen Sicherheitsbegriff, der nahezu (all)umfassend ist. „Zivile Sicherheit“ bezieht sich dabei grundsätzlich auf die Vorbeugung, Abwehr und Linderung aller Risiken und Gefahren, die nicht-militärisch sind. Aufgezählt werden neben ökologischen auch ökonomische, kulturelle und gesellschaftliche Risiken. Während in KIRAS der Begriff „umfassende Sicherheit“ gewählt wird, wird in Sicherheitsforschung 2012-2017 mit dem Begriff „erweiterte Sicherheit“ gearbeitet:

*Österreich:* „Der Sicherheitsbegriff, welcher KIRAS zugrunde liegt, ist umfassend angelegt. Er bezieht sich auf nichtmilitärische, ökonomische, ökologische, kulturelle und gesellschaftliche Gefahren und Risiken und alle Maßnahmen der öffentlichen Hand zur Erhaltung bzw. Verbesserung der öffentlichen Sicherheit, einschließlich der Vorbeugung und Abwehr von Gefahren sowie der raschen Hilfe im Falle von Ereignissen, die die öffentliche Sicherheit maßgeblich beeinträchtigen.“ (bmvit 2015a: 6)

*Deutschland:* „Erweiterte Sicherheit: Bezeichnet ein Verständnis von Sicherheit, das über die klassische Definition der militärischen Sicherheit hinausgeht und im Zuge der Globalisierung auch zivile Aspekte von Sicherheit einschließt, unter anderem kulturelle, soziale, ökologische und ökonomische.“ (BMBF 2016e)

Im deutschen Programm wird auch auf die Globalisierung Bezug genommen. Zwischen der Globalisierung und der Erweiterung des Sicherheitsbegriffs auf nicht-militärische Bedrohungen wird eine kausale Beziehung konstruiert, es entsteht der Eindruck eines Sachzwangs der Erweiterung des Portfolios an potenziellen Gefahren und Risiken aufgrund der globalen Vernetzung und Komplexität der heutigen Welt.

Im Programm der EU wird keine entsprechende Definition vorgenommen, der Begriff „Sicherheit“ hat dort trotz des Adjektivs „secure“ im Titel eine geringere Bedeutung. Stattdessen wird die Erhöhung der „Resilienz“ der europäischen Bürger\*innen als primäres Ziel des Programms bereits in der Einleitung genannt (vgl. Europäische Kommission 2015b: 7). Damit einhergehend wird im Programm der EU auch ein

„kohärenterer Zugang“ zur Gefahren- und Risikobetrachtung im Sinne eines „strong risk reduction innovative frame“ hervorgehoben, es ist von Maßnahmen die Rede, die über „traditional risk concepts“ hinausgehen und Resilienz „inkludieren“ (Europäische Kommission 2015b: 24).

Das deutsche Programm sticht dadurch hervor, dass Sicherheit nicht nur als anzustrebender Zustand, sondern insbesondere auch als Wert und als menschliches Grundbedürfnis in Szene gesetzt wird: „Sicherheit bedeutet unter anderem Angstfreiheit, Geborgenheit und Vertrauen. Sicherheit stellt damit ein elementares menschliches Grundbedürfnis und eine zentrale gesellschaftliche Leitidee dar“ (BMBF 2016e: 12). An anderer Stelle wird Sicherheit als „zentraler Wertbegriff der Gegenwartsgesellschaft“ ins Feld geführt und darauf hingewiesen, dass Sicherheit ein „wichtiger Faktor des wirtschaftlichen Wohlstands in Deutschland“ (BMBF 2016e: 8) sei.

#### **4.1.3 Referenzobjekte**

In allen drei Programmen wird Aufschluss darüber gegeben, welchen Schutzziele die geförderten Forschungs- und Technologieprojekte dienen sollen. Österreich fällt hier gegenüber der Europäischen Union und Deutschland mit einem vergleichsweise „engen“, am Schutz der nationalen Bevölkerung orientierten Ansatz auf. So heißt es im KIRAS-Programmdokument:

„Das unter der Programmverantwortung des Bundesministeriums für Verkehr, Innovation und Technologie (bmvit) stehende österreichische Sicherheitsforschungsförderprogramm „KIRAS“ unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der Sicherheit Österreichs und seiner Bevölkerung.“ (BMVIT 2015: 4)

Erklärte Referenzobjekte im österreichischen Programm sind demnach die Souveränität des Nationalstaats Österreich und die körperliche Sicherheit und Unversehrtheit der Bürger\*innen dieses Staates als Kollektiv (und je nach Zugehörigkeit zur „Bevölkerung“ auch als Individuen). Im deutschen Programm heißt dazu im Vergleich zunächst: „Es ist ein zentrales Anliegen der Bundesregierung, möglichst allen Menschen Sicherheit zu gewähren“ (BMBF 2016e: 3). Hier werden als Referenzobjekt „möglichst alle Menschen“ genannt, was einen größeren Interpretationsspielraum lässt und die deutschen Forschungsförderungsmaßnahmen per definitionem weniger stark an die nationale Sicherheitspolitik bindet. Zum einem

ist von „Menschen“ und nicht von „der Bevölkerung“ die Rede, was die Kritik vorwegnimmt, deutsche Forschung für die zivile Sicherheit sei lediglich dem Schutz deutscher Staatsbürger\*innen vorbehalten. Des Weiteren entsteht kein Widerspruch mit der expansiven, exportorientierten Haltung „Deutschlands als führende Industrienation in der Mitte Europas“ (ebda.: 19), wonach deutsche Sicherheitstechnologien und -modelle nicht auch der zivilen Sicherheit „möglichst aller Menschen“ im Ausland, unabhängig ihrer Nationalität, zunutze kommen könnten. Dieser an der menschlichen Sicherheit orientierte Wahl des Referenzobjekts wird jedoch in den meisten Ausschreibungsdokumenten nicht beibehalten. Dort wird durchwegs auf die „Bürgerinnen und Bürger“ verwiesen (vgl. BMBF 2012c, 2014c, 2016d, 2017b, uvm.), deren Sicherheit und Sicherheitsempfinden im Rahmen der Forschungsprojekte erhöht werden soll.

Sowohl Deutschland als auch die EU geben als Referenzobjekte jedoch von vornherein nicht nur den Schutz von Souveränität und menschlichen Lebens (im Kollektiv oder als Individuen) an, sondern artikulieren ein breiteres Kontinuum an Dingen, Werten und Zuständen, die als Referenzobjekte in Frage kommen. *Secure Societies* und *Sicherheitsforschung 2012-2017* weisen in dieser Hinsicht Parallelen auf.

*EU: "This Work Programme is about protecting our citizens, society and economy as well as our assets, infrastructures and services, our prosperity, political stability and well-being. Any malfunction or disruption, intentional or accidental, can have detrimental impact with high associated economic or societal costs" (Europäische Kommission 2015b: 7, Herv. d. Verfin.)*

*Deutschland: „Sicherheit ist die Basis eines freien Lebens und ein wichtiger Faktor des wirtschaftlichen Wohlstandes in Deutschland. Wenn wir auch in Zukunft die individuelle Freiheit, die Unversehrtheit aller Bürgerinnen und Bürger und lebenswichtige staatliche und wirtschaftliche Infrastrukturen wirksam schützen wollen, müssen wir nach neuen Wegen und Lösungen suchen.“ (BMBF 2016e: 8), Herv. d. Verfin.)*

Im Programm der EU werden als erstes Referenzobjekt „our citizens“, also die Bürger\*innen der Europäischen Union angeführt. Sie stehen jedoch gleichberechtigt neben der Wirtschaft, Infrastrukturen ohne das Adjektiv „kritisch“, ökonomischem Wachstum und Wohlstand, die als direkte Referenzobjekte miteinbezogen werden. Im deutschen Programm werden die Wirtschaft und der Wohlstand nicht explizit als Referenzobjekte ausgewiesen. Sicherheit wird jedoch als Bedingung „eines freien

Lebens“ dargestellt, deren Ergebnis auch „wirtschaftlicher Wohlstand“ ist. Sie werden auf diese Weise diskursiv miteinander in Beziehung gesetzt.

#### **4.1.4 Sicherheitsakteure**

Im deutschen wie im österreichischen Sicherheitsforschungsprogramm wird der Staat als Gewährleister ziviler Sicherheit grundsätzlich nicht in Frage gestellt. Innere Sicherheit wird als eine Aufgabe des Staates gegenüber der Bevölkerung festgeschrieben:

*Österreich:* „Sicherheit ist in vielfältigen Ausformungen *Kernkompetenz staatlicher Souveränität* (innere Sicherheit, äußere Sicherheit, soziale und wirtschaftliche Sicherheit und Stabilität, etc.). Ein Nationales Sicherheitsforschungsprogramm hat daher die Unterstützung der für die Sicherheit verantwortlichen Institutionen in Österreich bei der Erfüllung dieser Aufgaben zu berücksichtigen.“ (bmvit 2015a: 8; Herv. d. Verfin.)

*Deutschland:* „Die Bürgerinnen und Bürger vor Gefahren zu schützen und für ihre Sicherheit Sorge zu tragen, *ist eine der Kernaufgaben staatlichen Handelns*. Dies gilt insbesondere mit Blick auf Risiken und Großschadenslagen, die durch Naturkatastrophen – wie Hochwasserlagen oder Stürme – oder durch technisches und menschliches Versagen verursacht werden.“ (BMBF 2016e: 21; Herv. d. Verfin.)

Das Programm der Europäischen Union unterscheidet sich in dieser Hinsicht nicht maßgeblich. Wenngleich nicht von nationalstaatlichem Handeln die Rede ist, so wird unter die Bezugnahme auf die Privatisierung öffentlicher Infrastrukturen hervorgehoben, dass deren Schutz in der Verantwortung der öffentlichen Hand liegen: “Whilst many infrastructures and services are privately owned and operated, protection of public safety and security are the responsibility of the public authorities” (Europäische Kommission 2015b: 7).

Das deutsche und das österreichische Programm unterscheidet sich besonders dahingehend, wer über die Kernkompetenz staatlichen Handelns hinaus als Player im Bereich Sicherheit adressiert wird. Im deutschen Programm wird der Schritt unternommen, die Verantwortlichkeit für die zivile Sicherheit – auf eine breitere Basis im Sinne einer geteilten Verantwortung und Zuständigkeit anzusiedeln. Als Akteure der zivilen Sicherheit werden regelmäßig *Staat, Wirtschaft* und *Gesellschaft* genannt und die Herausforderungen adressiert, vor denen „staatliche wie private Sicherheitsakteure“ stehen (BMBF 2017: 10). Diese breite Ansprache erfolgt unter

der erklärten Zielsetzung, mit der zivilen Sicherheitsforschung auch einen Beitrag zur Hightech-Agenda 2020 zu leisten und „den Markt für Sicherheitstechnologien und -dienstleistungen weiterzuentwickeln, sodass innovative deutsche Unternehmen sowie forschende Einrichtungen von diesem boomenden Markt profitieren können“ (BMBF 2017: 13). Im österreichischen Programm heißt es im Vergleich dazu wie folgt: „Sicherheit im Sinne von ‚security‘ ist – im Gegensatz zu ‚safety‘ – ein öffentliches Gut, für dessen Bereitstellung primär die öffentliche Hand zu sorgen hat und für das es daher keinen ‚freien‘ Markt im klassischen Sinne gibt.“ (bmvit 2015a: 7).

Das deutsche und das österreichische Programm unterscheiden sich in maßgeblich dadurch, dass KIRAS der Fokus auf einer Förderung der „heimischen Sicherheitswirtschaft“ (da auch private Unternehmen und Dienstleister\*innen) durch eine öffentliche Bedarfsträger\*innen liegt und nicht von langfristigen Kooperationen ausgegangen wird. Im deutschen Programm hingegen wird eine Sicherheitsarchitektur proklamiert, durch die öffentliche wie private Akteure im Zuge öffentlich-privater „Sicherheitspartnerschaften“ langfristig profitieren sollen (BMBF 2016e).

#### **4.1.5 Forschungsbegriff**

Was die Vorstellung anbelangt, unter welchen Rahmenbedingungen Wissen und Technologie für den Bereich zivile Sicherheit hergestellt werden soll, sind die Programme weitgehend homogen. *Anwendungsorientiertheit, Transdisziplinarität*, die Einbindung von sogenannten *Stakeholdern* oder *Bedarfsträgern*, die gezielte Förderung von Klein- und Mittelunternehmen (*KMUs*) als Projektträger sowie *die kommerzielle Verwertbarkeit* der produzierten Technologien sind Ziele, die in allen drei Programmen an die Forschung herangetragen werden.

*Österreich:* „Sicherheitsforschung ist vor diesem Hintergrund technologieoffen, interdisziplinär und missionsorientiert. Die beforschten Lösungen/Technologien sind eingebettet in den politisch-strategischen Gesamtkontext (z.B. Forschungs- und Technologiepolitik, Sicherheitspolitik, Industrie- und Wirtschaftspolitik).“ (bmvit 2015a: 6)

*Deutschland:* „Im Rahmenprogramm werden mit Hilfe eines interdisziplinären Ansatzes verschiedene Sichtweisen von Akteuren aus Wissenschaft, Wirtschaft und Praxis einbezogen. So entwickeln Kooperationspartner aus den Natur-, Ingenieur- und Gesellschaftswissenschaften gemeinsam mit Anwendern wie der Feuerwehr, Polizei oder

Flughafenbetreibern neue Konzepte, um unser Leben sicherer zu machen. Vorrangig werden Forschungsthemen bearbeitet, die eine enge fachübergreifende Zusammenarbeit mehrerer wissenschaftlicher Disziplinen erforderlich machen.“ (BMBF 2016e: 2)

*EU:* “[T]his Work Programme addresses both private companies/industry and institutional stakeholders. [...] The expected outcomes will result in a faster transposition of the research results into commercial products or applications responding to well identified needs by the end-users, be it market operators, law enforcement agencies, border guards, first responders or the citizens.” (Europäische Kommission 2015b: 7)

Darüber hinaus gibt es jedoch jeweils einige Spezifika der einzelnen Programme, die im Folgenden beleuchtet werden sollen. Das Alleinstellungsmerkmal von KIRAS ist die Vorgabe, sogenannte „GSK-Expertise“ in alle Projekte verpflichtend zu inkludieren:

„Die verpflichtende Einbindung von GSK-Expertise in jedem einzelnen Projekt gewährleistet, dass KIRAS auf einer breiten Basis steht und technologische Forschungsergebnisse von Beginn an auf ihre Angemessenheit, gesellschaftliche Akzeptanz und Anwendbarkeit (z.B. Nutzerperspektive) geprüft werden“ (bmvit 2015a: 12).

GSK-Expertise wird dabei weit definiert als „Sammelbegriff für alle wissenschaftlichen Disziplinen [...], welche die Gesellschaft oder Teile davon als Gegenstand ihrer Forschung berühren“ (BMVIT 2015: 13). Im deutschen Programm ist die Ausrichtung ähnlich, jedoch nicht auf verpflichtender Basis. Die Einbindung „gesellschaftswissenschaftlicher Forschung“ wird mit einer „ganzheitlichen“ und anwendungsorientierten Sicherheitsforschung kausal in Beziehung gesetzt:

„Für die Erarbeitung ganzheitlicher und umsetzungsfähiger Sicherheitslösungen ist es notwendig, alle relevanten Disziplinen aus den Technik-, Natur- und Gesellschaftswissenschaften einzubinden und auf gemeinsame Anwendungsziele auszurichten. Deswegen ist es unser ausdrückliches Ziel, die Inter- und Transdisziplinarität in den Projekten vor allem durch die gleichberechtigte Integration gesellschaftswissenschaftlicher Forschung zu fördern.“ (BMBF 2016e: 29)“

Die Besonderheit des deutschen Programms ist indes die generelle Vorgabe einer sogenannten „systemischen“ (BMBF 2016e: 13, 39) und „szenariorientierten“ (ebda. 29) Forschung und der gleichzeitigen Bedingung, „isolierte Einzellösungen“ zu vermeiden (ebda.: 30, siehe auch BMBF 2016a).

„Die Szenariorientierung vermeidet isolierte Einzellösungen. Sie ermöglicht anwendungsnahe Systeminnovationen, aus denen sich praxistaugliche Sicherheitsprodukte und -dienstleistungen erfolgreich entwickeln lassen, die sich am Bedarf der Endnutzer orientieren und zu einer freiheitlichen Gesellschaft passen.“ (BMBF 2016e: 30)

#### **4.1.6 Strategische Ziele**

In den Forschungsrahmenprogramm wurden neben konkreten Forschungsvorhaben und -zielen auch übergeordnete strategische Zielsetzungen formuliert. Wissenschafts-, wirtschafts-, technologie- und innovationspolitische Ziele gesellen sich dort zum sicherheitspolitischen Aspekt. Deren Formulierung gibt zusätzlichen Aufschluss über die Ausrichtung und angestrebte Reichweite der Programme.

Ein wiederkehrendes Narrativ im Programm des Bundesministeriums für Bildung und Forschung ist die Positionierung Deutschlands sowohl als führende Industrienation Europas als auch als wichtigste politische Kraft innerhalb der Europäischen Union, deren Ziel es dementsprechend nur sein kann, im Bereich der zivilen Sicherheit neue Maßstäbe zu setzen und eine Führungsrolle zu übernehmen: „Ziel des Rahmenprogramms ist es, die wirtschaftlichen Chancen der zivilen Sicherheitsforschung zu nutzen und Deutschland als führenden Anbieter von Sicherheitstechnologien zu etablieren“ (BMBF 2016e: 4).

Mit der nationalen Forschung soll sowohl der eigene als auch der europäische Sicherheitsdiskurs geformt werden: „Ziel der Forschung ist es, unter Einbeziehung rechtlicher, sozialer und ökonomischer Dimensionen die Entwicklung und Veränderung ziviler Sicherheitslösungen, -kulturen und -architekturen proaktiv mitzugestalten“ (BMBF 2016e: 4).

In einer Ausschreibung, die sich aufgrund einer aktuell laufenden bilateralen Kooperation zwischen Deutschland und Österreich in beiden Programmen findet, ist lediglich in der deutschen Bekanntmachung der Satz zu lesen: „Österreich und Deutschland wollen mit ihrer bilateralen Kooperation bei der Sicherheitsforschung nicht nur die zukünftige nationale Sicherheit stärken, sondern auch einen Beitrag zur europäischen Sicherheitsarchitektur leisten“ (BMBF 2015). Angestrebt wird aus deutscher Sicht „die Entwicklung und Harmonisierung europäischer Lösungen und Märkte“ (BMBF 2016e: 40) durch „deutsche Akteure mit ihren innovativen Ideen“ (ebda.).

