Einleitung

Hans-Jürgen Lange und Astrid Bötticher

Die Cyber-Welt hat in den letzten Jahren Furore gemacht – in sämtlichen sozialen Zusammenhängen. Die Frage nach der Cyber-Welt lässt sich in ganz verschiedenen Sachzusammenhängen stellen. Dieses Buch gibt einen Einblick in die verschiedenen Aspekte von Cybersicherheit und ihren mannigfaltigen Berührungspunkten mit unserer hochkomplexen, vielschichtig organisierten Gesellschaft. Das wohl wichtigste Schlagwort, welches medial bemüht wird, ist das der Informationsgesellschaft. Die Informationsgesellschaft löse unwiderruflich die Industriegesellschaft ab und dies bewirke mannigfaltige Änderungen nicht nur in der Gesellschaftsstruktur, sondern auch in unserer Alltäglichkeit. Der Cyberspace ist eine spiegelbildliche Welt. Dadurch, dass sie von Menschen konstruiert ist, haben Eingriffe auch viel größere Folgen als in der realen Welt – Handlungen besitzen dort eine größere Potenz. Der Cyberspace ist letztlich auch eine Umwelt, von Menschen geschaffen und prinzipiell sogar kontrollierbar. Das Internet ist zu einer Quelle von gesellschaftlicher Innovation vielfältigster Art geworden. Dies spiegelt sich auch in den Kulturprodukten wieder – so besingt die Musikgruppe Deichkind die „illegalen, radikalen, digitalen Fans" und positioniert sich, inspiriert von Anonymous, im politischen Streit um Urheberrechte, der von Content-Industrie und Usern ausgefochten wird. Die Technikinnovation hat selbst einen rasanten Wandel erfahren – noch vor 25 Jahren kannte man das Autotelefon; das Handy, erst in den 1990ern populär geworden, wurde durch das Smartphone abgelöst; Kamera, Videogerät, der Zugriff auf die digitale Welt wurde damit in ein Gerät integriert und hat zu neuen Vernetzungen geführt. Mit den heutigen Kameras können wir unsere Fotos gleich in sozialen Netzwerken posten und uns durch die Evolution der Telekommunikationstechnik Freunde durch virtuelle Gemeinsamkeit verschaffen. Soziale Netzwerke werden auch dadurch immer beliebter. Dies hat aber zu weitreichenden Implikationen geführt, die mehr beinhalten, als die vordergründige Fähigkeit, unser Leben mit örtlich weit entfernten Menschen zu teilen. Die Wissenschaft kann

Hans-Jürgen Lange, A. Bötticher (Hrsg.), *Cyber-Sicherheit,* Studien zur Inneren Sicherheit 18,
DOI 10.1007/978-3-658-02798-8_1, © Springer Fachmedien Wiesbaden 2015

heute auf ganz neue Formen von Daten zugreifen – Geodatenanalysen stellen für sie genauso eine Herausforderung dar, wie auch Bewegungswelten heute eine neue Dimension erfahren, die neue Techniken zur Datenerhebung evozieren; das Milieu etwa bekommt eine neue Dimension. Neben neuen Forschungsmethoden sind auch die Geschlechterrollen von der Evolution der Telekommunikation erfasst; neben traditionelle Begriffe treten vollkommen neue hinzu. So kennen wir die ‚Netzwelt', die ‚Online-Community', ‚Digital Natives', ‚Digital Immigrants' und den durch die Politik so gefürchteten ‚Shitstorm'; das Wort ‚Vernetzung' hat einen neuen Bedeutungsgehalt bekommen. Wir haben begonnen in Netzwerken zu denken. Die Ökonomie bleibt gleichwohl zentral betroffen: Telekommunikation gilt heute als die vierte Schlüsselindustrie der Weltgesellschaft (Wu 2005: 12; vgl. auch Bötsch 1995: 347). Telekommunikation ist zentrale Grundlage für die geschäftliche Betätigung des (globalisierten) Handels und tritt neben die für die Produktion maßgeblichen Faktoren Arbeit, Kapital und Boden. Auch deshalb hat die Ordnung und Regelung der Telekommunikation im Strafprozessrecht eine erhebliche Bedeutung erhalten, ihre handelnden (auch intermediären) Akteure beraten Problemkonstellationen, die sich nicht nur auf die Bundesrepublik beziehen lassen. Nicht zuletzt ist die Bundesrepublik Deutschland zu einer globalen Wirtschaftsmacht geworden und stark vernetzt mit den Ökonomien dieser Welt.

