Dr.-Ing. Christof Leng

Die Vorstandsperspektive

Der erweiterte Vorstand der GI zeichnet regelmäßig im Informatik-Spektrum für eine Kolumne verantwortlich, in der aktuelle Themen der Informatik zur Diskussion gestellt werden. Die Texte eröffnen Perspektiven auf aktuelle Fragen, die Informatiker und Informatikerinnen betreffen. Im vorliegenden Heft betrachtet Christof Leng den schmalen Grat zwischen militärischer und ziviler Forschung, der gerade in der Informatik oft sehr schwer zu bestimmen ist. Neben der militärischen Nutzung gibt es noch eine Reihe weiterer sensibler oder missbräuchlicher Einsatzmöglichkeiten von IT-Technologien, wie etwa in Diktaturen oder für kriminelle Zwecke. Das Schlagwort für dieses Problem lautet „Dual-Use Technologien“.

Dual-Use-Technologien Die dunkle Seite der Informatik

Eine der schönsten Aufgaben, die ich in der GI wahrnehmen darf, ist die Mitarbeit an unserer Posterserie „Persönlichkeiten der Informatik“. Im letzten Heft fanden Sie als krönenden Abschluss des ersten Jahres Konrad Zuse, und auch in diesem Jahr werden spannende Personen aus der Informatik folgen. Die Poster sind zwar keine „Informatik Hall of Fame“ als die sie manchmal missverstanden werden, sondern eine Auswahl von interessanten Lebensläufen und Errungenschaften, die junge Menschen für unser Fach begeistern sollen, aber sie sollen auch einen Querschnitt über das Schaffen der Informatik darstellen.

Ein Aspekt hat mich im Rückblick auf die ersten Poster nachdenklich gestimmt. Drei der sechs Persönlichkeiten, Turing, Hopper und Zuse, sind auf die eine oder andere Weise in militärische Projekte involviert gewesen, Grace Hopper sogar mit einer militärischen Karriere bis zum Rang eines Admirals. Das erscheint zunächst überraschend, lässt sich aber in vielen Bereichen der Informatik beobachten.

Die Kryptografie zum Beispiel ist seit jeher ein militärisch hoch interessantes Thema. Auch die Entwicklung von immer leistungsfähigeren Supercomputern wurde zur Simulation von Atombombenexplosionen vorangetrieben. Selbst das heute allgegenwärtige Internet hat seine Wurzeln in einem militärischen Forschungsprojekt. Diese Liste ließe sich beliebig fortsetzen.

Das unterscheidet uns wahrscheinlich nicht von anderen Disziplinen im MINT-Spektrum, ist aber – wie ich befürchte – vielen Informatikerinnen und Informatikern nicht wirklich bewusst. Ob und unter welchen Umständen eine militärische Forschung verwerflich ist, darüber lässt sich vortrefflich streiten. Diese Diskussion möchte ich an dieser Stelle nicht führen.

Stattdessen möchte ich mich auf den schmalen Grat zwischen militärischer und ziviler Forschung konzentrieren, der gerade in der Informatik oft extrem schwer zu bestimmen ist. Neben der militärischen Nutzung gibt es noch eine Reihe weiterer sensibler oder missbräuchlicher Einsatzmöglichkeiten von IT-Technologien, wie z. B. in Diktaturen oder für kriminelle Zwecke. Das Schlagwort für dieses Problem lautet „Dual-Use Technologien“. Viele IT-Produkte lassen sich gleichermaßen für militärische wie für zivile Zwecke nutzen, und genauso auch zum Aufbau einer freiheitlichen Gesellschaft oder zur Durchsetzung eines totalitären Systems. Dies zeigt sich deutlich bei Exportkontrollen: Während die USA lange Zeit den Export von Kryptografie – die heute unter anderem die Grundlage für den sichern elektronischen Geschäftsverkehr bildet – aus militärischen Gründen

stark eingeschränkt hat, lieferten andererseits deutsche und amerikanische Firmen in den vergangenen Jahren Netzwerkmanagementsoftware nach Syrien, welche das dortige Regime zur Ausspähung und Unterdrückung der Bevölkerung nutzt. Mit Hilfe dieser Infrastruktur werden heute Dissidenten ausfindig gemacht, die dann verschleppt, gefoltert und ermordet werden. Erschwerend kommt hinzu, dass der Export von Software wesentlich schwieriger zu überwachen ist als beispielsweise der von Sprengköpfen, Panzern oder Kampflugzeugen. Ein USB-Stick oder eine Internetverbindung reichen dafür vollkommen aus.

