

Inhalt

1. Vorwort	13
2. Einleitung.....	15
3. Eingrenzung des Themas und Begriffsbestimmungen	21
4. Die signalerfassende Aufklärung und Kommunikationsüberwachung in der Bundesrepublik Deutschland in den Jahren 1989/1990	31
Der Bundesnachrichtendienst und seine "Technische Aufklärung"	31
Die "Signalerfassende Aufklärung der Bundeswehr" 1989/1990.....	31
Die Folgen der politischen Umwälzungen für den Bundesnachrichtendienst und die Bundeswehr	33
Die Funkbeobachtung durch den Bundesgrenzschutz (BGS)	34
Das Netz des Bundesamtes für Post und Telekommunikation (BAPT).....	34
Die Kommunikationsüberwachung durch die deutschen Sicherheitsbehörden	34
Die Funk- und funktechnische Aufklärung der DDR und anderer Warschauer-Pakt-Staaten gegen die Bundesrepublik und ihre Partner im Bündnis bis zum Jahre 1989	35
Die Reorganisation der "Signalerfassenden Aufklärung" der US-Streitkräfte in Deutschland bis 1990	35
Der Stand der "Signalerfassende Aufklärung" der Vereinigten Staaten in Deutschland nach 1990	36
Die signalerfassende Aufklärung der britischen Streitkräfte in Deutschland in den Jahren 1989/1990.....	36
Die "Signalerfassende Aufklärung" der französischen Streitkräfte in Deutschland zur Jahreswende 1989/1990	37
5. Die Intelligence Community - IC der Vereinigten Staaten	39
Die Bedeutung der Anschläge am 11. September 2001 in New York und Washington (9/11)	39
Die Rolle Deutschlands im Anti-Terrorkampf der Vereinigten Staaten	40
Grundlegende Veränderungen in den Nachrichtendiensten der Vereinigten Staaten in der Folge von 09/11	41
Trends und Entwicklungen in den Nachrichtendiensten der Vereinigten Staaten ab 2004 ..	43
Der Generationswechsel in den Nachrichtendiensten der Vereinigten Staaten und die künftige Qualität nachrichtendienstlicher Informationen	44
Technische Lösungen in der Nachrichtengewinnung und Auswertung der US-Nachrichtendienste	47
Die Doktrin für den Heimatschutz	48
Die Fähigkeiten der US-Nachrichtendienste zur globalen Aufklärung.....	48
Strategien und Konzeptionen der US-Administration zur Nachrichtengewinnung und Terrorbekämpfung	49
Zugriff der US-Nachrichtendienste auf Bank- und andere Daten in der Europäischen Union.....	57
Die Rolle des US-Financial Crimes Enforcement Network - FinCen	58
Umfassende Vorbereitungen für Aufstandsbekämpfungsmaßnahmen durch die US-Streitkräfte	58
Die nächsten Schritte bei der Transformation der US-amerikanischen Nachrichtendienste	59
Die "Document and Media Exploitation" der US-Nachrichten- und Sicherheitsdienste - eine neue Waffe im Kampf gegen Terrorismus und transnationale Kriminalität?.....	60
Ziele der Reorganisationsmaßnahmen in den US-Nachrichtendiensten.....	63
Der Datenzugriff "ohne Limits" - erleichterte Bestimmungen für die US-Grenz- und Sicherheitsbehörden.....	66
Die künftigen Strategien der US-Nachrichtendienste.....	67
Einsatz eines Satelliten-Systems in erdnaher Umlaufbahn durch die Vereinigten Staaten.	68
Die Central Intelligence Agency - CIA.....	69
Die Rolle der Defense Intelligence Agency - DIA der US-Streitkräfte	70

Die Ausweitung der militärischen Auslandsaufklärung der USA und ihre Folgen	71
Das strategische Umfeld und künftige Interessenbereiche des militärischen	
Nachrichtendienstes der Vereinigten Staaten	71
Das Threat and "Local Observation Notice (TALON) Report"-Program der US-Streitkräfte	
zur Terrorbekämpfung - Rahmenbedingungen und Ergebnisse.....	73
Das Federal Bureau of Investigations auf dem Wege zum allumfassenden	
