IPG

CYBER-SICHERHEIT 15.08.2016 | Eva Jobs

Die Onlinekrieger

Wie Bundeswehr und BND sich für virtuelle Schlachten wappnen.

Laut FBI wurde die nationale Organisation der Demokratischen Partei der Vereinigten Staaten von russischen Hackern angegriffen – ist das Cyberkrieg?

Ich würde das nicht als einen Akt der Cyberkriegsführung bezeichnen. Möchte man Cyberkrieg definieren, kann man grundsätzlich die Definition eines konventionellen Krieges zugrundelegen. Es geht darum, welche Wirkung ein Angriff hat, also die physische Zerstörung von Infrastruktur und Verletzung oder Tötung von Menschen – beides ist beim Angriff auf das DNC nicht gegeben.

Die Rückverfolgbarkeit ist das Kernproblem vieler Cyberangriffe. Um den eigentlichen Ursprung der Attacke zu verstecken, geht der Angreifer gezielt über Dritt-, Viert- oder sogar Fünftstaaten. Eine Bestimmung des eigentlichen Angreifers ist so selten unmittelbar oder schnell möglich, vielmehr müssen meist aufwändige Analysen oder forensische Untersuchungen vorgenommen werden.

Bei den Akteuren ist es wichtig, Cyberkriminelle von staatlichen Akteuren zu unterscheiden. Cyberkriminelle sind vor allem ein Problem der Privatwirtschaft. Ein prominentes Beispiel für staatlichen Ressourceneinsatz ist „Stuxnet“. Dieser Computerwurm wurde für einen gezielten Angriff auf das iranische Nuklearprogramm entwickelt. Er führte dazu, dass tausende Rechner weltweit infiziert wurden, ohne dass diese einen nennenswerten Schaden nahmen. Der gewünschte Effekt entstand jedoch an den Zentrifugen zur Anreicherung von Uran in Iran. Kriminelle wären kaum in der Lage gewesen, eine solch komplexe Waffe zu konstruieren.

Der Vorbereitung ausgefeilter Cyberangriffe geht oft Geheimdienstarbeit voraus. Glauben Sie, dass Cyberkrieg eher eine Aufgabe der Geheimdienste ist und in Deutschland nicht durch die Bundeswehr ausgeführt werden sollte?

Wichtig ist der Aspekt, dass Geheimdienste zivil, militärisch oder eine Mischform aus beidem sein können. Die NSA ist ein militärischer Nachrichtendienst mit – zum Teil – zivilem Personal und arbeitet mit den anderen nachrichtendienstlichen Akteuren in den USA zusammen. Die Trennlinie ist hier also sehr unscharf. Der Bundesnachrichtendienst (BND) geht in eine ähnliche Richtung. Allerdings ist der BND ein ziviler Geheimdienst, der zu einem Teil militärisches Personal hat. Der BND verfügt derzeit nicht über die Mittel, um defensive oder offensive Maßnahmen signifikanter Größenordnung im Cyberspace durchführen zu können.

Der BND verfügt derzeit nicht über die Mittel, um defensive oder offensive Maßnahmen signifikanter Größenordnung im Cyberspace durchführen zu können.

Daher ist zu begrüßen, dass Kapazitäten bei der Bundeswehr aufgebaut werden. Allerdings ist die Bundeswehr bisher in diesem Bereich nur unzureichend aufgestellt und verfügt beispielsweise über veraltete Soft- und Hardware. Das um ein Vielfaches höhere Budget im Vergleich zum BND ermöglicht der Bundeswehr allerdings, hier in der Zukunft von Grund auf Kapazitäten in Form eines Cyberstabs aufzubauen. Das wäre im laufenden Betrieb beim BND so nicht möglich. Die Voraussetzungen sind bei der Bundeswehr daher deutlich besser.

Wie sehen Sie das Verhältnis von Bundeswehr und BND im Cyberbereich?

Vorstellbar ist, dass Mitarbeiter des BND in einzelne Cyberoperationen der Bundeswehr involviert werden. Die Manipulation von Hardware bereits im Produktionsprozess oder das Einschmuggeln eines infizierten USB-Sticks wären Szenarien, die man sich in diesem Kontext vorstellen könnte und wofür der BND die Kapazitäten und Kompetenzen hätte.

