Gastbeitrag aus
Streitkräfte und Strategien - NDR info
28. Juli 2012

Kriegsführung im Cyberspace ein neues Aufgabenfeld für die Rüstungskontrolle

Gastbeitrag von Joachim Hagen

Die deutschen Cyberkrieger heißen im Bundeswehr-Jargon: CNO-Kräfte. CNO steht für Computer-Netzwerk-Operationen. Diese Soldaten gehören zum Kommando Strategische Aufklärung in Gelsdorf bei Bonn. Wie viele CNO-Soldaten dort arbeiten, wie sie ausgebildet sind und was sie können – das ist streng geheim. Bundesverteidigungsminister Thomas de Maizière war denn auch entsprechend einsilbig, als er am Rande eines Truppenbesuchs im rheinland-pfälzischen Birkenfeld nach den Cyberkriegern gefragt wurde:

> *O-Ton de Maizière*
> *„Die Hauptaufgabe der Bundeswehr ist, das eigene Netz zu sichern. Cyber-Sicherheit ist nach dem strategischen Konzept der NATO von Lissabon eine Aufgabe der NATO im Ganzen und darum beteiligen wir uns daran. Aber all das ist nicht für eine Diskussion in der Öffentlichkeit geeignet.“*

Als die Reporter nicht locker ließen und nachfragten, wie sie sich das denn vorstellen dürften, verlor de Maizière die gewohnte Zurückhaltung:

> *O-Ton de Maizière*
> *„Sie dürfen sich gar nichts vorstellen, weil wir darüber nichts öffentlich mitteilen. Das ist in vielen Bereichen der Sicherheit so, hier auch.“*

Anlass für die kritischen Nachfragen war ein Bericht des Verteidigungsministeriums an den Bundestag, der kurz zuvor bekannt geworden war. Darin heißt es über die vor wenigen Jahren gegründete CNO-Abteilung der Bundeswehr:

> *Zitat*
> *„Eine Anfangsbefähigung zum Wirken in gegnerischen Netzen wurde erreicht. Für die Ausbildung bzw. zur Erprobung von Verfahren besteht die Möglichkeit zur Durchführung von Simulationen in einer abgeschlossenen Laborumgebung.“*

Diese beiden Sätze haben seitdem eine heftige Debatte ausgelöst. Was heißt „Anfangsbefähigung zum Wirken in gegnerischen Netzen“? Ist dies das Eingeständnis, dass die Bundeswehr mit selbst programmierten Würmern im Internet unterwegs ist? Oder ist der Hinweis auf die abgeschlossene Laborumgebung als Versicherung zu verstehen, dass fremde Computer nicht mit solchen Schadprogrammen infiziert werden? Der stellvertretende Direktor des Instituts für Friedensforschung und Sicherheitspolitik an der Universität Hamburg,

Götz Neuneck, fordert von der Bundeswehr, diese Unklarheit zu beseitigen. Es dürfe nicht der Eindruck entstehen, dass hier ein Angriff vorbereitet wird:

O-Ton Neuneck
„Im Internet hat die Offensive, würde ein klassischer Clausewitz-Schüler sagen, immer einen Vorteil gegenüber der Defensive, weil sich alles mit Lichtgeschwindigkeit bewegt. In einem Raum, in Netzen, Kabeln, Weltraum, wo auch immer, der sehr schwer zu kontrollieren ist, und der in Millisekunden viele nationalstaatliche Grenzen überschreitet. Deshalb ist die Formulierung „das Wirken in andere Netze“ eine Formulierung, die eine Offensive impliziert.“

