RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

Schwerpunkt

VERBRECHEN

FORENSIK:
Wie Maden einen Mord aufdecken

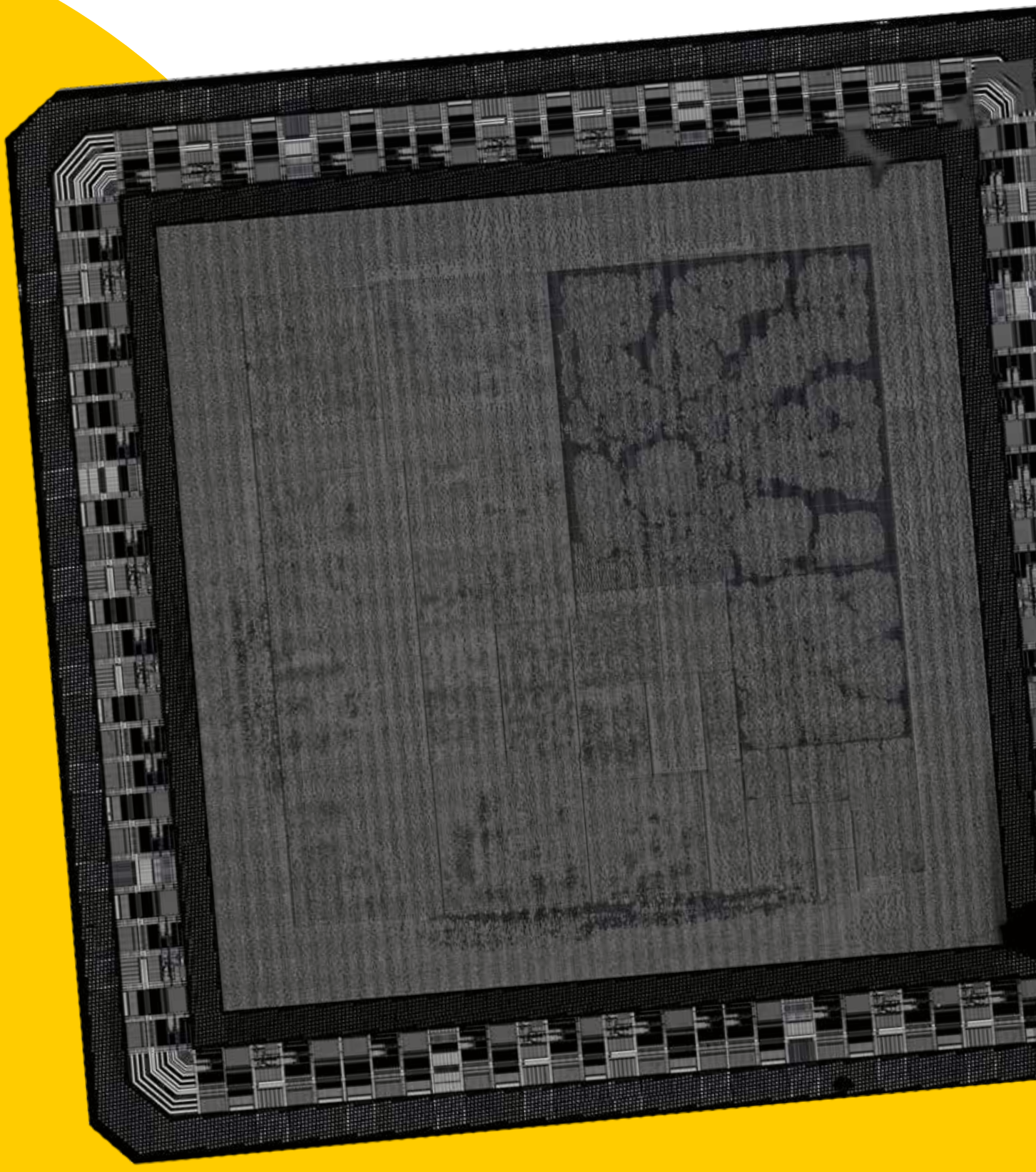
PARTNERINNENTÖTUNG:
Warum die Strafen so milde sind

TRAUMA:
Wenn die Bilder immer wiederkommen

#32
Jahrgang

Nr. 1 | 2022

WIE IDEENKLAUER TICKEN



Konstruktionspläne von Chips zu klauen kann sich rentieren. Ein interdisziplinäres Forschungsteam will dem Ideendiebstahl zuvorkommen.