Der Begriff der Cybersicherheit ist ein auf das Informations- und Telekommunikationsverhalten und -vermögen bezogener Sicherheitsbegriff. Der Sicherheitsbegriff ist dynamisch und seine ihm zukommenden Entitäten bilden selbst ein Netzwerk:

> „‚Danger' is here defined as the possibility of occurrence of an incident that entails consequences of damage. ‚Risk' is understood as product of operationalized danger. ‚Security' therefore is a state, where risks have been minimized to a level that is below a threshold that society has discursively defined as acceptable. This means, while dangers can remain unknown to society, risk is based on the perception of danger and security is directed at perceived dangers and subject to the condition of following societal discussions. The Concept of Security is subject to changing times and expression of the socio-political development and therefore it is dynamic." (Bötticher 2012)

Das an der Universität Witten/Herdecke und der Universität Bielefeld beheimatete und durch das Bundesministerium für Bildung und Forschung (BMBF) geförderte Sicherheitsgesetzgebungsprojekt (SIGG)[1] hat sich im Rahmen des Teilprojektes

1 Das Projekt „Sicherheitsgesetzgebung" (SIGG) war ein Verbundprojekt aus den Teilvorhaben Sicherheitspolitik und Sicherheitsrecht (2010 bis 2013). Kooperationspartner waren Wissenschaftler des Lehrstuhls für Politikwissenschaft, Sicherheitsforschung und Sicherheitsmanagement der Universität Witten/Herdecke, Prof. Dr. Hans-Jürgen Lange, und Wissenschaftler des Lehrstuhls für Öffentliches Recht, Staatslehre und

Telekommunikationsüberwachung mit telekommunikationsbasierten Informationssystemen auseinandergesetzt und die verschiedenen Dimensionen des Netzes in seinen Bezügen zum Sicherheitsbegriff erörtert. Im Rahmen des Interdisziplinären Arbeitskreises Innere Sicherheit (AKIS) wurde 2012 zusammen mit dem Wittener Lehrstuhl für Politikwissenschaft, Sicherheitsforschung und Sicherheitsmanagement der Workshop „Cyber-Sicherheit – Aspekte, Handlungsfelder und Konzepte" durchgeführt.

Das Motto *Einheit durch Vielheit* könnte dem vorliegenden Buch, welches aus dem Workshop hervorgegangen ist, vorangestellt werden, denn die „fünfte Dimension" (Skala 2011), die der Mensch mit dem Cyberspace entwickelt hat, bringt Veränderungen großen Ausmaßes mit sich, die die Digital- und Informationsgesellschaft noch verarbeiten bzw. bearbeiten muss, um diese künstliche Dimension mit der natürlichen Lebenswelt und den darin sich historisch entwickelten Regelungen, Einrichtungen und Einigungen in Einklang zu bringen. Das Paradigma der digitalen Gesellschaft ist verhältnismäßig jung. Es scheint, als würde mit dem Stand der Technik auch unsere Gesellschaft geformt. Diese Entwicklung ist Menschengemacht und steuerbar, wenngleich es scheint, als würde die Komplexität der Welt unsere Fähigkeit zur Organisation ebendieser übersteigen. Der vorliegende Sammelband stellt einige Entwicklungen vor, die sich direkt auf den Sicherheitsbegriff und der gesellschaftlichen Organisation dieser ‚neuen' Dimension beziehen lassen.

Die unterschiedlichen Autoren haben jeweils andere Blickpunkte, von denen sie auf ‚Sicherheit', ‚Gefahr' oder ‚Risiko' schauen. Dennoch eint die Beiträge ein Grundkonsens: Die Sicherheitslage hat sich durch Telekommunikation genauso geändert wie die Lage der Freiheit. Diese erneuerte Abgrenzung, die Suche nach einer Sicherheit, die unsere Freiheit nicht so sehr einschränkt, dass wir von Unsicherheit sprechen müssten, ist in den einzelnen Beiträgen herauslesbar, dennoch kommen die Autoren zu graduell unterschiedlichen Ergebnissen. Das Spannungsverhältnis zwischen Freiheit und Sicherheit ist ein vieldiskutiertes Thema, ein fundamentales Problem. In der Sicherheitsforschung werden Freiheit und Sicherheit meist gegenübergestellt; im Cyberspace sind die Sphären zwischen Freiheit und Sicherheit nicht so einfach zu lokalisieren, sie sind miteinander verschränkt.