Der Krieg zwischen Russland und Georgien vor vier Jahren gilt als erste Auseinandersetzung zwischen zwei Staaten, bei der auch gegnerische Computer in großer Zahl über das Internet angegriffen wurden. Ziel waren vor allem die Server georgischer Banken, deren Verbindungen ins Ausland blockiert wurden. Ein Jahr später attackierte ein Computerwurm namens Stuxnet die Uran-Anreicherungsanlage im iranischen Natanz. Stuxnet manipulierte die Motorsteuerung der Hochgeschwindigkeits-Zentrifugen, so dass diese mal schneller und mal langsamer rotierten. In den Maschinen entstand eine Unwucht und sie explodierten. Das Uran-Programm des Iran wurde so um mehrere Monate zurückgeworfen. Der New York Times Autor David E. Sanger berichtet in seinem neuen Buch, dass der ehemalige amerikanische Präsident George W. Bush den Auftrag gegeben habe, Stuxnet zu entwickeln. Sein Nachfolger Barak Obama soll dann den Angriffsbefehl gegeben haben, auch um Israel von einem Angriff gegen den Iran abzuhalten. Offiziell bestätigt wurde das allerdings nie. Klar ist aber, dass es möglich ist, moderne Industrie-Anlagen mit Computer-Würmern zu sabotieren. Die Auswirkungen eines solchen Angriffs sind nur schwer vorher zu sagen, meint der ehemalige Sicherheitsberater der amerikanischen Präsidenten Clinton und George W. Bush, Richard Clarke:

O-Ton Clarke (overvoice)
„Jedes Versorgungs-System, das von Computern gesteuert wird, wie etwa das Stromnetz, die Bahn, Gaspipelines oder Raffinerien, ist verwundbar. Jede Infrastruktur, die von Computern gesteuert wird, kann angegriffen werden, unterbrochen oder sogar beschädigt werden.“

Um solche Angriffe abwehren zu können, haben die Vereinigten Staaten vor zwei Jahren ein sogenanntes Cyber-Kommando gegründet. In der eigenen Aufgabenbeschreibung heißt es: Das Cyber-Kommando führt, wenn befohlen, militärische Aktionen der gesamten Bandbreite im Cyberraum durch – nach den geltenden Gesetzen und Anweisungen. Ähnliche militärische Behörden gibt es bereits in elf weiteren Staaten – darunter auch in Deutschland. Der Hamburger Friedensforscher Neuneck spricht von einem digitalen Wettrüsten:

O-Ton Neuneck
„Das zeigt deutlich, dass hier eine neue Schwelle überschritten worden ist. Dass man sich darauf einrichtet, dass es aggressive Akte gegen die eigene Infrastruktur geben könnte, seien es militärische, seien es zivile. Und das kann man schon als digitales Wettrüsten bezeichnen, weil man davon ausgeht, dass andere Staaten über diese Fähigkeit verfügen, dass man dann selber investieren muss, um in einem Krisenfall oder in einem Kriegsfall, tatsächlich irgendwie einwirken zu können.“

Das Problem bei der Abwehr solcher digitalen Angriffe: Der Verursacher ist meistens nicht auszumachen. Auch wenn man den Weg eines Wurms bis zu einem bestimmten Computer zurückverfolgen kann - es kann sich um einen gekaperten Computer handeln, dessen Besitzer von dem Angriff nichts weiß.

Jetzt wird darüber diskutiert, wie das digitale Wettrüsten eingedämmt werden kann. Götz Neuneck hat gerade eine internationale Konferenz über die Herausforderungen der Cyber-Sicherheit mit organisiert. Das Ergebnis ist ernüchternd: Für internationale Verträge ist es noch zu früh:

> *O-Ton Neuneck*
> *„Die Staaten sind im Augenblick noch nicht bereit dazu, einen Vertrag abzuschließen. Dazu gibt es enorme juristische Probleme, definitorische Probleme, auch Umsetzungsprobleme: Wer soll das tun, wer soll das verifizieren? All das ist im Wesentlichen unklar. Deswegen ist Vertrauensbildung im Augenblick das Gebot der Stunde. Nämlich das Signal, dass man hier nicht neue Waffenentwicklungen forciert."*

Aber für die Glaubwürdigkeit eines solchen Signals wäre es natürlich gut, wenn die Bundeswehr erklärte, was sie meint, wenn sie von der „Anfangsbefähigung zur Operation in gegnerischen Netzen" spricht. Da hilft es auch nicht, wenn das Verteidigungsministerium während einer Fragestunde im Bundestag versichert, dass vor jedem Einsatz bewaffneter Soldaten im Ausland das Parlament zustimmen müsse.