Mit ihren Millionen von Leiterbahnen und Transistoren erinnern elektronische Mikrochips beinahe an futuristische Metropolen mit einem komplexen Straßennetz, das sich über mehrere Etagen erstreckt. Heutzutage sind sie jedoch oft so klein, dass man die einzelnen Wege und Gebäude mit bloßem Auge nicht erkennen kann. Die Miniatur-Landschaften sorgen dafür, dass die Elektronik in modernen Autos funktioniert, der Kühlschrank mit dem Handy steuerbar ist oder automatisierte Produktionsprozesse in der Industrie ablaufen. Mikrochips sind nicht mehr wegzudenken.

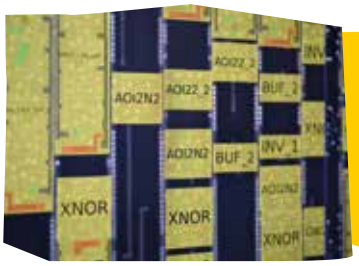
Die Entwicklung eines solchen Bauteils kann mehrere Millionen Euro kosten. Da ist mancherorts die Versuchung groß, sich die Elektronik-Landschaft nicht selbst von null an auszudenken, sondern zu schauen, was die Konkurrenz schon hat. Das sogenannte Hardware Reverse Engineering hilft beim Ideenklau. Wie Menschen dabei vorgehen, interessiert Kognitionsforscherin Dr. Carina Wiesen und IT-Sicherheitsforscher Dr. Steffen Becker. Die beiden haben ihre Promotion an der RUB als Forschungstandem im Forschungskolleg SecHuman zu dem Thema abgeschlossen. Warum es eine zähe Angelegenheit ist, das Hardware Reverse Engineering zu untersuchen, erzählen die beiden im Interview.

Einen Chip rückwärts zu bauen, um den Konstruktionsplan zu klauen, klingt aufwendig. Ist das wirklich günstiger, als die Technik selbst zu entwickeln?

Steffen Becker: Tatsächlich ja, zumindest, wenn es um Brot-und-Butter-Chips geht, die millionenfach verbaut werden, nicht um die neusten Hightech-Produkte von Apple oder Intel. Wer sich den Konstruktionsplan für einen Chip klaut, spart sich die Kosten für Forschung und Entwicklung, muss kein eigenes Marketing machen und sich nicht um Treiber kümmern.

Und wie funktioniert das Hardware Reverse Engineering?

Becker: Ein vollumfängliches Reverse Engineering ist aufwendig. Auf einem Chip mit einer Fläche von einem Quadratmillimeter können einige Hunderttausend Gatter drauf sein. Der Chip ist dreidimensional aufgebaut und besteht aus bis zu 20 Schichten. Zu Beginn fertigt man einen Querschnitt des Chips an, um zu sehen, wie viele Schichten er hat, wie dick er ist und welche Materialien er enthält. Dann trägt man nacheinander jede einzelne Schicht mit chemischen Verfahren ab und macht mit dem Elektronenrastermikroskop Bilder jeder freigelegten Schicht – mehrere hundert oder mehrere tausend Bilder pro Schicht. Die werden schließlich zu einem dreidimensionalen Bild zusammengefügt. ▸



Hier zu sehen sind einige Gatter auf der zweitniedrigsten Schicht eines Chips, die einen Teil der Netzliste ausmachen. Die komplette Netzliste enthält Informationen zu allen Elementen und Verbindungen auf einem Chip.

