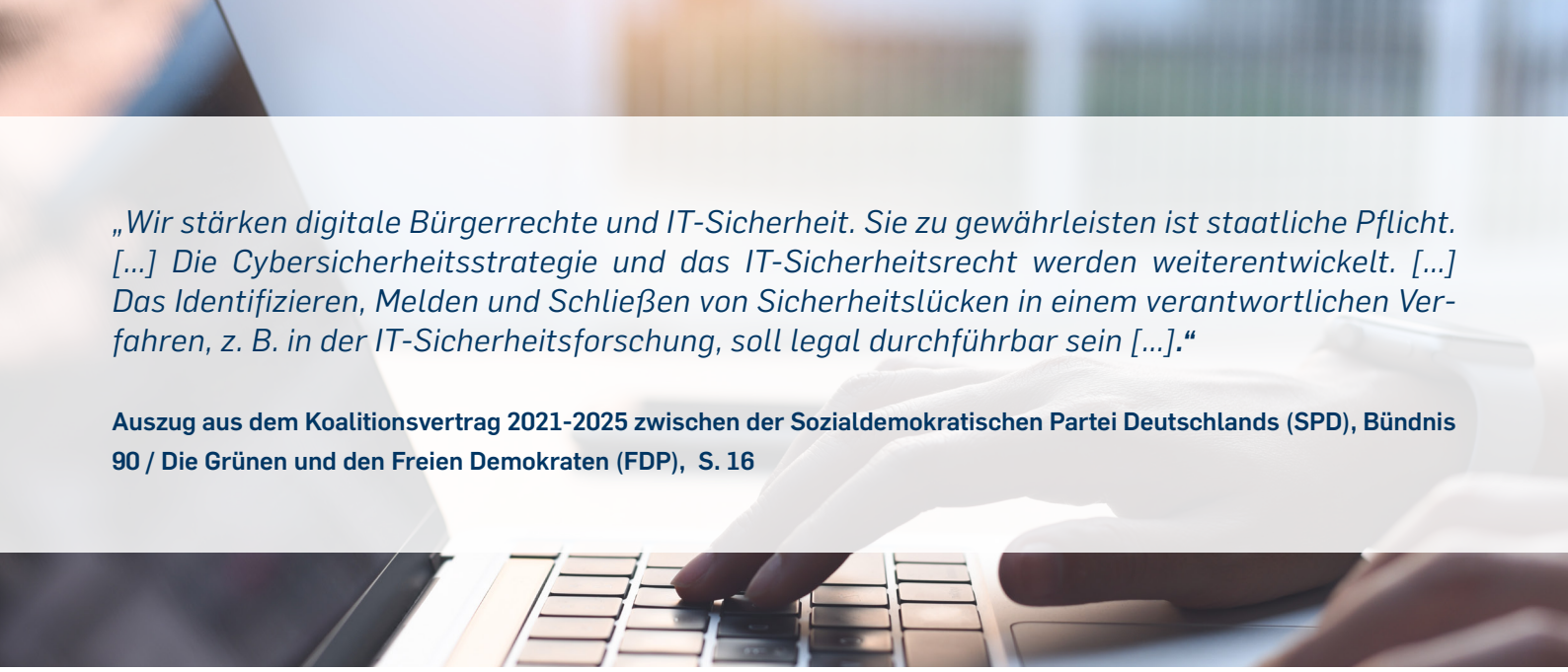
HORST GÖRTZ INSTITUT

No 1 | 2022

WHITEPAPER

WHITE-HAT-HACKING IN DER FORSCHUNG

Wie das deutsche Strafrecht Forschende in der IT-Sicherheit kriminalisiert – und wie die Politik dagegen vorgehen möchte



„Wir stärken digitale Bürgerrechte und IT-Sicherheit. Sie zu gewährleisten ist staatliche Pflicht. […] Die Cybersicherheitsstrategie und das IT-Sicherheitsrecht werden weiterentwickelt. […] Das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, soll legal durchführbar sein […].“

Auszug aus dem Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokraten (FDP), S. 16

I. Einleitung

Im Zuge der fortschreitenden Digitalisierung steigt auch die Anzahl und Qualität von Cyberangriffen auf staatliche Institutionen, Unternehmen und Privatpersonen. Als Konsequenz dieser Entwicklung gewinnt IT-Sicherheit nicht nur an Bedeutung, sondern wird vielmehr zur Voraussetzung für eine funktionierende digitalisierte Welt.

