

RUBIN

WISSENSCHAFTSMAGAZIN

Schwerpunkt

GRENZEN DER WISSENSCHAFT

MEDIZIN: SCHNITTSTELLE MENSCH/MASCHINE

ASTRONOMIE: AN DER GRENZE DES MESSBAREN

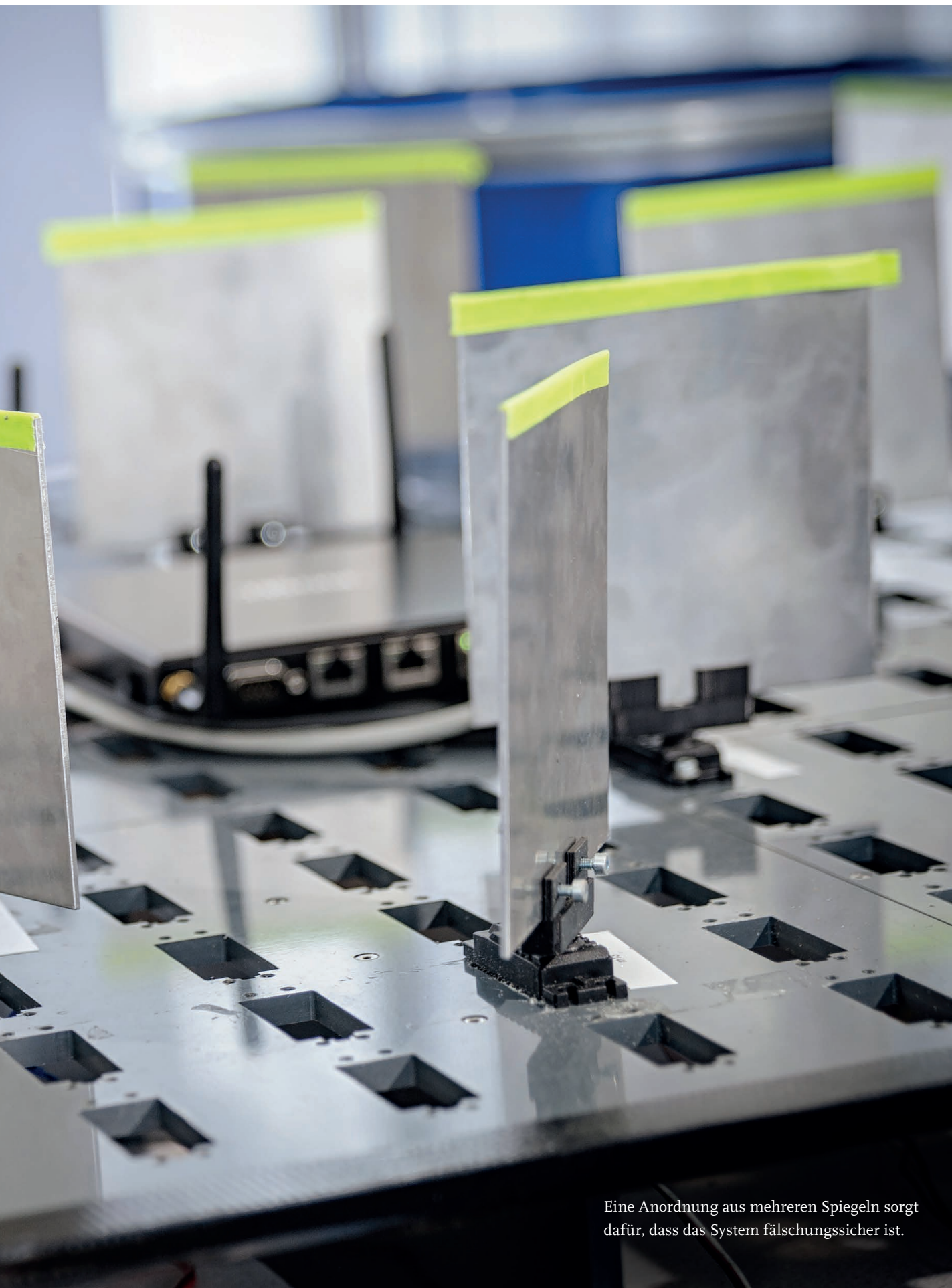
THEOLOGIE: GLAUBE ODER WISSENSCHAFT

IT-Sicherheit