Inwiefern könnte der Aufbau von Cyberfähigkeiten mit der defensiven Ausrichtung der Bundeswehr kollidieren? Erfordert der digitale Raum nicht schnellere Reaktionen, die vom Parlamentsvorbehalt nicht gedeckt wären?

Durch den Aufbau von Cyberkapazitäten schafft man sich unweigerlich die Möglichkeit, auch offensiv zu agieren. Der Parlamentsvorbehalt ist dennoch gültig und wäre auch bei einer möglichen offensiven Attacke, die zur Zeit weder angedacht noch vorstellbar erscheint, anzuwenden. Das bedeutet: Es würden dieselben Voraussetzungen gelten wie bei einem konventionellen Einsatz.

Die vermeintliche Notwendigkeit einer schnellen Reaktion muss relativiert werden. Man kann nur schnell reagieren, wenn klar ist, wer angegriffen hat. Dies aufzuklären dauert meist sehr lange und verhindert jedwede Form von „Schnellschüssen“, auch wenn das grundsätzlich mit dem digitalen Raum assoziiert wird. Aber auch die Entwicklung einer Offensivwaffe im digitalen Raum hat eine bestimmte Vorlaufzeit. Der Parlamentsvorbehalt würde hier nicht so stark ins Gewicht fallen.

Wie würden Sie die Fähigkeiten Deutschlands im Cyberbereich im Vergleich zu anderen Nationen einschätzen? Welchen Charakter sollen die Cyberfähigkeiten Deutschlands haben?

Deutschland als Staat und somit auch die Bundeswehr wird in diesem Bereich niemals mit China oder Russland konkurrieren können oder wollen. Auch der Vergleich mit den USA, hier vor allem mit der NSA, ist schwierig.

Sinnvoll ist es dennoch, die Verteidigungsfähigkeiten zu erhöhen. Es wird Jahre dauern, bis die Bundeswehr über einen funktionalen Cyberstab verfügt, der mit der Geschwindigkeit der technologischen Entwicklung mithalten kann. Sowohl beim Neuaufbau des Cyberstabs der Bundeswehr als auch beim BND wird nur von einer defensiven Ausrichtung gesprochen. Insgesamt strebt Deutschland eine Abrüstung im Cyberspace an und sucht keinesfalls die Konfrontation mit anderen Staaten.

Ein Übergang von Cyberkrieg zu einem konventioneller Krieg ist nicht auszuschließen. Ab wann lassen sich Cyberangriffe konventionell vergelten? Kann es glaubhafte Abschreckung im Cyberspace geben?

Die bisherige Diskussion geht davon aus, dass der Übergang dort liegt, wo infrastruktureller Schaden in einer Größenordnung der Gefährdung der allgemeinen Sicherheit oder der nachhaltigen physischen Zerstörung entsteht. Ob das über digitale oder konventionelle Maßnahmen herbeigeführt wurde, ist unerheblich und wird in der weiteren Betrachtung gleich behandelt. Hier gibt es allerdings keine klaren, rechtlich bindenden Gesetze, sondern bisher nur Expertenmeinungen.

Hinsichtlich der Abschreckung lassen sich Parallelen zum konventionellen Krieg ziehen. Denn auch zu Zeiten des Kalten Krieges gab es lediglich Einschätzungen zu den tatsächlichen Fähigkeiten des Gegenübers. Man wusste damals auch nicht, wie die Antwort auf bestimmte Aktionen sein würde. Im digitalen Raum verhalten sich die Akteure ähnlich.

Die Fragen stellten Johann Ivanov und Christoph Mohr.



Eva Jobs
Berlin

Eva Jobs ist Historikerin und Doktorandin an der Philipps-Universität Marburg. In ihrer Dissertation geht sie auf die Rolle von Vertrauen in den transatlantischen nachrichtendienstlichen Beziehungen ein. Sie war u.a. für das Militärhistorische Museum der Bundeswehr und als wissenschaftliche Mitarbeiterin der unabhängigen Historikerkommission zur Erforschung der Geschichte des BND tätig.