Vor diesem Hintergrund erscheint folgender Sachverhalt paradox: **Forschende in der IT-Sicherheit, die eine IT-Sicherheitslücke identifizieren und melden, können dafür in Deutschland strafrechtlich verfolgt werden.** Möglich machen dies die Paragraphen 202a und 202c des deutschen Strafgesetzbuches (StGB), die 2007 in Kraft getreten sind. Per gesetzlicher Regelung wird dadurch das Hacken von Schwachstellen unter Strafe gestellt.

Wie aus dem Koalitionsvertrag für die Legislaturperiode 2021 bis 2025 von SPD, Bündnis 90/Die Grünen und FDP hervorgeht, sind im Rahmen des IT-Sicherheitsrechts nun weitreichende Änderungen geplant. So soll künftig „**[d]as Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z. B. in der IT-Sicherheitsforschung, […] legal durchführbar sein**“ (siehe Auszug oben). Kurzum: Die neue Bundesregierung plant die Legalisierung von White-Hat-Hacking. Eine Novellierung der genannten Paragraphen wäre die Folge.

White-Hat- versus Black-Hat-Hacking

Als White-Hat-Hacking wird eine Form des Hackings bezeichnet, die auf eine Verbesserung der IT-Sicherheitslage abzielt. Während White-Hat-Hacker*innen stets gute Absichten beim Hacken von IT-Systemen verfolgen und zur Aufklärung und Behebung von IT-Sicherheitslücken beitragen, handeln Black-Hat-Hacker*innen mit krimineller Energie. Ziel des Black-Hat-Hackings ist es, über identifizierte Schwachstellen ein IT-System zu kompromittieren und dort Schäden anzurichten, z. B. durch Datendiebstahl oder persönliche Bereicherung.

II. § 202a StGB – „Digitaler Hausfriedensbruch“ durch IT-Sicherheitsforschung

Schwachstellen aufzuspüren, ist in der IT-Sicherheitsforschung gängige Praxis. Eine ethisch verantwortliche Vorgehensweise ist hier selbstverständlich. Dennoch kann dieser Modus Operandi nach **§ 202a StGB** als „**Ausspähen von Daten**“ gewertet werden und für Wissenschaftler*innen in einem Strafprozess münden. Der Grund: Es wird der Anschein erweckt, als verschafften sich Forschende auf diese Weise unbefugt Zugang zu gesicherten Daten. Es fände quasi ein „digitaler Hausfriedensbruch“ statt. Damit wäre der Tatbestand von Paragraph 202a StGB erfüllt (siehe Rechtsnorm in der Infobox auf Seite 2). Dabei spielt es keine Rolle, ob die Handlung unter das White-Hat-Hacking fällt und eine durch Forschung herbeigeführte Verbesserung der IT-

Sicherheitslage zum Ziel hat. Denn die gesetzliche Regelung ist äußerst **vage formuliert** und unterscheidet nicht nach dem Motiv, das einer Handlung zu Grunde liegt. Sie differenziert also nicht eindeutig zwischen Black-Hat- und White-Hat-Hacking bzw. krimineller und nicht-krimineller Absicht. Sobald eine unberechtigte „Überwindung der Zugangssicherung" zwecks Datenzugriff erfolgt, ist der Tatbestand des „Ausspähens von Daten" prinzipiell erfüllt.

Doch wie sollten sich Wissenschaftler*innen verhalten, wenn sie eine IT-Sicherheitslücke identifizieren? Im Kontext dieser Fragestellung hat sich das **Responsible Disclosure Verfahren** bewährt, auch bekannt unter dem Begriff Coordinated Vulnerability Disclosure. Es handelt sich dabei um einen koordinierten Abstimmungsprozess. Wer eine Schwachstelle entdeckt, setzt sich mit den verantwortlichen Parteien, zum Beispiel Herstellern und Behörden, in Verbindung und gibt ihnen die Möglichkeit, innerhalb einer bestimmten Frist die Lücke zu schließen, bevor die Öffentlichkeit informiert wird. Die Responsible Disclosure genießt internationale Anerkennung und stellt einen Common Sense der Branche dar. White-Hat-Hacker*innen halten sich an dieses implizite Abkommen und Betroffene reagieren ihrerseits nicht mit rechtlichen Schritten. Auch am Horst-Görtz-Institut für IT-Sicherheit (HGI) sowie am Max-Planck-Institut für Sicherheit und Privatsphäre (MPI-SP) findet die Responsible Disclosure Anwendung, wenn eine Schwachstelle gefunden wird.

