# WISSEN

EINE MINUTE PHYSIK

## Hebelgesetz

Finanzexperten reden in diesen Tagen viel über das Hebelgesetz. Was bedeut es in der Physik?

NORBERT LOSSAU

Gebt mir einen festen Punkt im All, und ich werde die Welt aus den Angeln heben.“ Es war ein Grieche, der vor mehr als 2200 Jahren diesen markigen Satz aussprach – Archimedes. Er spielte damit auf das bereits in der Antike bekannte Hebelgesetz an. Wer am längeren Hebel sitzt, kann bekanntlich mit geringem Aufwand viel erreichen. Kein Wunder also, dass uns das Hebelprinzip überall begegnet – vom Klavier bis zum Nussknacker.

Ob sich mithilfe des Hebelgesetzes auch die Euro-Krise bewältigen lässt, erscheint aus physikalischer Sicht eher fraglich. Denn die allgemeine Formulierung dieses Gesetzes besagt, dass die Summe aller an einem in Ruhe befindlichen Körper null ist. Doch von Ruhe, geschweige denn einem festen Punkt, kann ja auf den Finanzmärkten derzeit keine Rede sein.

In der Technik werden Hebel als mechanische Kraftwandler genutzt. Dabei gibt es immer einen Dreh- und Angelpunkt, der bei einer Wippe auf dem Spielplatz augenfällig ist. Übergewichtige Kinder können sich näher an den Drehpunkt setzen und dadurch mit leichteren Kameraden ins Gleichgewicht kommen. Je länger Hebelarme werden, umso brachialer sind mögliche Anwendungen. Ein Beispiel ist die Brechstange. Mit ihr lässt sich eine Tür aus den Angeln heben, da der Lasthebel unter der Tür im Vergleich zum Krafthebel sehr kurz ist. Für Hebelnutzer gilt in der Praxis generell die Formel „Kraft mal Kraftarm gleich Last mal Lastarm“.

Rechnen Sie doch mal aus, um welchen Faktor Sie ihre Kraft beim Knacken einer Walnuss verstärken. Ein Nussknacker ist anders aufgebaut als eine Wippe. Einen Drehpunkt gibt es auch hier, doch wo lassen sich an den daran befindlichen Armen die Längen von Kraft- zu Lastarm erkennen? Ein Nussknacker ist ein „einseitiger Doppelhebel“, bei dem der Kraftarm vom Drehpunkt bis zum Ende der Arme gebildet wird. Der Lastarm ergibt sich aus dem Abstand des Gelenks zur Nuss. Mit einem Lineal können Sie beide Strecken ausmessen. Teilen Sie die Länge des Kraft- durch jene des Lastarms und Sie erhalten den Faktor, um den der Nussknacker die Kraft Ihrer Hand verstärkt.

Auch Schubkarren sind einseitige Doppelhebel. Drehpunkt ist hier die Achse des Rades. Der Abstand des Transportgutes von dieser Achse ist deutlich kleiner als zu den Handgriffen. Selbst schwere Lasten lassen sich daher leicht anheben und dank des Rades auch problemlos bewegen.