Das Thema ist nicht neu, aber es hat eine beunruhigende Aktualität. Aus selbstfahrenden Autos können autonome Roboterpanzer werden, Computerspiele werden zu Kampfsimulatoren umgebaut, und Intrusion Detection Systeme haben große Gemeinsamkeiten mit Zensurinfrastrukturen. Nicht zufällig gab es Proteste aus der Netzgemeinde, als ausgerechnet Karl-Theodor zu Guttenberg, der eben noch Internet-Stoppsschilder propagierte, plötzlich zum Berater der EU-Kommission für die „No disconnect“-Strategie ernannt wurde. Der Politik fehlt eben oft das Problembewusstsein, und manchmal werden Gefahrenpotenziale bewusst ausgeblendet. Wir müssen uns also selbst mit dieser Frage auseinandersetzen.

Die Informatik-Fachschaft an der TU Darmstadt hat als Maskottchen das „Wesen der Informatik“ gewählt, ein lachendes Baby mit einem Maschinengewehr in der Hand. Das soll auf der einer Seite das oft überraschende Gefahrenpotenzial der Informationstechnik und auf der anderen Seite den manchmal naiven Umgang mit diesen Möglichkeiten darstellen. Dass man mit einer Atombombe Millionen von Menschen töten kann, ist allgemein bekannt. Dass Informationstechnik für Kriege und Unterdrückung heute eine viel größere Rolle spielt, ist hingegen weitgehend unbekannt.

Als Entwicklerin/Entwickler oder Wissenschaftlerin/Wissenschaftler steht man auf verlorenem Posten. Eine Technikfolgenabschätzung ist anspruchsvoll und wird normalerweise weder gefordert noch gefördert. Entsprechende Studieninhalte sind vielerorts aus den immer überfrachteteren Lehrplänen verschwunden. Wir drücken den Studierenden technische Möglichkeiten in die Hand ohne die Zeit dafür zu finden, über deren potenzielle Folgen zu reden. Das ist wie ein Sportwagen ohne Fahrunterricht.

Wir haben die Verantwortung, uns der Frage der Nutzungsmöglichkeiten unserer Forschungs- und Entwicklungsergebnisse jederzeit zu stellen. In der GI findet dieser Diskurs an vielen Stellen statt, und ich bin stolz, dass das für uns – unter anderem durch unsere Ethischen Leitlinien – auch zu unserem Selbstverständnis gehört. In Universitäten und Unternehmen vermisse ich – von lobenswerten Einzelinitiativen abgesehen – diese Art der Selbstreflexion jedoch viel zu oft. Statt die Lehrpläne mit technischem Wissen zu überfrachten, das oft schneller veraltet als es gelehrt werden kann, sollte die konstruktive Auseinandersetzung mit den Nutzungs- und Missbrauchsmöglichkeiten ein fundamentaler Bestandteil des Studiums sein.

Bereits heute wird das öffentliche Vertrauen in die Informatik immer wieder durch ihre missbräuchliche oder gedankenlose Verwendung erschüttert. Wenn wir das Vertrauen zurückgewinnen wollen, müssen wir als Informatikerinnen und Informatiker eine Kultur der Verantwortlichkeit etablieren, und können uns nicht länger auf technische Fragestellungen zurückziehen. Derzeit herrscht noch die Euphorie über die vielen neuen Gadgets und die schöne neue Internetwelt vor. Was aber, wenn der Cyberkrieg, der gläserne Bürger oder irgendein anderes Horrorszenario uns einholt? Dann sollten wir eine gute Antwort auf die Frage haben, was wir getan haben, um unserer Verantwortung gerecht zu werden.

Es bleibt also von zentraler Wichtigkeit, dass wir unsere eigene Disziplin, die Nutzung ihrer Errungenschaften und ihre Auswirkungen auf die Gesellschaft mit großer Aufmerksamkeit kritisch zu begleiten. Wie passend, dass eines der nächsten Poster in unserer Serie Joseph Weizenbaum gewidmet ist.

Dr.-Ing. Christof Leng
International Computer Science Institute
1947 Center Street Suite 600, Berkeley, CA 94704, USA
christof.leng@gi.de