Dennoch schützt das Verfahren nicht zwangsläufig vor einer Strafverfolgung, wie das prominente Beispiel der **Sicherheitsforscherin Lilith Wittmann** zeigt. Diese hatte im Mai 2021 eine **Sicherheitslücke in einer Wahlkampf-App der CDU** entdeckt, über die sie Zugriff auf mehr als 18.000 persönliche Daten der Wahlkampfhelfer*innen erhielt sowie auf weitere 1.350 Datensätze zu angeworbenen Unterstützer*innen. Im Anschluss daran meldete sie die Schwachstelle unter Berücksichtigung des Responsible Disclosure Prozesses sowohl dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Berliner Datenschutzbeauftragten, als auch der CDU selbst. Was folgte, war eine Strafanzeige der CDU wegen des Verdachts des Ausspähens von Daten. Wittmann erhielt Post vom Berliner Landeskriminalamt. Das eröffnete Ermittlungsverfahren wurde im September 2021 eingestellt, die CDU entschuldigte sich bei der Forscherin. Die Folgen für die Partei und ihre Mitglieder sind dennoch von größerer Tragweite. So hat der Chaos Computer Club (CCC) seine Konsequenzen aus dem Fall gezogen. Da die Partei das implizite Responsible Disclosure Verfahren einseitig aufgekündigt habe, sehe man sich gezwungen, bei Schwachstellen in CDU-Systemen künftig auf eine Meldung zu verzichten, um rechtliche Auseinandersetzungen zu vermeiden, verkündete der CCC.

Ähnliche **Vorsichtsmaßnahmen** werden auch am **Forschungsstandort Bochum** getroffen, um rechtliche Risiken zu minimieren. So werden gefundene IT-Sicherheitslücken nur dann an die Hersteller gemeldet, wenn diese sich eindeutig zum Responsible Disclosure Verfahren bekennen oder sich in ihren Sicherheitsrichtlinien positiv dazu äußern. Forschung in einer **künstlich geschaffenen Testumgebung** ist ebenfalls eine Maßnahme zum Schutz vor rechtlichen Folgen. Software-Schwachstellen werden beispielsweise an handelsüblichen Produkten unter Laborbedingungen validiert und Online-Accounts im Rahmen simulierter Angriffe mit Hilfe von eigenen Benutzerkonten der Forschenden analysiert. Findet Forschung unter **realen Praxisbedingungen** statt, unterliegt sie einer strengen wissenschaftlichen Selbstkontrolle. Zum Beispiel werden wissenschaftliche Paper auf renommierten Sicherheitskonferenzen nur dann angenommen, wenn die in der Praxis betroffenen Hersteller vorab in einem Responsible Disclosure Verfahren über die gefundenen Sicherheitslücken informiert wurden. Die Grenzen des ethisch Vertretbaren werden zudem ständig diskutiert und zweifelhafte Ergebnisse unter Umständen von der Veröffentlichung ausgeschlossen. Für die Sicherheitsforschung ist es relevant, neben der theoretischen Forschung den Blick gleichsam auch auf die Praxis zu richten. Möchte man etwa erfahren,

§ 202a StGB – Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

wie viele schwache Passwörter real verwendet werden, müssten passwort-geschützte Accounts weltweit analysiert werden. Aktuell stehen jedoch nur relativ kleine, freiwillige Nutzerstudien sowie Passwortsammlungen zur Verfügung. Gleichermaßen sind großskalige Analysen und Netzwerk-Scans im globalen Internet zur Schwachstellenerhebung für Forschende oft unabdingbar, nur können diese von ins Ziel genommenen Betreibern kaum von echten Angriffen unterschieden werden. Hierbei ergibt sich eine besondere Kritikalität bei der Analyse von Finanzinfrastrukturen und Kryptowährungen: Werden Proof-of-Concept-Implementierungen eingesetzt, die die Machbarkeit von Angriffen nachweisen können, wie z. B. das unzulässige doppelte Verausgaben von Bitcoins, könnte allein diese Tätigkeit in verschiedener Hinsicht strafbar sein. Daher stößt Forschung unter diesen Bedingungen oftmals dann an ihre Grenze, wenn es darum geht, **wissenschaftliche Erkenntnisse über die ‚reale Welt'** zu gewinnen. Wird jedoch unter Praxisbedingungen geforscht, steigt an dieser Stelle das Risiko einer Strafbarkeit nach Paragraph 202a StGB.

