FriedensForum

Cyberpeace —
eine Kampagne des FIfF gegen die ‚digitale' Aufrüstung

Dietrich Meyer-Ebrecht

Zuerst war das Internet eine faszinierende neue Technologie. Es förderte die internationale Zusammenarbeit in der Wissenschaft. Dass es mit seiner globale Ausbreitung und der zunehmenden Verbreitung des Zugangs für private NutzerInnen auch zur Völkerverständigung und Friedenstiftung beitragen würde, war eine schöne Hoffnung. Dann sah die Wirtschaft ihre Chance: Das Internet wird zum globalen Handelsplatz. Fertigungs- und Versorgungs- und Verwaltungsprozesse werden durch Vernetzung optimiert, Verkehrsflüsse werden gesteuert, Information wird immer und überall zugänglich. Das Internet ist heute ein ‚backbone' der Zivilgesellschaft, von dem lebenswichtige Prozesse abhängen, auf dessen ungestörtes Funktionieren wir uns in zunehmendem Maße verlassen müssen. Und bei alledem ist ziemlich in Vergessenheit geraten, dass die technische Grundlage des Internets – die Vernetzung von Computersystemen weltweit – ursprünglich in militärischem Auftrag angelegt wurde.

Nicht in Vergessenheit geraten ist dies bei den Militärs. Ganz im Gegenteil, *network centered warfare* war bereits 1996 die Kernbotschaft in einem Positionspapier des US-Generalstabs, der *Joint Vision 2010*. Gefordert wird eine gründliche Restrukturierung der US-Streitkräfte mit dem Ziel einer umfassenden Nutzung moderner Kommunikations- und Informationstechnologie in Waffen, in Waffensystemen und in den zu ihren Einsatz notwendigen Infrastrukturen. Eine besondere Rolle kommt in der Doktrin der ‚Neuen Kriege' dem *cyberspace* zu, dem weltweiten virtuellen Verkehrsraum für digitale Daten aus Kabeln, Mobilfunk und vernetzten Computersystemen. Er ist geradezu prädestiniert für die Ausspähung.

Nun haben die Enthüllungen Edward Snowdens – vor allem das nicht geahnte ungeheure Ausmaß der digitalen Ausspähung, das sie offenbarten – uns zunächst vornehmlich als Eingriff in unsere Privatsphäre betroffen gemacht. Wenig ist die militärische Dimension thematisiert worden. Und die Risiken, die daraus entspringen – für uns persönlich, und für die Gesellschaft. Unser persönliches Risiko: Wir können zum ‚Beifang' der Rasterfahndung nach Personen werden, die nach undurchsichtigen Kriterien als gefährlich eingestuft werden. Denn die Ausspähungsaktivitäten der NSA, des GCHQ, des BND etc. unterliegen militärischen Denkkategorien. Kennzeichnend dafür sind die Erfolgskriterien: Sie sind nicht wie im Zivilen orientiert am bestmöglichen Erreichen eines Zieles unter geringst möglichen Schäden

– der Erfolgsfall ist, wenn das Ziel überhaupt erreicht wird, unter Inkaufnahme jedweder Kollateralschäden, hier der Personen, die unbescholten ins Netz geraten. Im Extremfall als *high value target* eines völkerrechtswidrigen Drohneneinsatzes, identifiziert auf Grund von verdächtig machenden Kommunikationsmustern und als Ziel geortet über das Mobiltelefon.

Im Kontext der aktuellen Kriegsführungsdoktrin ist digitale Ausspähung bereits ein wesentliches Element des Cyberwarfare, des Informationskrieges. Die strategischen Szenarien beschreiben den Einsatz militärischer Cyberoperationen in Phasen: Phase 0 „Konditionieren" dient dem Erkennen der Absichten des Gegners – oder auch des ‚Freundes' – mittels geheimer Zugänge zu dessen Netzwerken. In Phase 1 „Abschreckung" werden dem Gegner mit spürbaren Operationen ‚die digitalen Muskeln gezeigt'. In Phase 2 „Dominieren" werden Operationen eingeleitet, die den Gegner schwächen sollen, wie Sabotageakte oder die Übernahme der Kontrolle über kritische System – mittels der in Phase 0 bereits eingerichteten geheimen Zugänge.

All diese hoch geheim gehaltenen Operationen schwimmen gleichsam mit in den zivilen Informationsströmen – ein Fundamentalrisiko für die Zivilgesellschaft in mehrere Hinsicht: Schwachstellen in Software oder Hardware, die Angriffspunkte für ein widerrechtliches Eindringen bieten, werden bewusst geheim gehalten, Hintertüren werden sogar absichtlich eingebaut, lebenswichtige Systeme werden mit staatlicher Duldung kompromittierbar. Cyberoperationen breiten sich viral aus, Kollateralschäden sind quasi vorprogrammiert. Cyberattacken können physische Wirkung haben, also Zerstörung oder Gefahren für Menschenleben nach sich ziehen. Sie betreten damit die Ebene der konventionellen Kriegführung und können militärische Reaktionen nach sich ziehen. Da die Quelle digitaler Attacken oft sehr schwer nachzuweisen ist (Problem der 'Attributierbarkeit'), kann ein Gegenschlag den Falschen treffen. Aus dieser Sicht können wir die gegenwärtige ungebremste Ausspähung staatlicher Institutionen, Wirtschaft und Industrie, Forschungseinrichtungen und privater Personen bereits als ‚kalten' Cyberkrieg verstehen.

Um der Öffentlichkeit die militärischen Herrschaftsansprüchen über das Internet und dessen regelmäßige Nutzung für militärische Cyberoperationen bewusst zu machen, hat das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) eine Kampagne gestartet: Ihr Motto heißt *Cyberpeace*. Mit der Kampagne will das FIfF öffentlichen Druck auf Politik und Wirtschaft wecken, das Internet dem Primat einer zivilen und ausschließlich friedlichen Nutzung unterzuordnen, den militärischen Missbrauch einzudämmen und ihn wenigstens einer demokratischen Kontrolle zu unterziehen. Als Fernziel ist in internationaler Zusammenarbeit ein umfassender Bann offensiver Cyberwaffen anzustreben. Die Kampagne wird gefördert durch die Stiftung *bridge*. (cyberpeace.fiff.de)