Mittels Elektronenmikroskopie ist hier die unterste Schicht eines Chips sichtbar gemacht, der dafür speziell von der Rückseite präpariert wurde. Die Aufnahme wurde aus 2.000 Einzelbildern zusammengesetzt. (Bild: RUB, Lehrstuhl für Eingebettete Sicherheit)

i GATTER

Gatter sind Bauteile, mit denen sich Logikschaltungen realisieren lassen. Ein Gatter bekommt einen oder mehrere Eingänge und verknüpft diese miteinander zu einem einzigen Output. Eingangs- und Ausgangsinformationen liegen binär vor, also als Nullen und Einsen. Ein Gatter, das die logische Operation „und" abbildet, gibt beispielsweise nur dann eine Eins als Ergebnis aus, wenn beide Eingänge auch Einsen waren; eine Kombination aus einer Null und einer Eins würde hingegen zu dem Output „Null" führen. Ein Oder-Gatter würde immer dann eine Eins als Ergebnis produzieren, wenn mindestens einer der beiden Eingänge eine Eins war.

Kognitionsforscherin Carina Wiesen und IT-Sicherheitsforscher Steffen Becker haben interdisziplinär zum Thema Reverse Engineering promoviert.

Das alles geht mit einem einzelnen Chip?
Becker: Nein, man braucht mehrere Dutzend Chips, weil man sie in dem Prozess kaputtmacht. Es ist auch nicht so simpel, wie es zunächst klingt. In dem Prozess kann viel schiefgehen; damit man es auch nur ansatzweise hinbekommt, braucht man viel Erfahrung. Wenn man das dreidimensionale Bild des Chips erzeugt hat, kann man daraus die sogenannte Netzliste generieren. Sie umfasst alle digitalen Schaltungen bestehend aus den logischen Gattern und Speicherelementen mit ihren Verbindungen. Die Netzliste ist aber noch kein fertiger Konstruktionsplan; will man einen Chip nachbauen, muss sie analysiert werden. Das Ziel ist aber nicht immer, die komplette Netzliste zu verstehen – das wäre der heilige Gral. Manchmal reicht es, wichtige Teilkomponenten zu finden und zu verstehen.

Das klingt zunächst nur nach einem technischen Prozess. Aber in Ihrer interdisziplinären Forschung beleuchten Sie auch eine psychologische Komponente.
Carina Wiesen: Das Hardware Reverse Engineering ist ein undurchsichtiger Prozess, der nicht gut verstanden ist. In der Regel laufen Teilprozesse automatisiert ab. Aber dann muss der Mensch dem Ergebnis einen Sinn verleihen. Diese menschlichen Analyseprozesse hat sich vor uns kaum jemand angeschaut. Die Netzliste verstehen – das kann man als ein großes Problem definieren, das man über verschiedene Strategien lösen kann. Wir wollen herausfinden, welche Strategien Menschen dafür nutzen, und wenden dazu psychologische Modelle aus dem Problemlösebereich an. Dafür mussten wir erst einmal eine Methode erarbeiten – das hat drei, vier Jahre gedauert.

Was ist das Ziel dieser Forschung?
Wiesen: Es geht darum, geistiges Eigentum besser schützen zu können. Wenn wir wissen, wie Menschen beim Hardware Reverse Engineering vorgehen, lassen sich eventuell Schutzmaßnahmen entwickeln, die es schwerer machen, die üblichen Problemlösestrategien anzuwenden.

Fällt es eigentlich manchmal auf, wenn Ideen durch Hardware Reverse Engineering geklaut werden? Und wird der Diebstahl bestraft?
Becker: Reverse Engineering ist beispielsweise in den USA grundsätzlich erlaubt. Dabei geht es vor allem darum, dass Kompatibilität mit Geräten von Fremdherstellern hergestellt werden kann. Letztlich ist es aber immer eine rechtliche Abwägung zwischen Gesetzen zum Patent- und Copyrightschutz auf der einen Seite sowie Handels- und Verbraucherschutzgesetzen auf der anderen Seite.

Es sind nur wenige Fälle von Ideenklau durch Reverse Engineering öffentlich bekannt. Hinter verschlossenen Türen tobt aber ein regelrechter Kampf um die Patente und das jeweilige geistige Eigentum, bei dem die großen Wettbewerber gegenseitig ihre Hardware auf den Diebstahl geistigen Eigentums untersuchen. Finden sie mögliche Verletzungen, wird aber im Normalfall der diskrete rechtliche Weg beschritten, und technische Details kommen nur in den seltensten Fällen an die Öffentlichkeit.