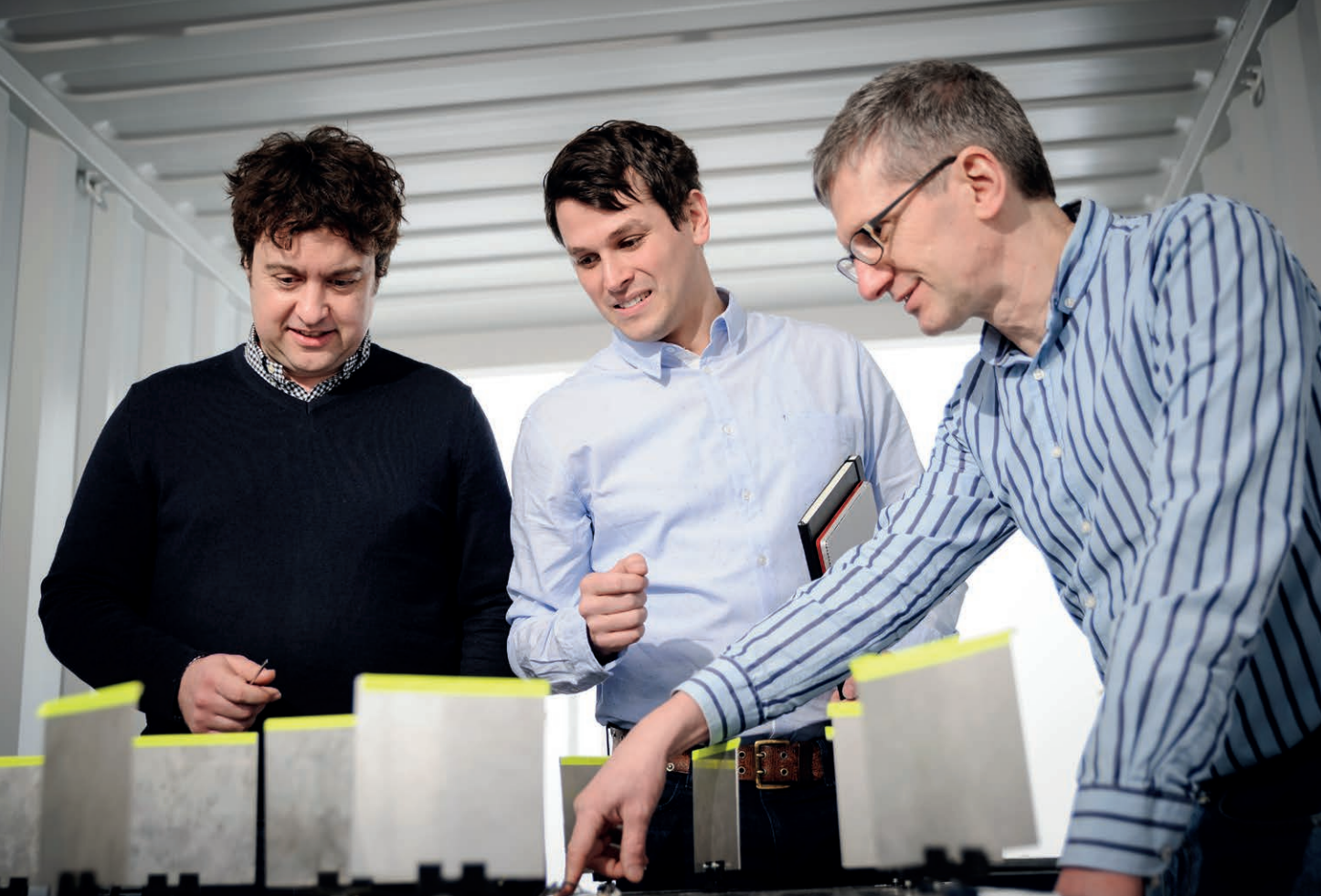
ATOMSPRENGKÖPFE ZÄHLEN, OHNE HINZUSCHAUEN

*Diese Technik könnte eines Tages helfen zu überprüfen,
ob Staaten sich an Abrüstungsverträge halten.*





Eine Anordnung aus mehreren Spiegeln sorgt dafür, dass das System fälschungssicher ist.