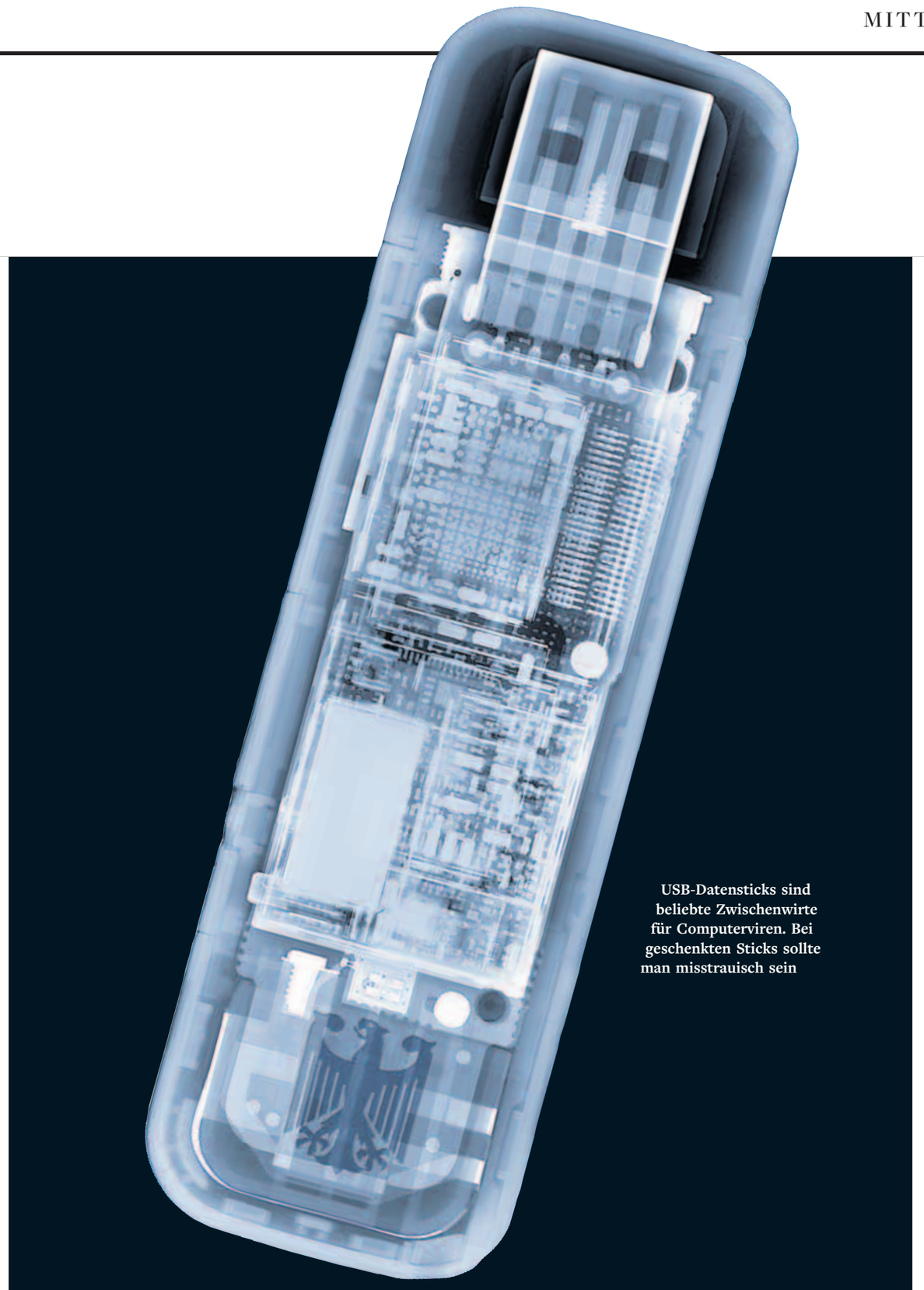
Es gibt auch Anwendungen des Hebelgesetzes, bei denen es darauf ankommt, dass beide Hebel exakt gleich lang sind. Ein wichtiger Fall ist die Waage der Justitia. Diese Frauengestalt der römischen Mythologie ist bis heute ein Symbol für Gerechtigkeit. Nicht auszudenken, wenn Justitia wegen unterschiedlich langer Hebel mit zweierlei Maß messen würde.

