/// Gefahr im Netz

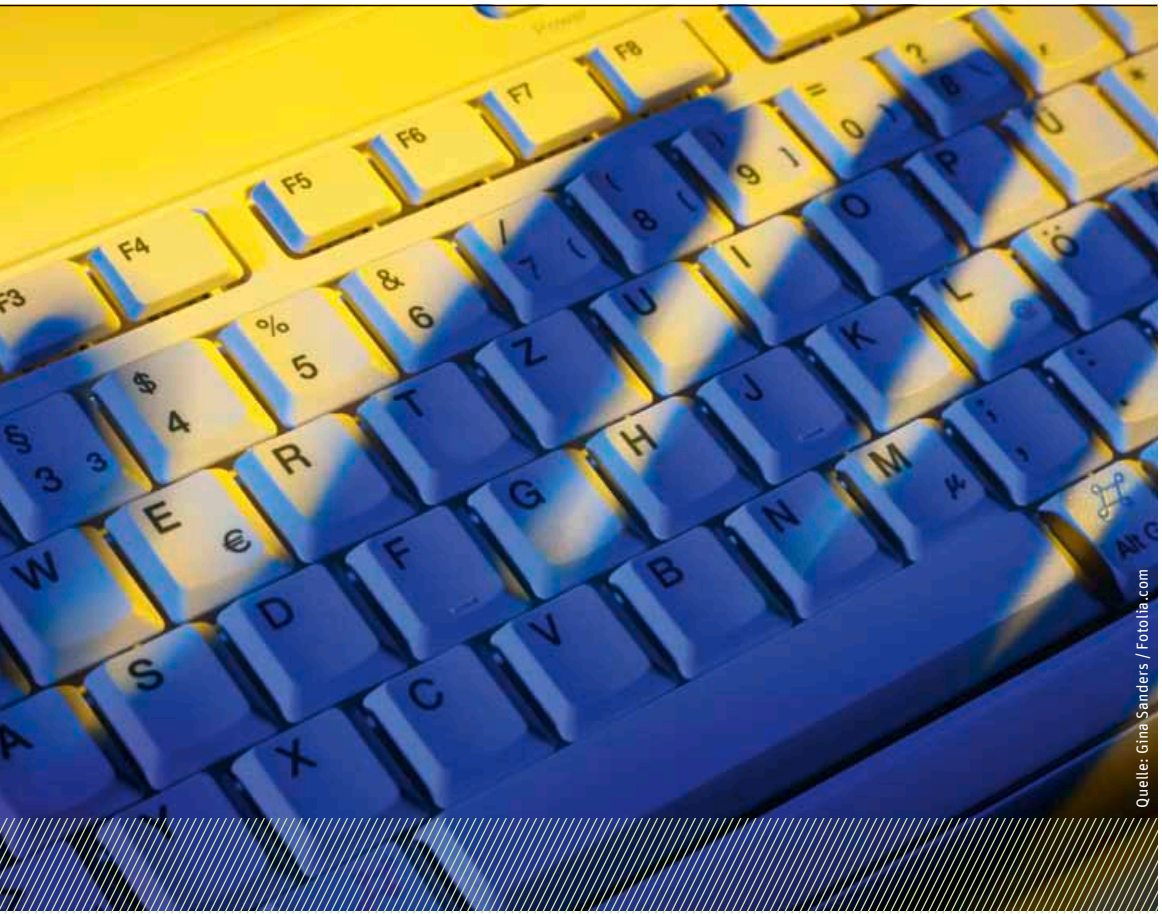
DARKROOM CYBER: WAS DROHT UNS DA?

GABI DREO /// ist Lehrstuhlinhaberin für Kommunikationssysteme und Internet-Dienste sowie Direktorin des Forschungszentrums CODE an der Universität der Bundeswehr München. Hier soll in den nächsten Jahren das größte deutsche Forschungszentrum für Cybersicherheit entstehen, mit dem Schwerpunkt, die „digitale Gesellschaft sicherer" zu machen. Forschungsthemen sind daher neben Cyberdefence auch Smart Data, Mobile Security, eHealth und Schutz kritischer Infrastrukturen.