KIRAS ist im Vergleich dazu weniger exportorientiert. Als Ziel 4 wird „ein Wachstum der heimischen Sicherheitswirtschaft“ angestrebt, die Investitionen sollen einen Beitrag zur „österreichischen Wertschöpfung“ leisten und „Arbeitsplätze in Österreich

zu schaffen bzw. zu sichern“ (BMVIT 2015: 8). Eine expansive Rolle Österreichs in der Gestaltung der europäischen Sicherheitsarchitektur wird nicht angestrebt – und würde im Widerspruch zu der Vorgabe stehen, dass nur Projekte einen „klaren Österreich-Bezug“ haben müssen, um die Förderkriterien zu erfüllen (ebda.: 11).

Der strategische Fokus von Secure Societies liegt deutlich erkennbar im Bereich der Digitalen Sicherheit, wobei der Ton im Vergleich zum deutschen *Sicherheitsforschungsprogramm* einen bescheiden ist. In Call „Digital Security“ heißt es, dass *Secure Societies* einen Beitrag dazu leisten wird, den europäischen „Single Market for cybersecurity products“ zu promoten. Dabei wird auf die Europäische Strategie für Cybersicherheit verwiesen (Europäische Kommission 2015b: 94).

## 4.2 Resilienz

Alle drei Programme haben das Thema Resilienz als sicherheitspolitische Perspektive und praxisorientiertes Feld der Sicherheitsforschung in ihre Ausschreibungen integriert. Das Grundverständnis von Sicherheit und Unsicherheit, das mit einer Resilienz-orientierten Sichtweise auf Gefahren und Bedrohungen einhergeht, ist dabei in allen Programmen ähnlich. Was darunter zu verstehen ist und welche Besonderheiten und Schwerpunkte darüber hinaus mit Maßnahmen einhergehen, die der Kategorie „Resilienz“ zuzuordnen sind, soll im folgenden Kapitel erläutert werden.

### **4.2.1 „Lernende Sicherheit“: Zyklische Betrachtungen von Gefahren und Risiken**

Die Integration von Resilienz in das Portfolio der Sicherheitsforschung zieht in allen drei Programmen die Wirkung nach sich, dass die Periode des „Danach“ im Kontext ziviler Sicherheit – also die Phase nach Schadenseintritt im Krisenmanagement und der Notfallplanung – quantitativ erheblich an Bedeutung gewinnt. Die Fokussierung auf das „Danach“ erfolgt jedoch nicht im Sinne einer Verdrängung oder Ersetzung des „Davor“, sondern im Zuge einer *zyklischen* Betrachtung von Gefahren, die in allen Programmtexten im Kontext von Resilienz zum Ausdruck gebracht wird (vgl. (Europäische Kommission 2017b; bmvit 2014; BMBF 2014b). In diesem als „Resilienz-Zyklus“ bezeichneten Kreislauf werden Prävention und Vorsorge nicht als ideologische Gegenspieler der Reaktion und Nachsorge präsentiert, sondern als zusammenhängende Teile eines Ganzen, das zu einer nachhaltigen und realitätsnahen Einschätzung und Bewältigung von Krisenfällen beitragen soll. Das „Danach“ tritt dabei als Dimension des Möglichen in Erscheinung, auf das es sich einzustellen gilt, durch das das „Davor“ jedoch nicht suspendiert oder herabgewertet wird. In den jeweiligen Programmen liest sich dies wie folgt:

*EU: Research on risk awareness should encompass the whole of the disaster management cycle, from prevention (e.g. through education) and preparedness (knowing how to react), emergency management (collaboration and communication before and during an event), response (empowering citizens to act efficiently by themselves according to more effective practices and following established guidelines), and recovery (knowledge to build back better).” (Europäische Kommission 2017b: 20)*

*Deutschland:* „Resilienz beschreibt im Zusammenhang mit der zivilen Sicherheit die Fähigkeit, sich auf bekannte wie unbekannte Krisen- und Katastrophenszenarien vorzubereiten, diese möglichst im Vorfeld zu verhindern, sich von einem potenziell entstandenen Schaden schnell zu erholen und die gesammelten Erfahrungen wieder in die Vorbereitung einfließen zu lassen. Resilienz stellt somit eine der Schlüsselkompetenzen der zivilen Sicherheit dar.“ (BMBF 2014b)

In KIRAS wird dieser Zyklus in zwei Phasen unterteilt, in jene *vor Schadenseintritt*, dazu gehört „Bewusstseinsbildung“, „Ereignisantikipation“, „Vorbeugung“ sowie jene *nach Schadenseintritt*, das sind „Reaktion auf Schadenseintritt“, „Rekonstruktion“ und „Konsolidierung“ (bmvit 2014: 10).

Einerseits bedienen sich sowohl Deutschland als auch Österreich einer Definition von Resilienz, deren Ziel es sein soll, nach einem schadhafte Ereignis zum Ursprungszustand zurückzukehren.

*Deutschland:* „Die Förderrichtlinien sollen einen Beitrag dazu leisten, die Vorsorge für und die Vermeidung von Krisen und Katastrophenlagen zu verbessern und zu deren Bewältigung und der Wiederherstellung des „Status-quo-ante“ beizutragen.“ (BMBF 2014b)

*Österreich:* „Wie kann der ursprüngliche Zustand schnellstmöglich wiederhergestellt werden?“ (bmvit 2014: 10)

*EU:* „Resilience concepts need also to take into account the necessity to anticipate, to plan and to implement in the crises time a substitution process aiming to deal with a lack of material, technical or human resources or capacities necessary to assume the continuity of basic functions and services until recovery from negative effects and until return to the nominal position.“ (Europäische Kommission 2015b: 18)

Zugleich finden sich jedoch Elemente der Anpassung und Veränderung, deren Ziel es sein soll, die systemische Widerstandsfähigkeit gegenüber schadhafte äußeren Einflüssen zu erhöhen, also den „status quo“ im Zuge von Lernprozessen aus vergangenen Krisen kontinuierlich zu verbessern.

*Österreich:* „Kann der ursprüngliche Zustand qualitativ im Hinblick auf einen erneuten Ereigniseintritt verbessert werden? [...] Wie kann der vor dem Eintritt des Ereignisses bestandene und nun wiederhergestellte Zustand technisch und organisatorisch möglichst langfristig aufrechterhalten werden?“ (bmvit 2014: 10)

*Deutschland:* „[...] Erfahrungsanalyse aktueller und vergangener Katastrophenereignisse inklusive best practice Auswertungen (sic!) und Rückspiegelung in die zukünftige Katastrophenvorsorgung“ (BMBF 2017a)

EU: "Expected impact: [...] a more resilient society by ensuring that cities are better prepared for and able to recover from emergencies." (Europäische Kommission 2015b: 40; Herv. i. O.)

Die zyklische Betrachtung führt dazu, dass sowohl Elemente der Anpassung und Veränderung als auch Elemente der Stabilisierung und Konservierung in die angestrebten konzeptionellen Umsetzungen von Resilienz integriert werden. Im deutschen Sicherheitsforschungsprogramm wird Resilienz als „ursprünglich aus der Kybernetik stammender Begriff“ definiert, „der die Toleranz oder Widerstandsfähigkeit eines Systems vor störenden äußeren Einflüssen beschreibt“ (BMBF 2016e: 51). In den anderen Programmen finden sich keine Bezugnahmen auf die Kybernetik, doch kann man sagen, dass sie insbesondere durch den zyklischen Aspekt von Resilienz mit der integrierten Feedback-Schleife durchaus Ähnlichkeiten zu Norbert Wiens Modell der Kybernetik aufweisen. So finden sich Parallelen zum kybernetischen „Regelkreis“ mit Lern- und Anpassungseffekten und dem Sich-Einstellen auf „bekannte wie unbekannte Katastrophen- und Krisenszenarien“ (BMBF 2014b), die eine systemische Veränderung bewirken (vgl. Brem 2018).

#### **4.2.2 Alle Gefahren – alle Kosten?**

Im theoretischen Teil wurde auf den „All-Gefahren-Ansatz“ hingewiesen, der als charakteristisch für Resilienz-bezogene Sicherheit gilt. Im vorherigen Kapitel wurde bereits klargestellt, dass sich alle drei Programmen auf eine Definition von Sicherheit stützen, die es erlaubt, eine Vielzahl heterogener Bedrohungen und Gefahren einzuschließen. Interessanter in Hinblick auf Unterschiede und Partikularitäten ist es möglicherweise, zu vergleichen, welche „Schäden“ mithilfe entsprechender Resilienz-Strategien und Resilienz-fördernden Maßnahmen verhindert oder abgemildert werden sollen.

Im österreichischen Programm dem bereits zuvor erwähnten Krisenmanagement im Kontext eines präventiv ausgerichteten Schutzes kritischer Infrastrukturen gegen Bedrohungen der Zukunft (mehr dazu in 4.6.2) und der Radikalisierungs-Prävention eine Rolle (mehr dazu in 4.3.3.).

Im deutschen Programm werden im Zusammenhang mit Resilienz schaffenden Maßnahmen nicht nur der Schutz des menschlichen Lebens, sondern auch die

„materiellen und sozialen Auswirkungen“ integriert, die Schadensereignisse und Katastrophen nach sich ziehen können:

„Ziel der Forschung ist, auf Basis der Analyse der Interdependenzen in einer Stadt oder Region, die materiellen und sozialen Auswirkungen von Schadensereignissen und Katastrophen zu begrenzen und die Fähigkeiten, auf solche Ereignisse zu reagieren, zu steigern.“ (BMBF 2012c)

Im Secure Societies erfolgt der Hinweis/Fokus auf sogenannte „sozioökonomische Kosten“, die über die unmittelbare Sicherung des Lebens im Notfall weit hinausgehen, noch häufiger und expliziter artikuliert. So heißt es zu den Zielen des Disaster Resilience Calls allgemein: “The objective of this call is to reduce the loss of human life, environmental, economic and material damage from natural and man-made disasters, including extreme weather events, crime and terrorism threats.” (Europäische Kommission 2015b: 9). Der “loss of human life” führt die Aufzählung zwar an, wird jedoch mit Umwelt-, ökonomischen und materiellen Schäden konjugiert. Dieser „All-Schadens-Ansatz“ wird in der Folge in vielen Ausschreibungen erneut artikuliert. Mehrfach wird daran die Erwartung geknüpft, bei „policy makern“ ein neues, nachhaltigeres Bewusstsein auf Gefahren und Krisen zu entwickeln. So zum Beispiel in einer Ausschreibung für Maßnahmen zur Verbesserung des Schutzes sogenannter „Seveso sites“ (daran sind – angelehnt an das Sevesounglück – Unternehmen, in denen mit hochgiftigen Gefahrenstoffe gearbeitet wird):

„Expected impact: [...] enhanced understanding by policy-makers and other stakeholders on how multiple sectors, community, region or nation could be affected in total by an accident from a Seveso site/area, and what the total impact might be (material, human, economic).“ (Europäische Kommission 2015b: 31; Herv. i. O.)

An anderer Stelle wird die Bedingung formuliert, dass in das Modell eines zu entwickelnder „Critical infrastructure resilience indicator“ auch „ökonomische Indikatoren“ integriert werden:

“The proposal shall demonstrate that a set of common and thoroughly validated indicators, including economic indicators, could be applied to critical infrastructures in order to assess its level of “resilience”, moreover a scale approach of “resilience” level should be proposed across critical infrastructures (energy grids, transportation, government, nuclear research infrastructures, water, etc.).“ (Europäische Kommission 2015b: 29)

Zugleich wird der “holistische” Zugang im Kontext des Schutzes kritischer Infrastrukturen besonders hervorgehoben:

„A holistic approach to the resilience of critical infrastructure should be followed, addressing a broad variety of issues including: human factors (i.e. safety issues radicalization), security, geo-politics, sociology, economy, etc. and increased vulnerability due to changing threats.” (ebda.)

Resilienz wird in *Secure Societies* als eine Art Sicherheitsmethode der Zukunft präsentiert, durch die der Blick für langfristige Entwicklungen und mögliche Risiken neuer Technologien geschärft werden soll – weshalb zu einem Paradigmenwechsel im Sicherheitsdenken angeregt wird:

“The analysis of resilience should therefore not only focus on potential threats caused by attacks or accidents (human error or terrorist/criminal attacks), but also on the expected developments in these areas and the impacts and potential challenges of new technologies. Proposals should also address the need for a paradigm shift in the area of design for safety and resilience.” (ebda.)

#### **4.2.3 Die Rolle der Bevölkerung**

Welche Rolle spielt die Bevölkerung in den jeweiligen Programmen? In keinem der Ausschreibungsdokumente wird der Anspruch formuliert, dass die Operationalisierung resilienzorientierter Maßnahmen mit einem Rückzug des Staates bzw. einer (teilweisen) Befreiung des Staates von der Verpflichtung des Bevölkerungsschutzes einhergehen soll. Im Gegenteil zielen zahlreiche Forschungsvorhaben auf die Entwicklung von Technologien ab, die im Krisenmanagement gerade die Einsatzfähigkeit der sogenannten „first responder“ verbessern und unterstützen soll (siehe z.B. Europäische Kommission 2015b: 15, 36; bmvit 2014: 15f.; BMBF 2016c). Wo die Einbindung der Bevölkerung als Ziel formuliert wird, erfolgt dies in der Regel auf „passive“ Art, nämlich dahingehend, wie Menschen auf *informationeller* Ebene in die Krisenkommunikation optimal einbezogen werden können, um Schäden zu verhindern oder zu begrenzen. In allen drei Programmen stehen Krisenkommunikation, Aufklärungs- und Informationsarbeit (unter anderem der sinnvolle Umgang mit modernen IKT und Sozialen Medien) sowie die optimale Einbindung freiwilliger Helfer\*innen im Vordergrund.

Darüber hinausgehend finden sich im Programm der Europäischen Union sowie im deutschen Sicherheitsforschungsprogramm einige Elemente, die zumindest in der Theorie auf das im Ereignisfall aktiv handelnden Individuum hinauswollen: „Die Bevölkerung soll nicht länger nur als Betroffene einer Krise betrachtet, sondern auch

als Akteur in die Krisenvorsorge und –bewältigung mit einbezogen werden,“ (BMBF 2014b) heißt es da in Sicherheitsforschung 2012-2017, wo mehrfach von der Verbesserung bzw. Erhöhung der „Selbsthilfefähigkeit“ (BMBF 2013, 2014c, 2014b) sowie vom „Aufbau von Sicherheitskompetenzen in der Gesellschaft“ (BMBF 2016e: 8) die Rede ist.

„Dazu gehört auch, die Bevölkerung sowie die Strukturen und Prozesse so vorzubereiten, dass sie weniger verletzlich gegenüber Schadensereignissen sind, dass sie auf unvorhergesehene kritische Situationen reagieren können und besser in der Lage sind, mit unsicheren Situationen und nicht vorhergesehenen Ereignissen umzugehen.“ (BMBF 2012c)

Konkrete Forschungsziele gehen jedoch nicht über die bereits erwähnten Themenkomplexe hinaus, sondern betonen immer die gesamtstaatliche Verpflichtung zur Gewährleistung von Sicherheit:

„Es gehört zu den gesamtstaatlichen Aufgaben von Kommunen, Ländern und Bund Sicherheit zu gewährleisten und Vorkehrungen zu treffen, dass die Bürgerinnen und Bürger auch im Krisen- und Katastrophenfall bestmöglich geschützt und versorgt werden.“ (ebda.)

Auch in Secure Societies gibt es Narrative, in denen vorgebracht wird, dass nicht Exekutive und Justiz allein für die Sicherung der Gesellschaft zuständig sein sollen. So heißt es in einem Sub-Call im Bereich Urban Security: „[T]here is a growing need to go beyond the idea that only the law enforcement and criminal justice systems are tasked to tackle urban security challenges.“ Was das „citizens’ engagement“ anbelangt, so heißt es dann, dass in erster Linie „innovative solutions, including sustainable, affordable and transferrable security technologies“ (Europäische Kommission 2015b: 61) dabei helfen sollen, den Bürger\*innen zur Seite zu stehen..

Gleichzeitig kann jedoch nicht stichhaltig argumentiert werden, dass in Secure Societies auf diesem Gebiet darauf abgezielt würde, Exekutivarbeit gegen Überwachungstechnologien zu tauschen und die Bürger\*innen unterstützt durch diese Technologien ihrem Schicksal zu überlassen. Denn an anderer Stelle wird nach Strategien verlangt, wie die Exekutive für eine bessere Beziehung und Zusammenarbeit auf durch das sogenannte „community policing“ sorgen soll. Hier wird der Einsatz von mehr Polizist\*innen auf der Straße verlangt: „Individual police inspectors are encouraged to spend considerable time and effort in developing and maintaining personal relationships with citizens and different community

organizations” (Europäische Kommission 2015b: 65). Die Verantwortung bleibt dabei bei der Exekutive und wird nicht an die Bürger\*innen abgetreten:

“Early identification, timely intervention, as well as better crime reporting, identification of risks, unreported and undiscovered crime through the community. Strengthened and accelerated communication between citizens and police forces. Overall, strengthened community feeling and lower feeling of insecurity.” (ebda.)

#### **4.2.4 Klimawandel-Adaption**

Wie bereits im theoretischen Teil dargelegt wurde, hat sich das Kontinuum an Gefahren und Risiken, auf die im Kontext ziviler oder innerer Sicherheit referiert wird, in den letzten Jahrzehnten sukzessive erweitert. Während in der Vergangenheit lediglich auf wahrscheinliche Symptome des Klimawandels als Referenzobjekte hingearbeitet wurde (Lawinen, Überschwemmungen, Erdbeben u.v.m., siehe dazu z.B. in den Ausschreibungen zu FP7, vgl. Europäische Kommission 2012), so hat sich in der jüngsten Vergangenheit der „globale Klimawandel“ zusehends selbst als ursächliche Bedrohung, die es auch aus einer sicherheitspolitischen Perspektive zu betrachten gilt, im globalen politischen Diskurs durchgesetzt<sup>3</sup>. Die drei zur Analyse ausgewählten Programme schließen sich dieser Auffassung an. In Sicherheitsforschung 2012-2017 heißt es dazu: „Aktuelle Forschungsergebnisse zeigen, dass auch in Deutschland die Folgen des Klimawandels zu einer Zunahme witterungsbedingter Naturkatastrophen führen können“ (BMBF 2016e: 22). In *Secure Societies* erfolgt erneut ein rhetorischer Appell an europäische und nationale Politiker\*innen, den Klimawandel als Sicherheitsbedrohung ernstzunehmen: „European policy makers and analysts as well as national governments should tackle climate change as today's non-traditional security hazard“ (Europäische Kommission 2015b: 40).