Nachrichtendienst - Die jüngste Aufgabenerweiterung beim FBI der Vereinigten Staaten. 74	
Das Department of Homeland Security - DOHS.....	77
Sonstige Dienste der Vereinigten Staaten.....	87
Die Rezeption der Aufklärungsergebnisse der US-Nachrichtendienste durch die	
politische Führung der Vereinigten Staaten	87
Das globale Netz zur Kommunikationsüberwachung der National Security Agency -	
NSA und ihrer Partner	87
Die totale Kommunikationskontrolle und Ausweitung der Kommunikationsüberwachung	
durch die National Security Agency der Vereinigten Staaten	89
Die Vorbereitungen für den globalen Informationskrieg - Das Cyber-Command	
der US-Streitkräfte	92
Der Bericht der Europäischen Union über ein globales Abhörsystem ECHELON	95
Die weltweite Signalerfassung - Signals Intelligence - SIGINT	96
Die Digital Network Intelligence - DNI-Initiative der NSA.....	97
Die Central Intelligence Agency (CIA) und ihre Rolle in der	
Kommunikationsüberwachung und Signalerfassung.....	98
Die erweiterte Rolle der Defense Intelligence Agency (DIA)	99
Die Intelligence-Architektur, SIGNALS Intelligence Erfassungs- und Auswertesysteme	
der USA	100
Die Reaktion der Europäischen Union auf die SIGINT-Aktivitäten der USA.....	103
Das Information Sharing Environment (ISE) der Nachrichten- und Sicherheitsdienste der	
Vereinigten Staaten - Zukünftige Entwicklungen	103
Die "Electronic Warfare"-Doktrin der Vereinigten Staaten	105
Die "Information Operations"-Doktrin der Vereinigten Staaten von Amerika	107
Das Intelligence Directorate des US European Command - USEUCOM	109
Das "Presidential Surveillance Program - PSP"	110
Die "Presidential Policy Directive/PPD-20" und das System PRISM	110
Die Ausweitung der weltweiten Kommunikationsüberwachung durch die National Security	
Agency der USA - "Vision 2015 - A Globally Networked and Integrated Intelligence	
Enterprise"	111
Der methodische Ansatz der westlichen Nachrichtendienste in der	
Kommunikationsüberwachung	113
Die wichtigsten Überwachungsprogramme der National Security Agency - NSA und des	
Government Communication Headquarters - GCHQ sowie anderer Dienste	114
Das System XKEYSCORE der National Security Agency - NSA	115
Weitere Systeme und Programme der NSA und des GCHQ.....	116
Die wichtigsten Komponenten des NSA/GCHQ-Überwachungssystems	128
Die Worldwide SIGINT/Defense Cryptologic Platform der NSA.....	134
Die Kooperationspartner der National Security Agency und des GCHQ.....	135
Die Überwachung kryptierter Kommunikationsverbindungen aller Art durch die National	
Security Agency - NSA und das Government Communications Headquarters - GCHQ	135
Die Data-Fusion Centers der US-Sicherheitsbehörden in den USA	137
Informationsverarbeitungssysteme der US-Intelligence-Community	138
Die Ausweitung der Kommunikationsüberwachung in den Vereinigten Staaten.....	141
Die weltweite Bedrohung kritischer Informationsstrukturen.....	144
LIBERTY AND SECURITY IN A CHANGING WORLD - Report and Recommendations of "The	
President's Review Group on Intelligence and Communications Technologies - der Bericht	
der NSA-Kommission vom 12. Dezember 2013"	146
Das strategische Kommando der russischen Streitkräfte im Fokus der National Security	
Agency der Vereinigten Staaten	148
Der neue "Joint Intelligence Analysis and Production Complex" der United States	
Air Force - USAF in Croughton/UK.....	148

Künftige Perspektiven für die National Security Agency - NSA	149