Politische Studien: Verschiedene Hackerangriffe haben in den vergangenen Monaten gezeigt, wie verwundbar wir sind. So waren nicht nur Banken, Telekommunikationsunternehmen und Online-Händler Ziel der Cyberattacken, selbst politische Institutionen waren betroffen. Auch für die kommenden Bundestagswahlen werden Hackerangriffe, aber auch gezielte Falschinformationen erwartet. Sprechen wir gerade öffentlich zu viel über vermeintliche Gefahren und bauschen das Problem auf oder stehen wir erst am Anfang einer Entwicklung und müssen uns an diese Form der Sicherheitsgefahren gewöhnen?

Gabi Dreo: Cybersicherheit ist ein hochrelevantes, gesellschaftliches Thema, da die Digitalisierung alle Bereiche unserer Gesellschaft durchdringt. Daher dürfen die Gefahren von Cyberattacken nicht verharmlost werden. Angriffe wie beispielsweise der vor kurzem bekannt gewordene Hack auf Yahoo, bei dem 1 Mrd. Nutzer betroffen waren, verdeut-

> Cybersicherheit ist ein hochrelevantes, **GESELLSCHAFTLICHES** Thema.



Zunehmend greifen Unbefugte mittels Hackerangriffen auf Daten im Netz zu. Was kann man gegen diese Cyberkriminalität tun?

lichen das sehr eindrucksvoll. Laut Bitkom sind ferner gut die Hälfte (51 %) aller Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Hinzu kommt, dass Cyberangriffe sehr lange unentdeckt bleiben. 2014 waren es im Durchschnitt 205 Tage. Cybersicherheit und Privatsphäre sind die Säulen des Vertrauens in die digitale Gesellschaft. Daher müssen wir einen tiefen gesellschaftlichen Diskurs darüber führen und insbesondere auch mehr in die Entwicklung einer „sicheren" digitalen Gesellschaft investieren. Security-by-Design und Privacy-by-Design sind leider immer noch Schlagworte als Basisgrundsätze des Entwicklungsprozesses.

Politische Studien: Mit der Digitalisierung moderner Gesellschaften wächst zugleich auch deren technische Verwundbarkeit. Erfolgreiche Cyberangriffe können erhebliche gesellschaftliche, wirtschaftliche, politische und auch persönliche Schäden verursachen. Die Funktionsfähigkeit zentraler Infrastrukturen und Netze kann sozusagen per Mausklick massiv beeinträchtigt oder gar lahm gelegt werden. Sehen Sie Politik, Wirtschaft, Verwaltung, letztlich uns alle ausreichend auf dieses Gefahrenpotenzial vorbereitet?

> Jede Technologie kann auch **MISSBRAUCHT** werden.

Gabi Dreo: Nein, bei weitem nicht. In der Vergangenheit hat man mehr auf die Funktionalität gesetzt und dabei die Cybersicherheit eher vernachlässigt. Jetzt müssen die Versäumnisse aufgeholt werden, was in der schnelllebigen digitalen Welt nicht einfach ist. Auch in der Wirtschaft nimmt Cybersicherheit einen immer höheren Stellenwert ein. Unternehmen haben längst erkannt, dass Prozesse mehr und mehr digitalisiert und vernetzt sind und hierbei ein erhebliches Gefahrenpotenzial für den Geschäftsbetrieb unmittelbar existiert. Cybersicherheit ist auf der Managementebene angekommen.

Die Verteidigungsministerin Ursula von der Leyen initiierte den Aufbau eines eigenen Organisationsbereichs Cyber- und Informationsraum in der Bundeswehr. In den Forschungsprogrammen des Bundesministeriums für Bildung und Forschung (BMBF) und der EU ist Cybersicherheit schon längst ein wichtiges Forschungsthema. Die Informations- und Kommunikationstechnologie (IKT) ist die Schlüsseltechnologie der digitalen Gesellschaft. Sie entwickelt sich rasant. Zum einem muss sich die Entwicklung der Cybersicherheit der Geschwindigkeit anpassen und zum anderen auch die Gesellschaft, wenn es z. B. um rechtliche Fragestellungen geht.

