Ingo Ruhmann

Forschung zu computergestützter Kriegsführung bewerten

FIfF-Studie für den Bundestag endlich online

Der Hack von Bundestagsservern und der Abfluss von Daten 2016 war nicht das erste Mal, dass sich das Parlament mit *Information Warfare* beschäftigt hat. Über 20 Jahre zuvor hatte der Bundestags-Unterausschuss *Abrüstung und Rüstungskontrolle* auf maßgebliches Betreiben von Egon Bahr, aber einvernehmlich von allen Fraktionen getragen, die Frage gestellt, welche Möglichkeiten bestehen, neue Rüstungswettläufe frühzeitig zu erkennen und durch Maßnahmen der Rüstungskontrolle zu vermeiden.

Dazu hatte das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) das FIfF Ende 1994 mit der Erarbeitung einer Studie über *Methoden für die Analyse und Bewertung militärisch relevanter Forschung und Entwicklung im Bereich Informations- und Kommunikations-Technologie* betraut. Die beiden mit dem Gutachten verfolgten Ziele waren erstens, Kriterien für eine Bewertung der militärischen Relevanz von IuK-Technologien zu finden, die sich noch in der Forschung und Entwicklung (FuE), also in der Technikgenese befinden. Zweitens sollten weiterführende Ansätze zu einer praktikablen Methodik der Rüstungskontrolle im Bereich FuE aufgezeigt werden. Die Untersuchung sollte zu einem Raster von Bewertungskriterien führen und als Ausgangspunkt für zukünftige Politikberatung und Methodenforschung dienen.

Die Studie war auf sechs Monate begrenzt. Parallel dazu hatte das TAB verschiedene Forscher aus anderen Fachdisziplinen mit einem Blick auf rüstungsrelevante Entwicklungen in der Technologieentwicklung betraut. Als gemeinsames Ergebnis dieser Arbeiten erschien der TAB-Bericht Nr. 45,[1] der im Frühjahr 1995 dem Ausschuss präsentiert wurde.

Der universelle Charakter der Informations- und Kommunikationstechnologie (IuK) erlaubt nur selten eine offensichtliche Unterscheidung in zivile und militärische Forschung und Entwicklung. Für eine differenzierte Analyse und Bewertung müssen daher die militärischen, politischen, wirtschaftlichen und wissenschaftlichen Rahmenbedingungen einbezogen werden. Bei der Analyse der militärischen Nutzung von IuK-Technologie lassen sich jedoch Invarianten identifizieren – Bestimmungsgrößen auf verschiedenen militärisch-technologischen Entwicklungsstufen mit entscheidender Bedeutung für militärische Operationen.

Schon 1995 war die Entwicklung zu Information Warfare klar erkennbar. Unstrittig war in den USA bereits das Ziel der *Informations-Dominanz*. Erste Beispiele von Auseinandersetzungen – etwa zwischen Peru und Ecuador auf dem Internet 1995 oder die der Zapatisten gegen die mexikanische Regierung Ende 1994 – lagen vor. Die Entwicklung autonomer Waffensysteme hatte begonnen.

Die Vorhersage der FIfF-Studie lautete damals, dass die Ausrichtung der IuK-Technik auf Information Warfare mit entsprechendem FuE-Bedarf und die Verlagerung der Abschreckung auf Information Warfare bestimmt werden würde. Genauer: „Information Warfare wird in den USA und damit nach einiger Zeit auch in Europa ein an militärischen Bedürfnissen ausgerichtetes FuE-Ziel der Zukunft sein." Und es war schon sehr klar erkennbar, dass „die militärische Nutzbarkeit von IT-Sicherheitsproblemen die Entwicklung effektiver ziviler Sicherheitssysteme behindern wird."

Es ist also mehr als 20 Jahre her, dass im Bundestag in sehr weitsichtiger Weise ein Blick in die Zukunft von Rüstung und den sicherheitspolitischen Konsequenzen geworfen wurde. Die Antworten der Wissenschaft waren – dies ist deutlich – nicht unmittelbar umsetzbar. Damals wie heute wäre mehr Forschungsarbeit notwendig, um Information Warfare einzuhegen und einer Rüstungskontrolle zu unterwerfen.

Im Unterschied zu damals ist heute allerdings kaum erkennbar, dass der Bundestag noch einmal die Initiative ergreifen würde, eine Rüstungskontrolle im Cyberspace politisch anzugehen. Stattdessen hat die Bundeswehr ihre Cybertruppe zu einem eigenen Kommando gemacht und plant, die Zahl der Soldaten zu verdoppeln. Solche Bilanzen machen die Rüstungskontrolle zwar einfacher, aber selbst dies wird von keiner Einrichtung oder friedenswissenschaftlichen Institut derzeit geleistet.

2016 haben die Parlamentarier selbst erlebt, was Information Warfare bedeuten kann. Eine Rüstungsspirale wird die Gefahren von Information Warfare für die zivile Informationsgesellschaft und die Risiken für die internationale Stabilität nicht vermindern oder gar beseitigen. Vielleicht ist es daher an der Zeit, dass wir uns daran erinnern, dass Rüstungskontrolle und Information Warfare kein Gegensatz sind, sondern die Erarbeitung von Konzepten und Lösungsansätzen erfordern.

Dafür liefert auch eine 20 Jahre alte Studie[2] heute noch durchaus Denkanstöße.

Referenzen

1 *TAB-Bericht Nr. 45: Kontrollkriterien für die Bewertung und Entscheidung bezüglich neuer Technologien im Rüstungsbereich*

2 *Die Studie ist unter https://cyberpeace.fiff.de/dokumente/tab.pdf verfügbar.*