Dr. Sebastian Golla, Juniorprofessor für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter, erforscht an der Ruhr-Universität Bochum **das komplexe Verhältnis von IT-Sicherheit und Strafrecht** und rät: „Eine wichtige Grundlage ist es, die möglichen Strafbarkeitsrisiken zu kennen und sich konkret beraten zu lassen. Vor der Durchführung eines Forschungsprojekts kann man sich dann überlegen, wie sich die jeweiligen Risiken ausschließen lassen – zum Beispiel, indem rechtssichere Einverständniserklärungen eingeholt werden, die vor einer Strafverfolgung schützen. Dies ist in der Forschungspraxis allerdings mit großem Aufwand verbunden und zudem nicht immer möglich."

III. § 202c StGB – Sicherungscodes und Hackertools zur Vorbereitung einer Straftat

Neben § 202a StGB führt auch **§ 202c StGB** zu Unsicherheiten und Risiken bei IT-Sicherheitsforschenden, da dadurch bereits das „**Vorbereiten des Ausspähens und Abfangens von Daten**" unter Strafe gestellt wird. Sich Passwörter oder andere Sicherungscodes zu verschaffen, die den Zugriff auf Daten erlauben, kann als Vorbereitung einer Straftat angesehen werden. Dies trifft ebenfalls auf das Herstellen, Überlassen, Verschaffen und Verbreiten von Computerprogrammen zu, deren Zweck die Begehung einer Straftat ist (siehe Rechtsnorm in der Infobox). Daher wird § 202c StGB umgangssprachlich als „**Hackerparagraph**" oder „**Hackertoolparagraph**" bezeichnet. Auch hier liegt die Problematik darin, dass die gesetzliche Regelung – ähnlich wie § 202a StGB – keine eindeutige Formulierung enthält und nicht explizit zwischen kriminell ausgerichteten und im Rahmen der Forschung üblichen Handlungen differenziert. Im Vordergrund steht weniger der Zweck als vielmehr das Mittel zum Zweck.

Dies wirft Fragen auf, da **Hackertools**, also Computerprogramme, die gezielt bei der Suche nach Schwachstellen eingesetzt werden, ein unverzichtbares Instrument im Arbeitskontext von IT-Sicherheitsforschenden darstellen. Unter diesen Hackertools befindet sich häufig auch so genannte **Dual-Use-Software**, die für ethische Forschungszwecke und kriminelle Absichten gleichermaßen eingesetzt werden kann. Auch am Forschungsstandort Bochum finden Hackertools Anwendung, die unter das Label Dual-Use fallen. Ferner kommen derartige Programme im Studium der IT-Sicherheit an der Ruhr-Universität Bochum bereits in der Bachelor-Phase in Vorlesungen und Übungen zum Einsatz. Doch wie verhält es sich mit der Nutzung von Dual-Use-Software im Forschungskontext? Und dürfen Lehrende ihren Studierenden diese Computerprogramme zugänglich machen? Aufgrund diverser **Verfassungsbeschwerden**, die auf ähnlichen Fragestellungen und damit einhergehenden Unklarheiten des Hackertoolparagraphen basieren, hat das Bundesverfassungsgericht mittlerweile entschieden, dass § 202c StGB in seiner Interpretation eng auszulegen

§ 202c – Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a (Ausspähen von Daten) oder § 202b (Abfangen von Daten) vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

ist. „Die Verwendung von Dual-Use-Software ist demnach nicht strafbar. Forschende wie Lehrende in der IT-Sicherheit haben daher kaum zu befürchten, nach § 202c StGB verurteilt zu werden," wie Golla erklärt. Allerdings ist zu betonen, dass sich ein **Restrisiko** nicht ausschließen lässt und daher für Wissenschaftler*innen, trotz der Eingrenzung durch das Bundesverfassungsgericht, nach wie vor Unsicherheiten hinsichtlich der Strafbarkeit bestehen, insbesondere bei neuen Forschungsansätzen im Bereich der Sicherheit real eingesetzter Systeme.