Politische Studien: Der Vorläufer des heutigen Internets, das ARPANET, wurde Ende der 60er-Jahre von einer kleinen Forschergruppe im Auftrag des US-Verteidigungsministeriums entwickelt. Das damals revolutionäre dezentrale Konzept eröffnete völlig neue Möglichkeiten und schien auch mehr Sicherheit zu garantieren. Heute sind intelligente und vernetzte Strukturen gang und gäbe, Begriffe wie „smart city", „smart mobility" oder „smart home" in aller Munde. Vernetzung wird als Lösung vieler Probleme beschrieben. Aber schaffen nicht gerade diese zunehmenden vernetzten Strukturen und Systeme neue Sicherheitsrisiken?

Gabi Dreo: Die zunehmende Vernetzung von „smart everything" bietet unglaubliche Entwicklungsmöglichkeiten der digitalen Gesellschaft. Das ARPANET, das als die „Mutter des Internets" bezeichnet wird, wurde natürlich auch für militärische Zwecke genutzt. Es ermöglichte aber Wissenschaftlern eine ganz neue Art des Austausches von Nachrichten und der Kommunikation für die gemeinsame Forschung. Wie das Internet heutzutage unser Leben dominiert, bedarf keiner weiteren Erläuterung. Die Vernetzung erhöht aber auch die Sicherheit. Heute eröffnen uns smarte Systeme viele neue Möglichkeiten wie z. B. autonomes Fahren oder intelligente Steuerung in Haushalten, industriellen Anlagen und Städten. Das taktile Internet mit 5G wird uns eine nie dagewesene Echtzeitvernetzung er-

möglichen. Genauso ermöglichen diese Technologien mehr Schutz, z. B. durch intelligente Überwachungs- und Alarmsysteme.

Der Fortschritt sorgt auch ein Stück weit für neues Gefahrenpotenzial. Jede Technologie kann auch missbraucht werden wie z. B. durch Zugriffe durch Unbefugte („Black Hat Hacker"). Eine hundertprozentige Sicherheit gibt es sowohl in der analogen als auch in der digitalen Welt nicht. Das Risiko in der digitalen Welt kann jedoch durch konsequente Umsetzung von Security-by-Design und Privacy-by-Design, insbesondere auch im Internet der Dinge, verringert werden.

Politische Studien: „Blackout", ein Bestseller-Roman von Marc Elsberg, erhielt 2016 große mediale Aufmerksamkeit. In dieser fiktiven Geschichte kommt es fast zum Bürgerkrieg in Europa, weil Nahrung knapp wird und sich aufgrund mangelnder Hygiene Seuchen ausbreiten. Ursache in diesem fiktiven Szenario ist aber keine Naturkatastrophe, sondern ein Hackerangriff von Terroristen auf sensible Punkte der Stromversorgung. Ist das nur Science-Fiction oder wie sensibel sind speziell unsere Einrichtungen der Energieversorgung tatsächlich?

Gabi Dreo: Spätestens seit STUXNET wissen wir, dass es sich hierbei nicht um Science-Fiction handelt, sondern eine reale Bedrohung vorliegt. Dieser Bedrohung sind sich die Betreiber der kritischen Infrastrukturen jedoch auch bewusst und unternehmen große Anstrengungen, um ihre Systeme zu schützen. In dem erwähnten Buch wurden intelligente Stromzähler manipuliert. Dass es sich hierbei ebenso nicht um reine Fiktion handelt, zeigte der Angriff auf finnische Haushalte 2016, der dazu führte, dass bei -7 Grad Celsius zahlreiche Heizungsanlagen ausfielen. Solche Beispiele sind erst der Anfang. IT-Sicherheitsspezialisten und Angreifer befinden sich in einem steten Wettlauf, wobei kritische Infrastrukturen (KRITIS) gerade in der Zukunft ein immer attraktiveres Ziel für Angreifer darstellen. Auch deshalb ist die Sicherheitsforschung im Bereich des Schutzes von kritischen Infrastrukturen eine der Säulen des Forschungszentrums CODE (Cyber Defence).