Das Nachrichtendienst-System Großbritanniens	150
Das britische "Terrorism Prevention and Investigation Measures (TPIMs)"-System.....	153
6. Entwicklung der Überwachung in der Europäischen Union	157
EU-Organisationen und deren Rolle in der europäischen Sicherheitspolitik	157
Das neue "Standing Committee on Operational Cooperation on Internal Security - COSI" der EU	163
Die geplante Ausweitung parlamentarischer Kontrolle der Sicherheits- und Nachrichtendienste in der Europäischen Union	165
Die Ausweitung der Kommunikationsüberwachung (Lawful Interception - LI) in der Europäischen Union.....	167
Das Stockholm-Programm - Der 5-Jahres-Plan der "Future Group" zur umfassenden Ausweitung der Kommunikationsüberwachung in Europa.....	169
Das europäische Informationsmodell, operative und strategische Informationen	170
Das Schengen-Informationssystem II (SIS II) der Europäischen Union	171
Die Ausweitung der Netzwerke europäischer Sicherheitsbehörden	174
Mögliche SIGINT-Fähigkeiten der EU	176
Der Datenaustausch zwischen den Sicherheitsbehörden Europas und weiteren Partnerstaaten	176
Deutsche nationale Datensammlungen	178
Die EU-Sicherheits- und Strafverfolgungsbehörden intensivieren den Austausch sensitiver, personenbezogener Daten.....	179
Die geplante "Police and Criminal Justice Data Protection Directive" der EU	179
Die Vorratsdatenspeicherung - "Mandatory Data Retention Directive"	180
Grenzüberschreitende, verdeckte Polizeioperationen innerhalb der EU.....	181
Der Datenaustausch mit den Sicherheitsbehörden der USA	181
Die European Investigation Order in Criminal Matters	182
Der Entwurf einer Direktive des EU-Parlaments und des Rates zur Abwehr von Cyberangriffen	182
Weitere Vorhaben und Projekte in der Europäischen Union	184
Die Telekommunikationsüberwachung und Europäische Ermittlungsanordnung - EEA	185
Das INDECT-Programm der EU	186
Das Projekt "HORIZON" der Europäischen Union	188
Das Projekt ENLETS (European Network of Law Enforcement Technology Services)	188
Das Positionspapier des Cyber Crime Convention Committee	189
Speicherung von Reisedaten in der Europäischen Union, Datenerfassung durch die EU ...	190
Geplante umfassende Datenbank des National Counterterrorism Center - NCTC des US-Heimatschutzministeriums (Department of Homeland Security-DOHS) - Auswirkungen auf die EU	190
Ausweitung der Kommunikationsüberwachung in den USA mit Folgen für EU-Bürger.....	190
Einführung von E-Discovery-Verfahren nach US-amerikanischem Recht (Lawful Computer Forensics) in Europa	191
Die Aufgaben und Zuständigkeiten der EU-Grenzschutzagentur FRONTEX - Das System EUROSUR	191
Die Soforteinsatzteams für Grenzsicherungszwecke - RABIT - Rapid Border Intervention Teams - Stellung und Zuständigkeit der Teammitglieder der FRONTEX-Agentur der EU ..	194
Die Projekte "CAPER" und "PROACTIVE" der Europäischen Union	194
Die EUROPOL übernimmt die Bekämpfung der Cyber-Kriminalität für die Europäische Union	195
Cloud Computing im Fokus der europäischen Sicherheitsbehörden und ihrer Partner	197
Der geplante Umfang der Lawful Interception (LI) Cloud/Virtual Services (CLI) im Vorschlag der ETSI	198
7. Die Entwicklung der Kommunikationsüberwachung und der signalerfassenden Aufklärung in Deutschland nach 1990	201
Der Bundesnachrichtendienst - BND	203
Das Bundesamt für Verfassungsschutz	209

Der Militärische Abschirmdienst - MAD	209
Sonstige Strafverfolgungs- und Sicherheitsbehörden in Deutschland	210