Anschließend wird der Klimawandel insbesondere im Kontext Resilienz bildender und stärkender Maßnahmen adressiert. Wie stark dabei der als Ursache genannte

---

<sup>3</sup> US-Präsident Donald Trump teilt diese Auffassung bekanntlich nicht. Er hat den Klimawandel von der Liste der globalen Bedrohungen aus der amerikanischen National Security Strategy streichen lassen (Borger 2017).

Klimawandel als zu bekämpfende Bedrohung tatsächlich in den Blick genommen wird, variiert jedoch erheblich. KIRAS tanzt hier durch eine „Insellösung“ und kreativen Überlegungen „zum Erreichen der staatlichen Klimaschutzziele“ (bmvit 2016) aus der Reihe (bmvit 2016). In Auftrag gegeben wird eine Studie, in der geprüft werden soll, inwieweit sich die Arbeit von Blaulichtorganisationen in Zukunft mit mobilbetriebenen Fahrzeugen bewerkstelligen lassen würde (vgl. ebda. 22f.)

Für das deutsche und das europäische Forschungsprogramm gilt, dass das eigentliche Target der Forschung nicht der Klimawandel ist, sondern dessen potenzielle gegenwärtige und zukünftige Auswirkungen. Diese werden dennoch als Symptome des Klimawandels bzw. als “climate-change related” artikuliert (Europäische Kommission 2015b: 22). In diesem Zusammenhang spielen *Adaption* – an die sich verändernden ökologischen Bedingungen – und eine davon erwartete regional-spezifische Vulnerabilitätsreduktion die größte Rolle. Das deutsche Programm widmet seine einzige Ausschreibung in dem Bereich Katastrophen, die – auf globaler Ebene – also außerhalb des deutschen Territoriums eintreten könnten. Gemäß des SENDAI Framework for Disaster Risk Reduction wird nach Maßnahmen gesucht, die dem Internationalen Katastrophenmanagement mit Partnerländern in Afrika und Asien zum Einsatz kommen sollen. Hervorgehoben wird dabei sowohl die menschlichen Opfer als auch die volkswirtschaftlichen Schäden, die es zu vermeiden/verringern gelte: „Naturereignisse wie Erdbeben, Überschwemmungen, Erdrutsche, Stürme, Dürren, aber auch technische Schadenslagen bedrohen Millionen Menschen und verursachen weltweit immense volkswirtschaftliche Schäden“ (BMBF 2017a). Ziel der Kooperationen sei die Reduktion der Verletzlichkeit und die damit einhergehende Erhöhung der Sicherheit:

„Die angestrebten Forschungs- und Entwicklungsprojekte sollen wirkungsvolle Impulse geben, um die Verletzlichkeit gegenüber Naturkatastrophen und technischen Risiken in den Partnerländern zu reduzieren und die Sicherheit für die Bevölkerung zu erhöhen.“ (ebda.)

Interessant ist, dass sich im Programm der Europäischen Union ähnliche Vorhaben finden, diese jedoch explizit mit einer territorialen Sicherheitslogik verknüpft werden. Dies erfolgt dadurch, dass die Gefahr von global von möglichen Klimakatastrophen betroffene Menschen mit dem Thema Migration verknüpft wird und die potenziellen Opfer solcher Katastrophen gleichzeitig als Bedrohung für den Schengen-Raums konstituiert werden. Im Programm der EU wird der Beitrag zur Katastrophenhilfe nicht

als „end in itself“ im Sinne der menschlichen Sicherheit konstituiert, sondern als gleichzeitiger Beitrag zur territorial begrenzten Inneren Sicherheit des EU-Raumes: “[C]limate-driven crises occurring outside the EU can have detrimental effects and direct or indirect security implications on the Union (e.g. climate-driven migration forcing large number of people to move from their homelands to another country“ (mehr dazu in Kapitel 4.4.2).

### 4.3 Terrorismus

Innenpolitische Maßnahmen der Terrorismusbekämpfung sahen sich im ersten und zweiten Jahrzehnt der 2000er-Jahre der Kritik der überschießenden proaktiven Massenüberwachung (mit den USA als einseitigen Profiteurinnen) ausgesetzt. Die Innenpolitik der frühen 2010er-Jahre hat einen starken an persönlichen Freiheits- und Datenschutzrechten orientierten Gegendiskurs hervorgebracht, der nicht nur zur teilweisen Verhinderung, Entschärfung oder Außerkraftsetzung konkreter Anlassgesetzgebungen geführt hat, sondern auch dazu beigetragen hat, dass „Anti-Terror“ als Sprechakt der Versicherheitlichung in Folge dessen auch aus politischer Sicht an Anziehungskraft verloren hat. Die Kritik machte auch vor der Sicherheitsforschung nicht Halt. So war vom „security theme“ des 7. Forschungsrahmenprogramms aufgrund einiger Projekte als „Überwachungsprogramm“ die Rede (Schumann und Simantke 2016) und in Deutschland werden Projekte, die im Rahmen der ersten, bis 2012 laufenden Programmphase entstanden sind, und nun vor der politischen Umsetzung stehen, kontinuierlich von einer kritischen Medienöffentlichkeit begleitet.

In den Ausschreibungen der für diese Arbeit zum Vergleich ausgewählten Programme nimmt der Terrorismus gegenüber anderen als gesellschaftlich definierten Bedrohungen und Risiken keine Sonderstellung ein. Er wird zwar in allen drei Programmen als eigene Kategorie angeführt und ist insofern nach wie vor prominent vertreten, jedoch als mögliches Risiko neben weiteren, denen quantitativ im Sinne der „All-Gefahren“-Perspektive gleiche Aufmerksamkeit geschenkt wird.

#### ***4.3.1 Datenmanagement, Data Mining, (transnationaler) Datenaustausch***

Ein großer Teil der Ausschreibungen in der Kategorie „Terrorismusbekämpfung“ befasst sich mit der Sichtung, dem Management und der elektronischen Weitergabe von Daten aus dem Internet als Fahndungsmaterial sowie als Beweismaterial vor Gericht. Das Element der „Automatisierung“ – also das Durchkämmen des Internets und/oder großer Datensätze mithilfe künstlicher Intelligenz – findet sich dabei in allen drei Programmen wieder. Unterschiede finden sich dahingehend, für welchen Zweck die Verwendung dieser Technologien angestrebt wird.

In Secure Societies wird der Ruf nach automatisierten Methoden in ein Narrativ der Notwendigkeit eingebettet, die sich aus der Benutzung des Internet durch global vernetzte Terrorzellen und einem damit einhergehenden Informationsüberfluss ergebe: „In order to cope with the dangers involved in the use of Internet by global terrorist organizations and grassroots terrorist cells, more efficient and effective automated techniques are required“ (Europäische Kommission 2015b: 56).

Der Nutzen einer solchen Technologie wird damit begründet, dass beim entscheidenden Faktor „Zeit“ ein Fortschritt erzielt werden könne: „The developed methodologies should be able to handle massive amounts of multilingual and multimedial web content in minimal time“ (ebda.). Darüber hinaus würde durch die automatisierte Filterung und Zusammenfassung entsprechende Inhalte der „information overload“ (ebda.: 49) der „web intelligence experts“ (ebda.: 57) reduziert. In Secure Societies wird der Einsatz dieser Technologien auch zur Prävention terroristischer Anschläge vorgesehen: „More effective prevention of terrorist activities planned and organized via the Internet through automated analysis of terrorist-generated content“ (ebda.).

Im Programm der EU wird das Thema vorbehaltlos adressiert, Ziel ist es, durch die „automatisation of as many steps as possible“, die „capabilities of man and machine“ (Europäische Kommission 2015b: 50) optimal zu nützen. Erklärungen, inwieweit die Arbeit zwischen „man“ und „machine“ aufgeteilt werden soll und an welchen Punkten der automatisierten Suche menschliche Kontrollen vorgesehen sind, bleiben dabei aus.

“The main challenges are the automation of as many analysis steps as possible; the countering of the obfuscation used by the attacker. The finding of an efficient way to identify an attacker despite use of anonymisation, performing automatic deep analysis of all data in the offense, and making optimal use of the capabilities of man and machine.” (Europäische Kommission 2015b: 50)

Im deutschen und österreichischen Programm ist man auf diesem Gebiet aufgrund der Antizipation verfassungs- und datenschutzrechtlicher Bedenken vorsichtiger: Im deutschen Programm heißt es dazu klar, dass die automatisierte Software „nach einem Anschlag bei der Aufklärung und Strafverfolgung unterstützen“ soll, da Zeit „bei der Ermittlung ein kritischer Faktor“ sei (BMBF 2015). Auch in KIRAS ist diese Einschränkung aufrecht, jedoch wird ihr mit einer Ausschreibung begegnet, die eine

Evaluierung zum Ziel hat, ob der Einsatz entsprechender Technologien „vor einem potenziellen Anschlag“ (bmvit 2015b: 24) unter rechtlichen und ethischen Gesichtspunkten denkbar wäre. In diesem Zusammenhang wird abschwächend die Formulierung „semiautomatische Suche und Analyse“ gewählt und wie die „Verknüpfung und Aufbereitung der Daten zur Entscheidungsunterstützung“ beitragen könne (ebda.: 25). In einer späteren Ausschreibung heißt es dann allerdings: „Eine gezielte Beobachtung und automatisierte Auswertung von Inhalten in sozialen Medien zur frühen Erkennung von Radikalisierungspotenzial und von Rekrutierungsaktivitäten von Terrororganisationen für bewaffnete Konflikte ist erforderlich (bmvit 2016: 9).

Das Thema des Austauschs von Daten als Beweismaterial oder zum Zweck der Strafverfolgung wird in Secure Societies unter vielen anderen Punkten im Kontext der Terrorismusbekämpfung ebenfalls beleuchtet. Technologisches Ziel ist hier lediglich, den Austausch auf technischer Ebene durch Harmonisierungen und bessere Standardisierungen zu verbessern und auf diese Weise „improved capabilities for trans-border LEA data-exchange and collaboration“ zu schaffen (Europäische Kommission 2015b: 50). Auf die Einhaltung rechtlicher Vorschriften sowie den Schutz persönlicher Daten wird dabei hingewiesen: „Expected impact: harmonisation of information formats at international level, improved cross-border acceptance and exchange of court-proof evidence, standardised evidence collection and harmonised procedures in the investigation of trans-border crimes in full compliance with applicable legislation on protection of personal data (Europäische Kommission 2017b: 33; Herv. i. O.).

#### **4.3.2 Terror im Zusammenhang mit anderen Delikten**

Secure Societies sticht dadurch hervor, dass ausgeschriebene Maßnahmen in der Kategorie Terrorismusbekämpfung zumeist mehr als nur diesem einem Zweck dienlich sein sollen. Der Titel des Sub-Calls „Fight Against Terrorism and Crime“ (vgl. Europäische Kommission 2015b, 2017b, 2017a) versucht dies nicht zu verschleiern, die Offenheit des Begriffs „Crime“, der ja theoretisch alle strafbaren Handlungen umfasst, wirft jedoch die Frage auf, in welche Richtung diese „Überstreckung“ im Sinne der Artikulation des „Terrorismus“ auf einem Kontinuum mit anderen Delikten vollzogen wird. In Secure Societies lautet die Antwort häufig „Cyber“: „cybercrime“

und „cyber-terrorism“ (die Begriffe werden nicht näher spezifiziert, aber meistens zusammen genannt – siehe Beispiel unten), darunter Delikte im Bereich der Wirtschafts- und Finanzkriminalität werden häufig im Kanon der Bedrohungen/Risiken gelistet, die mithilfe einer u.a. der Terrorismusbekämpfung dienlichen Maßnahme mitadressiert werden sollen.

“The ambition of this call is both to avoid an incident and to mitigate its potential consequences. This requires new technologies and capabilities for fighting and preventing crime (including cyber-crime), illegal trafficking and terrorism (including cyber-terrorism), including understanding and tackling terrorist ideas and beliefs to also avoid aviation related threats.” (Europäische Kommission 2015b: 48)

Neben dem Schwerpunkt auf Cyber-Kriminalität und dem Tatort Internet kommt es zuweilen vor, dass durch das Kontinuum „crime and terrorism“ nach Methoden für Delikte gesucht wird, die grundverschieden sind und nach unterschiedlichen Maßnahmen verlangen. So finden sich innerhalb einer einzigen Ausschreibung mit dem Titel “Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts“ (Europäische Kommission 2017a: 24) neben „New methods for the protection of crowds during mass gatherings“ (ebda.: 25), „New methods to prevent, investigate and mitigate corruption and financial crime to fight the infiltration of organised crime in the European Union (licit) economy“ (ebda.) auch „New methods to prevent, investigate and mitigate high impact petty crimes“ (ebda.) und “New methods to prevent, investigate and mitigate high impact domestic violence“ (ebda.). Darauf, was dabei unter “high impact“ zu verstehen ist, wird nicht näher eingegangen.

Wenngleich auch in KIRAS „Kriminalität“ als „Risiko/Bedrohung“ einen eigenen Unterpunkt darstellt, so beziehen sich die Forschungsvorhaben in der Kategorie „Anti-Terror“ singulär auf die Terrorismusbekämpfung. Synergien mit unter Umständen minderscheren – und für die öffentliche Sicherheit nicht relevanten Delikten – werden in diesem Bereich mit der Ausnahme von Großschadensereignissen keine hergestellt (vgl. bmvit 2015b: 9ff.).

Der deutsche Weg kann als Mittelweg zwischen dem österreichischen und dem der EU gesehen werden: Terror wird semantisch nicht wie im Falle von Secure Societies mit Delikten verknüpft, die – wie im Falle von Cyber-Kriminalität – allenfalls ökonomische oder datenschutzrechtliche, aber wahrscheinlich keine menschlichen Opfer zur Folge haben, jedoch mit Delikten in Verbindung gebracht, die nicht den

politischen Charakter einer terroristischen Tat aufweisen, jedoch eine Bedrohung im öffentlichen Raum darstellen können: „Kriminalität, Übergriffe auf Fahrgäste und Personal oder Terroranschläge können die Sicherheit und Zuverlässigkeit des öffentlichen Nahverkehrs massiv beeinträchtigen. Ziel der Forschung ist die Erhöhung der Sicherheit und des Sicherheitsempfindens der Fahrgäste im ÖPNV“ (BMBF 2012c).

#### **4.3.3 „Vulnerable Personen und Gruppen“: (De-)Radikalisierung**

Der Prozess der Radikalisierung von Individuen und Gruppen ist ein Bedrohungsbild, das in allen Programmen in unterschiedlichem Ausmaß im Kontext der Prävention im Sinne einer *Deradikalisierung* oder einer Verhinderung der Radikalisierung adressiert wird. Im Programm der Europäischen Union markiert das Thema *Deradikalisierung* den Bereich, in dem am stärksten auf soziale und ökonomische Ungleichheiten als potenziell ursächlich für Bedrohungen durch extremistische Gewalttaten referiert wird. Es ist gleichsam auch jener Bereich, indem quantitativ am stärksten auf die Schaffung von Wissen gesetzt wird, die außerhalb der Sphäre technologisch-ingenieurstechnischer Forschung, also im geistes- und sozialwissenschaftlichem Bereich angesiedelt ist.

Im Zusammenhang mit Radikalisierungstendenzen ist von „economic and political disparities who have proven to be a breeding ground for political extremism, violent radicalisation and terrorism“ (Europäische Kommission 2015b: 88) die Rede, es wird nach einer Studie verlangt, in der unterschiedliche soziale Indikatoren (genannt werden politische Partizipation, Diskriminierung aufgrund der Klasse, der Ethnie, des Geschlechts oder des Alters genannt (vgl. Europäische Kommission 2015b: 68) im Zusammenhang mit dem Phänomen gewalttätiger radikalierter Individuen untersucht werden sollen. Dabei wird betont, dass es zwischen „radical thought“ (Europäische Kommission 2017b: 22), den es zu tolerieren und gewalttätigen Handlungen, die es rechtzeitig zu vermeiden gelte, zu unterscheiden sei. In diesem Zusammenhang wird auch auf die Meinungsfreiheit und „citizens’ rights to free thought“ (ebda.) hingewiesen. Terrorismus wird in *Secure Societies* auch in diesem Kontext nicht allein adressiert, sondern als Begriffspaar mit organisiertem Verbrechen als Begriffspaar adressiert: „Proposers could also adopt a further approach by focusing on the impact of social cohesion in the prevention of

individuals' engagement in organized crime and terrorist networks“ (Europäische Kommission 2015b: 68).

KIRAS unterscheidet sich von den anderen Programmen in diesem Themenbereich deutlich dadurch, dass nur dort die islamische Religion als Bedrohung für die öffentliche Sicherheit artikuliert wird. Während sich in Sicherheitsforschung 2012-2017 überhaupt keine Referenzen auf den Islam oder islamistische Bedrohungen finden und in Secure Societies lediglich „Al Qaida- or Daesh-inspired ideologies“ neben „nationalist, anarchist, separatist, violent leftwing or right-wing ideologies“ aufgelistet werden, so findet im österreichischen Programm der „europäische Islam“ (bmvit 2017a: 26) als sicherheitspolitische Forderung wieder. Referenzobjekt dieser Forderung ist der Rechtsstaat, der laut Ausschreibungsleitfaden aus dem September 2017 durch die zunehmende religiöse Radikalisierung gefährdet sei: „Religiöse Radikalisierung, der daraus entstehende Extremismus und die daraus rechtfertigende organisierte Gewalt terroristischer Akte drohen diesen zentralen Sicherheitsfaktor zunehmend zu unterhöhlen“ (ebda.: 26).

„[A]ls Beitrag zur inneren Sicherheit Österreichs“ sei es daher „wichtig zu erfahren, wie die österreichischen Muslime und Muslimas das Verhältnis ihrer Religion zur Bundesverfassung und den daraus resultierenden Gesetzen sehen“ (ebda.) Der sogenannte europäische Islam oder Euro-Islam wird „als mögliche Lösung in Hinblick auf radikalen Islam sowie Islamismus“ präsentiert, dessen Grundlage die Anerkennung der Trennung zwischen Staat und Religion sei (ebda.). Neben dem Islam werden in KIRAS keine weiteren Religionen, ideologischen oder politischen Strömungen als Gefahr für den Rechtsstaat genannt.