Verfassungsgeschichte der Universität Bielefeld, Prof. Dr. Christoph Gusy. Das Projekt ist im Rahmen des BMBF aus Mitteln des Sicherheitsforschungsprogramms der Bundesregierung gefördert worden. Es beschäftigte sich mit den Akteuren und den informellen Prozessen, die auf die Sicherheitsgesetzgebung Einfluss nehmen. Es wurden dabei Gesetzgebungsprozesse auf Landes-, Bundes- und EU-Ebene anhand von drei Fallstudien im Bereich Videoüberwachung, Telekommunikationsüberwachung sowie der Einführung biometrischer Kontrollsysteme untersucht.

Die Innere Sicherheit ist von den Entwicklungen der Cyberwelt vielfach betroffen. Wie kann Sicherheit in dieser neuen Dimension organisiert werden ohne auch gleich den Demiurgen „Staat" überpräsent zu machen? Welche Antworten hat das in sich vielgestaltige und vernetzte institutionelle Sicherheitssystem gefunden? Wie ändert sich die Produktion von Sicherheit und welche Formen der Freiheit sind betroffen? Die User haben sich vielfältig vernetzt und auch schon Geschichte geschrieben. Während Anonymous sich noch einen Kleinkrieg mit der GEMA lieferte, kam es zum arabischen Frühling, der mittels neuer Analysetechniken, die auf Datenerhebungen im Internet basierten, bereits vorausgesagt worden war (Die Welt 08.11.11). Gerade Anonymous ist ein auf der sozialen Ebene neues Phänomen, welches sich erst durch das Netz etablieren konnte. Neben der Voraussage von Aufständen hat sich die Analyse von Massendaten auch im Konfliktfall bewährt. Der Konflikt in Libyen wurde auch dadurch beeinflusst, dass durch die neue Technologie der sozialen Vernetzung ein Informationsvorsprung gewonnen war und so beinahe in Echtzeit reagiert werden konnte.

Es tritt generell, in allen Gesellschaften, ein neuer Anspruch auf Transparenz zutage, der zumindest zweideutig ist. Einerseits sprechen die Befürworter des Web 2.0 von den neuen Möglichkeiten totaler Transparenz für das eigene Leben, fordern dieses geradezu ein, andererseits fordern Bürger gegenüber den Sicherheitsinstitutionen eine neue Form von Transparenz. Dies äußert sich vornehmlich unter dem Bezug auf das in Deutschland neu entwickelte Grundrecht auf Vertrauen in digitale Kommunikationssysteme. Hier ist einerseits die Transparenz über Maßgaben der Datensammlung, ihrer Verwendung und Speicherung gemeint, die durch Sicherheitsakteure vorgenommen werden, andererseits ist damit die Zusammenarbeit im Rahmen internationaler Abkommen zur Herstellung von Sicherheit gemeint. Neben Wikileaks und der durch diese Gruppe veröffentlichten Regierungsdepeschen ist Edward Snowden getreten, der durch die Veröffentlichung einer ganzen Fülle von Material auf die Dimensionen der Datenerhebung und Verwendung hinwies.

