Im Internet wird hochgerüstet

Experten diskutieren in Bremen über die Gefahren des Informationskrieges

Von unserer Mitarbeiterin
Imke Zimmermann

Bremen. Nach den Anschlägen in den USA geht die Angst um: Wozu sind Terroristen noch fähig? Zum Einsatz von Biowaffen oder chemischen Keulen mit ungeahnter Durchschlagskraft? Zu Hacker-Attacken über das Internet auf Einrichtungen wie Atomkraftwerke oder Börsen? Zumindest diese Furcht hält der Berliner Politologe Ralf Bendrath für unbegründet.

„Terrorismus ist eine Kommunikationsstrategie." Lautlose Angriffe nützten Terroristen nicht – sie brauchten den sichtbaren Effekt. Außerdem seien Rechner in sicherheitskritischen Zielen wie Kernkraftwerken meist nicht ans allgemein zugängliche Netz angeschlossen. Das mache ein Eindringen außerordentlich schwierig. Offenkundig „haben die Terroristen bislang dazu auch nicht die Fähigkeiten", sagt der Forscher, der sich seit langem mit Möglichkeiten des „Cyberwarfare", dem Informationskrieg, beschäftigt.

Diese Möglichkeiten haben nach Meinung der Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik, deren Geschäftsführer Bendrath ist, ganz andere: nämlich die USA. Und sie nutzten sie systematisch, so dass „eine neue Rüstungsspirale zu befürchten ist". Im Kosovo-Krieg hätten sie ihre Kenntnisse erstmals praktisch eingesetzt: „Die Amerikaner hackten sich in serbische Flugabwehr-Computer, spielten ihnen falsche Ziele auf den Bildschirm und lenkten so von eigenen Angriffen ab", sagt Bendrath. Inzwischen rüsteten sich auch China oder Russland für den Krieg im Internet. Ein Wettlauf drohe, wenn nicht bald Kontrollgespräche aufgenommen würden.

Positionen wie diese wird Bendrath an diesem Wochenende auch in Bremen vortragen – bei der Jahrestagung des „Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung" (FifF). Thema der Tagung, die gestern begann, sind „Wege und Irrwege der Informatik". In Vorträgen und Arbeitsgruppen beschäftigen sich etwa 120 Wissenschaftler bis morgen mit „Gencomputing", „Informatik und Dritte Welt", „Verantwortlichkeiten im Internet", „Raketenabwehr und Weltraumrüstung" oder eben dem Thema „Cyberwar".

Die Tagung war lange geplant. Vor dem Hintergrund des Terrors in den USA gewinnen viele Veranstaltungen aber eine neue Dimension. Das gelte auch für Arbeitskreise über Verschlüsselungstechniken und Sicherheit im Internet, sagt FifF-Vorstandsmitglied Ralf Streibl. „Gleich nach den Attacken ist der Ruf nach mehr Kontrolle, nach Verschlüsselungsverboten für E-Mails laut geworden", erläutert Streibl. Dies würde aber einen erheblichen Eingriff in die Freiheitsrechte bedeuten: „Ich lege Wert darauf, nicht nur Postkarten durchs Web zu schicken, sondern auch Briefe, die ich zukleben kann", beschreibt er Wirkung und Bedeutung von Kryptographie bildlich.

Zur Weltlage passt auch die öffentliche Diskussion über „Informatik und Krieg – Das Ende der Machbarkeiten". Ein Ansatz des FifF: Solche Angriffe seien weder mit weltraumgestützten Abwehrsystemen noch mit konventionellen militärischen Mitteln zu verhindern.

An der Diskussion am Sonntag um 11 Uhr im Bremer Innovations- und Technologiezentrum, Fahrenheitstraße 1, nimmt auch Ralf Bendrath teil. Eingeladen wurden zudem Informatiker von Universitäten, darunter Hans-Jörg Kreowski aus Bremen und Nazir Peroz von der TU Berlin, der in Kabul aufgewachsen ist. Auf dem Podium ist schließlich der nach FifF-Angaben weltbekannte Software-Spezialist David L. Parnas aus Canada, der am Raketenabwehr-Programm der USA zu Zeiten Ronald Reagans mitarbeitete, aber nach kurzer Zeit wieder ausstieg.