Im deutschen Programm heißt es zum Thema Radikalisierung, dass mit der Sicherheitsforschung „Beiträge zur Ursachenforschung zu politischem Extremismus, Terrorismus und Radikalisierungstendenzen in der Gesellschaft sowie die Entwicklung präventiver Maßnahmen bzw. staatlicher und gesellschaftlicher Gegensteuerungsmöglichkeiten“ geleistet werden sollen (BMBF 2016e: 14). Im zur Analyse stehenden Ausschreibungszeitraum 2012-2017 findet sich lediglich die Bekanntmachung „Zivile Sicherheit – Aspekte und Maßnahmen der Terrorismusbekämpfung“, in der diesem Thema am Rande Rechnung getragen wird. Dabei ist interessant, dass jene, deren Radikalisierung sie später zu Täter\*innen

machen könnte gleichsam als Opfer, nämlich als „vulnerable Gruppen und Personen“, für die es „zielgruppenspezifische Schutzmaßnahmen“ zu erschaffen gelte (BMBF 2015), adressiert werden.

Im österreichischen Programm wird ein ähnlicher Duktus verwendet, nämlich ist hier von „vulnerablen Lebenssituationen“ die Rede. Interessant ist, dass im österreichischen Programm analog zur Vulnerabilität mancher Lebenssituationen auch das Thema Resilienz im Kontext von Radikalisierung auf das Tapet gebracht wird, nämlich als eine Art Hybrid aus psychologischer Resilienz, die an der Widerstandsfähigkeit des Einzelnen orientiert ist und sozialer (systemischer) Resilienz, die das Kollektiv betrifft. So heißt es unter „Resilienzstärkende Maßnahmen zur Radikalisierungsprävention junger Menschen“: „Präventive Maßnahmen sollten möglichst an den Ursachen von Radikalisierungsprozessen ansetzen und die Resilienz gegenüber extremistischen Sinn- und Identitätsangeboten erhöhen“ (bmvit 2017a: 27).

Individuen und Gruppen werden hier zwar tatsächlich als vulnerabel konstruiert, jedoch wird dies prinzipiell in jedem der Programme in ein Narrativ integriert, dass die Lebensumstände der „Zielpersonen“ als möglicherweise ursächlich in Betracht zieht. Auch im europäischen Programm – bzw. dort sogar mehr als beispielsweise im deutschen Programm – wird beim präventiven Fokus auf strukturelle Faktoren wie ökonomische und soziale Ungleichheit hingewiesen. Möglichen Betroffenen wird also nicht die „Schuld“ an ihrem Verhalten gegeben: “Research should investigate the role of social, psychological and economic factors in progression of individuals who had unremarkable and ordinary lives into organised crime and terrorist networks” (Europäische Kommission 2015b: 67).

## **4.4 Migration**

Wanderungsbewegungen von Gebieten außerhalb der EU in den Schengen-Raum werden in allen drei Programmen im Kontext ziviler/innerer Sicherheit aufgegriffen, wenngleich das Thema in Secure Societies diesem Thema ob der Zuständigkeiten bei der Sicherung der Schengen-Außengrenzen am stärksten vertreten ist. „Migration“ als Zustand, Prozess und politisches Problem wird dabei in den Ausschreibungen aus unterschiedlichen politischen Blickwinkeln adressiert und erfordert zum Teil das Überbrücken inhaltlicher/diskursiver Widersprüche, die in den nachfolgenden Unterkapiteln skizziert werden sollen. Das Ineinandergreifen entwicklungs-/außenpolitischer Belange mit innen-/wirtschaftspolitischen Zielen zeichnet sich in dieser Kategorie am stärksten ab.

### ***4.4.1 Menschliche Sicherheit***

Ein Teil der Ausschreibungen befasst sich mit Maßnahmen, die eine Verbesserung des Schutzes individuellen Lebens in Fluchtsituationen auf dem Gebiet der EU beziehungsweise auf österreichischem und deutschem Staatsgebiet gewährleisten sollen.

Im Programm der Europäischen Union sowie in Sicherheitsforschung 2012-2017 sind die Zielsetzungen in diesem Bereich technologisch orientiert und mehrheitlich im Bereich der Sensoren- und bildgebenden Überwachungstechnik angesiedelt. Sie sollen dem Anspruch gerecht werden, dem Schutz menschlichen Lebens, einem möglichst unbehinderten Personen- und Warenverkehr an Grenzübergängen sowie einer personaleffizienten Grenzsicherung Rechnung zu tragen (siehe mehr dazu in 4.6.1).

So findet sich im deutschen Forschungsprogramm in einer Ausschreibung vom 12.10.2016 ein Call für Technologien zur „[...] Optimierung der Aufdeckung von Schleuserkriminalität durch mobile, nichtinvasive Untersuchungsmethoden im Schwerlastverkehr (zum Beispiel Infrarot-, Terahertz- und Röntgenrückstreutechnologie sowie deren Kombination)“ (BMBF 2016a). Die ausgeschriebene Technologie steht zeitlich und inhaltlich in Korrespondenz zum

Unglück auf der (österreichischen) A4 im August 2015 und ist die einzige Maßnahme, die im deutschen Sicherheitsprogramm auf diesem Gebiet vorzufinden ist.

Im Programm der Europäischen Union ist der Fokus einmal mehr breiter angelegt. Das Thema Migration – und darunter auch Aspekte menschlicher Sicherheit – wird neben einer Reihe von anderen „Delikten“ abgehandelt, die mithilfe neuer Technologien für die Hauptaufgaben des europäischen Grenzüberwachungssystems EUROSUR synergetisch von Nutzen sein sollen. In den Ausschreibungstexten liest sich dies wie folgt (mehr zu EUROSUR im folgenden Unterkapitel):

“Current border control systems involve a wide range of heterogeneous assets – manned and unmanned – to survey from air, surface (land and sea) and underwater. Similarly the objects of their surveillance may be vessels, land vehicles, aircrafts, and underwater vehicles used, for instance, for smuggling and trafficking. Only enhanced command and control systems using advanced 3D computer graphics technology may allow to represent accurately the position of surveillance assets – including autonomous agents – and external objects in such complex environments.” (Europäische Kommission 2017a: 46-47)

Auch im österreichischen Programm KIRAS können Inhalte der Perspektive „menschlicher Sicherheit“ zugeordnet werden, nämlich jene im Zusammenhang von Strategien zur Hilfe Schutzbedürftiger auf der Flucht – unabhängig von deren Nationalität.

„Hier steht einerseits die Sicherheit der Opfer (meist Frauen und Kinder) im Zentrum des Interesses, da diese meist nur beschränkt (oder gar nicht) Zugriff auf Rechtsmittel und Unterstützung durch staatliche Institutionen haben, andererseits aber auch die Sicherheitsimplikationen, die sich durch die OK-Komponente ergibt. Die Bekämpfung von Menschenhandel und "modern slavery" inkl. der Entwicklung entsprechender Strategien, Evaluationen von Maßnahmen etc. stellt in demokratischen Systemen somit eine Kernaufgabe staatlichen Handelns dar.“ (bmvit 2015a: 21)

Der Schutz von „Opfern“ (von Menschenhandel) wird dabei als „Kernaufgabe staatlichen Handelns“ „demokratischer Systeme“ eingeführt, der Schutz universeller Menschenrechte und damit die Rechtssicherheit von Personen auf österreichischem Terrain geben Anlass für diese Ausschreibung. Auch das physische Überleben wird durch die Blume vage als „Sicherheitsimplikationen die sich durch die OK-Komponente ergibt (sic!)“ mitadressiert.

#### **4.4.2 Die Inszenierung „illegaler Migration“ als systemische Bedrohung**

Migration bleibt ein politisch höchst explosives Thema, das nicht in alle Programme im selben Ausmaß integriert wurde. Wie bereits erwähnt wurde, wird das Thema im deutschen sowie im österreichischen Programm lediglich in jenen Ausschreibungen abgehandelt, die als Beispiele bereits abgearbeitet wurde. Im Programm der Europäischen Union nimmt das Thema jedoch nicht zuletzt aufgrund des Europäischen „multipurpose“-Grenzüberwachungssystems EUROSUR (Europäische Kommission 2017a: 44) eine Art Sonderstellung ein, die sich diskursiv auch in den Ausschreibungen in komplexer Art und Weise manifestiert. Da EUROSUR 2014 unter *anderem* geschaffen wurde, um Migration zu überwachen und zu bekämpfen, wird selbige in *Secure Societies* neben weiteren Aspekten als systemische Bedrohung für den EU-Raum etabliert, die es neben anderen Straftaten allein ob ihrer „Illegalität“ zu bekämpfen gelte. Dies geschieht ungeachtet des völkerrechtlichen Aspekts der Flucht, der eine illegale Grenzübertretung legitimieren würde.

Versehen mit den Adjektiven „illegal“ oder „irregular“ bildet Migration ein Kontinuum zur Legitimation der Investition in eine Vielzahl unterschiedlicher Überwachungstechnologien, die entweder die Grenzsicherheit oder Gebiete außerhalb des Schengen-Raumes betreffen. Sie steht selten für sich allein, sondern wird häufig mit Delikten unterschiedlicher Art artikuliert, für die dieselbe Maßnahme anwendbar sein soll. Nicht selten wird der nach außen hin legitimätsstiftende Aspekt der humanitären Sicherheit in dieses Kontinuum integriert – „illegale Migration“ somit als Bedrohung artikuliert und der menschlichen Sicherheit („search-and-rescue operations“) gleichzeitig Rechnung getragen:

“Activities in the Mediterranean Sea related to border surveillance, including fight against drug trafficking and illegal immigration as well as search-and-rescue operations require for the authorities to detect at a long distance (typically: over the horizon) the presence of small vessels.” (Europäische Kommission 2015b: 74)

Ein weiteres Beispiel ist ein Sub-Call zum Thema Container-Sicherheit, wo ausgehend von einem Objekt zum grenzüberschreitenden Transport von Gütern „illegale Migration“ sich neben terroristische Bedrohungen, Diebstahl und Schmuggel einreicht: „Container security associated with terrorist threats, illegal immigration, theft

and smuggling is therefore an important factor in the overall EU border security“ (Europäische Kommission 2015b: 85).

Reagiert wird angesichts dieser mannigfaltigen Bedrohungen aber bewusst nicht mit der „totalen Sicherheit“, sondern mit technologischen Maßnahmen, die es möglich machen sollen, physische Überprüfungen aus wirtschaftlichen und personellen Gründen weitestgehend obsolet zu machen (mehr dazu in Kapitel 4.6.1):

“One main challenge is to manage the flow of travellers and goods arriving at our external borders, while at the same time tackling irregular migration and enhancing our internal security. Any novel technology or organisational measure will need to be accepted by the European citizens.” (Europäische Kommission 2017b: 36)

Die „European citizens“ werden dabei als imaginäre „audience“ adressiert, an die als legitimatorische Kraft appelliert wird. Sie sollen die Zustimmung für den Einsatz einschlägiger Überwachungstechnologien geben. In diesem Zusammenhang stellt sich die Frage, wer die „European citizens“ sind, die hier als homogene Masse und Souverän inszeniert wird. Die „acceptance of the citizens“ wird so positioniert, als stehe sie als entscheidungsgebende Gewalt über politischen Gesetzgebungsverfahren, rechtlichen Vorschriften und ethischen Grundsätzen.

## **4.5 Gefühle und Werte und Objekte als Referenzobjekte ziviler Sicherheit**

Dieses Kapitel widmet sich der Frage, wie Objekte, Werte, Gefühle und Wahrnehmungen in der Sicherheitsforschung adressiert werden. Ein Fokus wird darauf liegen, in welche Narrative diese Elemente verpackt werden und mit welchen Begründungen sie in das Portfolio schützenswerter Referenzobjekte integriert werden.

### ***4.5.1 „Freies Leben“: (Un)Sicherheitsempfinden im Kontext der Lebensqualität***

Bereits bei den Sicherheitsbegriffen (4.1.2) wurde festgehalten, dass in allen drei Programmen auch subjektive Gefühle/Eindrücke wie das (Un)Sicherheitsempfinden, die (Un)Sicherheitswahrnehmung oder die Lebensqualität zu Referenzobjekten der Forschung erklärt werden, womit das Verständnis von Sicherheit über Maßnahmen, die das Sichern des physischen Lebens betreffen, hinausgeht. Wie weit und auf welche Weise darüber hinausgegangen wird bzw. wie das Forschungsinteresse in diesem Bereich begründet wird, variiert von Programm zu Programm jedoch.

Das Alleinstellungsmerkmal des deutschen Programms in dieser Kategorie ist die Häufigkeit, mit der „Sicherheit“ mit „Freiheit“ in Beziehung gesetzt wird. Und zwar in einer Weise, in der die Freiheit zum Referenzobjekt der Sicherheit an sich stilisiert wird. Dem in Deutschland ausgesprochen starken, historisch gewachsenen Diskurs gegen ein „zu viel“ an Sicherheit, (Massen)Überwachung und Kontrolle wird implizit mit einem immer wiederkehrenden „Disclaimer“ begegnet, in dem Sicherheit meliorativ als Grundlage eines „freien Lebens“ stilisiert wird. Im Zusammenhang damit wird nicht verleugnet, sondern gezielt artikuliert, dass Sicherheit auch als Grundlage für die Erhaltung von Deutschlands wirtschaftlichem Wohlstand als zentral erachtet wird: „Sicherheit ist die Basis eines freien Lebens und ein wichtiger Faktor des wirtschaftlichen Wohlstandes in Deutschland“ (BMBF 2016e).

In den Ausschreibungen werden individueller Nutzen („Lebensqualität“) und systemischer Nutzen („Wertschöpfung“) auf ähnliche Weise durch eine Konjunktion

miteinander verbunden: „In Deutschland ist die zivile Sicherheit eine der prioritären Zukunftsaufgaben für Lebensqualität und Wertschöpfung“ (siehe z.B. BMBF 2016d).

Neben dem bereits in 4.1.2 erwähnten „zentralen Wertbegriff“ wird Sicherheit an anderer Stelle auch „elementares menschliches Grundbedürfnis“ (BMBF 2016e) und als „zentrale gesellschaftliche Leitidee“ (ebda.) artikuliert. Der strukturelle Nutzen von „Sicherheit“ für das Gemeinwohl und Alltagsleben wird im deutschen Programm besonders hervorgekehrt. Zivile Sicherheit – oder die Investition in sie – wird als Dienst an der Bevölkerung mit hohem gesellschaftlichen und systemischen Nutzen verkauft, der weit über die Sicherung des Lebens in Notsituationen hinausgeht. Darüber hinaus wird Sicherheit als notwendige Bedingung von „Freiheit“ artikuliert und dadurch nicht als ihr Gegenpol, sondern als ihr Ermöglicher und Garant positioniert.

Das „freiheitliche Leben“ steht dabei für den öffentlichen Raum und die sich darin frei bewegenden Menschen, als Symbolbild dient die Abbildung eines Dorffestes (BMBF 2016e). In den konkreten Ausschreibungen sollen die „Lösungen“ in diesem Bereich „dazu beitragen, das freiheitliche Leben in Räumen, wie zum Beispiel „Märkten, Fußgängerzonen, Einkaufszentren, Parks, Schulen sowie kulturellen, historischen und religiösen Stätten, zu stärken“ (BMBF 2016b). Das Sicherheitsgefühl wird im Zuge dessen gleichbedeutend mit der objektiven Sicherheit, jedoch strenggenommen unabhängig voneinander betrachtet – gefördert werden Maßnahmen, die „Kriminalitätsfurcht und Unsicherheitsgefühlen“ präventiv entgegenwirken sollen.

„Kriminalitätsfurcht und Unsicherheitsgefühle können das öffentliche Leben in städtischen Räumen spürbar einschränken. Ziel der Forschung ist die Entwicklung ganzheitlicher Präventionsansätze und Schutzmaßnahmen zur Erhöhung der Sicherheit und des Sicherheitsempfindens von Bürgerinnen und Bürgern.“ (BMBF 2012c)

Im Programm der Europäischen Union wird die Sicherheitswahrnehmung und die Lebensqualität ebenfalls gemeinsam mit wirtschaftlichen Faktoren artikuliert. Ein negativer Einfluss auf die Sicherheitswahrnehmung wird hier mit den beiden Letztgenannten kausal in Verbindung gebracht:

„European large urban environments are subject to various challenges and threats to urban security linked to their big size and large population. These challenges have also a strong

impact on the security perception of the citizens and, by this, they can impact on the economic development and the quality of life.” (Europäische Kommission 2015b: 61)

In KIRAS wird das Sicherheitsempfinden oder die Wahrnehmung von Sicherheit und Unsicherheit in der Bevölkerung nicht explizit mit der Lebensqualität, der Vorstellung eines freien Lebens oder wirtschaftlichen Faktoren artikuliert. Es scheint im österreichischen Fall diskursiv nicht notwendig, die Sicherheit gegen die Freiheit zu verteidigen, wie das im deutschen Programm der Fall zu sein scheint. Das Thema „Sicherheitsempfinden“ ist in den Ausschreibungen lediglich einmal vertreten, und zwar im Kontext des demographischen Wandels in der Bevölkerung. Konkret geht es dabei um die Frage, wie älteren und hochaltrigen Personen als wachsende Zielgruppe durch konkrete Maßnahmen ein besseres subjektives Sicherheitsempfinden vermittelt werden kann.

„Der demographische Wandel stellt eine zunehmende strategische Herausforderung für Gesellschaft und Staat, unter anderem auch für Sicherheitsakteure wie die Polizei, dar. Insbesondere aufgrund der fortschreitenden Alterung der Bevölkerung besteht die Notwendigkeit, ältere und hochaltrige Menschen unter Einbezug der objektiven Sicherheitslage und des subjektiven Sicherheitsempfindens stärker als Zielgruppe zu berücksichtigen.“ (bmvit 2014: 21)

Ziel der Ausschreibung ist es, dieser „vulnerablen“ Bevölkerungsgruppe durch einen präventiven, in die Zukunft gerichteten, diversitären Fokus mit zugeschnittenen Maßnahmen entgegenzukommen:

„Für eine effektive, zukunftsorientierte Präventions- und Kommunikationsarbeit ist es wesentlich, die besonderen Bedürfnisse und Risiken, die diese Gruppen aufweisen bzw. denen sie ausgesetzt sind, zu kennen und zu verstehen und darauf aufbauend entsprechende Strategien und Maßnahmen zu entwickeln.“ (ebda.)