Die Politikwissenschaft hat dem Trend des Internets und dessen „Leitströmung der digitalen Welt" (Glaser 2012) noch nicht vollends die Beachtung geschenkt, die sie verdient. So fragte etwa die Zeitschrift *Internationale Politik* „Was bewegt die Welt?" und bezog die technologiebasierte soziale Vernetzungsfähigkeit, die das Internet bietet, nicht mit ein.[2] Oftmals bleibt Netz- und Netzpolitik im Hintertreffen und andere Themen stehen im Vordergrund. Anders geht es da ganzen Wissenschaftszweigen, die dem Thema nicht nur Beachtung schenkten, sondern zutiefst mit dem Aufstieg des Internets zur sozialen Macht verbunden sind. Einen rasanten Aufstieg erlebte etwa die Computerlinguistik, die heute wichtige Analy-

2 IP Internationale Politik. Mai/Juni 2011.

sewerkzeuge für die verschiedenen Sozialwissenschaften, für die Wirtschaft und auch für die Sicherheitsbehörden bereitstellt. Neben der Computerlinguistik ist die Kognitionswissenschaft und deren Möglichkeiten in Bezug auf augmented reality, der erweiterten Realität, immer wichtiger für eine Gestaltung des Netzes geworden. Einige sehen dies als Möglichkeit zu einem „Lauschangriff auf unser Weltbild" (Schramm, Wüstenhagen 2012), andere versuchen mittels dieser Techniken Sicherheit herzustellen, ohne zu sehr in die Bürgerrechte einzugreifen.[3] Gerade Bürgerrechtler sind besorgt um die Privatsphäre, die im Netz meistens in Frage gestellt ist. So hat sich gerade die Rechtswissenschaft intensiv um den Einklang von Bürgerrechten mit der Netzrealität bemüht, wenngleich oftmals auf verlorenem Posten: Während einige Teilerfolge gegenüber einzelnen Anbietern kommunikationsbasierter sozialer Vernetzung zu verzeichnen waren, wie die Datenschutzdebatte um Facebook und die genommene Entwicklung eindrücklich zeigt, so ist gegen den bekanntesten Anbieter von strukturierter Information, Google, noch kaum ein erwähnenswerter Erfolg der Datenschützer zu verbuchen, wenngleich Google durch seine hohen Anwenderzahlen als machtvoller Spieler gelten kann. Auch ist hier die Wirtschaft angesprochen – denn mit Google hat sich ein faktisches Informationsanbietermonopol herausgebildet, welches sich nicht so sehr durch das Fehlen von Konkurrenz, als durch die fehlende Nutzung von Konkurrenzanbietern beschrieben werden kann. Vielfach erscheint es uns heute so, als sei das, was in den Google Rankings nicht oder zu weit hinten erscheint, auch nicht mehr existent.

Neben einzelnen Unternehmen können auch einfache Internetnutzer weit mehr über Personen durch das Netz erfahren, als diese freiwillig ihren Nachbarn anvertrauen würden. Die Aufklärung über Sachverhalte ist hier angesprochen, denn Daten können heute über Yasni, 123People oder namechk.com verknüpft werden mit der Auswertung von Inhaltsdaten (Twitter, Facebook) oder Bildern (Picasa), die von Internetnutzern zur Verfügung gestellt werden. Es können ganze Biographien mit persönlichen Details ausgeforscht werden, ohne dass der Nutzer sich über die Verknüpfung von an verschiedenen Orten der ins Netz gestellten Daten je Gedanken gemacht hat. So ergeben sich neue Notwendigkeiten für die Erziehungswissenschaft – wie kann es gelingen, Datenschutz als zentrales Thema in den Unterricht zu integrieren, um die Gesellschaft für die zukünftigen Entwicklungen zu wappnen? Doch auch neue technische Herausforderungen für die Polizei haben sich entwickelt, wie dem Abhören von Internet Relay Channels (IRC)[4], z. B. Skype oder MSN, aber auch für Einsatzmöglichkeiten in virtuellen Welten oder die Fahndung über Soziale Netzwerke und mit Hilfe der User. Gerade hier wird die Schnittstelle

3 Etwa mittels Massendatenanalyse von Twittereinträgen oder Blogs.

4 http://www.netzwelt.de/news/68425-irc-spitzel-chatroom.html (letzter Abruf 7.2.2014).

zwischen physischer Welt und virtual reality offenbar, denn die privat schon längst durchgesetzte Suche nach vermeintlichen Übeltätern über Soziale Netzwerke, ist in einigen Fällen bereits umgeschlagen in Aufrufe zum Lynchmord. Ganz neue Formen der Strafverfolgung haben sich durch die Computerforensik ergeben.

