Editorial

Der NSA-Überwachungsskandal hat deutlich gemacht, in welchem Umfang und mit welcher Reichweite westliche Geheimdienste die Überwachung der Kommunikationsnetze betreiben. Der damit verbundene finanzielle, technische und personelle Aufwand lässt erahnen, dass es dabei keineswegs nur um die Ausforschung der Privatsphäre mehr oder weniger ahnungsloser Bürger_innen geht. Die Zeiten, in denen der Cyberspace nur dem Gedankenaustausch diente, sind längst vorbei; die Datennetze sind zur zentralen Infrastruktur unserer Gesellschaft geworden. Ihre Überwachung zielt deshalb nicht nur auf jene, die per E-Mail, Chat oder Onlineplattformen kommunizieren, sondern kann buchstäblich jede_n treffen: ob am Bankautomaten, in der Arztpraxis, bei der Arbeit oder im vernetzten Heim. Der „Cyberspace" ist zu einem Ort geworden, an dem sich neue Formen der Kriminalität, des Krieges und der terroristischen Bedrohung entwickeln, aber auch neue Strategien der Sicherheit erprobt werden. Diese Ausgabe der **vor***gänge* widmet sich dem Thema Cybersecurity, der zunehmenden sicherheitspolitischen Durchdringung des digitalen Raumes.

Den Themenschwerpunkt eröffnen *Stefan Hügel* und *Dietrich Meyer-Ebrecht* mit einem Beitrag, in dem sie den rationalen Kern der Debatte um Cybersecurity herausarbeiten wollen. Sie gehen der Frage nach, ob es sich bei den immer wieder beschworenen Gefahren in der digitalen Welt um „Panikmache oder unterschätzte Gefahren" handelt. Die Rede von den ebenso vielfältigen wie akuten Gefahren im Cyberspace gehört zum sicherheitspolitischen Diskurs dazu – sie wird nicht selten benutzt, um neue, weitergehende Überwachungsmaßnahmen zu rechtfertigen.[1] Für die beiden Autoren steht noch nicht fest, ob sich im Cyberspace ein „neuer wilder Westen" auftut. Ihr Beitrag führt in zentrale Probleme der Cybersecurity ein und erklärt die wichtigsten Begriffe: Woher rührt die grundsätzliche Verletzbarkeit informationstechnischer Systeme? Welche Arten von Angriffen auf IT-Infrastruktur lassen sich unterscheiden und wer steckt (möglicherweise) dahinter? Welche Optionen der Absicherung von IT-Systemen gibt es?

Welche technische Möglichkeiten für den Selbstdatenschutz in der Ära nach Snowden noch existieren, dieser Frage geht *Rüdiger Weis* in seinem Beitrag über „Kryptographie, Open Source und Gesellschaft" nach. Die Grundannahme des Kryptologen ist ernüchternd: einmal gespeicherte Daten in IT-Anlagen können auf technische Weise nicht (absolut) geschützt werden. Deshalb sind Datensparsamkeit und eine Stärkung des Datenschutzrechts unabdingbar für sichere Kommunikation. Weis listet auf, welche Sicherheitsstandards nach den Snowden-Dokumenten als kompromittiert und damit als unsicher gelten – um zugleich praktische Tipps zu geben, was beim Einsatz kryptografischer Verfahren (der nach wie vor unbedingt zu empfehlen ist) beachtet

werden muss und welche Verfahren nach derzeitigem Stand von Wissenschaft, Technik und Geheimdienstfähigkeiten noch eine gewisse Sicherheit bieten.

Dass Sicherheit im Cyberspace nicht allein mit technischen Mitteln, sondern auch politischer und rechtlicher Rahmenbedingungen bedarf, unterstreicht auch *Martin Kutscha*. Er hebt die Bedeutung der (Grund-)Rechte für die Cybersecurity hervor. Sicherheit im Netz dürfe sich nicht allein auf repressive Aspekte, etwa die Gewährleistung einer lückenlosen Strafverfolgung, beschränken - die Sicherheit, Vertraulichkeit und Integrität der Kommunikationssysteme sei für die Nutzer_innen mindestens ebenso wichtig. Kutscha untersucht, inwiefern die bisherigen Cybersicherheitsstrategien überhaupt mit der Gewährleistung grundrechtlicher Freiheiten vereinbar sind. Seine Bilanz fällt negativ aus: er geht davon aus, dass das Internet bereits auf dem Weg zu einem grundrechtsfreien Raum sei.

Diese Zweifel nähren auch *Ute Bernhardt* und *Ingo Ruhmann*, die in ihrem Artikel bisherige Erkenntnisse über durchgeführte bzw. vorbereitete Cyberangriffe zusammenfassen. Dabei wird deutlich, dass die Entwicklung und der Einsatz sogenannter Cyber-Angriffswaffen sehr schnell voranschreitet. Vergleicht man die Etats, die mittlerweile für Cyberangriffe einerseits und Verteidigungs- bzw. Aufklärungsbemühungen andererseits zur Verfügung gestellt werden, zeigt sich ein deutliches Übergewicht der Ressourcen für militärische bzw. geheimdienstliche Angriffe im Cyberspace. Das die Militarisierung der digitalen Welt keine Vision einer fernen Zukunft ist, sondern sehr real vorangetrieben wird, dokumentiert nicht zuletzt das Talinn-Manual, welches *Michael Bothe* vorstellt. Das Manual gibt wieder, mit welchen Auswirkungen eines Cyberwarfare zu rechnen ist und wie die völkerrechtlichen Regeln für die Begrenzung bewaffneter Konflikte auf die digitale Kriegsführung übertragen werden können. Das von einer Expertenkommission erstellte Dokument verdeutlicht die Bemühungen der NATO um Regeln für die künftige Cyberkriegsführung.