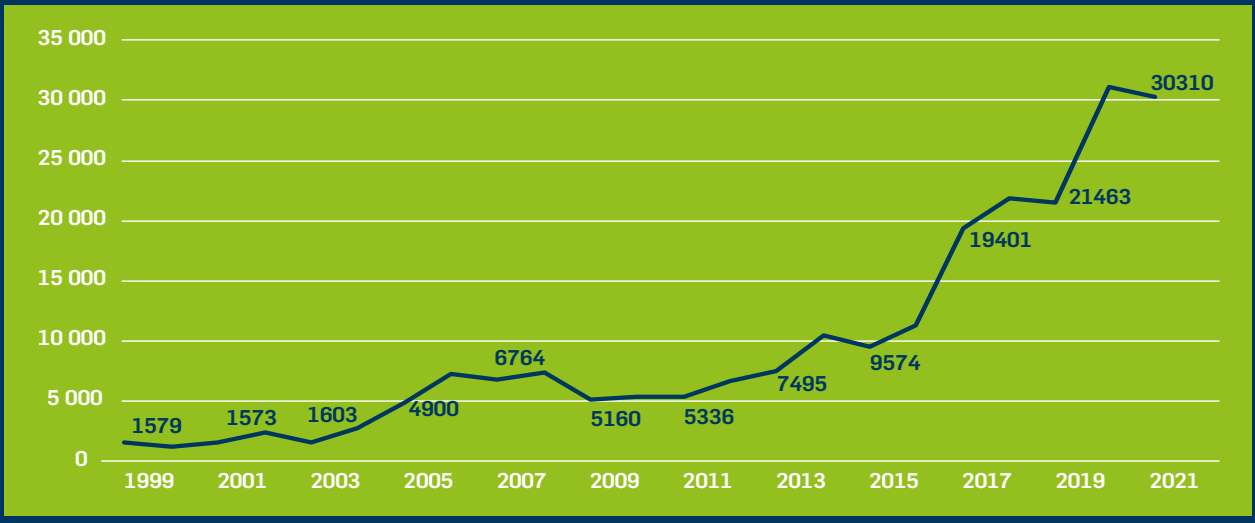
IV. Strukturelle Probleme im IT-Strafrecht

Anhand der skizzierten Auswirkungen wird ersichtlich, dass **keineswegs Einheitlichkeit bei der Auslegung** der beiden Paragraphen besteht und IT-Sicherheitsforschende als juristische Lai*innen dadurch mit rechtlichen Unsicherheiten und aus ihrer Sicht nicht einschätzbaren Risiken konfrontiert werden. Auch wenn eine strafrechtliche Verurteilung nach den Paragraphen 202a StGB und 202c StGB eher unwahrscheinlich ist, besitzen die Rechtsnormen einen **Abschreckungseffekt**, der sich negativ auf die Forschung zur IT-Sicherheit auswirkt. Zu bedenken ist in diesem Kontext, dass auch Ermittlungsverfahren der Staatsanwaltschaft ohne spätere Verurteilung sehr belastend für Wissenschaftler*innen sein können. „Es ist durchaus realistisch, dass Strafverfolgungsbehörden wegen eines Verdachts von § 202a StGB oder § 202c StGB zunächst ausführlich ermitteln, auch wenn sich letztlich herausstellt, dass das untersuchte Verhalten der Forschenden nicht strafbar war", betont Golla.

Auch mehr als zehn Jahre nach Inkrafttreten der gesetzlichen Regelungen hat die damit verbundene Problematik nicht an **Aktualität** verloren, wie der Fall Wittmann eindrücklich zeigt. Die **Spielräume in der Interpretation der Paragraphen** tragen maßgeblich zur Verunsicherung bei. „Zum Schutze der IT-Sicherheitsforschung muss das IT-Strafrecht hier zwingend klarer werden und Tatbestände zuspitzen, damit es nicht Tätigkeiten verhindert, auf die wir im digitalen Zeitalter angewiesen sind," so der Fachexperte.