Die „objektive Sicherheitslage“ sowie das „subjektive Sicherheitsempfinden“ werden hier allerdings gemeinsam betrachtet, die „besonderen Bedürfnisse“ dieser sozialen Gruppe sowie die „Risiken, die diese Gruppe aufweisen bzw. denen sie ausgesetzt sind“, werden als Teil eines Kontinuums oder zumindest parallel behandelt.

#### **4.5.2 Der Schutz von kulturellen Werten und Gütern**

Kunst- und Kulturgüter werden in die Forschung für die zivile Sicherheit ebenso integriert. Während sich im europäischen und im österreichischen Programmen

konkrete Ausschreibungen dem Schutz von kulturellen Gütern widmen, so wird im deutschen Programm das Thema zwar erwähnt, (nämlich, dass der der Schutz von Kulturgütern in bewaffneten Konflikten durch die Haager Konvention geregelt ist, vgl. BMBF 2016e: 32), konkrete Ausschreibungen zu diesem Thema finden sich jedoch im Zeitraum 2012-2017 nicht.

In KIRAS werden Kunst- und Kulturgüter als „Definitionsbasis einer Gesellschaft“ als schützenswerte Referenzobjekte konstruiert. Österreichs Aufgabe sei es auch „in einem europäischen Kontext“ (bmvit 2014: 21), diese Güter zu schützen. Österreichs kulturelles Erbe wird nicht nur als identitätsstiftend für die österreichische Gesellschaft artikuliert, sondern – aufgrund seines unermesslichen Werts – zugleich auch für die europäische. Aus dieser Überhöhung folgt implizit, dass es Österreichs Kulturgut nicht (nur) aus eigenem, nationalem Interesse zu schützen gelte, sondern gewissermaßen auch im Dienste Europas. Als konkretes Forschungsvorhaben wird in KIRAS ein Pilotprojekt für eine „Sicherheitsanalyse für ein Museum, Kunstsammlung, Bibliothek oder sonstige sammelführende Einrichtung“ (bmvit 2014: 21, bmvit 2015b:26) in Auftrag gegeben.

In Secure Societies wird der identitätsstiftende und identitätsbewahrende Charakter kulturellen Erbes ebenfalls betont. Dabei bleibt es jedoch nicht. Zugleich wird auch der (sozio)ökonomische Nutzen der „cultural heritage“ adressiert. Die individuelle und kollektive Identität sowie der Tourismus werden dabei als immaterielle und materielle Werte miteinander verknüpft. Dies erfolgt auf eine partikulare Weise, in die Elemente der „community resilience“ hineinfließen. Kulturelle Artefakte werden in diesem Kontext aus der Perspektive ihres systemischen Nutzens auf lokaler Ebene beleuchtet: „Cultural heritage, an important component of individual and collective identity, also fuels Tourism in Europe, a significant economic sector on which many communities depend (Europäische Kommission 2015b: 25)“. Dieses wird – unter Anrufung der klimatischen Veränderungen – als akut bedroht konstruiert:

„Europe's cultural heritage is being lost at an alarming rate, not only due to natural decay and human impacts but frequently also as a result of environmental changes, climatic conditions or natural hazards. This non-renewable resource, in all its diverse physical forms needs safeguarding for future generations.“ (ebda.: 25)

Der „Rettungsansatz“ steht im Zeichen von Nachhaltigkeit und Adaption:

“[T]he increased frequency and intensity of extreme weather events together with risks associated to natural hazards present an added challenge for the sustainable management and conservation of cultural heritage in Europe, calling for improved adaptation and mitigation strategies in this vulnerable sector.” (ebda.: 25)

Sicherheit steht in diesem Kontext eher für Nachhaltigkeit, gleichzeitig wird das kulturelle Erbe, um es im Kontext von Sicherheit platzieren zu können, als bedroht inszeniert. Referenzobjekt ist im Grunde das „Überleben“ beispielsweise strukturschwacher, aber kulturell gesegneter Gegenden in der EU, die im Falle eines Wegfalls des Tourismus von Arbeitslosigkeit, Abwanderung und wirtschaftlichen Problemen konfrontiert wären.

## **4.6 „Sicherheit für die Wirtschaft“: Die Versicherunglichung wirtschaftlichen Wohlstands**

In den vorangegangenen Kapiteln wurde bereits thematisiert, dass bestimmte Maßnahmen und Technologien darauf zugeschnitten sind, einerseits eine Sicherheitsaufgabe zu erfüllen, jedoch andererseits effiziente wirtschaftliche Abläufe nicht im Weg zu stehen. Im letzten Kapitel soll nun abschließend direkt der Frage nachgegangen werden, wie die Wirtschaft in den jeweiligen Programmen selbst als Referenzobjekt der Sicherheitsforschung positioniert wird und mit welchen diskursiven Mitteln dies umgesetzt wird.

### ***4.6.1 Die Volkswirtschaft und Unternehmen als Referenzobjekte ziviler Sicherheitsforschung***

Bereits im ersten empirischen Kapitel wurde erörtert, dass für Deutschland und die EU die Wirtschaft – also ökonomisches Wachstum und Wohlstand der Volkswirtschaft – ein Referenzobjekt ziviler Sicherheit ist. So steht im deutschen Programm „Sicherheit der Wirtschaft“ auf einer Ebene mit Themen wie Katastrophenschutz und Terrorismusbekämpfung (vgl. BMBF 2016e: 3). In Secure Societies bilden „citizens, society and economy“ die Dreifaltigkeit der Schutzziele (Europäische Kommission 2015b: 7). In KIRAS sind hier zumindest der Definition nach mit der Beschränkung auf Maßnahmen zur Wahrung der „öffentlichen“ Sicherheit engere Grenzen gesetzt. Die Stärkung der heimischen Sicherheitswirtschaft ist zwar ein strategisches Ziel, dazu gehört jedoch nicht die Versicherunglichung der Volkswirtschaft insgesamt. Inwieweit die Wirtschaft auch in KIRAS als Referenzobjekt adressiert wird, soll im Folgenden analysiert werden.

Doch auch im deutschen und im europäischen Programm wird die Volkswirtschaft trotz der erklärten Zielsetzung selten als alleiniges Referenzobjekt konkreter Lösungen und Technologien eingesetzt. Im deutschen Programm häufen sich Artikulationen, in denen die „Wirtschaft“ zusammen mit „etablierten“ Referenzobjekten wie den „Bürger\*innen“, der „Bevölkerung“ oder der „Gesellschaft“ synergetisch adressiert werden. Einige Beispiele sollen dies veranschaulichen:

„Bürgerinnen und Bürger sind ebenso wie Unternehmen und Betriebe auf diese Versorgungseinrichtungen angewiesen, auf ihr reibungsloses Funktionieren und ihre Verlässlichkeit.“ (BMBF 2014c)

„Hafenanlagen dienen als zentrale Versorgungs- und Umschlagsplätze für den Seehandel. Somit sind Häfen von zentraler Bedeutung für die Versorgung der Bevölkerung und die deutsche Wirtschaft.“ (BMBF 2012a)

„Für Unternehmen ebenso wie für kritische Infrastrukturbetreiber stellen Natur- und Umweltkatastrophen, Pandemieausbrüche oder Großunfälle erhebliche Risiken dar.“ (BMBF 2016e)

„Gleichwohl bleiben biologische Erreger und Gefahrstoffe eine potentielle Bedrohung für die Zivilgesellschaft. Überregionale bedrohliche Infektionsgeschehen durch Epidemien und Pandemien können zudem erhebliche wirtschaftliche Schäden verursachen.“ (BMBF 2014a)

„Verkehrsinfrastrukturen bilden die Lebensadern unserer Gesellschaft, die auf die Mobilität von Menschen und Gütern angewiesen ist.“ (BMBF 2016d)

Parallel zu diesen Artikulationen wird jedoch durchaus auch das systemische Risiko wirtschaftlicher Instabilität betont und in den Kontext nationaler Sicherheit gebracht: „Zugleich ist eine gute Wirtschaftskraft die wesentliche Grundlage für den Wohlstand der Bevölkerung und die Stabilität des Staates“ (BMBF 2012b). Diese „Grundlage“ wird als bedroht konstruiert: „Die Wirtschaftskraft der Bundesrepublik Deutschland wird jedoch durch kriminelle Handlungen gefährdet“ (ebda.). Bemerkenswert ist, dass im Fall Deutschlands als „kriminelle Handlungen“, gegen die auch mithilfe der Forschung vorgegangen werden soll, nicht nur von außen eindringende Bedrohungen (z.B. Cyberangriffe, Wirtschaftsspionage, Produkt- und Markenpiratie) aufgezählt werden, sondern auch dem Inneren des Systems entspringende schädliche Verhaltensweisen wie „Steuerbetrug“ und „Korruption“ die Liste vervollständigen (vgl. ebda.). In dieser Ausschreibung mit dem Titel „Schutz vor Wirtschaftskriminalität“ wird die Volkswirtschaft direkt als Referenzobjekt eingesetzt, steht jedoch symbolisch für eine Quelle der Sicherheit, des Wohlstands und der Machtstellung Deutschlands in der Welt, die in Zeiten, in denen „der Wettbewerb zwischen Unternehmen und Volkswirtschaften“ (vgl. ebda.) zunehme, durch innere und äußere Kräfte dauerhaft bedroht ist. Eine Bedrohung, die sowohl privaten Ursprungs als auch staatlichen Ursprungs sein könne und damit die Grenzen zwischen Wirtschafts-, Innen- und Außenpolitik verwischt bzw. nachrangig erscheinen lässt:

„Solche Angriffe werden nicht nur von kriminellen Organisationen, die über entsprechende monetäre und personelle Ressourcen verfügen, ausgeführt, sondern auch von einzelnen Staaten genutzt („state sponsored hacks“), um kritische Infrastrukturen zu schwächen oder Wettbewerbsvorteile zu erzielen.“ (ebda.)

Die Globalisierung wird in diesem Zusammenhang einmal mehr als Tatsache ins Feld geführt, die Vorteile mit sich bringt, jedoch auch Gefahren und Risiken. Insbesondere im Kontext dieser „äußeren“ Bedrohung wird hier der Staat als schützende Hand ins Szene gesetzt, der angesichts der wachsenden Bedrohung „informationeller Angriffe“ gezwungen oder verpflichtet sieht, im Sinne der Allgemeinheit durch entsprechenden Maßnahmen und Technologien nicht *nur* kritische Infrastrukturen zu schützen: „Bereits heute führen die internationalen Unternehmens- und Informationsverflechtungen dazu, dass informationelle Angriffe bzw. Industriespionage hohe wirtschaftliche Schäden insbesondere in mittelständischen Unternehmen verursachen“ (ebda.).

Im KIRAS ist der Zugang in dieser Hinsicht auch in der Ausschreibungspraxis beschränkter. Der Schutz der Wirtschaft ist durch die Maßgabe „öffentliche Sicherheit“ entsprechend tatsächlich auf den Schutz kritischer Infrastrukturen limitiert. Deren Schutz wird expliziter stärker im Kontext von Krisensituationen und Notfällen beleuchtet, die volkswirtschaftliche Variable wird als Teilaspekt jedoch nicht unter den Tisch gekehrt: „Die Erforschung der gesellschafts- und wirtschaftspolitischen Auswirkungen bei Ausfall von kritischen Infrastrukturen ist eine wesentliche Grundlage für entsprechende Schutz- und Sicherungsmaßnahmen der betroffenen Unternehmen und der Behörden“ (bmvit 2014: 19).

In Secure Societies liegt der Fokus auf dem Schutz wirtschaftlicher Prozesse, die den europäischen Binnenmarkt betreffen. Der effiziente, unterbrechungsfreie Austausch von Waren und Humankapital an den Grenzübergängen der europäischen Volkswirtschaft steht dabei zumeist im Zentrum der Projektausschreibungen. Inhaltlich sind sie von dem Spagat gekennzeichnet, den zwischen dieser Vorgabe und eines „traditionell“ sicherheitspolitisch orientierten Grenzschutzes zu überbrücken gilt. Das europäische Sicherheitsforschungsprogramm wird von der Idee eines möglichst ununterbrochenen Personen- und Warenfluss dominiert, der nur im Extremfall – und

durch den Einsatz neuartiger Überwachungssysteme möglichst überhaupt nicht unterbrochen werden soll (vgl. z.B. Europäische Kommission 2017a: 38f.).

Argumentiert wird dies von dem wirtschaftlichen Standpunkt aus, wonach jede Unterbrechung des Prinzips „panta rhei“ Einbußen für die europäische Wirtschaft zufolge habe und demnach wachstumshemmend sei. So werden beispielsweise im Bereich der Flugsicherheit im Sinne dieser Logik technologische Lösungen empfohlen, die das nach 9/11 etablierte Regime „hundertprozentiger“ Kontrollen anhand der „Flightpath 2050“-Ziele sukzessive ersetzen sollen:

“The challenge for aviation security research shall be to explore new ways and ideas that are conceptually very different to those already in development or deployed.” (Europäische Kommission 2015b: 31)

„Possible areas of research (not exclusive) could be: alternative screening processes and interventions; investigate how, where and when aviation security controls shall take place to provide the most effective and efficient results.“ (ebda.: 32)

Ähnliches gilt für die Schengen-Außengrenzen, wo „risikobasierte“ stichprobenartige Kontrollen und/oder das „nicht-invasive“ oder „nicht-disruptive“ Screening von Menschen und Waren im Zentrum stehen, deren Kernelement die Aufrechterhaltung eines ununterbrochenen Waren- und Menschenstroms und größere Effizienz sind.

“The concept of 'borders' has changed in recent times. The purpose and function of borders have been, and remain, to delineate and demarcate one sovereignty from another. However, borders must also allow for the smooth movement of people and goods. Maintaining the current level of checks is becoming increasingly expensive given the ever growing volumes of people and goods on the move, and increasingly more disruptive of flows. It would remain sustainable if thorough checks could be limited to fewer individual goods and people pre-selected further to a preliminary (and non-disruptive) risk-based screening of the flows.” (Europäische Kommission 2017a: 38)

“The use of biometrics "on the fly" techniques for identification in a non-intrusive manner and without interrupting the flow of people is an area for further development, testing and validation.” (Europäische Kommission 2017b: 38)

„This solution would typically be applied to a “non-divest” situation. It must be able to work in real-time, not to disrupt passenger flow or movement of a crowd. Preferably the solution should be able to deal with more than one person within the field of view, or at least other people in the frame should not interfere with the performance of the primary target.“ (Europäische Kommission 2015b: 83)

Menschen bzw. humanes Kapital spielen für den Versuch der Legitimation entsprechender Maßnahmen in der diskursiven Praxis eine wichtige Rolle. Sie werden als erste Profiteure dieser Technologien konstruiert, wobei mit größerem Komfort und geringerem Zeitverlust argumentiert wird (vgl. Europäische Kommission 2015b: 32). Der Wunsch nach möglichst schnellen, effizienten und ungehinderten Übergängen wird als allgemeiner politischer Wille artikuliert: „Policy is moving towards more risk-based, outcome-focused, passenger-facilitation oriented measures“ (Europäische Kommission 2015b: 31).

Als legitime Reisende gelten jedoch nur jene, die der Volkswirtschaft von vornherein nützlich sind. Die ausgeschriebenen Maßnahmen verfolgen unumwunden das Ziel, unerwünschte Einreisende und erwünschte Einreisende (diese werden als „non-critical travellers“ bezeichnet, vgl. Europäische Kommission 2015b: 81) auf eine Weise auseinanderzuidividieren, die mit knappen personellen Ressourcen zu bewältigen ist und insbesondere das „smooth movement of people and goods“ (Europäische Kommission 2017a: 38) nicht unterbricht. Dem Wert der „non-critical“ travellers für die europäische Volkswirtschaft wird im Diskurs besonders herausgestellt:

“Non-EU residents contributed €271 billion to the economy of Member States and Associated Countries when travelling to the EU in 2011. Business travellers, workers, researchers and students, third country nationals with family ties to EU citizens or living in regions bordering the EU are all likely to cross the borders several times a year.” (Europäische Kommission 2015b: 81)

“Making it as easy as possible for them to come to the EU would ensure that Europe remains an attractive destination and would help boosting economic activity and job creation.” (ebda.)

Durch die Anrufung und Hervorhebung all jener, deren Einreise insbesondere aus einem volkswirtschaftlichen Gesichtspunkt erwünscht ist, wird zugleich implizit – und in manchen Fällen auch explizit – auf all jene verwiesen, deren Betreten des Schengen-Raums nach Möglichkeit verhindert werden soll:

“The outcome of the research should be assessed in terms of improved border control modalities with a view to dedicate more time and resources to identify those who may pose a threat. The expected impact is to make the daily work of border control authorities more efficient and to significantly facilitating non-EU citizens and goods/economic operators in crossing EU external borders.” (Europäische Kommission 2015b: 82)

Da das Referenzobjekt in diesem Fall primär die Wirtschaft und erst sekundär die Sicherheit ist, resultiert daraus eine Nachfrage nach Maßnahmen und Technologien, die vorgeben, Sicherheit, Wirtschaftsfreundlichkeit und Personaleffizienz vereinen zu können. Hinzukommt, dass die Technologien im Idealfall einen Mehrfachnutzen erfüllen sollen, von dem auch Zollbeamt\*innen bei der Kriminalitätsbekämpfung profitieren. So heißt es z.B. in einer Ausschreibung zum mit dem Titel „Technologies for inspections of large volume freight“:

“1) Atomic property based interrogation (e.g. X-ray, muon, neutron), particularly to detect threat materials shielded in dense cargos, interrogation technology being directed towards the detection of organic products of relevance to Customs; 2) Evaporation based interrogation (e.g. mass spectrometry, biological detection, ion mobility spectrometry), with targeted selectivity at approximately femtogram/ litre level, to be directed towards a wider scope.”  
(Europäische Kommission 2015b: 85)

Insofern vermischen sich in den Narrativen von Secure Societies Elemente der Desecuritisierung (es ist aus Effizienz- und volkswirtschaftlichen Gründen „unmöglich“, alle Grenzen zu überwachen) mit Elementen der Überwachung aus der Distanz (Kontrolle muss dennoch sein), die in der Endsumme zu keiner Desecuritisierung führen (wir nehmen illegale Migration und organisierte Kriminalität in Kauf, damit die Wirtschaft wenigstens fließt), sondern zu einer Transformation, in der Überwachungstechnologien als einzig sinnvoller Kompromiss konstruiert werden.