Das Bochumer Projektteam: Ulrich Rührmair, Christian Zenger und Christof Paar (von links)

Auch wenn der Kalte Krieg lang vorbei ist, gibt es Schätzungen zufolge heute immer noch 14.550 Atomsprenköpfe auf der Welt. Das ist zwar deutlich weniger als auf dem Gipfel der atomaren Aufrüstung, als fast fünfmal so viele Nuklearwaffen existierten, aber dafür sind moderne Systeme bis zu 1.000-fach zerstörerischer als die Bombe von Hiroshima.

Experten unterscheiden zwischen einsatzbereiten Waffen, die auf Interkontinentalraketen oder Bombern montiert sind und schnell abgefeuert werden können, und solchen, die in Silos oder Containern lagern. Die Zahl von Letzteren zu kontrollieren, ist eine Herausforderung. Hierbei könnte künftig eine Technik helfen, die Forscher vom Horst-Görtz-Institut für IT-Sicherheit (HGI) in Bochum entwickeln.

Nach Schätzungen der Federation of American Scientists besaßen die USA und Russland im Jahr 2017 jeweils rund 1.700 einsatzbereite Nuklearwaffen mit hoher Reichweite, wobei genaue Informationen aufgrund der strengen Geheimhaltung nicht verfügbar sind. Bei der Anzahl der Waffen ist das Gleichgewicht zwischen den zwei Supermächten entscheidend. Um dieses zu wahren und sich auf Abrüstungsverträge einigen zu können, ist es wichtig, dass beide Seiten wissen, ob sich die jeweils andere an Abmachungen hält. „Bei der Kontrolle von Atomwaffen gibt es viele technische Probleme, die man als Laie zunächst nicht ahnt“, erzählen die Bochumer Forscher. Denn etwas zu kontrollieren, das streng geheim ist, ist nicht trivial. Auf der einen Seite sollen Nuklearwaffen inspiziert werden, weil die Gegenseite zum Beispiel wissen möchte, ob ein Staat nicht heimlich Spreng-

köpfe aus dem Lager in Einsatzbereitschaft versetzt. Auf der anderen Seite soll so wenig Information wie möglich über die Atombomben bekannt werden. Für die Kontrolle muss also im Grunde etwas gezählt werden, das niemand sehen soll.

Hier setzt ein Projekt an, das ursprünglich zwischen HGI-Forscher Dr. Dr. Ulrich Rührmair und der Princeton University entstanden ist und an dem in der Zwischenzeit auch Dr. Christian Zenger und Prof. Dr. Christof Paar vom HGI sowie die Harvard University eng beteiligt sind. Das internationale Team hat eine Technik entwickelt, die lagernde Atomwaffen überwachen kann, ohne geheime Informationen über diese Waffen preiszugeben und ohne Vertrauen in die Hardware vor Ort haben zu müssen. „Dabei dürfen wir nur die Oberfläche der Transportcontainer der Waffen betrachten, also kein Röntgenbild oder die radioaktive Signatur der Bombe aufzeichnen, weil das etwas über die Zusammensetzung und die Konstruktion verraten würde“, erklärt Christian Zenger. „Es ist auch zwecklos, Kameras im Silo aufzuhängen, da deren Hardware kompromittiert und somit die Bilder einfach manipuliert werden könnten.“ Trotzdem soll feststellbar sein, ob sich in dem Lager etwas ändert, zum Beispiel heimlich ein Nuklearsprengkopf entfernt wird.