Aus juristischer Perspektive würden sich **eindeutige Privilegierungen für die Forschung** im Sinne einer Ausnahmeregelung empfehlen. „Es ließe sich zum Beispiel darüber nachdenken, neue rechtliche Regelungen zu schaffen, die eine Strafbarkeit explizit ausschließen, wenn Forschende nach Entdecken einer IT-Sicherheitslücke sofort die notwendigen Maßnahmen ergreifen, um diese zu schließen," ergänzt Golla. Die Festlegung dieser Maßnahmen sollte jedoch unbedingt **international einheitlich im Dialog mit weltweit anerkannten IT-Sicherheitsexpert*innen** erfolgen, da Forschung heute nur noch inter-

Infografik: Dokumentierte Schwachstellen in der IT-Sicherheit weltweit und ihre Entwicklungskurve



Quelle: Common Vulnerabilities and Exposures / CVE (https://www.cve.org/Downloads, Zugriff am: 03.03.2022)
CVE ist ein Referenzier-System aus den USA, das öffentlich bekannt gemachte IT-Sicherheitslücken auf der ganzen Welt identifiziert, eindeutig katalogisiert und veröffentlicht.

national denkbar ist. Aber auch schädliche Handlungen durch das Black-Hat-Hacking sollten strafgesetzlich konkretisiert werden, beispielsweise bei Hackerangriffen auf kritische Infrastrukturen. „Die geschilderten Szenarien in der IT-Sicherheitsforschung sind letztlich nur ein Symptom dafür, dass in diesem gesetzlichen Regelungskomplex etwas grundsätzlich nicht mehr passt. Teilweise sind die Rechtsnormen veraltet, teilweise wurden sie ungeschickt ergänzt. Zugleich sind die einschlägigen Straftatbestände durch die Digitalisierung auf mehr Sachverhalte anwendbar als früher," resümiert Golla. Daher stehen die genannten Paragraphen und die damit verbundenen Unsicherheiten und Risiken in der IT-Sicherheitsforschung sinnbildlich für **größere, strukturelle Problematiken des IT-Strafrechts**, die perspektivisch in den Blick genommen werden müssen.

V. Plädoyer für einen dringenden Handlungsbedarf durch die Politik

Die **Bedrohungslage zur IT-Sicherheit** in Deutschland gilt laut BSI weiterhin als „angespannt bis kritisch". Dabei sind gravierende Schwachstellen in IT-Systemen eines der größten Risiken im Kampf gegen die Cyberkriminalität, wie dem aktuellen Lagebericht zur IT-Sicherheit 2021 zu entnehmen ist. Diese Entwicklung gilt nicht nur für Deutschland, sondern ist weltweit zu verzeichnen (siehe Infografik auf Seite 4). IT-Sicherheitsforschung ist in diesem Zusammenhang ein **zentraler Eckpfeiler zur Verbesserung der IT-Sicherheitslage in Deutschland** und der „Schlüssel" für „ein digitalisiertes Leben auf Basis von Vertrauen und Sicherheit", wie das Bundesministerium für Bildung und Forschung im aktuellen Forschungsrahmenprogramm zur IT-Sicherheit bekräftigt.

Dazu gehört auch die **Erforschung von Sicherheitsmechanismen in der Informationstechnologie und deren Schwachstellen**. In den vergangenen Jahren haben Wissenschaftler*innen am Forschungsstandort Bochum in Kooperation mit Fachkolleg*innen diverse IT-Sicherheitslücken identifiziert und in einem abgestimmten, verantwortlichen Verfahren gemeldet und behoben – wie etwa Schwachstellen in Sicherheits-Chips von Garagentoren (2008), im etablierten IEEE-Standard von modernen Hardwaresystemen (2021), in PDF-Dokumenten (2021) oder Smartphones (2021). Sie stehen damit exemplarisch für eine Vielzahl von Forschenden, die sich in Deutschland aus einer wissenschaftlichen Perspektive heraus mit IT-Sicherheitslücken befassen und damit zu einer Verbesserung der IT-Sicherheitslage beitragen. Um ihrem Forschungsauftrag adäquat nachkommen zu können, bedarf es entsprechender rechtlicher Rahmenbedingungen. Statt zu mehr Rechtssicherheit führt die aktuelle Gesetzeslage im IT-Strafrecht jedoch zu einem **Eingriff in die Forschungsfreiheit und in die Grundrechte der Wissenschaftler*innen**, die dadurch kriminalisiert werden. Wie hoch die Anzahl nicht gemeldeter IT-Sicherheitslücken ist, lässt sich statistisch nicht erfassen und daher nur erahnen. Fest steht jedoch, dass die IT-Sicherheitslage in Deutschland durch diese Entwicklung nicht gestärkt werden kann und mit **potenziellen Standortnachteilen** für die Forschungslandschaft und die Wirtschaft einhergeht.

