sem technischem und logistischem Aufwand zurück.

Die organisierte Kriminalität ist jedoch bei weitem nicht die einzige Bedrohung im Cyberspace. Für die Nachrichtendienste ist dieser schon seit langem eine wichtige Informationsquelle für die passive Ermittlung im Kampf gegen Terrorismus und andere Bedrohungen gegen den Staat. Einige Nachrichtendienste nutzen aber auch die Möglichkeiten des Netzes, um sich aktiv unerlaubten Zugang zu Informationen zu verschaffen. Auch das ist keinesfalls ein neues Phänomen. Bereits Mitte der 80er-Jahre wurde ein spektakulärer Fall aufgedeckt, bei dem deutsche Hacker gegen Bezahlung für den KGB massenhaft in amerikanische Rechner eingedrungen waren, um sensible Daten zu entwenden. Seither wurden immer wieder Angriffe entdeckt, welche mehr oder weniger eindeutig als Tat staatlicher Akteure identifiziert werden konnten. Auch die Schweiz wurde schon Opfer solcher Angriffe. Diese Attacken werden in den Medien oft als Zeichen für den Cyberwar gewertet; allerdings handelt es sich dabei wohl eher um unerlaubten Nachrichtendienst denn um einen bewaffneten Angriff, was völkerrechtlich eindeutig unter der Kriegsschwelle liegt.

«Diese Angriffe werden immer gezielter und technisch raffinierter.»

Kosovo, Estland, Georgien, Iran

Die Frage, was ein bewaffneter Angriff im Sinne des Völkerrechts und damit eine kriegerische Handlung im Cyberspace ist, ist nicht abschliessend beantwortet. In der jungen Geschichte des Cyberspace wurden schon verschiedenste Ereignisse als erster Cyberwar betitelt. Als populärstes Beispiel gelten sicherlich die Attacken gegen Estland im Sommer 2007. Bereits 1999 war aber im Zusammenhang mit den NATO-Angriffen im Kosovo auch schon vom ersten Cyberwar gesprochen worden. Der damalige NATO-Kommandant General Wesley Clark war allerdings der Meinung, dass man in diesem Bereich noch mehr hätte tun können. Wegen der rechtlich unsicheren Situation und den schwer abzuschätzenden Folgen solcher Angriffe wurde jedoch davon abgesehen. So waren es am Ende primär die Amerikaner, die im Internet unter Angriffen zu leiden hatten. Nach dem versehentlichen Beschuss der chinesischen Botschaft wurden amerikanische Webseiten – unter anderem die des Weissen Hauses – von chinesischen Hackern angegriffen. Der angerichtete Schaden war zwar deutlich geringer als derjenige in Estland 2007, die Ereignisse sind aber durchaus vergleichbar. In beiden Fällen ist davon auszugehen, dass die jeweiligen Regierungen von China bzw. Russland wohl nicht direkt an den Angriffen beteiligt waren, diese aber zumindest geduldet haben.

Im Konflikt um Ostossetien, zwischen Russland und Georgien, kam es begleitend zum Einmarsch der russischen Truppen zu Attacken im Cyberspace. Das Timing der Angriffe deutet darauf hin, dass die Angriffe vom Kreml zumindest indirekt koordiniert wurden, auch wenn dies offiziell dementiert wird.

Bei all den genannten Angriffen normalisierte sich die Lage relativ schnell