Das Bundesministerium für Verteidigung und das militärische Nachrichtenwesen der Bundeswehr - MilNwBw	212
Die Systeme der EloKa-Kräfte der Bundeswehr zur mobilen Signalerfassung.....	214
Die Vorstellungen des Innenministers zu künftigen Befugnissen, Strukturen und der Zusammenarbeit mit den Strafverfolgungsbehörden.....	221
Die Entwicklung der Kommunikationsüberwachung und "Signalerfassenden Aufklärung" in Deutschland nach den Anschlägen vom 11. September 2001	224
Der Stand der "Technischen Kommunikationsüberwachung und akustischen Raumüberwachung" in Deutschland in den Jahren 2010/2011	233
Auswertung von Kommunikations-Verkehrsdaten durch die Ermittlungsbehörden	234
Die akustische Raumüberwachung in Deutschland.....	235
Quellen-Telekommunikationsüberwachung/Bewegungsüberwachung	235
Die Abwehrzentren der deutschen Sicherheitsbehörden als Teil der neuen Sicherheitsarchitektur.....	236
Die nationale Cyber-Abwehrstrategie Deutschlands	240
Das Cyber-Abwehrzentrum	242
Der IT-Planungsrat	242
Die neue Unterabteilung "Cyber-Abwehr und Cyber-Spionage" im Bundesministerium des Innern	242
Die Sicherheit kryptierter Verbindungen im Internet und anderer Kommunikationskanäle.....	245
Die geplante Ausweitung der Kommunikationsüberwachung durch die deutschen Sicherheitsbehörden.....	246
Die geplanten Cyber-Abwehrmaßnahmen der deutschen Sicherheitsbehörden	247
Die geplante Ausweitung der Kommunikationsüberwachung durch den Bundesnachrichtendienst (BND)	248
Die Ausweitung der staatlichen Kommunikationsüberwachung auf Datenbestände in der Cloud.....	249
Die Überwachung mobiler Datenendgeräte	250
Behördliche Datenbanken in Deutschland und ihre Vernetzung zu EU-Datensammlungen	251
Die Datenbank-Systeme der Nachrichtendienste in Deutschland.....	252
Die Datensammlungen der Landesbehörden mit Sicherheitsaufgaben.....	253
Die Datensammlungen der Zoll-, Finanz- und Steuerbehörden in Deutschland	253
Sonstige Stellen in Deutschland mit Zugriff auf sensitive, personenbezogene Daten	253
Die Überwachung der weltweiten Finanztransaktionen durch nationale Financial Intelligence Units und Nachrichten- und Sicherheitsdienste und ihr Einfluss auf das nationale Finanzwesen in Deutschland	254
Das Financial Crimes Enforcement Network (FinCen) des US-Finanzministeriums (Treasury) und seine Bedeutung für Deutschland	256
Internationale Abkommen zur zwischenstaatlichen Übermittlung von Finanztransaktionsdaten, die auch für Deutschland Bedeutung haben.....	256
Die Bedeutung der Kommunikationsüberwachung für die Überwachung von Finanztransaktionen	257
Fähigkeiten der National Security Agency - NSA und ihrer Partner in der Kommunikationsüberwachung zur Kontrolle von Finanztransaktionen	257
Die Überwachung von Finanztransaktionen in Deutschland	258
Das geplante IT-Sicherheitsgesetz-Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme - Referentenentwurf des BMI	260
Behördliche Bestandsdatenabfrage im Rahmen des "Gesetzes zur Änderung des Telemediengesetzes" (TMG) und des "Telekommunikationsgesetzes" (TKG).....	261
Kontendatenabfragen bei Finanzdienstleistern aller Art	264
Die Fähigkeiten deutscher Dienste in der "Signalerfassenden Aufklärung" und bei der "Kommunikationsüberwachung" in Kooperation mit den west-alliierten Diensten in Deutschland.....	265
Die automatisierte Massenabfrage von Kraftfahrzeugkennzeichen und die Nutzung von Mobilfunkeinrichtungen in Deutschland	269