Die Autoren des Buches greifen diese vielfältigen und unübersichtlichen Symptome in unterschiedlichen Herangehensweisen und Perspektiven auf. Der Beitrag von Matthias Kettner und Oskar Brabanski beschäftigt sich mit der Demokratie im Zeitalter des Internets. Im Fokus des Beitrages steht die Kommunikation in der Demokratie und über die Demokratie im Rahmen neuer Möglichkeiten des Internets. Die Autoren sehen einen Nachholbedarf der parlamentarischen Demokratie im Rahmen netzbasierter Medienpraktiken, die „Attraktivität des Geistes der Demokratie" aufrecht zu erhalten und zu fördern. Insbesondere das netzbasierte Werkzeug Liquid Democracy wird hier als Möglichkeit dargestellt, dieses Interesse an der Demokratie und für die Demokratie zu sichern. Liquid Democracy wäre so der Weg, den Nachholbedarf netzbasierter, demokratischer Kommunikation aufzuarbeiten. Dabei sehen die Autoren auf philosophischer Ebene Anklänge an die Habermassche Diskurstheorie erfüllt, und sehen in den neuen Möglichkeiten der Kommunikation zugleich einen Schritt hin zur deliberativen Demokratie realisiert. Die Autoren zeigen auf, dass die von Richard Rorty gedachte Kultur ohne Zentrum im Sinne einer Liquidität von Einstellungen, Entscheidungen etc. schon betreten ist. Die repräsentative, parlamentarische Demokratie wird durch die hauptsächlich von ihr ausgeübten Kommunikationsformen als eine „solide Demokratie" der „liquiden Demokratie" gegenübergestellt. Die Attraktivität dieser Demokratieform begründen die Autoren durch die Interessen und Kommunikationsgewohnheiten der jungen Netzgemeinde. So stehen sich festgelegte Abläufe und Way of Life gegenüber. Gleichzeitig sehen die Autoren hier auch eine Gefahr, denn die Demokratie gerät so leicht in die Haltung, sich unverbindlich zu zeigen. Dieses Gefährdungspotenzial auf beiden Seiten – die fehlende Attraktivität der Abläufe der institutionellen Demokratie und ihren dringenden Nachholbedarf netzbasierter, demokratischer Kommunikation sowie die Gefahr der Unverbindlichkeit im Rahmen liquider Aushandlungsprozesse und einer Pseudo-Deliberativität beschreiben die Autoren sehr genau.

Die Autorin Gabriella Coleman legt eine Soziologie der digitalen Protestbewegung vor und zeigt auf, dass die Netz-Aktivisten bereits in der Öffentlichkeit breit diskutierte Debatten entzünden konnten und so zu einem gesellschaftlichen Diskurs über das Netz beitragen. Die neuen Protestformen der digitalen Welt sind durch eine digitale Bewegungsförmigkeit geprägt, die ohne das Netz so kaum möglich wäre. Dabei unterscheidet die Autorin zwischen verschiedenen Protestlern inner-

halb der digitalen Protestbewegung, die sie nach Kenntnisstand und technischer Visiertheit in Hacker und Geeks unterteilt.

Der Beitrag von Martin Bastl, Miroslav Mareš und Kateřina Tvrdá analysiert den Rahmen politischer Prozesse zur Herstellung von Cybersicherheit. Die Autoren entwickeln dabei einen Rahmen zur Analyse von Prozessen zur Herstellung von Cybersicherheit, der sich im Feld der Policy-Analyse bewegt. Dabei kritisieren die Autoren, dass die bis heute erschienenen Arbeiten über Felder der Cybersicherheit mehrheitlich die traditionelle Kommunikation der Sicherheitsstudien und der hier entwickelten Begriffe – ohne Notwendigkeit – verlassen und die Sicherheitsstudien so nur noch als Anhängsel aus der Analogwelt erscheinen. Demgegenüber bearbeiten die Autoren Fragen der Organisation von Cybersicherheit auf Basis des Sicherheitskonzepts der Kopenhagener Schule und der hier ausgearbeiteten Ebenen und Formen der Sicherheit. Hier tritt insbesondere die Entwicklung von Cybersicherheit als Aufgabe in den Blickpunkt, die nicht allein durch staatliche Akteure geleistet wird. Stattdessen diagnostizieren die Autoren, wie verschiedene Akteurskreise in einer multipel organisierten Umwelt in Form einer Ebenenstruktur zusammenspielen. Diese netzartig in einander übergreifende Ebenenstruktur dient zur Entscheidungsfindung von Maßnahmen, die wiederum darauf ausgerichtet sind, Cybersicherheit herzustellen.