Neben Militär und Geheimdiensten existieren weitere Akteure der Cybersicherheit, die in den drei folgenden Beiträgen vorgestellt werden: *Matthias Monroy* informiert über die aktuellen Cybersicherheits-Initiativen der europäischen Polizeiagentur Europol und weiterer EU-Einrichtungen. Er geht dabei auch auf die beteiligten deutschen Behörden ein – allen voran das Bundeskriminalamt, dass in Sachen Internetüberwachung eine Vorreiterrolle in Europa einnehme. Welcher Logik die digitale Sicherheitspolitik folgt, erschließt sich nicht, solange man nur auf die staatlichen Akteure schaut. Cybersecurity ist längst zum Geschäft geworden, hinter dem eine einflussreiche Industrie steht. Wie eng parlamentarische Entscheidungen zur europäischen Sicherheitsforschung und industrielle Lobbybemühungen miteinander verwoben sind, beschreiben *Martin Ehrenhauser* und *Alexander Sander.* Ihr Beitrag fasst eine frühere Studie zum „Lobbyismus der Sicherheitsindustrie in der Europäischen Union“ der beiden Autoren zusammen. Eine gegenläufige Perspektive nimmt *Markus Euskirchen* ein, der als engagierter Beobachter sozialer Proteste im Internet über den sogenannten Hacktivismus schreibt, jene Form der Wiederaneignung der Technik, mit der Aktivist_innen ein freies Netz verteidigen wollen.

Abschließend stellen wir drei aktuelle sicherheitspolitische Initiativen vor, die die Koordinaten der Cybersecurity in Deutschland und Europa für die nächsten Jahre bestimmen werden: *Zora Siebert* skizziert, wie sich die EU-Kommission seit zwei Jahren

um eine EU-weite Richtlinie für Netzsicherheit bemüht – und ihre Ansprüche nicht zuletzt dank massiver Lobbybemühungen immer weiter nach unten korrigiert hat. Der Deutsche Bundestag hat dagegen kürzlich ein IT-Sicherheitsgesetz verabschiedet, das am 25. Juli 2015 in Kraft trat. *Stefan Hügel* fasst die Kritik am neuen Gesetz zusammen, das erstmals für bestimmte Bereiche Meldepflichten für Störungen und fremde Eingriffe in deren IT-Systeme einführt – nach Einschätzung vieler Kritiker_innen jedoch kaum zu mehr Sicherheit im Cyberspace beitragen kann. *Kurt Graulich* schließlich kommentiert das gegenwärtig laufende Gesetzgebungsverfahren zur Wiedereinführung der Vorratsdatenspeicherung in Deutschland – nachdem der Europäische Gerichtshof die entsprechende EU-Richtlinie für nichtig erklärt und immer mehr EU-Staaten von dem Vorhaben Abstand nehmen. Warum die Daten so begehrt sind und weshalb die Vorratsdatenspeicherung gegen alle juristischen wie politischen Bedenken wieder eingeführt werden soll – das sollte nach der Lektüre dieser **vor***gänge* deutlich werden; schließlich sind Benutzerdaten eine zentrale Ressource der Sicherheitspolitik.

Neben dem Schwerpunkt bietet die aktuelle Ausgabe weitere Beiträge zu bürgerrechtlichen Fragen unserer Zeit: *Felix Herzog* kritisiert in seinem Essay zunehmend „Moralische Kreuzzüge auf dem Gebiet des Sexualstrafrechts" und bezieht sich dabei u.a. auf die Debatte um die Ausweitung des Straftatbestands der Vergewaltigung. Dazu berichtet *Mara Kunz* von einer Sachverständigenanhörung des Deutschen Bundestags, bei der sehr gegensätzliche Positionen zu mutmaßlichen Strafbarkeitslücken und der Wirksamkeit bzw. Angemessenheit eines schärferen Sexualstrafrechts vertreten wurden. *Anna Luczak* und *John Philipp Thurn* kommentieren die Entscheidung des Landesverfassungsgerichts von Sachsen-Anhalt zu verschiedenen Befugnissen des Sicherheits- und Ordnungsgesetzes. *Till Müller-Heidelberg* schließlich setzt sich kritisch mit einer Entscheidung des Bundesverfassungsgerichts zum kirchlichen Sonderarbeitsrecht auseinander. Die gesamte Redaktion wünscht Ihnen wie immer eine anregende Lektüre mit der neuen Ausgabe und freut sich über Ihre Kommentare und Kritiken.

Claudia Krieg und Sven Lüders
für die Redaktion

Heftvorschau:

Heft 210/211	Gesetzgebung zum Verbot der Suizidbeihilfe
Heft 212	Reflexhaftes Strafrecht

1 Jüngstes Beispiel ist die Erweiterung der Befugnisse zur geheimdienstlichen Kommunikationsüberwachung durch das „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“, mit dem BND, Verfassungsschutz und MAD internationale kriminelle, terroristische oder staatliche Angriffe „mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln“ abwehren sollen (s. BT-Drs. 18/4654 v. 20.4.2015).