Big Data - Wirtschaft und Behörden bereiten die umfassende Auswertung anfallender Massendaten vor	269
Big Data bei den Nachrichten- und Sicherheitsdiensten Deutschlands	270
Die Aktivitäten der National Security Agency der Vereinigten Staaten in Deutschland....	271
Die Kooperation deutscher Dienste mit fremden Nachrichtendiensten	273
Die West-Alliierten und die Kommunikationsüberwachung in Deutschland nach 1990....	274
Die Bedeutung der in Deutschland befindlichen Internet-Knoten	276
Eingriffsmöglichkeiten fremder Dienste in das deutsche Kommunikationssystem	276
Die totale Kommunikationsüberwachung Deutschlands durch fremde und befreundete Nachrichtendienste und Abfluss von Informationen aus Kommunikationsnetzen aller Art	278
Der umfassende Zugriff auf das deutsche und europäische Kommunikationssystem durch NSA und GCHQ	278
Die Quellen-Kommunikationsüberwachung der NSA in Deutschland	280
"No-Spy-Garantie" als Geschäftsbedingung - Die Bundesregierung verschärft Auflagen bei IT-Aufträgen.....	281
Stand der Kommunikationsüberwachung der Jahre 2011 und 2012 durch deutsche Behörden - Behördliche Telekommunikationsüberwachungsverfahren nach §§ 100a und 100b StPO	282
Die Ergebnisse der strategischen Fernmeldeaufklärung durch den Bundesnachrichtendienst	283
Der Transparenzbericht der "Deutschen Telekom für das Jahr 2013" - Auskunft an deutsche Sicherheitsbehörden	283
Ersuchen von Sicherheitsbehörden und Abfragen bei TK-Diensteanbietern	284
8. Die Fähigkeiten ausgewählter Staaten und Organisationen zur Signalerfassung und zur Führung von Informationsoperationen	287
Die Fähigkeiten der NATO zur Führung von Informationsoperationen	287
Die Strukturen der signalerfassende Aufklärung und Kommunikationsüberwachung Frankreichs.....	288
Die signalerfassende Aufklärung und Kommunikationsüberwachung der Republik Österreich.....	299
Die SIGINT-Organisation und Kommunikationsüberwachung der Schweiz.....	301
Die Kommunikationsüberwachung und signalerfassende Aufklärung Italiens, Spaniens und Portugals	308
Die signalerfassende Aufklärung und Kommunikationsüberwachung in den nordischen Staaten	308
Die Nachrichtendienste Russlands nach deren Reorganisation.....	308
Die Bedrohung der Informationsgesellschaft durch den Anstieg der Cyber-Operationen im Nahen und Mittleren Osten	321
Israel und ausgewählte Staaten des Nahen und Mittleren Ostens	321
Türkei	325
Die Kommunikationsüberwachung in Saudi-Arabien	325
Die Fähigkeiten Syriens und des Iran zur Durchführung von SIGINT- und Informationsoperationen.....	326
Die Grundlagen der iranischen Informations- und Kommunikationstechnologie	326
Syriens Fähigkeiten zu Informationsoperationen.....	328
Ägypten.....	328
Die Situation im Irak.....	329
Die übrigen Staaten des Nahen und Mittleren Ostens und angrenzender Regionen	329
Indien	329
Pakistan	330
Fähigkeiten zur Kommunikationsüberwachung und Informationsoperationen in den zentralasiatischen Staaten	330
Die Nachrichtendienste in Südostasien und ihre Fähigkeiten zur Kommunikationsüberwachung, signalerfassenden Aufklärung und Informationsoperationen.....	331
Die nachrichtendienstlichen Strukturen der Volksrepublik China (VR China) und deren Fähigkeiten	332
Nordkorea und seine Nachrichtendienste	347

Südkorea und seine Cyberverteidigung	349
Taiwan (Nationalchina)	349
Japan	351
9. Der Einsatz von Special Operation Forces und polizeilicher Sondereinheiten zur Unterstützung nachrichtendienstlicher Operationen in asymmetrischen und hybriden Konflikten und außergewöhnlichen Lagen.....	353