Die Autorin Astrid Bötticher beschreibt in ihrem Beitrag die Strukturlandschaft der Inneren Sicherheit in der Bundesrepublik Deutschland auf Bundesebene und deren Verknüpfungen mit internationalen oder multinationalen Stakeholdern der Sicherheit. Die Autorin etabliert hier ein neues Analysemodell, indem sie Fragen der Cybersicherheit mit der Aufgabe der Demokratiesicherung verknüpft. Die Lücke der Wahrnehmung, die zwischen behördlichen bzw. ministeriellen Sicherheitsakteuren und parlamentarischen Sicherheitsakteuren besteht und sich erst langsam schließt, begründet autonome Vernetzungs- und Technisierungsentscheidungen der mittleren Verwaltungsebene. Die Prozesse der Selbststeuerung sind durch diachrone Emergenz und kontextuelle Einbindung geprägt. Mannigfaltige Kommunikationsstrukturen haben sich gebildet. Angesichts der autonom gesteuerten Akteursvernetzung fehlt infolgedessen weitgehend die parlamentarische Kontrolle der neuen Knotenpunkte. Wenngleich das Parlament heute keinesfalls mehr als Tal der Ahnungslosen bezeichnet werden kann, so hat das Parlament auch keine wirklichen Initiativen entwickelt, um autonome Steuerungsprozesse der mittleren Akteursebene des Politikfeldes der Inneren Sicherheit durch politisch gesteuerte und strategische Prozesse abzulösen.

Michael Freiberg, der Leiter des Umsetzungsplans KRITIS der Bundesrepublik Deutschland, zieht eine erste Bilanz und stellt den bisherigen Sachstand des Umsetzungsplans dar und analysiert den Ansatz des Public Private Partnership

zum Schutz kritischer IT-Infrastrukturen. Der Autor stellt dabei insbesondere auf die Probleme des normalen Betriebs ab und relativiert die Gefahren, die von Cyberwar, Cyberterrorismus und Cyberkriminalität ausgehen. Der normale Betrieb als solches ist für den Autor bereits ein Raum mit einem Sicherheitsbedürfnis, welches durch vielfältige Gefahrenlagen in Frage gestellt wird. Für den Schutz von Kritischen Infrastrukturen stehen die Sicherheit des Geldes und die Sicherheit der Energieversorgungssysteme im Vordergrund, deren Rahmenbedingungen in der Verknüpfung von Risiko und Verantwortung liegen. Zu der Abhängigkeit der Wirtschaft von traditionellen Primärgütern wie Öl und Gas ist eine neue externe Abhängigkeit hinzugekommen – die Abhängigkeit vom Primärgut der Telekommunikation. Dem branchenübergreifenden Risiko der Wirtschaft ist zu begegnen, indem Ausfallprozeduren ersonnen und erprobt werden – auf diese Weise würden Abhängigkeit und Risiko relativiert. Die Zusammenarbeit von öffentlicher Hand und Privatwirtschaft trägt zur verbesserten Einschätzung von IT-Sicherheitslagen bei und verteilt die Verknüpfung von Risiko und Verantwortung auf viele Schultern. Damit verbunden ist die neue Notwendigkeit zur freien Kommunikation zwischen Unternehmungen und staatlichen Institutionen sowie vice versa. Dieser Kommunikationsprozess bietet potenziell die Möglichkeit, Wege der Selbstorganisation von Kommunikationssicherheit zu eröffnen und eine netzartige Struktur zu etablieren, die Risiko und Verantwortung neu verknüpft.