#### ***4.6.2 Primat des Fortschritts? Die Positionierung technologischer Risiken als Chancen ökonomischen Wachstums***

In allen zur Analyse stehenden Programmen werden Risiken, die mit technologischen Entwicklungen der näheren Zukunft (in erster Linie der fortschreitenden Digitalisierung/Robotik) einhergehen werden, als erstens unumkehrbare und zweitens grundsätzlich positiv zu bewertenden Prozesse präsentiert, aus deren Risiken neue Wachstumsmärkte für Sicherheitstechnologien entstehen können. Zu Innovations skepsis und -kritik im Kontext ziviler Sicherheit wird in den Ausschreibungen angeregt, das Framing steckt jedoch den Rahmen des Möglichen ab – die Innovation wird aufgrund ihres ökonomischen Nutzens mit dem Prädikat „schützenswert“ versehen. Wie mit dieser affirmativen Grundhaltung in der Praxis der Ausschreibungen umgegangen wird, soll anhand der folgenden Beispiele erörtert werden.

Die KIRAS-Ausschreibung „Sicherer Verkehr - Cyber Sicherheit für autonomes Fahren“ (bmvit 2016: 12) behandelt die Risiken des autonomen Fahrens. Darin wird nicht zur Diskussion gestellt, ob das autonome Fahren für die öffentliche Sicherheit erstrebenswert ist, reagiert wird antizipativ auf die Sicherheitsrisiken, die sich aus dem autonomen Fahren ergeben könnten: „Für autonomes Fahren ist eine Kommunikation zwischen Fahrzeugen (Car2Car) als auch mit der Verkehrsinfrastruktur (Car2X) erforderlich. Die damit notwendigen Kommunikationssysteme sind potentiellen Cyber-Angriffen ausgesetzt und Bedrohen (sic!) die Sicherheit für autonomes Fahren“ (ebda.: 12) Und um diesen potenziellen Angriffen entgegenzuwirken, ist das Ziel der Ausschreibung die „Entwicklung von Maßnahmen zur Verhinderungen von Cyber Attacken“ (ebda.).

Ein weiteres Beispiel aus KIRAS handelt vom „Smart Home“ und der „Smart Industry (Industrie 4.0)“ (bmvit 2015b: 29, 2016: 19) und geht der Frage nach, wie „Cybercrime durch Prävention, Ermittlung und Forensik“ in diesen Bereichen „bestmöglich zu verhindern oder zu bekämpfen“ ist (ebda.). Einer kritischen Einschätzung der Risiken dieser neuen Technologien wird in einer der Sub-Forschungsfragen Raum gegeben: „Welche Technologie wird die größte negative Auswirkung (=Einfallstor für CyberKriminalität) erzeugen?“ Der Blick in die Zukunft ist auf den vorausschauenden Umgang mit diesen Risiken gerichtet: „Bei wem ist Präventionsarbeit daher bestmöglich in welcher Form zu leisten?“ (ebda.).

Im deutschen Programm spielt die „Wirtschaft 4.0“ in Ausschreibungen ebenfalls eine Rolle. Der den zukunftsweisenden Technologien innewohnende Antagonismus wird dort auf verwandte Weise artikuliert. Während zuerst Vorteile genannt werden,

„Die Realisierung von dezentralen, sich selbst organisierenden und steuernden Produktions- und Logistikprozessen bietet vielfältige Möglichkeiten – von weiteren Produktivitäts- und Effizienzsteigerungen bis hin zu neuen Produkten und Geschäftsmodellen.“ (BMBF 2017b)

werden im Anschluss im gewohnten Duktus mögliche Gefahren aufgezählt, die mit diesen Prozessen in Zukunft einhergehen könnten: „Die interdependenten, miteinander vernetzten Prozesse bei den Akteuren sowie entlang der Wertschöpfungsketten führen aber auch zu einer stark steigenden Komplexität“ (ebda.).

Die ausgeschriebenen Maßnahmen orientieren sich an den technologischen Innovationen an der Schwelle von Gegenwart und Zukunft. Im Mittelpunkt der Forschung stehen die Verwundbarkeiten, die aus diesen Technologien mit einer gewissen Wahrscheinlichkeit oder durch erste Erfahrungswerte entstehen. Gesucht werden ähnlich wie bei KIRAS u.a. „Methoden zur Analyse des Sicherheitsniveaus und der Zuverlässigkeit von besonders schützenswerten Elementen in Produktions- und Lieferketten sowie zur Bewertung von möglichen Maßnahmen zur Verbesserung des Sicherheitsniveaus und der Zuverlässigkeit unter Berücksichtigung aktueller Entwicklungen im Zusammenhang mit Industrie/Wirtschaft 4.0 (Vernetzungen, Manipulationen, Angriffe)“ (ebda.).

In Secure Societies wird im Zusammenhang mit den rasanten Entwicklungen im Bereich der Informations- und Kommunikationstechnologien einmal mehr das wirtschaftliche Wachstum direkt als Referenzobjekt eingesetzt, um das technologische Innovationspotenzial ergänzt und pro forma mit der „society“ konjugiert:

„ICT-driven transformations bring opportunities across many important sectors but also vulnerabilities to critical infrastructures and digital services, which can have significant consequences on the functioning of society, economic growth and the technological innovation potential of Europe.“ (Europäische Kommission 2017a: 49)

Im europäischen Programm werden die Technologien der Zukunft auch durch die Brille der Resilienz betrachtet. Entsprechende Maßnahmen stehen dann im Zeichen einer Risiko-Abschätzung und einer in die Zukunft gerichteten Vulnerabilitätsreduktion, aus der heraus sich selbst Möglichkeiten technologischer Innovation ergeben. Ein Beispiel ist eine Ausschreibung zum Thema intelligente Stromzähler („smart meters“), die künftig kraft EU-Verordnung vorgeschrieben sind. Von ihnen gehe ein Risiko für Cyber-Attacken auf das Stromnetz aus: „[T]he massive proliferation of ‚Smart Meters‘ as mandated by the Third energy Package introduces new threats“ (Europäische Kommission 2015b: 26). Als Ziel wird formuliert, diesen Implementierungsprozess zu begleiten und die Resilienz der Smart Grids zu erhöhen:

„The objective is to analyse potential new threats generated by the massive introduction of “smart meters” on the distribution grid system and propose concrete solutions in order to mitigate the risks, guarantee the electromagnetic compatibility, improve resilience and reduce vulnerability of critical infrastructure “smart grid”, due for example to cyberattacks“ (ebda.)

Dahingehende Tendenzen sind auch im deutschen und österreichischen Programm vorzufinden, wenngleich sie weniger häufig artikuliert werden. So ist in KIRAS in einer Ausschreibung von „ausfallsresilienten Energiesystemen der Zukunft“ (bmvit 2016: 12) die Rede, in Sicherheitsforschung 2012-2017 wird nach Möglichkeiten für begleitende „Anpassungsstrategien für ein robustes Business Continuity Management im Zuge von Wirtschaft 4.0 sowie Ansätze für neue zukunftsfähige Sicherheitsservices, Dienstleistungen, Geschäftsmodelle und Systemlösungen im Bereich Produktion und Logistik“ verlangt (BMBF 2017b). Sicherheit steht auf diese Weise von staatlicher/supranationaler Seite nicht im Widerspruch zum Fortschritt oder könnte sogar als dessen Feind gedeutet werden. Sie zieht sich jedoch nicht zurück, sondern tritt im Gegenteil im Gewand eines wachsamem und großzügigen Beifahrers auf, der aus Prinzip nicht zum Bremsen animiert, da auch er vom Sieg zu profitieren glaubt.

#### **4.6.3 Digitale Sicherheit**

Digitale Sicherheit ist ein Thema, das sowohl bei der privaten Nutzung des Internets als auch in öffentlichen Behörden und den dazwischen anzusiedelnden privatwirtschaftlichen Unternehmen stetig an Bedeutung gewinnt. In einigen Beispielen aus den zwei vorangegangenen Unterkapiteln ging es bereits um digitale Sicherheit. Dennoch erscheint es aufgrund des Querschnittscharakters dieses Gebiets interessant und notwendig, dem Thema in der Analyse noch einmal exklusiv zu begegnen mit einem speziellen Fokus auf Secure Societies. Zum Thema digitale Sicherheit gibt es nicht in allen drei Programmen eine Vergleichsgrundlage. In der deutschen neuen High-Tech-Strategie wurde mit „Digitale Wirtschaft und Gesellschaft“ eine Sub-Kategorie geschaffen, die sich exklusiv dem Thema Digitalisierung widmet. Dementsprechend ist das Thema in Sicherheitsforschung 2012-2017 unterrepräsentiert, mit Ausnahme jener Beispiele, die in den vorangegangenen Kapiteln bereits genannt wurden.

In KIRAS gibt es das Thema, es ist jener Bereich, wo man dem Anspruch, „safety“ und „security“ nach eigener Definition strikt voneinander zu trennen (auch die Ausschreibung zum autonomen Fahren könnten unter diesem Gesichtspunkt diskutiert werden), mitunter am wenigsten gerecht wird. So heißt es in einer Ausschreibung zum Thema „Advanced Persistent Threats“:

„Advanced Persistent Threats (APT) sind komplexe, zielgerichtete und effektive Angriffe auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen aller Branchen, die aufgrund ihres Technologievorsprungs potenzielle Opfer darstellen oder als Sprungbrett auf solche Opfer dienen können.“ (bmvit 2017a: 29)

Bedrohungen für IT-Infrastrukturen und vertrauliche Daten werden als gesamtgesellschaftliche Bedrohung inszeniert, deren Bekämpfung einen synergetischen Nutzen für die öffentliche Sicherheit (Behörden, kritische Infrastrukturen) einerseits als auch für Unternehmer\*innen und die Volkswirtschaft hat.

„APT Angriffe nehmen in ihrer Zahl und in Bezug auf die dadurch verursachten Schäden laufend zu und sind mittlerweile auch ins öffentliche Interesse gerückt. Auch österreichische kritische Infrastrukturen sind in den vergangenen Jahren Ziel solcher Angriffe geworden. Daher ist auch die professionelle Behandlung solcher Vorfälle auf Behördenseite erklärtes Ziel.“ (ebda.: 25-26)

In Secure Societies nimmt die digitale Sicherheit strukturell einen besonderen Platz ein, da sie an der Schnittstelle zwischen der „Digital Single Market Strategy“ und der „European Agenda on Security“ angesiedelt ist. Im Programm wird dies als Mehrwert deklariert: „Trust and security are at the core of the Digital Single Market Strategy, while the fight against cybercrime is one of the three pillars of the European Agenda on Security“ (Europäische Kommission 2017b: 55). Das Referenzobjekt des Calls zur digitalen Sicherheit ist der europäische Binnenmarkt:

“The proposed activities in this domain address the economic and societal dimension of security and privacy in the digital ecosystem, for the purposes of ensuring the well-functioning of the internal market.” (Europäische Kommission 2015b: 94)

In der Praxis der Ausschreibungen ist die Digitale Sicherheit quantitativ stark vertreten (zum Vergleich: im FP7 gab es „Digitale Sicherheit“ als Kategorie überhaupt noch nicht; siehe z.B. Europäische Kommission 2012). In Secure Societies kommt es inhaltlich trotz – oder je nach Auslegung wegen – des ohnehin schon sehr weit gefassten und beinahe beliebig ausdehnbaren Begriffs ziviler Sicherheit zu einer Pervertierung dessen, was Gegenstand einer Förderung unter dem Motto „Secure societies – Protecting freedom and security of Europe and its citizens“ sein könnte.

Hauptgegenstand der Ausschreibungen auf diesem Gebiet sind sogenannte „Privacy by Design“-Lösungen, in denen es um Datensicherheit bei der Verarbeitung personenbezogener Daten durch Unternehmen geht. Vorgebliches Referenzobjekt dabei ist zunächst auch der/die EU-Bürger\*in bei der individuellen Nutzung ihrer Computer oder anderer internetfähiger Geräte: „[T]he users have no control over what happens with their data, e.g. they cannot verify the data is not passed on to third parties. This situation may influence individuals notion of privacy which may be perceived as a non-valuable asset“ (Europäische Kommission 2015b: 95).

Wie es bereits aus dem Sub-Text dieser Aussage herauszulesen ist, geht es in weiterer Folge jedoch nicht lediglich darum, die Individuen beim Schutz ihrer Daten zu unterschützen, sondern auch darum, sie dafür zu sensibilisieren, welchen ökonomischen Wert die Weitergabe ihrer Daten für die Privatwirtschaft hat: „Data protection and privacy frameworks in Member States and Associated Countries need to be implemented in a transparent and user-friendly way to help users understand how their personal data might be used, including the economic value of their data“ (Europäische Kommission 2015b: 95).

Ein solches „Wissen“ über den geschulten Umgang mit den eigenen Daten könne dazu beitragen, dass die „durchschnittlichen User\*innen“ aus Wertschätzung für die „freie“ Nutzung von Internetseiten diese bereitwilliger zur Verfügung zu stellen: „Such knowledge will enable them to exercise choice and know and assert their rights. As the economic value of their data is not known to the average user, they are not able to evaluate the value of their data relative to the value they assign to a "free" service“ (ebda.). Dem „average user“ wird hier in einer Ausschreibung, die den Titel „Privacy“ trägt vermittelt, dass er sich durch schieres Unwissen möglicherweise dagegen entscheidet, seine Daten im Tauschgeschäft gegen die Benutzung einer Gratis-Internetseite zur Verfügung zu stellen. Es trifft hier paradoxerweise in einem Sicherheitsforschungsprogramm das Element der Desecuritisation des individuellen Datenschutzes auf den Versuch, ein Bewusstsein für die Bedeutung von Nutzer\*innendaten für das „well-functioning“ des europäischen Binnenmarktes zu schaffen.

## 4.7 Tabellarische Zusammenfassung der Forschungsergebnisse

Als Abschluss des empirischen Teils soll in Form einer Tabelle eine zusammenführende Übersicht über die wichtigsten Forschungsergebnisse geboten werden. Dabei geht es vor allem darum, die besonderen Charakteristika der einzelnen Programme, die im Zuge der Analyse ermittelt wurden, einander systematisch gegenüberzustellen. Im Anschluss daran wird in den Schlussfolgerungen noch eine abschließende Interpretation der Ergebnisse vorgenommen.

**Tabelle 1: Vergleichende Darstellung der Forschungsergebnisse**

	<i>EU</i>	<i>Deutschland</i>	<i>Österreich</i>
<b>Ausrichtung, Bedrohungsbilder, Zielsetzungen</b>			
▷ Bedrohungsbilder	Negativeffekte global vernetzter Handels- und Kommunikationsstrukturen, Risiken durch neue IKTs	die Welt im Wandel, unvorhersehbare Veränderungen, erhöhte Vernetzung und Komplexität durch Globalisierung	die Welt im Wandel, unvorhersehbare Veränderungen
▷ Sicherheitsbegriff	Umfassend; Hervorhebung von Resilienz als Faktor ziviler Sicherheit	Umfassend; Sicherheit als Wert, Sicherheit als Faktor wirtschaftlichen Wohlstands, zivile Sicherheit als „Resultat“ der Globalisierung	Umfassend; Beschränkung auf öffentliche und nationale Sicherheit
▷ Referenzobjekte	die Bürger*innen, die Gesellschaft; die europäische Volkswirtschaft, Infrastrukturen, Dienstleistungen, politische Stabilität, Wachstum und Wohlstand	„möglichst alle Menschen“, deutsche Bürger*innen, Wirtschaftsstandort Deutschland, das freie Leben	Bevölkerung Österreichs, nationalstaatliche Souveränität
▷ Sicherheitsakteure	„public authorities“ als	der Staat als	der Staat als Gewährleister

	Verantwortungsträger bei der Gewährleistung ziviler Sicherheit	Gewährleister von Sicherheit; geteilte Verantwortung von „Staat, Wirtschaft und Gesellschaft“; öffentliche und private Sicherheitsdienstleister	von Sicherheit; Sicherheit als „öffentliches Gut“, für das die öffentliche Hand Sorge zu tragen hat
▷ Forschungsbegriff	anwendungsorientiert; stakeholderorientiert; marktorientiert (= kommerzielle Verwertbarkeit der Forschungsergebnisse)	interdisziplinär, anwendungsorientiert, empfohlene Einbindung der Gesellschaftswissenschaften	interdisziplinär, missionsorientiert, verpflichtende Stakeholder-Einbindung, verpflichtende GSK-Einbindung
▷ Strategische Ziele	den europäischen Markt für Cybersicherheitsprodukte stärken	Deutschland als führender Anbieter von Sicherheitstechnologien; Mitgestaltung der europäischen Sicherheitsarchitektur durch deutsche Akteure	Stärkung der heimischen Sicherheitswirtschaft durch Schaffung von Arbeitsplätzen
<b>Resilienz</b>			
▷ zyklische Gefahrenbetrachtung	Katastrophenvor- und Nachsorge, Wiederherstellung des Status Quo; Lernprozesse	Katastrophenvor- und Nachsorge, Wiederherstellung des Status Quo, Lernprozesse	Katastrophenvor- und Nachsorge, Wiederherstellung des Status Quo, Lernprozesse
▷ Alle Gefahren – alle Kosten?	Integration materieller und ökonomischer Schäden; Gesamtbetrachtung sozioökonomischer Kosten	„materielle und gesellschaftliche Schäden“	umfassende Gefahrenbetrachtung, jedoch Beschränkung auf Bevölkerungsschutz und kritische Infrastrukturen
▷ die Rolle der Bevölkerung	passiv; Krisenkommunikation mit „first responders“, Aufklärungs- und Informationsarbeit	eher passiv; Verbesserung der Selbsthilfefähigkeit im Krisenfall durch Aufklärungsarbeit	passiv; verbesserte Krisenkommunikation mithilfe neuer Kommunikationsmedien