Das Special Operations Command (SOCOM) der US-Streitkräfte und seine erweiterte Rolle bei unkonventionellen, weltweiten Einsätzen in asymmetrischen Konflikten.....	354
Militärische Führungsstellen für den Einsatz von militärischen Spezialeinsatzkräften (Special Forces) der Vereinigten Staaten in Europa	358
Der Kampf gegen die "Islamische Terrormiliz - IS"	363
Die NATO und der Einsatz von militärischen Spezialeinsatzkräften -	363
Das Special Operations Headquarters - NSHQ der NATO in Mons/Belgien.....	363
Die Bedrohung der Flanken der NATO durch irreguläre Kräfte	365
Das "NATO HUMINT Centre of Excellence" in Oradea	366
Die Bedeutung nationaler polizeilicher und militärischer Sondereinheiten.....	367
Die Gendarmerie in der Europäischen Union	368
Spezialeinheiten der Bundeswehr	369
Die Truppen "besonderer Bestimmung - Voiska Spezialnovo Nasnadzenia (SPEZNAS)" der russischen Streitkräfte	370
10. Die Zukunft der globalen Überwachung, Informationsoperationen und neuartige Bedrohungen.....	373
Die Rolle der Nachrichtendienste in künftigen Informationsoperationen	373
Die Intelligence Community der Vereinigten Staaten	374
Das Government Communications Headquarters - GCHQ Großbritanniens	384
Künftige Perspektiven für die deutschen Sicherheitsbehörden	385
Die Gefährdung der mobilen geschäftlichen und privaten Kommunikation durch Angriffe aus dem digitalen Raum	391
Wege zur sicheren nationalen Regierungskommunikation	395
Untersuchungsausschüsse des Deutschen Bundestages	398
Künftige Aktionsfelder in der Kommunikationsüberwachung, Signalerfassung, Überwachung, Gewinnung und Auswertung von Massendaten, intelligente Vernetzung von Systemen und Nutzung des Weltraumes, Gefährdung von IT-Systemen und sonstige Bedrohungen.....	400
Die französischen Sicherheitsbehörden.....	400
Die russischen Sicherheitsbehörden.....	400
Die chinesischen Sicherheitsbehörden.....	401
Die Technische Kommunikationsüberwachung	402
Signalerfassende und raumgestützte abbildende Aufklärung	402
Einsatz von Drohnen durch die europäischen Sicherheitsbehörden	402
Datenbestände in der Cloud - Big Data, Meta-Daten	402
Social Media, Social Media Intelligence, Social Network Analysis und Social Engineering	403
Die Intensivierung der Grenzüberwachung und Überwachung von Reisebewegungen.....	403
Ausweitung der Open Sources Intelligence, Business Intelligence und des Social Engineering	403
Die Gefährdung der Informations- und Kommunikationssysteme und "Kritischer Infrastrukturen" durch Informationsoperationen aller Art	405
Die intelligente Vernetzung von Anwendungen aller Art in der Wirtschaft, Haushalt (Smart Homes, Smart Meter), im Verkehr - Smart Cars, Home-Entertainment - Smart TV, Identitätsdiebstahl, berührungslose Bezahlsysteme, RFID-Tracking und Erpressung per Internet.....	406
Die Sicherheit in der Informationstechnik, ungewollte Abstrahlung sensibler Kommunikationsinhalte, Lauschabwehr und Penetrationstests, "Bring Your Own Device - BYOD" und die Integrität von Fire-Wall-Lösungen.....	407
Wachsende Zweifel an der Integrität von Fire-Wall-Lösungen.....	408

Ausweitung der Verhaltenskontrolle durch Netzüberwachung, NOVEL BIG DATA/Global Database of Events, Language and Tone - GDELT.....	409
Die Ausweitung der geospatialen Nachrichtengewinnung und Auswertung durch die National Geospatial Intelligence Agency - NGA der Vereinigten Staaten	409