Politische Studien: Manchmal macht es den Eindruck, als würden die IT-Sicherheitsmaßnahmen den Angreifern immer einen Schritt hinterherlaufen. Welche Möglichkeiten gibt es, die IT-Sicherheit zu verbessern und zum Beispiel Hackerangriffe bereits im Vorfeld zu vermeiden?

Gabi Dreo: Es ist sicherlich ein ungleicher Wettlauf. Der Angreifer muss nur eine Schwachstelle ausnutzen, die Abwehrmaßnahmen müssen jedoch alle Schwachstellen schließen. Cybersicherheit muss ganzheitlich gedacht werden

> Cybersicherheit muss **GANZHEITLICH** gedacht werden.

und zwar von der Technologie bis zu Prozessen und insbesondere den Nutzern, die immer noch das schwächste Glied in der gesamten Kette sind.

Politische Studien: Hackerangriffe erfolgen meist nicht innerhalb staatlicher Grenzen. Gibt es im Bereich Cybersicherheit überhaupt nationale Lösungen?
Gabi Dreo: In der Tat gibt es in der digitalen Welt keine staatlichen Grenzen. Daher ist die Cybersicherheit eine gesamtstaatliche Aufgabe, die zunächst national und ressortübergreifend zu bewerkstelligen ist. Das ist auch die Voraussetzung für eine Kooperation auf internationaler Ebene.

Politische Studien: Abschließend will ich auf Ihren konkreten Arbeitsbereich eingehen. Auf dem Campus der Universität der Bundeswehr München wird ein neues bundesweit einzigartiges Cyber-Cluster entstehen sowie ein neuer internationaler Master-Studiengang „Cyber-Sicherheit" etabliert. Sie sind bei diesem Projekt maßgeblich involviert. Wie kam es dazu und was versprechen Sie sich davon?
Gabi Dreo: Die Fakultät für Informatik an der Universität der Bundeswehr München beschäftigt sich seit über zehn Jahren mit der Thematik der vernetzten Systeme und der Cybersicherheit. Dafür haben wir das Forschungszentrum CODE gegründet. Schon damals war es unser Bestreben, die Forschungskompetenzen im Bereich der Cybersicherheit zu stärken. Durch den Aufbau eines Cyber-Clusters@Uni-BwM soll nun eines der größten Ökosysteme für die Forschung und Entwicklung von Sicherheitstechnologien

VERNETZTE, SMARTE WELT

Internet der Dinge/Dienste/Daten

Die reale Welt

- Milliarden von vernetzten (mobilen) Geräten, hohe Bandbreiten von 1 Terabit/s und mehr, Heterogenität, Technologien wie Cloud Computing, usw.
- und alles wird immer „smarter"
  - Smartphone, Smart Meter, Smart Grid, Smart Home, SmartFactory, Smart City, Smart Car, Smart Attack, ...
    - ▸ **Smart Everything**

© Mimi Potter / Fotolia.com

> Die einzigartige **BÜNDELUNG** von Forschung, Entwicklung, Behörden, Industrie und Startups auf dem Campus der Universität bietet ein exzellentes Umfeld.

und -produkten sowie Innovationen in Europa entstehen. Die einzigartige Bündelung von Forschung und Entwicklung, Behörden, Industrie und Startups auf dem Campus der Universität bietet ein exzellentes Umfeld für Forschung, Entwicklung und Innovationen. Die Berufung 11 neuer W3-Professuren im Bereich der Cybersicherheit unterstreicht den Willen hierzu. Ich verspreche mir, durch die weitreichende Bündelung von Kompetenzen und den neuen Studiengang einen essenziellen Beitrag zur Verbesserung der Cybersicherheit für alle Bereiche der digitalen Welt leisten zu können.

Politische Studien: Frau Prof. Dreo, wir danken Ihnen für das Gespräch.

Die Fragen stellte Karl Heinz Keil, Referent für Politisches Management und Kommunikation, Medien und Innovation, Institut für Politische Bildung, Hanns-Seidel-Stiftung, München. ///

/// PROF. DR. GABI DREO

ist Direktorin des Forschungszentrums CODE (www.unibw.de/code), Universität der Bundeswehr München.