A MQ-9 Reaper during a training mission, U.S. Air Force photo by Paul Ridgeway

Dietrich Meyer-Ebrecht

Rüstung und Informatik – Editorial zum Schwerpunkt

Schon gegen Ende der 1950er-Jahre umwarb die damals noch junge Bundeswehr uns frisch eingeschriebene Ingenieurstudenten, und ich erinnere unsere bange Frage in einer Werbeveranstaltung, ob wir nun – die allgemeine Wehrpflicht wurde gerade eingeführt – mitten in unserem Studium zum Pflichtdienst eingezogen werden würden. Die Tragweite der Antwort – „uns ist viel mehr damit gedient, wenn Sie Ihr Studium brav absolvieren und in Ihrem Beruf erfolgreich sein werden" – ist mir erst viel später bewusst geworden. Was wir aus unserer zivilen Perspektive nicht sehen konnten oder in einer Zeit des Umbruchs nach einem schrecklichen Krieg auch nicht sehen wollten, war den Militärs spätestens seit Beginn des 20. Jahrhunderts selbstverständlich: Technik ist per se eine unverzichtbare Grundlage für die Kriegführung, und alle technischen und technologischen Innovationen im zivilen Anwendungsbereich sind per se auch Stimuli und Ressourcen für die Rüstungstechnik.

Zunehmend erfahren wir, dass wir zwischen ziviler Technik und Rüstungstechnik keine klare Trennlinie mehr ziehen können, auch und gerade in der Informatik und Informationstechnik. In der Rückschau war es besonders in der Forschung und Entwicklung auf diesem Gebiet immer schon eine Illusion, dass wir trennen könnten, was einmal der Zivilgesellschaft dienen würde und was ausschließlich den Militärs. Gerade die Entwicklung der digitalen Technologien und Systeme war von Anbeginn militärisch motiviert und finanziert. Das Internet startete als militärisches Projekt ARPAnet. Das Silicon Valley, Brutplatz für die Cybertechnologie, verdankt sein Entstehen großzügigen Förderprogrammen aus den Töpfen der Militärs – „cyber-militärischer Komplex" nennt *Daniel Leisegang* diese Liaison in seinem Beitrag in diesem Heft.

Treibende Kraft des Evolutionsprozesses, der mit der rasanten Entwicklung und globalen Ausbreitung digitaler Technologien und Methoden einherging, war die Zivilgesellschaft mit ihrem ungehemmten Konsum informationstechnischer Produkte. Wenn heute auf 3x3x1 mm³ Silizium für fünf US-Dollar ein Gyroskop, ein Beschleunigungssensor, ein Magnetometer – alles in drei Achsen! – zusammen mit einem Prozessor für die Datenaufbereitung untergebracht werden können,[1] verdanken wir dies dem Masseneinsatz in Lifestyleprodukten. Produkte wie dieses und ihre Derivate landen umgehend in Waffensystemen, erfüllen preisgünstig eine geforderte Aufgabe oder inspirieren sogar neue Waffenfunktionen.

„Macht Eure Arbeit gut und wir schauen Euch dabei über die Schulter" – so fließen die Innovationen der Informatik und Informationstechnik ständig aus allen Anwendungsbereichen in die Rüstungstechnik ein – auch ungewollt von ihren Schöpfern, vor allem unkontrollierbar durch die Gesellschaft. Junge Menschen an der Schwelle von einer technischen Ausbildung in eine berufliche Laufbahn, zumal in der Informatik und Informationstechnik, stehen in der Wahl ihres zukünftigen Tätigkeitsfeldes vor zunehmend schwierigen Entscheidungen: Zu fließend sind die Grenzen zwischen ziviler und militärischer Technik, um vorausschauend erkennen zu können, ob der anvisierte Arbeitsplatz die gesuchte rüstungsferne Perspektive bietet. Zu sehr verlocken die Gelder der Militärs die Leitungen von Unternehmen und Forschungsinstituten, die vorgetragenen moralischen Ansprüche alsbald hintanzustellen.

Rüstung und Informatik ist ein zentrales Thema des FIfF seit seiner Gründung vor nunmehr 31 Jahren. Eines der Ziele ist es,

Dietrich Meyer-Ebrecht

Prof. (em) Dr.-Ing. **Dietrich Meyer-Ebrecht** war von 1984 bis 2004 Inhaber des Lehrstuhles für Bildverarbeitung an der RWTH Aachen, zuletzt mit dem Forschungsschwerpunkt digitale Bildanalyse für medizinische Anwendungen. Seit 2001 ist er Mitglied des FIfF-Vorstandes.