Die Idee der Forscher basiert zum einen auf den sogenannten Virtual Proofs of Reality, einem Konzept, das Rührmair mit Kollegen 2015 vorschlug. Zum anderen sind sogenannte Physical-Layer-Security-Ansätze entscheidend, mit denen sich Christian Zenger bereits seit 2012 intensiv beschäftigt. Was es mit den Virtual Proofs of Reality auf sich hat, erklärt Ulrich Rührmair: „Wir haben uns Gedanken gemacht, wie



In einem Container an der RUB testen die Forscher die Sicherheit der Technik mit Atomwaffenattrappen.

man eine physikalische Aussage zwischen zwei Parteien an unterschiedlichen Orten über einen digitalen Kommunikationskanal beweisen kann.“ Zum Beispiel, wie eine Person in Berlin einer Person in Bochum beweisen kann, dass die Temperatur in der Hauptstadt gerade 21 Grad Celsius beträgt. Das Konzept funktioniert aber auch für wesentlich komplexere physikalische Aussagen als die aktuelle Temperatur, etwa

wenn es darum geht, wo welche Gegenstände sich in einem Raum befinden. Beispielsweise Atomwaffen in einem Lager. Um Veränderungen in einem solchen Lagerraum feststellen zu können, nutzen die Forscher elektromagnetische Wellen im Radiobereich. Diese werden über eine Antenne ausgestrahlt und breiten sich in dem Raum aus. Dabei werden sie von Wänden und Gegenständen reflektiert. Eine Antenne ►

Anzeige

Das tut nix mehr. Dank Leuten wie Ihnen.

Wir suchen IT-Sicherheitsexperten. Für unsere spannenden Kunden – darunter Unternehmen, Behörden und internationale Organisationen – definieren wir seit 20 Jahren den Standard im kryptografischen Bereich. Unsere IT-Sicherheitslösungen sind führend – und genau solche Leute suchen wir. Ob Junior oder Senior: Was zählt, ist Ihre Begeisterung. Und Ihre Eigenschaft, erst dann zufrieden zu sein, wenn es wirklich perfekt ist.

Wir freuen uns auf Ihre Bewerbung.

www.secunet.com/karriere



secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

fängt die zurückkommenden Wellen wieder auf. So erstellen die IT-Experten eine Art Radiowellenkarte des Raums. Jede Veränderung – etwa wenn ein Sprengkopf aus dem Lager entfernt würde – würde das Reflexionsmuster ändern und könnte so detektiert werden.

In der praktischen Anwendung könnte das wie folgt laufen: Staat A möchte wissen, ob die Nuklearwaffen von Staat B wie vereinbart gelagert und nicht einsatzbereit sind. Die beiden Staaten müssten sich darauf einigen, das Überwachungssystem in den Lagerräumen zu installieren. Staat A könnte dann über das Internet die aktuelle Radiowellenkarte des Lager-raums von Staat B anfordern.