## KOMPAKT

RAUMFAHRT

### Rosat stürzte über dem Golf von Bengalen ab

Der deutsche Forschungssatellit Rosat ist über Asien auf die Erde gestürzt – mögliche Trümmerteile fielen sehr wahrscheinlich ins Meer. Nach Auswertung von Daten aus den USA trat Rosat am Sonntagmorgen um 3.50 Uhr MESZ über dem Golf von Bengalen in die Atmosphäre ein. Ob Trümmerteile die Erdoberfläche erreichten, sei nicht bekannt. In diesem Fall dürften sie ins Wasser gestürzt sein. Der DLR-Vorstandsvorsitzender Johann-Dietrich Wörner erklärte, nun habe „eine der erfolgreichsten wissenschaftlichen Raumfahrtmissionen Deutschlands ihren Abschluss“ gefunden. Rosat registrierte bei seinem knapp neunjährigen Einsatz im All rund 80 000 kosmische Röntgenquellen.



USB-Datensticks sind beliebte Zwischenwirte für Computerviren. Bei geschenkten Sticks sollte man misstrauisch sein

# Der Bundestrojaner stieg am Airport zu

Gute Spionagesoftware bleibt meist unentdeckt, sagt Dunn Cavelty, Schweizer Expertin für Cybersicherheit

GETTY IMAGES / MONTAGE: DIE WELT; DUNN CAVELTY

Die Schweizerin Myriam Dunn Cavelty ist Expertin für Cybersicherheit. Sie leitet das Forschungsteam „Neue Risiken“ am Center for Security Studies der ETH Zürich und ist Fellow der Stiftung neue Verantwortung in Berlin. Über Computerviren, den deutschen Staatstrojaner und die neuen Risiken in einer global vernetzten Welt sprach mit ihr Norbert Lossau.

**DIE WELT: Spätestens der Bundestrojaner hat viele für das Thema Internetviren sensibilisiert. Wozu werden Trojaner und andere Computerviren sonst noch eingesetzt?**

**MYRIAM DUNN CAVELTY:** Als Schadprogramme oder Malware bezeichnete Programme sind sehr divers und bezeichnen alles, was unerwünschte oder sogar schädliche Funktionen auf einem Computer ausführt. Das kann das Manipulieren oder Löschen von Daten sein, das nicht autorisierte Sammeln von Daten oder die Verwendung des infizierten Computers für kriminelle Zwecke, ohne dass der Benutzer davon weiß.

**Wie groß ist der Schaden, der durch Malware entsteht?**

Hersteller von Antivirensoftware und andere private wie öffentliche Stellen veröffentlichen regelmäßig Berichte über Art und Verbreitung von Viren sowie über das Ausmaß von Schäden. Diese Angaben sind jedoch mit großer Vorsicht zu genießen, denn es gibt keine repräsentativen Statistiken. Was wir sehen, ist wohl nur die Spitze des Eisbergs. Denn wirklich gut gemachte Software kann ganz oder zumindest sehr lange unentdeckt bleiben. Das gilt insbesondere für Spionagesoftware, die sich normalerweise ganz unauffällig verhält. Und was nicht entdeckt wird, taucht in keiner Statistik auf. Wer, wie, bei wem was im Rechner ausspioniert, ist einfach nicht bekannt. Hinzu kommt, dass es keine Meldepflicht gibt – viele Betroffene in der Wirtschaft schweigen lieber, als Imageschäden in Kauf zu nehmen.

**Kann man den angerichteten Schaden dennoch ungefähr beziffern?**

Das lässt sich schon deshalb nicht leicht beantworten, weil es darauf ankommt, welche Phänomene man betrachtet und wie man den Wert von gestohlenen oder manipulierten Daten einschätzt. Insgesamt – und insbesondere, wenn Computerkriminalität sehr breit verstanden wird – gehen einige Studien von einem jährlichen Schaden allein für die deutsche Wirtschaft in Milliardenhöhe aus. Doch gesicherte Zahlen gibt es nicht.