Kann Hardware Reverse Engineering eigentlich auch für andere Zwecke eingesetzt werden – oder nur um Know-how zu stehlen?
Becker: Die kriminelle Seite ist nur eine Seite der Medaille. Reverse Engineering kann beispielsweise auch helfen, Manipulationen an Hardware zu finden.

Wie lässt sich dieser Prozess überhaupt erforschen? Ideendiebe werden sich kaum bei der Arbeit über die Schulter schauen lassen.
Wiesen: Es gibt nur wenige Expertinnen und Experten für Hardware Reverse Engineering. Also haben wir uns gefragt: Wie können wir Leute beobachten, während sie unbekannte Netzlisten analysieren? Steffen hat schließlich einen Kurs für Studierende der IT-Sicherheit, Informatik und Elektrotechnik entwickelt, die sechs Monate in das Hardware Reverse Engineering eingeführt wurden. Am Ende dieses Kurses

i SECHUMAN

Im Forschungskolleg „SecHuman – Sicherheit für Menschen im Cyberspace" beleuchten Promovierende technische und gesellschaftliche Probleme der IT-Sicherheit in interdisziplinärer Zusammenarbeit. In diesem Rahmen schlossen Carina Wiesen vom Arbeitsbereich Pädagogische Psychologie am Institut für Erziehungswissenschaft (Prof. Dr. Nikol Rummel) und Steffen Becker vom Horst-Görtz-Institut für IT-Sicherheit (Prof. Dr. Christof Paar) eine Tandempromotion ab.

Chips sind oft winzig klein – trotzdem versteckt sich darauf eine vielschichtige Landschaft von elektronischen Bauteilen und Leiterbahnen.

mussten sie Teile einer Netzliste analysieren. Dabei wurden Logfiles aufgezeichnet, aus denen wir nachher ableiten konnten, wie sie vorgegangen sind.

Becker: Wir haben den Kurs mittlerweile sechsmal durchgeführt, einmal auch in den USA. Hilfreich ist es für uns, dass wir Kontakt zu Expertinnen und Experten von Sicherheitsbehörden oder aus der Industrie haben. Sie geben uns Feedback, ob wir in unserem Kurs von den richtigen Angreifermodellen ausgehen und die richtigen Probleme analysieren lassen. Bislang scheint das der Fall zu sein.

Gibt es schon Ergebnisse aus dem Kurs?

Wiesen: Wir haben zum einen gesehen, dass die Studierenden nach dem Kurs ähnlich schnell wie Experten beim Analysieren der Netzlisten waren. Bei den verwendeten Strategien gab es Überlappungen, aber trotzdem macht jeder es auch irgendwie auf seine Weise.

Wir haben auch den IQ der Teilnehmenden erhoben und ihre Arbeitsgedächtniskapazität getestet. Dabei kam heraus: Personen mit einem besseren Arbeitsgedächtnis waren auch besser beim Verstehen der Netzlisten. Man könnte also versuchen, Schutzmaßnahmen so zu konzipieren, dass das Arbeitsgedächtnis beim Hardware Reverse Engineering überlastet wird.

Mittlerweile haben Sie sich noch etwas Neues einfallen lassen, um Ihre Stichprobe zu vergrößern.

Wiesen: Ja, wir haben ein Online-Spiel entwickelt, das Einzelprozesse des Reverse Engineerings abbildet. Jeder und jede soll es ohne Vorwissen spielen können. Auf diese Weise hoffen wir, an mehr Daten zu kommen. Erste Pilotversuche sind erfolgreich gelaufen.

Becker: Mit dem Spiel wollen wir herausfinden, was Reverse Engineering schwierig macht. Daraus können wir ableiten, wie Hardware-Bausteine aussehen müssen, damit die Schaltungen weniger leicht zu verstehen sind. Diese neuen Ideen können wir dann in echte Netzlisten, aber auch wieder als Aufgaben in das Spiel einbauen und schauen, ob es schwieriger geworden ist, sie zu lösen.