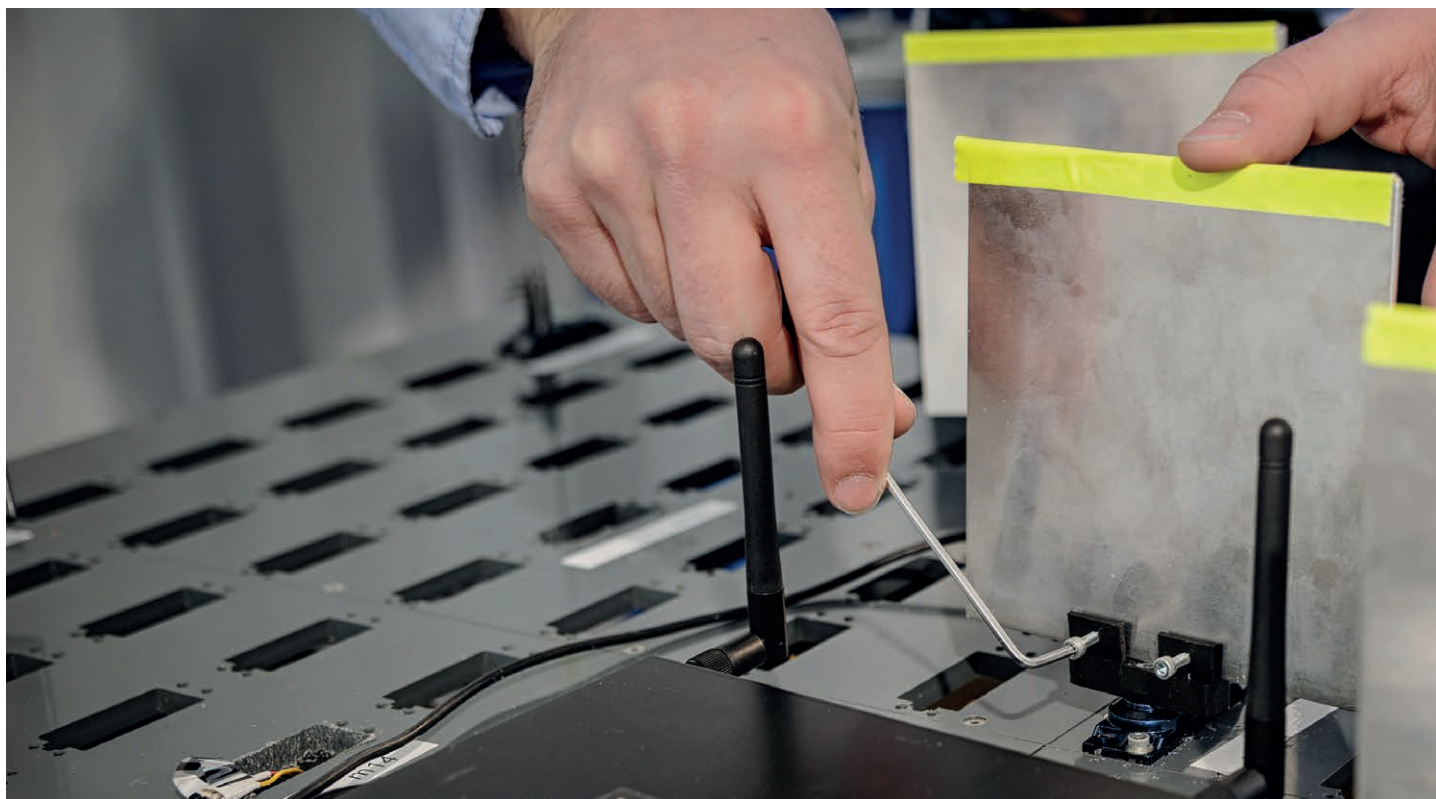
Fälschungen vorbeugen

Allerdings braucht das System noch eine weitere Komponente, um fälschungssicher zu sein. „Wir müssen verhindern, dass Staat B eine Radiowellenkarte von einem voll bestückten Atomwaffenlager erstellt, speichert und dann immer wieder an Staat A schickt, obwohl längst Waffen aus dem Lager entfernt wurden“, erklärt Ulrich Rührmair. Dafür haben die Forscher eine sogenannte Challenge in das System eingebaut. Zusätzlich zu den Sendern und Empfängern für die Radiowellen werden in dem zu kontrollierenden Raum 20 drehbare Spiegel installiert, die sich ferngesteuert ausrichten lassen. Die Spiegel reflektieren die Radiowellen und ändern so das Reflexionsmuster des Raums, wobei jede Spiegelstellung ein individuelles Muster erzeugt. Vor jeder Abfrage der Radiowellenkarte würde Staat A die Spiegel in eine bestimmte Anordnung drehen. Als Antwort müsste Staat B die Radiowellenkarte des Raums mit exakt dieser Spiegelanordnung schicken. Um an das korrekte Reflexionsmuster heranzukommen, muss Staat B den Raum mit der aktuellen Spiegelstellung ver-

messen – eventuell gespeicherte Radiowellenkarten von früher wären nicht mehr gültig. Damit Staat A die Antwort auf Richtigkeit prüfen kann, müsste er bei Inbetriebnahme der Technik die Reflexionsmuster des Raums für eine bestimmte Anzahl verschiedener Spiegelstellungen gemessen und gespeichert haben. Aus diesem Pool von Spiegelstellungen könnte Staat A dann bei jeder neuen Abfrage eine Anordnung auswählen. Schickt Staat B das richtige Reflexionsmuster als Antwort, weiß Staat A, dass der Raum neu vermessen wurde und ob er unverändert geblieben ist.