▷ Klimawandel-Adaption	Adaption an Auswirkungen des Klimawandels; Klimawandel als territoriale Bedrohung durch klimabedingte Migration	Adaption an Auswirkungen des Klimawandels; Beitrag zum internationalen Katastrophenmanagement	Beitrag zu den österreichischen Klimaschutzziele durch E-Mobilität
<b>Terrorismus</b>			
▷ Daten	automatisierte Datenauswertung zur Herausfilterung relevanter Inhalte aus großen Datenmengen, Standardisierungen für erleichterten Datenaustausch zwischen europäischen Strafverfolgungsbehörden	automatisierte Software zur Unterstützung der Strafverfolgung <i>nach</i> einem Anschlag	Technologien zur semiautomatisierten Suche und Analyse, Erwägung automatisierter Analysen zur Untersuchung sozialer Netzwerke nach Radikalisierungstendenzen
▷ Terror im Kontext anderer Delikte	Maßnahmen gegen Terror <i>und</i> Cybercrime, Cyberterrorismus, Wirtschaftskriminalität, organisiertes Verbrechen, Menschenhandel, „high impact petty crimes“, häusliche Gewalt	Maßnahmen gegen Terror <i>und</i> kriminelle Übergriffe im öffentlichen Raum	Maßnahmen gegen Terror <i>und</i> Großschadensereignisse
▷ (De)-Radikalisierung	Radikalisierungsprävention , Fokus auf sozioökonomische Ursachen von Radikalisierung	-	Radikalisierungsprävention , der Islam als Bedrohung für die innere Sicherheit
<b>Migration</b>			
▷ menschliche Sicherheit	Überwachungstechnologien für search and rescue operations auf See	mobile, nichtinvasive Überwachungsmethoden für den Schwerlastverkehr	Gewährleistung der Rechtssicherheit für Opfer von Menschenhandel
▷ Inszenierung “illegaler Migration” als	EUROSUR-Überwachungstechnologie	-	-

systemisches Risiko	n gegen „illegale Migration“ <i>und</i> Schmuggel, Drogenhandel, terroristische Bedrohung; Aussiebung „bedrohlicher“ Migrant*innen ohne den Personen- und Warenverkehr zu unterbrechen		
<b>Gefühle und Werte als Referenzobjekte</b>			
▷ Sicherheitsempfinden und Lebensqualität	Sicherheitswahrnehmung <i>und</i> ökonomische Entwicklung <i>und</i> Lebensqualität	freies Leben, Freiheit ( <i>und</i> wirtschaftlicher Wohlstand), Lebensqualität, Sicherheitsempfinden (Kriminalitätsfurcht und Unsicherheitsgefühle)	objektive Sicherheitslage <i>und</i> subjektives Sicherheitsempfinden
▷ Schutz kultureller Werte und Güter	kulturelles Erbe als Quelle individueller und kollektiver Identität <i>und</i> kommunaler Wirtschaftsfaktor	-	Kulturgüter als „Definitionsbasis einer Gesellschaft“, das österreichische als Teil des europäischen kulturellen Erbes
<b>„Sicherheit für die Wirtschaft“</b>			
▷ die Volkswirtschaft und Unternehmen als Referenzobjekte	„panta rhei“ → diskursive Transformation der Grenz- und Flugsicherheit, Fokus auf „nicht-invasive Überwachungstechnologie n aus der Distanz, „risikobasierte“ Sicherheit, „illegale“ Migration <i>und</i> Zollkriminalität	die Bürger*innen <i>und</i> Unternehmen, die Bevölkerung <i>und</i> die deutsche Wirtschaft, Unternehmen <i>und</i> kritische Infrastrukturbetreiber; Bedrohung der deutschen Wirtschaft durch äußere und innere Kräfte	Gesellschafts- <i>und</i> wirtschaftspolitische Auswirkungen bei Ausfall kritischer Infrastrukturen
▷ Primat des Fortschritts?	„ICT-driven	proaktiver Ausgleich der	proaktiver <i>und</i> Ausgleich

	transformations“ als Gefahr für Gesellschaft <i>und</i> das wirtschaftliche Wachstum <i>und</i> das technologische Innovationspotenzial der EU	Risiken der Wirtschaft/Industrie 4.0	negativer Seiteneffekte der fortschreitenden Digitalisierung/Robotisierung
▷ Digitale Sicherheit	Desecuritisation des individuellen Datenschutzes; Schutz des europäischen Digital Single Markets	-	Groß- und Mittelstandsunternehmen als Referenzobjekt

## 5 Schlussfolgerungen

Zu Beginn wurde die Frage gestellt, wie Sicherheit in den Forschungsprogrammen zur zivilen Sicherheit diskursiv konstruiert wird. Um einer Beantwortung dieser Frage näherzukommen wurden sechs empirische Kategorien gebildet, in denen unterschiedliche Narrative und diskursive Besonderheiten analysiert wurden. Als theoretischer Hintergrund wurden Konzepte und empirische Arbeiten herangezogen, die dem Komplex polit-technologischer Entwicklungen im Bereich der inneren/zivilen Sicherheit skeptisch gegenüberstehen bzw. sich kritisch damit auseinandergesetzt haben. Daraus entwickelte sich die Sub-Forschungsfrage, ob die Themen und Gewichtungen in der Sicherheitsforschung Ausdruck einer tiefgreifenden neoliberalen Gouvernamentalität sind oder nicht.

Was in der Analyse zum Ausdruck kam, ist ein starker Fokus auf die Wirtschaft in Fragen ziviler Sicherheit. Das Verständnis von ziviler Sicherheit, für das im *europäischen* Programm am stärksten und im *deutschen* Programm in subtilerer Form geworben wird, ist eines, dass sich nicht mehr daran gebunden sehen will, dass unter „zivil“ zwingend auch der Schutz einer wie auch immer zu definierenden *Zivilbevölkerung* gemeint sein muss. Argumentativ kommt bei diesem Versuch das Konzept einer sogenannten „systemischen“ und „ganzheitlichen“ Perspektive auf Sicherheit zu Hilfe, die es ermöglicht, die Volkswirtschaft und potenzielle wirtschaftliche Verluste nie aus den Augen zu lassen. Insofern kann von einem „Wirtschaftsdispositiv“ gesprochen werden, der das Feld der Akteure in der europäischen Sicherheitsforschung derzeit dominiert. Er macht sich auf unterschiedliche Art und Weise bemerkbar: (1) Durch die Wirtschaft als direktes oder indirektes Referenzobjekt, (2) durch die wachsame Haltung gegenüber den Risiken der fortschreitenden Digitalisierung, (3) in der Priorisierung der Förderung marktauglicher, hochtechnologischer Forschung und (4) durch eine Vorwegnahme des Effizienzgedankens bei sicherheitspolitischen Überlegungen.

Das deutsche und das europäische Programm sind von dieser Denkstruktur in ihren Narrativen viel stärker durchdrungen als das österreichische Programm. Das *österreichische* Programm geht im Vergleich dazu – entsprechend seiner engeren Definition ziviler Sicherheit – einen „traditionelleren“ Weg. Die ausgeschriebenen

Maßnahmen sind oftmals partikular und weniger ganzheitlich ausgelegt, wirken dadurch jedoch auch gezielter an der tatsächlichen Arbeit der Exekutive und anderen Einsatzorganisationen im Bereich der öffentlichen Sicherheit orientiert. Der Fokus auf kritische Infrastrukturen wird – bis auf einige Grenzüberschreitungen – nicht maßgeblich dazu verwendet, die Volkswirtschaft oder wirtschaftliche Prozesse und Akteure miteinzusetzen. Ein starker Fokus auf Cyberbedrohungen sowie andere unerwünschte Nebeneffekte der Digitalisierung ist auch in KIRAS vorhanden.

Die Frage ist, ob ein „Wirtschaftsdispositiv“ gleichzeitig auch Ausdruck einer neoliberalen Gouvernamentalität sein muss oder umgekehrt. Meines Erachtens kann keines der drei Programme schwarz oder weiß gesehen werden. Tatsache ist, dass wir in einer bis auf wenige Ausnahmen kapitalistisch organisierten Wirklichkeit leben und es im Interesse von Nationalstaaten wie auch der supranationalen Institution EU (deren Existenzgrundlage ein gemeinsamer Wirtschaftsraum ist), auf das reibungslose Funktionieren und zugespitzt – das Überleben – dieser Volkswirtschaften in der Welt zu achten. Dieser Gedanke drückt sich in vielen Maßnahmen aus, deren Referenzobjekt nicht die physische Unversehrtheit (oder meinetwegen tatsächlich das Wohl und die Lebensqualität) der Bürger\*innen ist, sondern Dinge sind, die weit darüber hinausgehen oder gelegentlich auch dazu in Widerspruch stehen. Auch führt es dazu, dass die zivile Sicherheit zu einem Spielfeld wird, wo es den Anschein hat, dass „klassische“ Bereiche der inneren Sicherheit gegenüber außen-/wirtschaftspolitischen Fragestellungen ins Hintertreffen geraten.

Was aus meiner Sicht gegenwärtig jedenfalls nicht vorherrschend ist, ist ein „Überwachungsdispositiv“, der den Terrorismus miteinschließt. Das Ziel einer möglichst flächendeckenden Überwachung des öffentlichen Raumes sowie der Kommunikations- und Bewegungsdaten von Personen mit unterschiedlichen (vernetzten) Technologien im Zeichen der Terrorismusprävention scheint keine Priorität mehr zu sein. Der Terrorismus erfüllt insbesondere im Programm der EU dort seine Funktion, wo er synergetisch auch zur Bekämpfung von Wirtschaftsdelikten im Bereich der Cyberkriminalität nützlich sein kann. Und für Technologien der Überwachung aus der Distanz sind Argumente des Komforts, der Effizienz und des volkswirtschaftlichen Nutzens ausreichend, um ihre Notwendigkeit zu begründen. Allenfalls ersetzt „Migration“ den „Terrorismus“ als alles legitimierenden Signifier auf dem Kontinuum, der den Vorteil besitzt, dass hier neben

dem Betreten europäischen Bodens durch „unerwünschte“ Personen („alles Kriminelle, die nur auf Sozialleistungen aus sind und die Volkswirtschaft gefährden“) auch die Fantasie einer potenziellen terroristischen Bedrohung („alles Terroristen“) bereits inbegriffen ist.

Gleichzeitig sind in allen Programmen auch „traditionelle“, personalintensive Bereiche der präventiven Sicherheit wie der Radikalisierungsprävention oder abgedeckt, wobei natürlich bei Secure Societies immer die Frage in den Raum gestellt werden kann, in welchem Mengenverhältnis Ausschreibungen im Bereich der digitalen Sicherheit und der Terrorismusbekämpfung zueinanderstehen. In der neoliberalen „Idealvorstellung“ sollte sich der Staat so weit wie möglich zurückziehen und so viele Aspekte des Lebens und der Wirtschaft den Kräften des „freien Marktes“ überlassen. Insofern widerspricht es diesem Prinzip, dass Millionen an öffentlichen Ressourcen dafür aufgewendet werden, wie sich Unternehmen besser vor Cyberattacken schützen können. Staaten und die Europäische Union müssten dabei zusehen, wie Unternehmen in einem freien Spiel der Kräfte Schaden nehmen und in Folge dessen entsprechende Maßnahmen setzen (z.B. entsprechende Technologien in Auftrag geben oder zusperren). Dies steht aber im Konflikt mit außenpolitischen Ängsten und Interessen, in denen die Sicherung und der Schutz des eigenen Wirtschaftsstandorts gegenüber äußeren (und auch inneren) Bedrohungen von großer Bedeutung ist. Es stellt sich in diesem Kontext jedoch auch die Frage, ob es erstens legitim und zweitens sinnvoll ist, die Bedingungen der zivilen Sicherheitsforschung a priori so zu setzen, dass sie nur Resultate erbringt, die dieser wirtschaftsfreundlichen oder sei es „ganzheitlichen“, „systemischen“ Perspektive gerecht wird. Zum europäischen Programm hätte der Untertitel „Security for the economy“ besser gepasst. Da wäre es aufrichtiger, von der ohnehin oft nur scheinbaren ganzheitlichen Perspektive wegzugehen und sich in einem Teil tatsächlich der Sicherheit der „citizens“ zu widmen und in einem anderen der „economy“. Die politische Realität und die Kompromisse, die dort gemacht werden müssen, sehen freilich oft anders aus.

Was durchaus als „neoliberal“ gedeutet werden kann, ist das als unumkehrbarer Sachzwang konstruierte „Effizienzargument“, dass allzu oft als Legitimation für die Wahl oder das Forschungsinteresse an einer bestimmten Technologie dient und mit dem Wirtschaftsdispositiv einhergeht. Es entspricht der politischen Wirklichkeit, dass

die Exekutive bis zu einem gewissen Grad effizient arbeiten sollte. Die Frage ist, ob Sicherheitsforschung Sparzwänge und das Diktat der Personaleffizienz bereits unhinterfragt vorwegnehmen muss. Auch ist fraglich, inwiefern Technologien, die diesem Effizienzdruck vermeintlich entgegenkommen, wie die Entwicklung automatisierter, mit künstlicher Intelligenz ausgestatteter Software, diesem Anspruch tatsächlich entgegenkommt. Mittlerweile ist bekannt, dass es in vielen Fällen trotz der vorhandenen rechtlichen Möglichkeiten aufgrund von Personalengpässen zur Sichtung und Nutzung dieser Daten insbesondere zu präventiven Zwecken gar nicht kommt (siehe dazu z.B. die aufschlussreiche Dokumentation „Der Anschlag“, Das Erste 2017). Um tatsächlich anwendungsorientiert zu sein, müsste Sicherheitsforschung sich in einer nicht nur scheinbar interdisziplinären Arbeit auch im Vorhinein intensiv mit der Frage auseinandersetzen, welche personellen Aufwendungen es brauchen würde, damit „man and machine“ unter Berücksichtigung aller rechtlichen Auflagen tatsächlich sinnvolle Resultate erzielen. Der Griff oder die Nachfrage nach Überwachungstechnologien insbesondere im Bereich der Grenzsicherheit scheinen meines Erachtens auch eher ein Ausdruck des Wirtschafts- bzw. Wirtschaftlichkeitsdispositivs zu sein als von einem Überwachungsdurst sui generis getrieben.

Das Resilienz-Konzept passt in seiner Formbarkeit in die wirtschaftsorientierte Sicht auf zivile Sicherheit gut hinein. Eine „neoliberale“ Transformation von Sicherheit verursacht Resilienz in der Art und Weise, wie es in den Programmen umgesetzt werden soll, jedoch meines Erachtens nach nicht. Es kann auf Notfallszenarien angewandt werden, ermöglicht jedoch auch einen weitsichtigeren, „systemischen“ Blick auf kollektive Entitäten unterschiedlicher Größe. Es verlangt nicht nach akuten Notsituationen, um sich mit Fragen auseinanderzusetzen, wie die Situation einer vulnerablen Gruppe (sei dies geographisch, sozial oder andersbedingt) nachhaltig verbessert werden könnte, noch bevor es zu einer katastrophalen Entwicklung kommt. Resilienz befasst sich nicht zwingend mit Ausnahmesituationen, fügt dem Sicherheitsdenken ein Element der Nachhaltigkeit hinzu, dass freilich auch aus volkswirtschaftlicher Sicht von Nutzen sein kann. Was das Verhältnis von Sicherheit und Resilienz anbelangt, so kann anhand der Analyse nicht argumentiert werden, dass die Integration des Resilienz-Konzepts in irgendeiner Form einem „Weniger“ an öffentlich-gewährter Sicherheit Vorschub leistet.

## Literaturverzeichnis

Aradau, Claudia (2014): The promise of security. Resilience, surprise and epistemic politics. In: *Resilience* 2 (2), S. 73–87. DOI: 10.1080/21693293.2014.914765.

Aradau, Claudia; van Munster, Rens (2007): Governing Terrorism Through Risk. Taking Precautions, (un)Knowing the Future. In: *European Journal of International Relations* 13 (1), S. 89–115. DOI: 10.1177/1354066107074290.

Aradau, Claudia; van Munster, Rens (2013): Politics of catastrophe. Genealogies of the unknown. Paperback [ed.]. London: Routledge (PRIO new security studies).

Beck, Ulrich (2007): Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit. 1. Aufl. Frankfurt am Main: Suhrkamp (Edition Zweite Moderne).

Bigo, Didier (2008): Globalized (in)security: the field and the ban-opticon. In: Didier Bigo und Anastassia Tsoukala (Hg.): Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11.: Routledge, S. 10–48.

Bigo, Didier (2013): Security. Analysing transnational professionals of (in)security in Europe. In: Rebecca Adler-Nissen (Hg.): Bourdieu in international relations. Rethinking key concepts in IR. 1. publ. London u.a.: Routledge (The new international relations series), S. 114–130. Online verfügbar unter <http://site.ebrary.com/lib/uniregensburg/Doc?id=10603747>.

Bigo, Didier (2016): Rethinking Security at the Crossroad of International Relations and Criminology. In: *CRIMIN* 56 (6), S. 1068–1086. DOI: 10.1093/bjc/azw062.

Bigo, Didier; Bonelli, Laurent; Chi, Dario; Olsson, Christian (2007): Mapping the Field of the EU Internal Security Agencies. Paper produced for the Changing Landscape of European Liberty and Security (CHALLENGE) Project of the Centre for European Policy Studies (CEPS). Online verfügbar unter [http://www.open.ac.uk/researchprojects/iccm/files/iccm/Bigo\\_Bonelli\\_Chi\\_Olsson.pdf](http://www.open.ac.uk/researchprojects/iccm/files/iccm/Bigo_Bonelli_Chi_Olsson.pdf), zuletzt geprüft am 14.02.2018.

Bigo, Didier; Tsoukala, Anastassia (2008): Understanding (in)security. In: Didier Bigo und Anastassia Tsoukala (Hg.): Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11.: Routledge, S. 1–9.

BMBF (2012a): Bekanntmachung. 01.06.2012 - 15.08.2012. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=745>, zuletzt aktualisiert am 31.05.2012, zuletzt geprüft am 30.04.2018.

BMBF (2012b): Bekanntmachung. 20.12.2012 - 15.03.2013. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=794>, zuletzt geprüft am 01.05.2018.

BMBF (2012c): Bekanntmachung. 29.03.2012 - 20.06.2012. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=734>, zuletzt aktualisiert am 26.03.2012, zuletzt geprüft am 07.05.2018.

BMBF (2013): Bekanntmachung - BMBF. 01.03.2013 - 24.05.2013. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=821>, zuletzt aktualisiert am 22.02.2013, zuletzt geprüft am 19.05.2018.

BMBF (2014a): Bekanntmachung. 02.05.2014 - 15.08.2014. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=937>, zuletzt aktualisiert am 28.04.2014, zuletzt geprüft am 30.04.2018.

BMBF (2014b): Bekanntmachung. 15.07.2014 - 26.09.2014. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung-950.html>, zuletzt aktualisiert am 03.07.2014, zuletzt geprüft am 14.05.2018.

BMBF (2014c): Bekanntmachung. 22.01.2014 - 05.05.2014. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=911>, zuletzt aktualisiert am 08.01.2014, zuletzt geprüft am 30.04.2018.