Die Autoren Borchert, Rosenkranz und Ebner betonen ebenfalls die starke Abhängigkeit der heutigen Gesellschaft von Informations- und Kommunikationstechnologie und stellen Maßnahmen der Republik Österreich zur Herstellung von Cybersicherheit vor. Auch in Österreich wird der Ansatz der Private Public Partnership zur Herstellung von Cybersicherheit verfolgt. Die Autoren grenzen zunächst Cybersicherheit und Kritische Infrastrukturen voneinander ab. Die teilweise Komplementarität beider Begriffe bedingt einen ganzheitlichen Ansatz zum Schutz, der in Österreich entwickelt wurde, so dass Umsetzungsmaßnahmen harmonisch ineinander greifen und ein erhöhtes Wirkpotenzial entfaltet. Das ganzheitliche Denken ist für die Autoren ein zentraler Ansatz der österreichischen Sicherheitspraxis. Im Vordergrund steht dabei die Indienstnahme sämtlicher Akteure, die auf ihre Weise Sicherheit benötigen und Sicherheit herstellen. Eine ganzheitliche Sicherheitspraxis schließt die Akteure nicht aus, sondern bezieht sie in sämtliche Prozesse der Sicherheitsherstellung mit ein. Für die verschiedenen Akteure ist die Basis der Zusammenarbeit in der Transparenz gefunden: Ziele und Regeln der Zusammenarbeit sind klar definiert, so dass das ganzheitliche Ineinandergreifen von Prozessen erleichtert wird. Neben der klaren Definition von Zielen, die den Teilnehmern bekannt sind, ging der österreichische Ansatz der ganzheitlichen Sicherheitsherstellung weiter, indem die Akteure in sämtliche Prozesse der Ziel-

definition integriert wurden. Akteure verschiedener Wirtschaftssektoren wurden eingeladen, den Risikoraum gemeinsam auszuleuchten und ein integrierendes Begriffs- und Risikoverständnis aufzubauen. Anhand des Beispiels wird von den Autoren dargestellt, dass das Aufkommen von neuen Gefährdungen auch zu neuen Denkmustern und Prozessen der Sicherheitspraxis führt. Der ganzheitliche Sicherheitsansatz, der hier in die Praxis überführt worden ist, bietet ein eindrückliches Beispiel für das integrativ orientierte, netzförmige Denken.

Der Autor Jürgen Fauth berichtet über neue Wege und Notwendigkeiten polizeilicher Praxis im Rahmen der Herstellung von Cybersicherheit. Dabei hat sich, so der Autor, insbesondere das Berufsbild des Polizisten bzw. der Polizistin stark verändert und neue Herausforderungen für die Polizeiausbildung, aber auch für die gewerkschaftliche Vertretung der Polizei mit sich gebracht. Die Alltäglichkeit der virtuellen Welt hat sich in der Polizei niedergeschlagen. Die Polizeiarbeit vollzieht sich heute nicht allein in der physischen Welt, die Strafverfolgung vollzieht sich heute auch im virtuellen Raum. Die Polizei reagiert so auf neue Kriminalitätsformen und verfolgt die Täter dort, wo sie tätig sind. Der Autor beschreibt beispielhaft strafrechtliche Vorgehensweisen und analysiert eingehend, in welcher Weise Polizisten heute mit der Notwendigkeit der Technikexpertise konfrontiert sind. Von der Beweissicherung auf elektronischen Datenträgern, der gerichtsfesten Belegpflicht im Rahmen elektronischer Formen der Strafverfolgung über zahlreiche weitere Erfordernisse der Technikkenntnis, die Polizisten heute für die alltägliche Polizeiarbeit benötigen, zeigt der Autor die veränderten Bedingungen für die Polizeiausbildung auf. Das Berufsbild des Polizisten hat sich stark gewandelt. Polizisten sind durch die Cyberwelt mit der Entgrenzung der Kriminalität konfrontiert. Sie müssen sich mit neuen, komplexen Vorgehensweisen von Tätern und der Anforderung, stets über Technikexpertise für neue und neueste Geräte zu verfügen, auseinandersetzen. Die Technisierung des Berufsbildes des Polizisten, die wachsende Tendenz, es mit vernetzten Prozesse im Rahmen der Strafverfolgung zu tun zu haben, sind heute wichtige Wegmarken für das Arbeitsfeld insgesamt. Die Polizeiausbildung steht so vor neuen Herausforderungen, derer sich die Interessenvertreter der Polizeibediensteten und die ministerielle Leitungsebene annehmen müssen. Neue Ausbildungskonzepte sind zu entwickeln und zu erproben. Wie vielfältig die Berührungspunkte der Polizei mit der Technikwelt sind, belegt der Autor eindrücklich und deutet so auch auf neue Ausbildungsfelder hin.