Mit 20 Spiegeln können die Forscher zurzeit 2^{100} verschiedene Reflexionsräume erzeugen; es gibt mit diesem Setting also Milliarden Trilliarden verschiedene Kombinationen von Spiegelstellungen. Eine Herausforderung dabei ist, dass der überwachte Staat nicht im Lauf der Zeit lernen darf, die nächste Spiegelstellung vorherzusagen. „Es könnte ja sein, dass er nach einer Milliarde verschiedener Spiegelstellungen, die er als Challenge bekommen hat, einen Algorithmus findet, mit der er die nächste Spiegelstellung vorhersagen kann“, so Christof Paar. Dann könnte er die erforderliche Radiowellenkarte eventuell selbst erzeugen, ohne den Raum neu vermessen zu haben – und sich in der Zwischenzeit unbemerkt an dem Atomwaffenlager zu schaffen machen. Um das zu verhindern, nutzen die Bochumer IT-Experten ein nicht vorhersagbares kryptografisches Protokoll, um die Spiegel einzustellen. „Wichtig ist unter anderem, dass der Zusammenhang zwischen der Challenge und der Antwort darauf nicht durch ein lineares Gleichungssystem eindeutig beschrieben werden kann“, sagt Christian Zenger, „weil die mathematisch relativ leicht zu durchschauen sind.“ Gleiches gilt für die Physik, also für die Spiegelmaterialien, deren Reflexionseigenschaften nicht linear sein sollten.

Mit dem Verfahren lässt sich prinzipiell jeder beliebige Raum überwachen, zum Beispiel auch ein Tresor oder Geldautomat.



Auf dem Campus der Ruhr-Universität Bochum haben die Wissenschaftler mittlerweile einen Container mit Sprengkopfatrappen und Spiegeln aufgebaut und testen dort die Sicherheit des Physical-Layer-Security-Protokolls im Realbetrieb. Sie untersuchen auch, wie sich die Reflexionsmuster verhalten, wenn sie Veränderungen im Raum vornehmen, zum Beispiel die Attrappen verschieben oder entfernen. Außerdem passen sie ihre Algorithmen an die Raumgröße an.

Tests in der Butterbrotdose

Die ersten Tests führte das RUB-Team in einem sehr kleinen System durch: in einer Butterbrotdose. Damit zeigten sie die Präzision ihrer Messtechnik: Wenn sie einen Gegenstand in der Dose um 0,4 Mikrometer bewegten, konnte das System das immer noch feststellen. So genau muss das Verfahren im Einsatz vielleicht gar nicht sein. „Denn“, so Paar, „in dem Kontext darf es natürlich keinen falschen Alarm geben.“ Daher muss das System möglichst robust sein. Gewisse Messungenauigkeiten müssen die Forscher einkalkulieren, da zum Beispiel die Spiegelstellung nicht beliebig genau kontrolliert werden kann. An all diesen Detailfragen feilt das Team der Ruhr-Universität derzeit.

Mit dem Verfahren, das eines Tages zur Kontrolle der atomaren Abrüstung beitragen könnte, lässt sich prinzipiell jeder beliebige Raum überwachen, zum Beispiel ein Tresor oder Geldautomat. Das 2015 aus dem HGI hervorgegangene Startup Physec macht die Technik auch für andere Anwendungen nutzbar und ist eng in das Projekt mit der Princeton und Harvard University involviert.