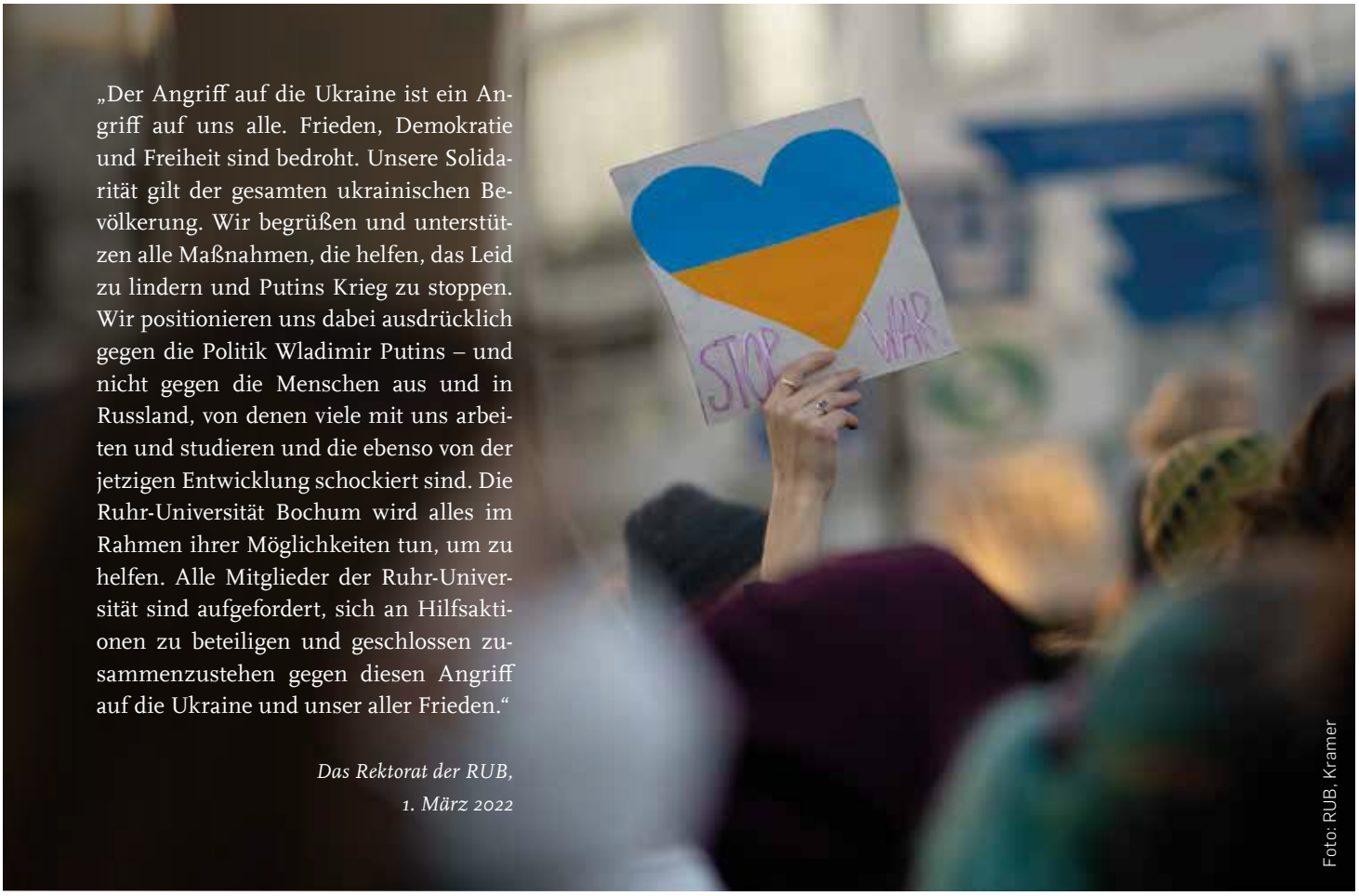
Sie müssen sehr kreativ sein, um an Ihre Daten zu kommen. Hatten Sie mal Bedenken, dass die methodischen Probleme Ihrer Arbeit im Weg stehen könnten?

