Informatik für den Frieden

Das PEASEC-Team forscht unter anderem zu resilienten IT-basierten kritischen Infrastrukturen.

Er forscht und lehrt an der Schnittstelle zwischen Informatik und Friedens- und Konfliktforschung. Was IT im Krieg und für den Frieden bewirken kann erklärt Professor Christian Reuter im Gespräch.

Abbildung: Hessen schafft Wissen – Jürgen Kneifel

Professor Christian Reuter

Herr Professor Reuter, der Wissenschaftsrat mahnt eine strukturelle Weiterentwicklung der naturwissenschaftlich-technischen Friedens- und Konfliktforschung in Deutschland an. Wie sind wir hierzulande aufgestellt?

Im Vergleich zur politikwissenschaftlichen Friedens- und Konfliktforschung deutlich weniger gut. Früher hatte dies eine höhere Bedeutung. Schon in den 1950er und 1960er Jahren haben sich Naturwissenschaftler und Naturwissenschaftlerinnen mit Dual-Use-Fragen beschäftigt, also zum Beispiel überlegt, was sie dazu beitragen können, dass Atomkraft nur für die Energieversorgung genutzt wird und nicht auch für die Herstellung waffenfähigen Materials. Heute ist diese Forschung an den deutschen Universitäten zu wenig vertreten. Strukturell, das heißt dauerhaft verankert, ist sie im Moment nur am Carl Friedrich von Weizsäcker-Zentrum der Universität Hamburg und bei uns an der TU Darmstadt. Dabei sind diese Themen aktueller denn je. Es ist mitnichten alles friedlich geworden. Ganz im Gegenteil: In Syrien werden Chemiewaffen eingesetzt, internationale Verträge über die Abrüstung von Langstreckenraketen werden gerade gekündigt. Und natürlich stehen wir im Cyber-Raum ganz neuen Herausforderungen gegenüber.

Welche Bedeutung spielen Cyber-Kriege und Cyber-Streitkräfte inzwischen?

Schädliche Aktivitäten zwischen den Staaten im Cyberspace werden gerade Normalität und Cyber-Streitkräfte sind neben den Boden-, Luft,- und See-streitkräften und den Aktivitäten im Weltraum zu einer neuen Säule der Kriegsführung geworden. Viele Staaten und Bündnisse rüsten ihre Cyber-Kapazitäten auf. Das gilt für die USA ebenso wie für die NATO oder Einzelstaaten wie Deutschland. Überall fließen Geld und Ressourcen in diesen Bereich und es werden neue Einheiten und Befugnisse geschaffen.

Was ist überhaupt eine Cyber-Waffe?

Jedenfalls nichts, was wir aus Star Wars-Filmen kennen. Das Ganze ist viel subtiler. Meistens handelt es sich um Sicherheitslücken in Software und Hardware, verbunden mit Code, um diese auszunutzen. Solche Lücken werden immer wertvoller. Wer sie für kriegerische Zwecke missbrauchen will, meldet sie nicht dem Hersteller, sondern sammelt sie für das eigene Waffenarsenal. Das exklusive Wissen über solche Hintertüren wird zum kriegsentscheidenden Vorteil. Die, die schon länger im Cyberspace aktiv sind, nutzen ihn, um in gegnerische IT-Systeme einzudringen. Das gefährdet nicht nur militärische, sondern auch zivile Systeme – zum Beispiel, wenn nicht nur der Raketenstützpunkt ins Visier gerät, sondern auch die Energieversorgung.

Kann man solche feindlichen Aktivitäten zurückverfolgen?

In der Regel können wir sie nicht zuordnen. Wenn irgendjemand eine Rakete abschießt, sieht man das auf Satellitenbildern. Der Hackerangriff auf die deutsche Bundesregierung im Dezember 2017 dagegen ist bis heute technisch nicht einwandfrei nachvollziehbar. Oft weiß man gar nicht, ob es sich einfach nur um kriminelle Aktivitäten handelt oder um Spionage – die zwar strafrechtlich verfolgt werden kann, aber keinen Kriegsfall auslösen würde – oder ob in Zusammenarbeit mit transnationalen Akteurinnen und Akteuren wirklich ein zwischenstaatlicher Konflikt provoziert werden soll. Es verschwimmt alles. Wir beobachten eine gefährliche Normalisierung von konstanten schädlichen Aktivitäten und von hybriden Konflikten. Das fördert nicht unbedingt das Vertrauen zwischen den Staaten.

Kontakt

Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Prof. Dr. Christian Reuter
Telefon: 06151/16 – 20941
E-Mail: reuter@peasec.tu-darmstadt.de
https://peasec.de

Abbildung: shock/stock.adobe.com

Sie haben das Thema „Dual-Use“ angesprochen. Was können Sie in der Informatik tun, damit neue, digitale Technologien nicht für die Kriegsführung missbraucht werden?