Text: jwe, Fotos: rs



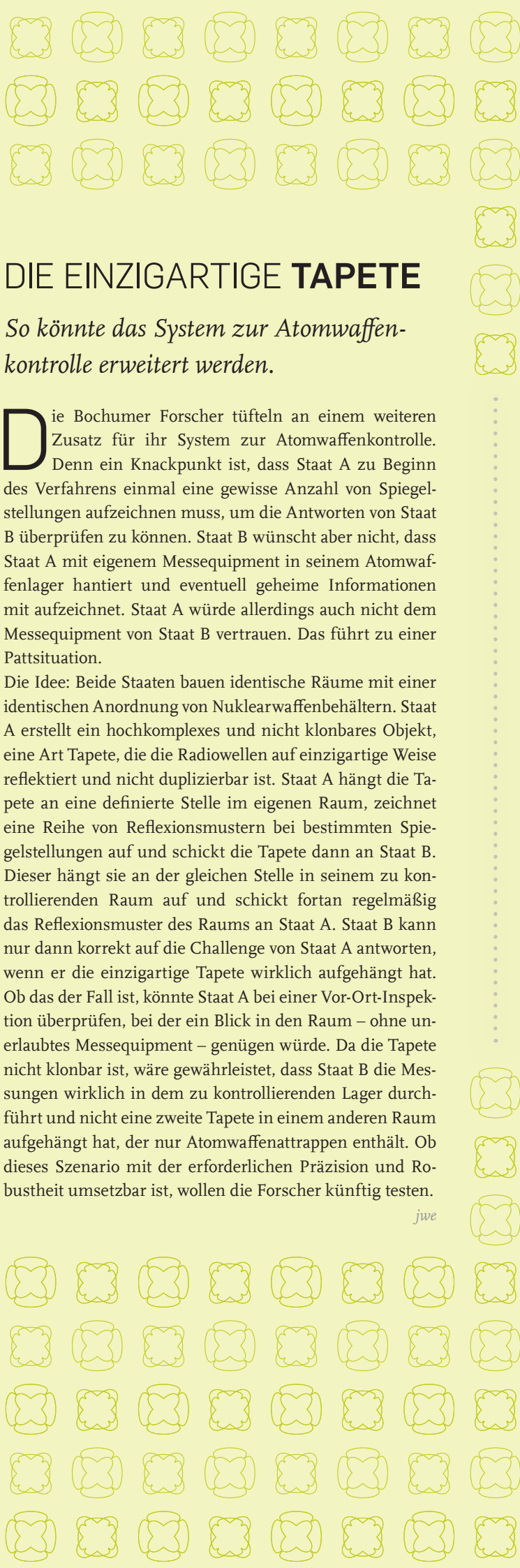
DIE EINZIGARTIGE TAPETE

So könnte das System zur Atomwaffenkontrolle erweitert werden.

Die Bochumer Forscher tüfteln an einem weiteren Zusatz für ihr System zur Atomwaffenkontrolle. Denn ein Knackpunkt ist, dass Staat A zu Beginn des Verfahrens einmal eine gewisse Anzahl von Spiegelstellungen aufzeichnen muss, um die Antworten von Staat B überprüfen zu können. Staat B wünscht aber nicht, dass Staat A mit eigenem Messequipment in seinem Atomwaffenlager hantiert und eventuell geheime Informationen mit aufzeichnet. Staat A würde allerdings auch nicht dem Messequipment von Staat B vertrauen. Das führt zu einer Pattsituation.

Die Idee: Beide Staaten bauen identische Räume mit einer identischen Anordnung von Nuklearwaffenbehältern. Staat A erstellt ein hochkomplexes und nicht klonbares Objekt, eine Art Tapete, die die Radiowellen auf einzigartige Weise reflektiert und nicht duplizierbar ist. Staat A hängt die Tapete an eine definierte Stelle im eigenen Raum, zeichnet eine Reihe von Reflexionsmustern bei bestimmten Spiegelstellungen auf und schickt die Tapete dann an Staat B. Dieser hängt sie an der gleichen Stelle in seinem zu kontrollierenden Raum auf und schickt fortan regelmäßig das Reflexionsmuster des Raums an Staat A. Staat B kann nur dann korrekt auf die Challenge von Staat A antworten, wenn er die einzigartige Tapete wirklich aufgehängt hat. Ob das der Fall ist, könnte Staat A bei einer Vor-Ort-Inspektion überprüfen, bei der ein Blick in den Raum – ohne unerlaubtes Messequipment – genügen würde. Da die Tapete nicht klonbar ist, wäre gewährleistet, dass Staat B die Messungen wirklich in dem zu kontrollierenden Lager durchführt und nicht eine zweite Tapete in einem anderen Raum aufgehängt hat, der nur Atomwaffenattrappen enthält. Ob dieses Szenario mit der erforderlichen Präzision und Robustheit umsetzbar ist, wollen die Forscher künftig testen.