**Dienen die meisten Viren dem Ausspähen von Unternehmen?**

Nicht unbedingt die meisten, aber es sind diejenigen, die besonders ernst genommen werden müssen. Es geht da um das Stehlen von Wirtschaftsgeheimnissen, etwa Entwicklungsunterlagen. Das kann insbesondere für mittelständische Unternehmen fatale Folgen haben. Darüber hinaus treten Cyber-Kriminelle auch als Erpresser auf. Etwa mit der Drohung, aus Rechnern gestohlene Daten oder entdeckte Sicherheitslücken im Computersystem einer Bank zu veröffentlichen. Da werden durchaus Erpressungsgelder gezahlt, auch wenn darüber naturgemäß wenig gesprochen wird.

**Kommt es zu Anzeigen, und gibt es Fälle, in denen Täter gefasst wurden?**

Ja, Anzeigen gibt es, und immer wieder werden Virenschreiber festgenommen. Das sind meist sehr aufwendige Vorgänge, da sie sich in der Regel im internationalen Raum abspielen. Wenn Behörden zum Beispiel Indizien dafür haben, dass eine Bande in Russland schädliche Software verbreitet, dann muss sie dort mit den lokalen Behörden zusammenarbeiten. Es gibt die „Convention on Cybercrime“ der EU, die diese Zusammenarbeit fördert. Doch Russland und auch China haben sie nicht unterzeichnet.

**Es wird gemunkelt, dass die meisten Cyber-Angriffe aus China kommen?**

Ich würde davon ausgehen, dass die Chinesen dort, wo sie es können, auch Spionage betreiben. Doch sie sind natürlich bei Weitem nicht die Einzigen. Spionage hat es immer schon gegeben und wird es immer geben. Doch im Internetzeitalter ist sie teilweise einfacher geworden. Das hängt auch mit dem fehlenden Bewusstsein für die Problematik zusammen. Viele Unternehmen gehen sehr fahrlässig mit ihren sensiblen Daten um. Dass im Moment China als Hauptbösewicht angesehen wird, hat auch viel mit den Medien zu tun, die recht undifferenziert China an den Pranger stellen.

**Doch es wurde festgestellt, dass diverse Angriffe aus China kamen?**

Das stimmt. Doch was bedeutet es, wenn man sagt, ein Angriff kam aus China? Selbst wenn man eine IP-Adresse in China identifizieren konnte, heißt dies noch lange nicht, dass dort der Ursprung des Angriffs war – oder dass er politisch gesteuert wurde. Es ist durchaus möglich, dass von einem Internetcafé in Berlin eine Attacke über chinesische Rechner auf irgendein Ziel durchgeführt wird – insbesondere deshalb, weil die chinesische Computerinfrastruktur aufgrund weitverbreiteter und schlecht gewarteter Raubkopien der Betriebssoftware zu den unsichersten der Welt gehört. Da lassen sich die Urheber von Viren- und Trojaner-Angriffen meist nicht ausmachen.

**Anders offenbar beim Bundestrojaner. Gute Spionagesoftware, sagten Sie, falle nicht auf. War der Bundestrojaner schlecht gemacht?**

Unter Experten gilt der Bundestrojaner in der Tat als nicht so gut programmiert – er ist auch relativ alt, denn er wurde bereits im November 2008 geliefert.

**Der Bundestrojaner wurde von einer privaten Firma programmiert. Ist das nicht verwunderlich?**

Nein, das ist nicht verwunderlich. Die Spitzenleute in der Informatik gehen nicht in den Staatsdienst, weil dort nicht annähernd die Gehälter der freien Wirtschaft gezahlt werden. Dieses Problem tritt nicht nur bei Spitzenprogrammierern auf, sondern etwa auch bei Experten für Spezialwissen wie etwa Computerforensik, die Spuren in Netzwerken und Computern sichern. Auch diese Leute müssen im Bedarfsfall bisweilen vom Staat angeheuert werden.