Persönliche Schutz- und Abwehrmaßnahmen gegen die Kommunikationsüberwachung ...	409
Die Bedeutung der Kryptografie für den Schutz sensibler Informationen und Kommunikationsverbindungen	410
Die verstärkte Einbeziehung des Weltraums in die Nachrichtengewinnung und Überwachung	411
Die künftige Bedrohung der Vereinigten Staaten durch die VR China und Russland, Politikwechsel der USA gegenüber Afrika	413
Die Bedrohung der Vereinigten Staaten, ihrer Alliierten und Partner durch interkontinentale-ballistische Flugkörper	414
Die Gefährdung betrieblicher, behördlicher und privater IT-Systeme durch Angriffe mit Hilfe von Hochenergie-Mikrowellen-Strahlung	414
Die künftige weltweite Nutzung des "elektromagnetischen Spektrums"	418
Die Entwicklung möglicher Cyber-Konflikte in der Zukunft	418
Die Bedrohung durch Cyber-Operationen und die "Elektronische Kampfführung" in Anfangsphasen von möglichen künftigen Konflikten.....	419
Der Ausfall von Transponder-Systemen der zivilen Flugsicherung über einem Teil Westeuropas am 5. und 10. Juni 2014	419
Aktivitäten Russlands zur "Signalerfassenden Aufklärung" an den Grenzen zur NATO, an der Grenze zu Finnland und auf Kuba.....	421
Verstärkung der Fähigkeiten der russischen Streitkräfte zum "funkelektronischen Kampf"	422
Die Bedeutung des "Elektronischen Kampfes" aus russischer Sicht	422
Das "Internet der Dinge" - Droht ein Krieg im digitalen Raum?	423
Folgerungen der Europäischen Union aus der Kommunikationsüberwachung der Vereinigten Staaten und deren Partner - Gefährdung der Sicherheit in Europa durch islamistische Terrorgruppen.....	425
11. Zusammenfassung und Ausblick	427
12. Index, Personen- und Ortsregister [in Auswahl]	441

Die technologischen Voraussetzungen für den Einsatz von KI und Big Data in der Kriegsführung sind inzwischen so weit fortgeschritten, dass sie die Informationsgewinnung und -auswertung in strategischer Zielsetzung, die in ihrer Wirkung auch bereits vor dem möglichen Ausbruch offener Feindseligkeiten, das Potenzial eines Angriffes so nachhaltig schwächen können, dass dieser zur Verteidigung nur noch eingeschränkt oder gar nicht mehr fähig sein wird. Der Kampf um "InformationsÜberlegenheit" stellt eines der wichtigsten Mittel künftiger politischer, wirtschaftlicher und militärischer Auseinandersetzungen dar und wirkt dabei bereits lange vor dem Ausbruch von Konflikten, die künftig vermehrt asymmetrischen Charakter haben werden.

Die Wirkung des Einsatzes von Nuklearwaffen (Strahlung, Fall Out und andere Effekte) sind bei Informationsoperationen jedoch nicht zu befürchten. Allerdings sind Kollateralschäden während Informationsoperationen, die durch die danach in ihrer Bedeutung massenhaft Schäden vergleichbar, die nach Nuklearangriffen erwartet werden könnten. Hierbei gewinnt der Einsatz der Internet "kritischer Infrastrukturen" aller Art entscheidende Bedeutung, da vor deren Funktionsausfall die Basis eines Staatswesens abhängen kann. Mögliche Schäden aus Informationsangriffen, insbesondere gegen Versorgungssysteme eines Staates, den informationstechnischen Infrastrukturen der Industrie, Wirtschaft, Verwaltung und im Finanzsektor können jedoch nicht abschätzbare Folgen verursachen. Dies wird auch hegemoniale Bestrebungen zu nutzen unterstützen, die über die Fähigkeiten zu unrasenden, globalen oder auf geografische Räume eingeschränkte Informationsoperationen zur Errichtung sozialer und militärischer Zielsetzungen verfügen.