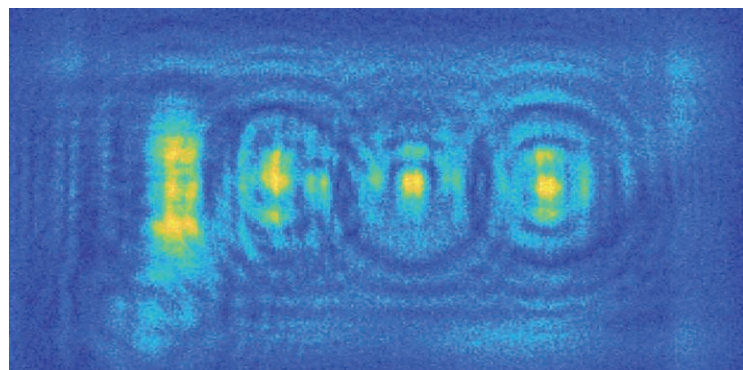
jwe



REDAKTIONSSCHLUSS

Mit Radartechnik kann man durch Wände schauen und Unsichtbares sichtbar machen. Zeichnet man ein Radarbild auf, ist es allerdings, als würde man mit einer Kamera fotografieren, der die Linse zum Fokussieren fehlt. Die Fokussierung erfolgt nachträglich im Computer. Dafür braucht es spezielle Algorithmen, so wie Dr. Jan Barowski sie während seiner Doktorarbeit am Lehrstuhl für Hochfrequenzsysteme entwickelt hat. Das obere Motiv zeigt das mit Barowskis Algorithmen korrigierte Radarbild einer Platine mit dem Schriftzug „RUB“. Die Originalplatine ist ganz unten zu sehen. Das mittlere Bild zeigt die unkorrigierte Rohversion des Radarbildes. Im fokussierten Bild kann man in Hellblau sogar die Leiterbahnen sehen, die auf der Rückseite der Platine vom Koaxialstecker (fünf gelbe Punkte) zu den Buchstaben verlaufen. (Aufnahmen: Jan Barowski)

➔ news.rub.de/radar-bildgebung



IMPRESSUM

HERAUSGEBER: Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum

WISSENSCHAFTLICHER BEIRAT: Prof. Dr. Gabriele Bellenberg (Philosophie und Erziehungswissenschaften), Prof. Dr. Astrid Deuber-Mankowsky (Philologie), Prof. Dr. Reinhold Gleis (Philologie), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Michael Hübner (Elektrotechnik/Informationstechnik), Prof. Dr. Denise Manahan-Vaughan (Medizin), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Andreas Ostendorf (Prorektor für Forschung, Transfer und wissenschaftlichen Nachwuchs), Prof. Dr. Michael Roos (Wirtschaftswissenschaft), Prof. Dr. Martin Tegenthoff (Medizin), Prof. Dr. Michael Wala (Geschichtswissenschaft)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Abteilung Wissenschaftskommunikation, 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)

FOTOGRAFIE: Damian Gorczany (dg), Hofsteder Str. 66, 44809 Bochum, Tel.: 0176/29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpfe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de

COVER: Agentur der RUB

BILDNACHWEISE INHALTSVERZEICHNIS: Teaserfotos für die Seiten 12, 24, 58: Roberto Schirdewahn; Teaserfoto für Seite 18: Fotolia, Olicki; Teaserfoto für Seite 28: Damian Gorczany; Teaserbild für Seite 34: ESO/IDA/Danish 1.5 m/R. Gendler and J.-E. Ovaldsen; Teaserfoto für Seite 54: Tim Kramer

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

DRUCK: VMK Druckerei GmbH, Faberstraße 17, 67590 Monsheim, Tel.: 06243/909-110, www.vmk-druckerei.de

AUFLAGE: 4.500

ANZEIGENVERWALTUNG UND -HERSTELLUNG: VMK GmbH & Co. KG, Faberstraße 17, 67590 Monsheim, Tel.: 06243/909-0, www.vmk-verlag.de

BEZUG: RUBIN erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter rubin.rub.de/abonnement.

ISSN: 0942-6639

Nachdruck bei Quellenangabe und Zusenden von Belegexemplaren