Es geht hier nicht nur um Technikfolgenabschätzung oder die Absicherung von Infrastrukturen. Es geht vor allem auch um eine bewusste Technikgestaltung. Wir müssen Software von Anfang an so entwickeln, dass es möglichst wenig missbräuchliche oder kriegerische Nutzungsmöglichkeiten gibt. Gerade in der Informationstechnologie ist die Dual-Use-Frage aber eine riesige Herausforderung. Denn Software kann immer noch relativ einfach verändert und für andere Zwecke als den ursprünglich gedachten adaptiert werden.

An Ihrem Fachgebiet arbeiten Informatiker und Informatikerinnen mit Friedens- und Konfliktforschenden zusammen. Wie läuft das in der Praxis ab?

Wir verorten uns dort, wo beide Disziplinen sich inhaltlich überlappen. Wir bedienen uns einerseits der Methoden der empirischen Sozialforschung und analysieren zum Beispiel die Rolle neuer Technologien für Frieden und Sicherheit. Da geht es um Fragen wie: Wie werden soziale Medien in Konfliktlagen genutzt? Welche Dynamiken entstehen dort? Welche Narrative gibt es, die Meinungen manipulieren? Darauf aufbauend entwickeln wir dann technische Lösungen, die Eskalationen wie sogenannte Information Warfare verhindern. Wir haben zum Beispiel „Trusty Tweet“ entwickelt, ein Plugin für Browser, das Indikatoren transparent macht, die auf Fake News hindeuten. Wir arbeiten auch an Software, die Social-Media-Daten analysiert, um Missbrauch wie das Tracking von Personen von Anfang an einzudämmen.

Ich stelle mir eine solche kontinuierliche interdisziplinäre Zusammenarbeit sehr voraussetzungsvoll vor.

Ja. Sie setzt voraus, dass man ein vertieftes Verständnis für den jeweils anderen Bereich entwickeln kann. Aber nicht nur das. Wir müssen gemeinsam die Problemstellungen komplett durchdringen, um uns klar zu werden, auf welche konkreten Punkte wir uns fokussieren wollen. Es ist nicht so, dass die technischen Fragestellungen am Anfang stehen. Ausgangspunkt ist immer ein Defizit, welches zunächst genauer analysiert werden muss, um darauf aufbauend mögliche technische Lösungen zu entwickeln, die der Gesellschaft nutzen. Gleichzeitig müssen wir es schaffen, in unserer jeweiligen Fachwelt Akzeptanz zu finden. Denn wir wollen unsere Ergebnisse natürlich auf höchstem Niveau in die einzelnen Disziplinen einbringen, damit wir mit unserer Forschung dort sichtbar werden und andere darauf aufbauen können. Da muss man dann meistens noch einmal den Extra-Meter gehen.

Und was würden Sie gerne in Ihrer eigenen Fachwelt bewegen?

Als Informatiker und Informatikerinnen haben wir heute praktisch Einfluss auf das ganze Leben. Deswegen möchte ich dafür sensibilisieren, dass unsere Arbeit auch Schaden anrichten kann und dass wir mehr auf eine werteorientierte Gestaltung achten müssen, bei der nicht nur monetäre Aspekte eine Rolle spielen. Software kann oftmals unbeabsichtigt Entwicklungen in die falsche Richtung treiben. Also müssen wir lernen, aktive Entscheidungen zu treffen und schon während der Softwareentwicklung Weichenstellungen vornehmen, zum Beispiel bestimmte Nutzungsarten ausschließen oder bestimmte Module nur verschlüsselt bereitstellen. Jeder und jede sollte hierfür ein Bewusstsein entwickeln.

Das Interview führte Jutta Witte. Sie ist Wissenschaftsjournalistin und promovierte Historikerin.

Hintergrund:

Prof. Dr. Christian Reuter ist Leiter des 2017 an der TU Darmstadt geschaffenen Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC). Er gehört dem Fachbereich Informatik und im Rahmen einer Zweitmitgliedschaft auch dem Fachbereich Gesellschafts- und Geschichtswissenschaften an. Das PEASEC-Team forscht zu den Schwerpunktthemen „Sicherheitskritische Mensch-Computer-Interaktion“, „IT für Frieden und Sicherheit“ sowie „Resiliente IT-basierte (kritische) Infrastrukturen“. Das Fachgebiet ist eng verflochten mit dem Profilbereich Cybersicherheit der TU Darmstadt sowie mit dem am Forum Interdisziplinäre Forschung (FiF) der TU Darmstadt verankerten multi- und transdisziplinären Netzwerk IANUS.

https://peasec.de/2020/it-frieden

Aktuelle Publikation:
„Towards IT Peace Research“:
https://peasec.de/2020/towards-it-peace-research