Die beschriebenen Auswirkungen machen eine Anpassung der Rechtsnormen im deutschen IT-Strafrecht unserer Ansicht nach unumgänglich. Dahingehend sind die **Pläne der aktuellen Bundesregierung** zur Legalisierung von White-Hat-Hacking in der IT-Sicherheitsforschung vielversprechend. Allerdings gilt es nun, seitens der Politik zu handeln und eine zeitnahe Novellierung anzustreben. Denn auch wenn IT-Sicherheit letztlich technisch zu gewährleisten ist, muss das IT-Strafrecht die passenden Rahmenbedingungen dafür bieten.

Autorin: Julia Laska

Junior-Professor
Dr. Sebastian Golla

Sebastian Golla studierte Rechtswissenschaften in Münster und Santiago de Chile. 2015 promovierte er an der Humboldt-Universität zu Berlin im Strafrecht zu dem Thema „Die Straf- und Bußgeldtatbestände der Datenschutzgesetze". Von 2012 bis 2020 war er wissenschaftlicher Mitarbeiter an der Humboldt-Universität zu Berlin und an der Johannes Gutenberg-Universität Mainz. Seit August 2020 ist er Juniorprofessor für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter an der Ruhr-Universität Bochum.

Weiterführende Informationen zum Thema
Sebastian Golla. IT-Sicherheit und Strafrecht – Neukalibrierung eines belasteten Verhältnisses. JuristenZeitung. 2021, S. 985-990.

Das Horst Görtz Institut für IT-Sicherheit (HGI) an der Ruhr-Universität Bochum (RUB)

Das Horst-Görtz-Institut für IT-Sicherheit (HGI), Research Department der Ruhr-Universität Bochum (RUB), gehört zu den größten und ältesten Instituten im Bereich der IT-Sicherheit in Europa. Rund 160 Wissenschaftler*innen forschen hier gemeinsam in Arbeitsgruppen der Elektro- und Informationstechnik, Mathematik und Informatik sowie den Geistes- und Gesellschaftswissenschaften. In diesem einzigartig interdisziplinären Umfeld werden nahezu alle Aspekte der IT-Sicherheit abgedeckt. Seit 2019 beheimatet das HGI den Exzellenzcluster „CASA – Cyber Security in the Age of Large-Scale Adversaries“. Er ist der einzige deutsche Exzellenzcluster im Bereich der IT-Sicherheit. Gefördert wird er durch die Deutsche Forschungsgemeinschaft (DFG) mit rund 30 Millionen Euro.

Neben der Spitzenforschung basiert das Institut auf den Pfeilern Studium und Transfer. Mit über 1.000 Studierenden gehört Bochum heute zum größten Standort für die Cybersicherheitsausbildung in Europa. Zudem ist das HGI in Deutschland führend bei der Gründung von Start-Ups im Bereich IT-Sicherheit. Seit 2021 ist das Institut Teil der neu gegründeten Fakultät für Informatik der RUB.

HGI.RUB.DE | CASA.RUB.DE

Das Max-Planck-Institut für Sicherheit und Privatsphäre (MPI-SP)

Das Max-Planck-Institut für Sicherheit und Privatsphäre (MPI-SP) wurde im Mai 2019 in Bochum gegründet. Die Aufgabe des Instituts besteht darin, die technischen Grundlagen und interdisziplinären Aspekte der IT-Sicherheit und des Datenschutzes zu erforschen und zu entwickeln. Neben international sichtbarer Spitzenforschung bemüht sich das Institut um die Ausbildung der nächsten Generation wissenschaftlicher Führungskräfte im Bereich Cybersicherheit und Schutz der Privatsphäre.

Zu den aktuellen Forschungsschwerpunkten gehören Grundlagen der Sicherheit und Privatheit, Post-Quanten-Kryptographie, Eingebettete Sicherheit, Kryptowährungen und Smart Contracts sowie Responsible Computing.

Das MPI-SP und HGI bündeln am stetig wachsenden Forschungsstandort Bochum ihre Fachexpertise und sind durch gemeinsame Forschungsvorhaben eng miteinander verbunden.

MPI-SP.ORG

Ruhr-Universität Bochum | Horst-Görtz-Institut für IT Sicherheit
Gebäude MC 0/75 | Universitätsstrasse 150
44780 Bochum | Deutschland
WWW.HGI.RUB.DE | WWW.CASA.RUB.DE