Der Autor Thomas-Gabriel Rüdiger geht im polizeilichen Zusammenhang auf neue Deliktsfelder ein. Er ordnet Online-Spiele in die Klasse der Suchtstoffe ein, die zu Formen der Begleit- und Beschaffungskriminalität führen können. So zeigt der Autor auf, dass nicht die polizeiliche Praxis allein von der Cyberwelt betroffen ist, sondern sich auch neue Aufgabenstellungen der Kriminologie mit dem Entstehen

der Cyberwelt herauskristallisieren. Die Entwickler von Online-Spielen haben verschiedene Bezahlmodelle etabliert. Durch verschiedene Techniken halten sie immerwährendes Spielen attraktiv und fördern das exzessive Spielerverhalten. Spieler entwickeln zum Teil suchtartige Reaktionsformen und geraten in Abhängigkeit, fast eine halbe Million süchtige Onlinespieler leben mittlerweile in der Bundesrepublik Deutschland. Die Suchtreaktionen werden durch die Spieleanbieter zum Teil bewusst befördert, den Sicherheitsbehörden sind dabei weitgehend die Hände gebunden. Jugendschutz und Polizeiarbeit müssen hier Hand in Hand gehen, um neue Reaktionsformen auf diese neue Suchtformen zu entwickeln. Die neuen Formen von Begleitkriminalität, im sozialen Nahraum der Online-Süchtigen zu finden, werden von dem Autor anhand von Beispielen aus der Praxis beschrieben. Die Loslösungsprozesse der Süchtigen von der Realwelt sind denjenigen ähnlich, die bei Suchtmittelabhängigen nachweisbar sind. Eindrücklich beschreibt der Autor das Leiden des betroffenen sozialen Nahraums der Süchtigen. Die Finanzierung des Spielens ist insbesondere in späteren Suchtphasen ein Problem für die Süchtigen. Der Autor belegt an Beispielen, zu welchen Formen der Beschaffungskriminalität es bisher gekommen ist und welche Ursachen diese haben.

Die Autorin Astrid Bötticher beschreibt in ihrem zweiten Beitrag die Überführung der traditionellen Open-Source-Überwachung der Nachrichtendienste in die Cyberwelt und die Aneignung nachrichtendienstlicher Mittel durch private Unternehmen. Sie deutet darauf hin, dass die nachrichtendienstliche Überwachung mittels öffentlicher Informationen eine immer zentralere Stellung im nachrichtendienstlichen Geschehen bekommt und dies ursächlich mit der sich immer schneller und stärker entwickelnden Cyberwelt zusammenhängt. Die Basis der cyberbasierten Analysemethode, die soziale Netzwerkanalyse, wird von der Autorin in ihren Grundzügen vorgestellt und belegt die immer zentraler werdende relationale Soziologie als Wissenschaftsparadigma nachrichtendienstlicher Erhebungen. Gewohnheiten, Beziehungsmuster und -netze, Beziehungsformen und Aufmerksamkeitsstrukturen wie auch Interessen können kaum verschleiert werden. Menschen können über diese Zusammenhänge nicht lügen. Die Masse an öffentlich zugänglichen Berichten hilft ebenfalls eine niedrige Fehlerquote zu erreichen, indem Big Data (Massendaten) zu Analysezwecken aufbereitet werden. Die Analyse in Echtzeit wird dabei immer mehr durch die zukunftsvoraussagenden Analysen abgelöst. Insbesondere im Rahmen von Sicherheitsmaßnahmen erhält diese Form der Datennutzung eine hohe Relevanz. Der Autorin zufolge hat sich dadurch eine neue Form von Staatlichkeit etabliert, die sie unter Zuhilfenahme der Ikonologie beschreibt und analysiert. Der Leviathan und der Behemoth werden vom Bild des Ziz abgelöst.

http://www.springer.com/978-3-658-02797-1

Cyber-Sicherheit
Lange, H.-J.; Bötticher, A. (Hrsg.)
2015, VI, 287 S. 22 Abb., 8 Abb. in Farbe., Softcover
ISBN: 978-3-658-02797-1