Wiesen: Es war und ist ein sehr interessantes Projekt, das Spaß macht. Aber weil es so neu ist, hatten wir Probleme, dazu zu publizieren. Wir mussten uns erst durchkämpfen. Letztendlich haben wir aber eine gute Publikation hinbekommen und ein weiterer Artikel ist gerade im Begutachtungsverfahren.

Becker: Ein Problem ist auch, dass viel von dieser Forschung im Kontext der nationalen Sicherheit stattfindet. Expertinnen und Experten werden direkt beim Militär oder Geheimdienst angestellt, um sich mit dem Reverse Engineering zu beschäftigen – dann kommt von den Ergebnissen nichts mehr an die Öffentlichkeit. Trotzdem sehen wir, dass sich aus unserer Forschung mittlerweile etwas entwickelt hat. Der Betreuungsaufwand für unsere Studien ist zwar sehr hoch, aber es lohnt sich auf jeden Fall.

Text: jwe, Fotos: rs

REDAKTIONSSCHLUSS



„Der Angriff auf die Ukraine ist ein Angriff auf uns alle. Frieden, Demokratie und Freiheit sind bedroht. Unsere Solidarität gilt der gesamten ukrainischen Bevölkerung. Wir begrüßen und unterstützen alle Maßnahmen, die helfen, das Leid zu lindern und Putins Krieg zu stoppen. Wir positionieren uns dabei ausdrücklich gegen die Politik Wladimir Putins – und nicht gegen die Menschen aus und in Russland, von denen viele mit uns arbeiten und studieren und die ebenso von der jetzigen Entwicklung schockiert sind. Die Ruhr-Universität Bochum wird alles im Rahmen ihrer Möglichkeiten tun, um zu helfen. Alle Mitglieder der Ruhr-Universität sind aufgefordert, sich an Hilfsaktionen zu beteiligen und geschlossen zusammenzustehen gegen diesen Angriff auf die Ukraine und unser aller Frieden."

Das Rektorat der RUB,
1. März 2022

Foto: RUB, Kramer

IMPRESSUM

HERAUSGEBER: Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation der Ruhr-Universität Bochum (Hubert Hundt, v.i.S.d.P.)

WISSENSCHAFTLICHER BEIRAT: Prof. Dr. Thomas Bauer (Fakultät für Wirtschaftswissenschaft), Prof. Dr. Gabriele Bellenberg (Philosophie und Erziehungswissenschaften), Prof. Dr. Astrid Deuber-Mankowsky (Philologie), Prof. Dr. Constantin Goschler (Geschichtswissenschaften), Prof. Dr. Markus Kaltenborn (Jura), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Dorothea Kolossa (Elektrotechnik/Informationstechnik), Prof. Dr. Günther Meschke (Prorektor für Forschung und Transfer), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Sabine Seehagen (Psychologie), Prof. Dr. Roland Span (Maschinenbau), Prof. Dr. Martin Tegenthoff (Medizin), Prof. Dr. Martin Werding (Sozialwissenschaft), Prof. Dr. Marc Wichern (Bau- und Umweltingenieurwissenschaft), Prof. Dr. Peter Wick (Evangelische Theologie)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, Fax: 0234/32-14136, rubin@rub.de, news.rub.de/rubin

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Lisa Bischoff (lb)

FOTOGRAFIE: Damian Gorczany (dg), Schiefersburger Weg 105, 50739 Köln, Tel.: 0176/29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de

COVER: Damian Gorczany

BILDNACHWEISE INHALTSVERZEICHNIS: Teaserfotos für die Seiten 18, 36 und 62: rs; Teaserfoto für die Seiten 40 und 50: dg

GRAFIK, ILLUSTRATION, LAYOUT UND SATZ: Agentur der RUB, www.rub.de/agentur

DRUCK: LD Medienhaus GmbH & Co. KG, Feldbachacker 16, 44149 Dortmund, Tel.: 0231/90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

ANZEIGEN: Dr. Julia Weiler, Dezernat Hochschulkommunikation, Redaktion Rubin, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, rubin@rub.de

AUFLAGE: 3.500

BEZUG: Rubin erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter news.rub.de/rubin/abo. Das Abonnement kann per E-Mail an rubin@rub.de gekündigt werden.

ISSN: 0942-6639