**Wenn das Thema so sensibel ist, müsste es für den Staat dann nicht möglich sein, einige Topleute mit einem Topgehalt einzukaufen?**

Im äußersten Notfall wird man sicher auf eine solche Möglichkeit verfallen. Wenn der deutsche Staat etwa auf die Idee kommen sollte, mit Trojanern bei Schweizer Banken nach Steuersündern zu suchen, dann würde es sich für diesen lukrativen Zweck sicher lohnen, ein paar hoch bezahlte Programmierer in den Staatsdienst zu locken. (lacht)

**Dann wäre es eine wirtschaftliche Abwägung, ob letztlich das Programmieren eines Trojaners oder der Ankauf einer CD preiswerter wäre?**

Ganz konkret, ja. Ich würde vermuten, dass der Ankauf der CD schlussendlich vielleicht nicht billiger kommt, aber um einiges erfolgversprechender ist. Doch Spaß beiseite. Ich bin überzeugt, dass derartige Überlegungen zur Wirtschaftlichkeit in den kommenden Jahren an Bedeutung gewinnen werden. Wenn sich der Einsatz von Trojanern lohnt und sie die gewünschten Ergebnisse liefern, dann werden sie auch eingesetzt. Ich kann mir durchaus vorstellen, dass bestimmte Firmen – Ethik hin oder her – Schadsoftware gezielt einsetzen werden, um Konkurrenten zu schädigen. Ein Vorbild ist hier Stuxnet, ein Computerwurm, der in einer Produktionsanlage reale Schäden anrichten konnte.

**Der Bundestrojaner wurde auch in die Schweiz verkauft und dort eingesetzt. In der Schweiz hat das Thema aber viel weniger Aufmerksamkeit erregt als in Deutschland. Warum?**

Die Empfindlichkeiten sind nicht die gleichen. Öffentliche Debatten zum Datenschutz gibt es in der Schweiz nur am Rande. Auch die Vorratsdatenspeicherung ist kein großes Thema, die gibt es in der Schweiz seit 2002. Und was den Einsatz des Trojaners aus Deutschland in der Schweiz betrifft, so war das rechtlich so weit sauber, auch wenn Online-Durchsuchungen in der Schweiz nicht ausdrücklich gesetzlich geregelt sind. Die weitergehende Frage, ob eine Software mehr Fähigkeiten haben darf, als konkret genutzt werden soll, oder ob sie über eine sogenannte Nachladefunktion verfügen darf, mit der nach dem Platzieren der Trojaner beliebig abgeändert werden kann, wird in verschiedenen Kulturkreisen unterschiedlich beantwortet. Das hat letztlich auch damit zu tun, wie sehr man dem eigenen Staat vertraut.

**Wie kommt denn der Bundestrojaner überhaupt in den Computer?**

Die meisten Trojaner werden über E-Mails versandt oder als sogenannte Drive-by-Downloads eingefangen. Im Falle des Bundestrojaners ist mindestens ein Fall bekannt, bei dem der Trojaner am Flughafen München direkt auf dem Laptop eines Verdächtigten installiert wurde. Auch Provider können ihn in den PC des Nutzers implementieren.

**Dann nutzt in so einem Fall die Antivirensoftware auf dem PC nichts?**

Richtig. In der Regel kann der Provider den Trojaner daran vorbeischleusen. Und wenn es sich um einen neuen Virentyp handelt, dann entdeckt die Antivirensoftware den Eindringling ohnehin nicht. Um Firmencomputer zu infizieren, wird übrigens mit Erfolg folgender Trick angewendet: Man platziert auf dem Parkplatz des Unternehmens einen sehr edel und teuer aussehenden USB-Stick, auf dem sich ein Trojaner befindet. Sie können darauf wetten, dass irgendein Angestellter diesen Stick aufhebt und nachschaut, was sich darauf befindet. Und schon ist der Virus im Firmennetzwerk. Hier wird die Psychologie der Menschen gezielt ausgenutzt.