BMBF (2015): Bekanntmachung. 05.10.2015 - 01.02.2016. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=1089>, zuletzt aktualisiert am 08.09.2015, zuletzt geprüft am 08.03.2018.

BMBF (2016a): Bekanntmachung. 12.10.2016 - 08.02.2017. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung-1252.html>, zuletzt aktualisiert am 29.07.2016, zuletzt geprüft am 09.03.2018.

BMBF (2016b): Bekanntmachung. 14.01.2016 - 25.04.2016. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung.php?B=1125>, zuletzt aktualisiert am 04.01.2016, zuletzt geprüft am 07.05.2018.

BMBF (2016c): Bekanntmachung. 20.07.2016 - 30.09.2016. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung-1208.html>, zuletzt aktualisiert am 27.06.2016, zuletzt geprüft am 10.04.2018.

BMBF (2016d): Bekanntmachung. 26.07.2016 - 12.10.2016. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung-1211.html>, zuletzt aktualisiert am 27.06.2016, zuletzt geprüft am 30.04.2018.

BMBF (2016e): Forschung für die zivile Sicherheit 2012 – 2017. Rahmenprogramm der Bundesregierung. Aktualisierte Auflage. Online verfügbar unter [https://www.bmbf.de/pub/Rahmenprogramm\\_Sicherheitsforschung.pdf](https://www.bmbf.de/pub/Rahmenprogramm_Sicherheitsforschung.pdf), zuletzt geprüft am 09.02.2018.

BMBF (2016f): Neuerungen in Horizont 2020 - Horizont 2020. Online verfügbar unter <http://www.horizont2020.de/einstieg-neuerungen.htm>, zuletzt geprüft am 10.02.2018.

BMBF (2017a): Bekanntmachung. 06.10.2017 - 15.12.2018. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung-1416.html>, zuletzt aktualisiert am 05.09.2017, zuletzt geprüft am 14.05.2018.

BMBF (2017b): Bekanntmachung. 15.09.2017 - 02.02.2018. Online verfügbar unter <https://www.bmbf.de/foerderungen/bekanntmachung-1402.html>, zuletzt aktualisiert am 27.07.2017, zuletzt geprüft am 01.05.2018.

BMBF (2017c): Innovationsunion. Online verfügbar unter <https://www.bmbwf.gv.at/forschung/europaeisch/innovationsunion/innovationsunion/>, zuletzt geprüft am 08.02.2018.

BMBF (2018): Startseite - BMBF Sicherheitsforschung. Online verfügbar unter <https://www.sifo.de/>, zuletzt aktualisiert am 12.01.2018, zuletzt geprüft am 09.02.2018.

bmvit (2014): FTI- Initiative KIRAS. Ausschreibungsleitfaden. Schutz kritischer Infrastrukturen Version 1.4. Wien.

bmvit (2015a): Das Österreichische Förderungsprogramm für Sicherheitsforschung KIRAS. Wien. Online verfügbar unter [http://www.kiras.at/fileadmin/downloads/allgem15/16122015\\_PD\\_KIRAS.pdf](http://www.kiras.at/fileadmin/downloads/allgem15/16122015_PD_KIRAS.pdf), zuletzt geprüft am 09.02.2018.

bmvit (2015b): FTI- Initiative KIRAS. Ausschreibungsleitfaden. Schutz kritischer Infrastrukturen Version 1.5. Wien.

bmvit (2016): FTI- Initiative KIRAS. Ausschreibungsleitfaden. Schutz kritischer Infrastrukturen Version 1.6. Wien.

bmvit (2017a): FTI- Initiative KIRAS. Ausschreibungsleitfaden. Schutz kritischer Infrastrukturen Version 1.7.

bmvit (2017b): Sicherheitsforschungsprogramm KIRAS. Was ist KIRAS. Online verfügbar unter <https://www.bmvit.gv.at/bilder/factsheets/kiras.jpg>, zuletzt geprüft am 09.02.2018.

bmvit (2018): Grundlagen von Kiras. Die Grundlagen des KIRAS-Programms. Online verfügbar unter <http://www.kiras.at/das-programm/grundlagen-von-kiras/>, zuletzt aktualisiert am 27.02.2018, zuletzt geprüft am 10.05.2018.

Borger, Julian (2017): Trump drops climate change from US national security strategy 2017, 19.12.2017. Online verfügbar unter <https://www.theguardian.com/us-news/2017/dec/18/trump-drop-climate-change-national-security-strategy>, zuletzt geprüft am 14.05.2018.

Brem, Richard (2018): Radiokolleg - Kybernetik. Zur Selbststeuerung von Systemen in Natur, Gesellschaft und Technik (2) (1). Ö1, 15.05.2018. Online verfügbar unter <https://oe1.orf.at/programm/20180515/517708>, zuletzt geprüft am 15.05.2018.

Buzan, Barry; Hansen, Lene (2009): *The evolution of international security studies*. Cambridge, UK, New York: Cambridge University Press. Online verfügbar unter <http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10349792>.

Buzan, Barry; Wæver, Ole (2009): Macrosecuritisation and security constellations. Reconsidering scale in securitisation theory. In: *Review of International Studies* 35 (02), S. 253–276. DOI: 10.1017/S0260210509008511.

Buzan, Barry; Wæver, Ole; Wilde, Jaap de (1998): *Security. A new framework for analysis*. Boulder, Colo.: Lynne Rienner.

Chandler, David; Coaffee, Jon (2017): Introduction. Contested paradigms of international resilience. In: David Chandler und Jon Coaffee (Hg.): *Routledge handbook of international resilience (Routledge handbooks)*, S. 3–9.

Chandler, David; Reid, Julian (Hg.) (2016): The neoliberal subject. Resilience, adaptation and vulnerability. Online verfügbar unter <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1229871>.

Collins, H. M.; Evans, Robert (2002): The Third Wave of Science Studies. Studies of Expertise and Experience. In: *Soc Stud Sci* 32 (2), S. 235–296. DOI: 10.1177/0306312702032002003.

Daase, Christopher (Hg.) (2002): *Internationale Risikopolitik. Der Umgang mit neuen Gefahren in den internationalen Beziehungen*. 1. Aufl. Baden-Baden: Nomos-Verl.-Ges.

Daase, Christopher (2010): Der Wandel der Sicherheitskultur. Ursachen und Folgen des erweiterten Sicherheitsbegriffs. In: Peter Zoche, Stefan Kaufmann und Rita Haverkamp (Hg.): *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitik*: transcript, S. 139–158.

Der Anschlag (2017) (Die Story im Ersten). Das Erste, 11.12.2017. Online verfügbar unter <https://www.ardmediathek.de/tv/Reportage-Dokumentation/Die-Story-im-Ersten-Der-Anschlag/Das-Erste/Video?bcastId=799280&documentId=48312570>, zuletzt geprüft am 18.05.2018.

Duden Online (o. J.): "Risiko" in Duden Online. Online verfügbar unter <https://www.duden.de/node/645699/revisions/1682711/view>, zuletzt aktualisiert am 11.05.2018, zuletzt geprüft am 11.05.2018.

Europäische Kommission (2005): Beschluss der Kommission vom 22. April 2005 zur Gründung des Europäischen Beirats für Sicherheitsforschung. Online verfügbar unter <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32005D0516>, zuletzt geprüft am 10.02.2018.

Europäische Kommission (2012): Work Programme 2013. Cooperation Theme 10 Security. Online verfügbar unter [http://ec.europa.eu/research/participants/data/ref/fp7/132153/k-wp-201301\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/fp7/132153/k-wp-201301_en.pdf), zuletzt geprüft am 10.02.2018.

Europäische Kommission (2013): Factsheet: Horizon 2020 budget. Online verfügbar unter [https://ec.europa.eu/research/horizon2020/pdf/press/fact\\_sheet\\_on\\_horizon2020\\_budget.pdf](https://ec.europa.eu/research/horizon2020/pdf/press/fact_sheet_on_horizon2020_budget.pdf), zuletzt geprüft am 08.02.2018.

Europäische Kommission (2015a): Cooperation: Security. Brüssel. Online verfügbar unter [https://ec.europa.eu/research/fp7/index\\_en.cfm?pg=security](https://ec.europa.eu/research/fp7/index_en.cfm?pg=security), zuletzt aktualisiert am 25.08.2015, zuletzt geprüft am 08.02.2018.

Europäische Kommission (2015b): HORIZON 2020. WORK PROGRAMME 2014-2015. Brüssel. Online verfügbar unter [http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014\\_2015/main/h2020-wp1415-security\\_v1.0\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_v1.0_en.pdf), zuletzt geprüft am 07.03.2018.

Europäische Kommission (2016): Strategie Europa 2020. Brüssel. Online verfügbar unter [https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy\\_de](https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/eu-economic-governance-monitoring-prevention-correction/european-semester/framework/europe-2020-strategy_de), zuletzt aktualisiert am 11.07.2016, zuletzt geprüft am 08.02.2018.

Europäische Kommission (2017a): Horizon 2020. Work Programme 2016 - 2017. Brüssel. Online verfügbar unter

[http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016\\_2017/main/h2020-wp1617-intro\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-intro_en.pdf), zuletzt geprüft am 07.03.2018.

Europäische Kommission (2017b): Horizon 2020. Work Programme 2018-2020. Online verfügbar unter [http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf), zuletzt geprüft am 07.03.2018.

Europäische Kommission (2018a): Register of Commission expert groups and other similar entities. Horizon 2020 Protection And Security Advisory Group (E03010). Online verfügbar unter <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010>, zuletzt aktualisiert am 06.02.2018, zuletzt geprüft am 10.02.2018.

Europäische Kommission (2018b): What is Horizon 2020? Online verfügbar unter <https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020>, zuletzt aktualisiert am 08.02.2018, zuletzt geprüft am 08.02.2018.

Evans, Robert (2015): What is expertise? Technical knowledge and political judgement. In: Trine Villumsen Berling und Christian Bueger (Hg.): Security Expertise. Practice, Power, Responsibility. London, New York: Routledge (PRIO new security studies), S. 19–36.

Filzmaier, Peter; Gewessler, Leonore; Höll, Otmar; Mangott, Gerhard (2006): Internationale Politik. Eine Einführung. Wien: WUV (UTB Politikwissenschaft, 2733).

Fjäder, Christian (2014): The nation-state, national security and resilience in the age of globalisation. In: *Resilience* 2 (2), S. 114–129. DOI: 10.1080/21693293.2014.914771.

Gibbons, Michael (1995): The new production of knowledge. The dynamics of science and research in contemporary societies. 1. publ., reprint. London u.a.: Sage Publ.

Höll, Otmar (2007): The Global System between Integration and Fragmentation. In: Ewa Czerwinska und Ewa Czerwinska-Schupp (Hg.): Values and Norms in the Age

of Globalization. 1. Aufl. Frankfurt a. M.: Peter Lang GmbH Internationaler Verlag der Wissenschaften (DIA-LOGOS, 9), S. 413–433.

Huysmans, Jef (2006): The politics of insecurity. Fear, migration and asylum in the EU. London, New York: Routledge (The new international relations).

Jäger, Siegfried (2015): Kritische Diskursanalyse. Eine Einführung. 7., vollst. überarb. Aufl. Münster: Unrast (Edition DISS, 3).

Joseph, Jonathan (2013a): Resilience as embedded neoliberalism: a governmentality approach. In: *Resilience* 1 (1), S. 38–52, zuletzt geprüft am 24.07.2017.

Joseph, Jonathan (2013b): Resilience in UK and French Security Strategy: An Anglo-Saxon Bias? In: *Politics* 33 (4), S. 253–264, zuletzt geprüft am 24.07.2017.

Joseph, Jonathan (2016): Governing through Failure and Denial: The New Resilience Agenda. In: *Millenium: Journal of International Studies* 44 (3370-390).

Korunka, Rita (2017): Re-Artikulation des Alltäglichen durch einen neuen feministischen Mainstream? Ein diskursanalytischer Vergleich der Onlinemedien Lenny, Broadly und Huffington Post. Masterarbeit. FHWien der WKW, Wien. Journalismus & Medienmanagement.

Kühn, Florian P. (2017): Risikopolitik. Eine Einführung: Springer Fachmedien Wiesbaden.

Merriam-Webster Online (o. J.): "Risk". Online verfügbar unter <https://www.merriam-webster.com/dictionary/risk>, zuletzt aktualisiert am 12.05.2018, zuletzt geprüft am 12.05.2018.

Münkler, Herfried; Wassermann, Felix (2012): Von strategischer Vulnerabilität zu strategischer Resilienz: Die Herausforderung zukünftiger Sicherheitsforschung und Sicherheitspolitik. In: Lars Gerhold, Jochen H. Schiller, Wolf R. Dombrowsky und Forschungsforum Öffentliche Sicherheit (Hg.): Perspektiven der Sicherheitsforschung. Beiträge aus dem Forschungsforum Öffentliche Sicherheit, S. 77–95.

Pospisil, Jan; Gruber, Barbara (2016): Resilience and the transformation of sovereign security. A look at policy challenges and interests. In: *Resilience* 4 (3), S. 202–216. DOI: 10.1080/21693293.2016.1210256.

Rogers, Peter (2015): Researching resilience. An agenda for change. In: *Resilience* 3 (1), S. 55–71. DOI: 10.1080/21693293.2014.988914.

Saldaña, Johnny (2009): *The Coding Manual for Qualitative Researchers*. First published 2009. Los Angeles, London, New Delhi: SAGE.

Schumann, Harald; Simantke, Elisa (2016): Europa plant den Überwachungsstaat. In: *Tagesspiegel* 2016, 10.12.2016. Online verfügbar unter <https://www.tagesspiegel.de/weltspiegel/sonntag/sicherheitspolitik-europa-plant-den-ueberwachungsstaat/14956574.html>, zuletzt geprüft am 15.05.2018.

Tierney, Kathleen J. (2014): *The social roots of risk. Producing disasters, promoting resilience*. Stanford, California: Stanford Business Books an imprint of Stanford University Press (High reliability and crisis management).

Villumsen Berling, Trine (2011): Science and securitization. Objectivation, the authority of the speaker and mobilization of scientific facts. In: *Security Dialogue* 42 (4-5), S. 385–397. DOI: 10.1177/0967010611418714.

Villumsen Berling, Trine; Bueger, Christian (2015): Security expertise: an introduction. In: Trine Villumsen Berling und Christian Bueger (Hg.): *Security Expertise. Practice, Power, Responsibility*. London, New York: Routledge (PRIO new security studies), S. 1–18.

Wæver, Ole (2015): The history and social structure of security studies as a practico-academic field. In: Trine Villumsen Berling und Christian Bueger (Hg.): *Security Expertise. Practice, Power, Responsibility*. London, New York: Routledge (PRIO new security studies), S. 76–106.

Yenneti, Komalirani (2012): Vulnerability. In: S. George Philander (Hg.): *Encyclopedia of Global Warming and Climate Change, Second Edition*. Three Volume Set: Sage Publ, S. 1444–1448.

Zebrowski, Chris (2016): The value of resilience. Securing life in the 21st century. Abingdon, Oxon, New York, NY: Routledge (Interventions).

## **Abstracts**

### ***[Deutsch] Konstruktionen ziviler Sicherheit in der Forschungsförderung: ein diskursanalytischer Vergleich zwischen der EU, Deutschland und Österreich***

Was Sicherheit bedeutet, ist seit jeher umkämpft. Unterschiedliche Definitionen dessen, was als sicher oder bedrohlich gilt, ziehen unterschiedliche politische Maßnahmen nach sich. Diese Arbeit beschäftigt sich mit der Frage, wie Sicherheit im Bereich der öffentlich-geförderten zivilen Sicherheitsforschung konstruiert wird. Zu diesem Zweck wurden die nationalen Sicherheitsforschungsprogramme Deutschlands (*Sicherheitsforschung 2012-2017*) und Österreichs (*KIRAS*) sowie das aktuelle Sicherheitsforschungsprogramm der Europäischen Union (*Secure Societies*, ist ein Teil von Horizon 2020) vergleichend analysiert. Die empirische Analyse hat gezeigt, dass im Feld der europäischen Sicherheitsforschung ein Verständnis von ziviler Sicherheit im Vormarsch ist, bei dem unter „zivil“ nicht zwingend auch der Schutz einer *Zivilbevölkerung* gemeint ist. Als Referenzobjekt wird in vielen Bereichen die Wirtschaft und deren Wachstum adressiert. Diskursiv eingebettet wird dies in „systemische“ und „ganzheitliche“ Perspektiven auf Sicherheit, die es ermöglichen, der Volkswirtschaft, privatwirtschaftlichen Unternehmen, wirtschaftlichen Prozessen und Abläufen einerseits sowie Effizienz- und Spargedanken andererseits im Kontext ziviler Sicherheit breite Aufmerksamkeit zu widmen. Besonders offensiv wurde dieser Ansatz im Programm der Europäischen Union verfolgt, subtiler und weniger exzessiv auch in Deutschland. Das österreichische Programm KIRAS folgt im Vergleich dazu einer „traditionelleren“, begrenzteren Auffassung ziviler Sicherheit, wodurch die Ausschreibungen gezielter an der tatsächlichen Arbeit der Exekutive und anderen Einsatzorganisationen im Bereich der öffentlichen Sicherheit orientiert sind. Partiiell ist der „Wirtschaftsdispositiv“ allerdings auch in KIRAS bemerkbar, insbesondere bei jenen Ausschreibungen, die sich proaktiv mit den Zukunftsrisiken der fortschreitenden Digitalisierung und Robotisierung auseinandersetzen.

***[English] Discursive constructions of “civil security” in public research funding: a comparative analysis between the EU, Germany and Austria***

The meaning of the term “security” has always been contested. Different concepts and definitions of security make for differing policies and strategies. This thesis deals with the constructions of civil security circulating in the realm of European security research. Two national research programmes (Germany’s *Sicherheitsforschung 2012-2017*, Austria’s *KIRAS*) and EU’s *Secure Societies* work programmes (belong to Horizon 2020) have been subject to analysis to find out which concepts and framings of civil security are structuring the field. It turned out that “systemic” and “holistic” approaches to civil security often serve to address the economy as a referent object for civil security matters. This goes far beyond the protection of critical infrastructure and is especially true for EU’s *Secure Societies* programme. The German programme goes in the same direction (if articulated in a subtler manner), whereas the Austrian programme follows a different, more “traditional” path. It is currently based on a narrower definition of civil security and does therefore not allow for private enterprises and other economy-related assets to become security referent objects regardless of their civil security function. However, sways of the “economy dispositive” have also been noticed in the calls of the Austrian programme, especially in the proactive way risks of future technologies are approached.