Cyberwarfare: Hype & Reality

Wolfgang Schwarz

Wer bei Benachrichtigungsdiensten wie News Reader ein Alert zum Stichwort „Cyberwar“ in Auftrag gibt, erhält nahezu täglich Meldungen. Und wer auf der Website der Norse Corporation, die „Internet security intelligence solutions“ anbietet, die Norse Attack Map anklickt, die global die jeweils stattfindenden Internetattacken – angeblich oder tatsächlich – in Echtzeit abbildet, sieht ein Stakkato von „Einschlägen“, das wie das virtuelle Remake einer Materialschlacht im Ersten Weltkrieg wirkt. Gleichwohl herrschen in der öffentlichen Darstellung und Wahrnehmung des als *Cyberwar* apostrophierten Phänomens Unschärfe und Unklarheit vor. Das beginnt beim Begriff *Krieg* („war“), der suggeriert, es fände ein solcher statt, mit klar auszumachenden Kombattanten, Frontlinien und Kriegszielen. Nichts davon ist der Fall. Wohl aber finden im World Wide Web feindliche Angriffe statt, die als Krieg*führung* („warfare“) interpretiert werden können, weil sie auf eine Schädigung der attackierten Seite zielen. In den seltensten Fällen konnten dabei bisher allerdings die Angreifer eindeutig identifiziert werden.

Zur Unklarheit und Unschärfe tragen auch die Medien bei, die in ihrem endlosen Run auf die nächste Headline permanent hyperventilieren und im Zweifelsfalle jede Hacker-Aktivität zum Cyberwar hochstilisieren. Hinter diesem medialen Aerosol von, gefühlt, 98 Prozent Nichtigkeiten verschwimmen zentrale Fragen wie: Was ist – im zwischenstaatlichen Bereich im Vergleich zu althergebrachter elektronischer Kampfführung – neu an Cyberwarfare? Und was droht modernen vernetzten Gesellschaften dadurch?

Die Ursprünge der elektronische Kampfführung reichen über 50 Jahre zurück, als erstmals Radar militärisch eingesetzt und sogleich auch (zunächst durch Abwerfen dünner Aluminiumstreifen) gestört wurde. Bis heute geht es im Wesentlichen um die Beeinträchtigung von Aufklärung und Kommunikation mittels Radar und Sonar. Demgegenüber zielt Cyberwarfare auf die Störung und Ausschaltung vernetzter gegnerischer hard- und softwarebasierter Steuerungssysteme, um die davon abhängenden Bereiche des Militärs (Frühwarnsysteme, Luftabwehr, U-Boot-Kommunikation usw.), der öffentlichen Infrastruktur (Energie- und

Wasserversorgung, Verkehr, Gesundheitsversorgung etc.) sowie der Wirtschaft (Finanzsektor u. a.) zu beeinträchtigen oder gänzlich lahmzulegen. In Friedenszeiten geschieht das vorrangig mittels Schadsoftware (Trojaner, Viren), in der Regel ohne Hardwareschäden. In Kriegszeiten könnte dies flächendeckend und hardwarezerstörend mittels elektromagnetischer Impulse (EMP) bewirkt werden. Die stärksten EMPs gehen von Nuklearexplosionen in größeren Höhen aus.

Die Internetanbindung gegnerischer Netze ist dabei keine Conditio sine qua non für Schädigungen durch Cyberwarfare. Urananreicherungszentrifugen des Iran wurden vor einigen Jahren durch das von den USA (möglicherweise zusammen mit Israel) entwickelte Stuxnet-Virus geschädigt oder zerstört, obwohl deren Steuerungsnetzwerk keine Verbindung zum Internet hatte. Der menschliche Faktor genügte – zum Einstöpseln eines USB-Sticks mit Schadsoftware in einen der Netzwerkcomputer. Darüber hinaus umfasst Cyberwarfare auch Aspekte wie Spionage, *defacement, social engineering* u. a. m.

Was modernen Gesellschaften mit ihrer Abhängigkeit von störungsfreien IT-Netzwerken durch Cyberwarfare droht, zeigt ein Blick auf eine Großstadt wie Berlin. Hier wird die gesamte Wasserversorgung von nur drei Leitstellen gesteuert. Ähnliches gilt für die Stromversorgung. Noch vor wenigen Jahren hätte man mindestens Umspannwerke physisch zerstören müssen, um eine längere Unterbrechung zu bewirken. Heute genügten die feindliche Übernahme oder die Ausschaltung der Steuerungscomputer via Internet. Ähnlich ließen sich der gesamte ampelgeregelte Straßen- und der Schienenverkehr sowie die Flughäfen „vom Netz nehmen". Auch die Telekommunikation wäre so zu unterbinden.

Wer meint, man solle den Teufel nicht an die Wand malen – die IT-Infrastruktur sei doch durch Firewalls geschützt, zum Teil überhaupt nicht ans Internet gekoppelt und es gäbe redundante Reservesysteme –, der hat die wiederholten Warnungen von Experten überhört, dass die Sicherheitsvorkehrungen in den zivilen Bereichen unserer Gesellschaft vielerorts, vor allem dort, wo die öffentliche Hand zuständig ist, geradezu sträflich vernachlässigt würden. Doch selbst wo das nicht so ist, ließen sich sämtliche nicht gegen EMP abgeschirmten Systeme – und das sind praktisch alle(!), einschließlich der redundanten – im Falle des Falles mit einem Male ausschalten.