**Dies wäre ja auch eine Methode zur Verbreitung von Bundestrojanern – als Werbegeschenk im Briefkasten.**

Das würde gewiss funktionieren. Grundsätzlich empfehle ich, bei geschenkten USB-Sticks immer skeptisch zu sein. Vorsicht ist auch bei mobilen Kommunikationsgeräten angesagt. Tablets, die sich mit dem Firmennetzwerk synchronisieren, sind ein neues Einfallstor für Viren und Trojaner. Auch die 2-D-Grafik-Codes, die jetzt überall zu sehen sind und die man mit seiner Handykamera einscannen soll, sind potenziell ein sogenannter Angriffsvektor. Da es ständig neue Technologien gibt und die Malware-Programmierer ziemlich kreativ sind, reicht es nicht, nur einmal ein Gefahrenbewusstsein zu schaffen. Man muss ständig dranbleiben und ein Gespür für neue Gefahren entwickeln. Ich gebe zu, dass dies eine Gratwanderung ist – sich der Gefahren immer bewusst zu sein und nicht paranoid zu werden.

**Ein guter Schutz vor Paranoia wäre ja eine Versicherung gegen Viren?**

Solche Versicherungen werden bereits angeboten. Doch nur dort, wo Schäden genau beziffert werden können. Wenn Sie etwa den Diebstahl von Kundendaten bemerken, so sind Telekommunikationsbehörden in der EU gesetzlich verpflichtet, alle Kunden darüber zu informieren. Das kostet Geld. Dafür gibt es eine Versicherung. Doch symbolische Schäden wie den Verlust von Vertrauen in eine Firma kann man eben bislang nicht versichern. Gerade diese Schäden können für ein Unternehmen gravierende, langfristige Folgen haben. Die Versicherungen sind jedoch sehr daran interessiert, diesen Markt zu erschließen.

**Wenn es aber um Angriffe auf sensible Infrastrukturen wie etwa die Stromversorgung geht, können Versicherungen wohl nur marginal helfen?**

Das ist richtig. In einer vernetzten Welt lassen sich Risiken nicht mehr auf null reduzieren. Ganz gleich, wie aufwendig unsere Vorsorgemaßnahmen sind – es bleibt immer ein Restrisiko. Deshalb halte ich es für überaus wichtig, eine gesellschaftliche Debatte darüber zu führen, welche Risiken man bereit ist zu akzeptieren und welche nicht. Wir müssen beispielsweise sehr ernsthaft darüber nachdenken, was passiert, wenn der Strom für mehrere Tage ausfällt. Weiß die Bevölkerung, wie sie sich in einem solchen Fall verhalten soll? Das Schlüsselwort heißt hier Resilienz. Wir brauchen eine neue Kultur der technischen und gesellschaftlichen Widerstandsfähigkeit. Es reicht nicht, sich einfach auf den Staat zu verlassen. Der ist mit der Komplexität der Dinge überfordert. In einer vernetzten Welt können nur komplexe Netzwerke zwischen vielen Institutionen und vielen Menschen Resilienz erzeugen. Das wird ein großes Thema, denn eines ist klar: Die Unsicherheit wird bleiben.

REGIERUNGSBERATERIN

Myriam Dunn Cavelty wurde 1976 in Zürich geboren. Sie ist Dozentin für **Sicherheitspolitik** in Wien und Zürich, Leiterin der Forschungsgruppe Neue Risiken am Center for Security Studies der ETH Zürich und Fellow der Stiftung neue Verantwortung in Berlin, wo sie 2010 das Projektteam **Cybersecurity** geleitet hat. Dunn Cavelty hat Internationale Beziehungen, allgemeine Geschichte und Völkerrecht studiert und absolvierte Forschungsaufenthalte in den USA, Großbritannien und Skandinavien. Sie publiziert in internationalen Fachzeitschriften und ist **Autorin** und Herausgeberin mehrerer Bücher. Sie berät Regierungen, internationale Institutionen und Unternehmen in den Bereichen **Cyberwar** und Cybersecurity.