diese Wechselwirkungen transparenter zu machen. Dazu dienen auch die in unregelmäßiger Folge erscheinenden Schwerpunkthefte der FIfF-Kommunikation zu diesem Themenbereich, so auch wieder dieses Heft. In seinem Schwerpunktteil *Rüstung und Informatik* werden dieses Mal vor allem ethische Fragen gestellt. Aus ethischer Blickrichtung reflektiert *Thomas Gruber* die Rolle der Informatik in der modernen Kriegführung. Wie die neuerlich einsetzende Aufrüstungsspirale auf die Hochschulforschung Einfluss nimmt, beschreiben *Reiner Braun* und *Lucas Wirl*, und auch welche Rolle Zivilklauseln in der universitären Forschung spielen. Dass die Vorbehalte gegen eine militärische Finanzierung von Forschung und Entwicklung in den USA deutlich weniger ausgeprägt sind, beschreibt Daniel Leisegang, oben bereits genannt, beispielhaft mit der „dunklen Seite" des Silicon Valley. Welchen Einfluss die alle Räume und alle Dimensionen durchdringende technische Vernetzung mit ganz neuen Verknüpfungen der Einflussgrößen, der Dimensionen und Akteure auf die globale Entwicklung von Konflikten, Gewalt und Krieg hat, analysiert *Jürgen Scheffran*. Auch wenn Vernetzung nicht allein die technische Domäne betrifft, sind Wissenschaft und Technik grundlegend beteiligt und mit in die Verantwortung zu nehmen.

Hans-Jörg Kreowski schreibt über eine Waffe, die aus ethischen Erwägungen besondere Aufmerksamkeit fordert, die Drohne. Sie wird vermutlich die erste Waffe sein, mit der bereits in naher Zukunft die Schwelle zu einem autonom operierenden Kampfgerät überschritten werden wird. Unkalkulierbare Konsequenzen und Risiken des Einsatzes autonomer Waffen haben eine Gruppe von über 2.000 Wissenschaftlern der Künstlichen Intelligenz und Robotik bewogen, zu einem Bann autonomer Waffen aufzurufen, den wir in diesem Heft abdrucken. Nochmals *Hans-Jörg Kreowski* und *Aaron Lye* kommentieren diesen dringend zu unterstützenden Aufruf. Zum Thema Drohnen und insbesondere zu ihrem Einsatz für die Tötung unter Terrorverdacht gesuchter Personen hat der Künstler *Florian Mehnert* ein bemerkenswertes Experiment gemacht, das er in diesem Heft beschreibt. Mit der Situation eines „High Value Targets" im Fadenkreuz des fernab agierenden Drohnenpiloten, abgebildet auf einen Rattenkäfig, führt er unsere Gesellschaft vor, die den Künstler ob des angedrohten (aber nie beabsichtigten) Todesschusses auf die Ratte lynchen möchte, jedoch hinterhältige, völkerrechtswidrige Drohnenoperationen auf fremder Staaten Terrain schweigend hinnimmt.

Wie sich die Aktivitäten der Geheimdienste seit Turings Entschlüsselung der Enigma zu einem unerklärten Informationskrieg entwickelt haben, in den wir längst verstrickt sind, und zu welchen Absurditäten die Geheimniskrämerei unserer Politiker führt, nehmen *Ute Bernhardt* und *Ingo Ruhmann* in ihrem Beitrag *Das Blaumilch-System* aufs Korn. Ihr Artikel und ein Interview mit dem Hacker *Felix FX Lindner* zur Frage, wie weit Cyberwar einen Angriff auf Freiheit und Demokratie darstellt, stimmen auf unser Dossier *Kriegführung im Cyberspace* ein, das der Ausgabe beiliegt, siehe Kasten.

Anmerkung

1 *InvenSense Inc. 9-Axis Gyro+Accel+Magn MPU-9250*

Dossier *Kriegführung im Cyberspace*

Diesem Heft liegt das 20 Seiten starke Dossier *Kriegführung im Cyberspace* bei, das das FIfF gemeinsam mit der Zeitschrift *Wissenschaft & Frieden* herausgibt. Es ist gleichzeitig Beilage der *W&F 3/15,* August 2015.

Während die Medien die ungebremste Ausspähung in den digitalen Netzen aufmerksam verfolgen, dient der virtuelle Raum weitgehend unbemerkt von der Öffentlichkeit den Militärs als Operationsraum. Militärische Szenarien beziehen Cyberoperationen als entscheidende Elemente der Kriegführung ein – für Spionageaktionen bis hin zum Einsatz von Cyberwaffen. Ihre beabsichtigte Wirkung reicht von Destabilisierung über Sabotage bis zu Eingriffen in digitale Infrastrukturen mit weitreichenden Folgen für die Zivilbevölkerung. In ihrer Unfassbarkeit und Unkontrollierbarkeit stellen die Cyberaktivitäten der Geheimdienste und Militärs eine verschwiegene, aber höchst reale Gefahr für den Frieden dar. Die fünf Beiträge des Dossiers umreißen die Problematik und machen die Notwendigkeit eines Gegensteuerns deutlich, wie es das FIfF in seiner Kampagne Cyberpeace fordert.

Die Herausgabe des Dossiers wurde im Rahmen dieser Kampagne durch die Stiftung *bridge* finanziell unterstützt.