Outsourcing des Cyberwar

Florian Rötzer 06.11.2015

Das US-Cyberkommando will für fast eine halbe Milliarde US-Dollar die offensive Cyber-Kriegsführung und die Entwicklung auch von tödlichen Cyberwaffen privatisieren

Das Wettrüsten im Cyberspace ist in vollem Gange, aber im Gegensatz zu neuen Waffen, die zwar auch geheim entwickelt, aber dann doch gerne mal bei Paraden, Manövern oder Kriegseinsätzen vorgeführt werden, findet alles bislang im Geheimen statt.

Einen kleinen Einblick bietet nun eine stattliche Ausschreibung[1] des US Cyber Command (USCYBERCOM) von fast einer halben Milliarde US-Dollar. Die Cyberstreitkraft wurde 2010 gegründet, wird vom Direktor des Geheimdienstes NSA geleitet, ist dem CentCom unterstellt und besitzt noch nicht den gleichen Rang wie die anderen vier Streitkräfte, genießt aber derzeit sicherheitspolitische Priorität. Das Cyber Command soll die Netzwerke des Pentagon vor Cyberangriffen schützen, Angriffe mit offensiven Mitteln in einem Cyberwar ausführen und die anderen Teilstreitkräfte bei der netzwerkzentrierten Kriegsführung stützen. Derzeit wird das Kommando noch aufgebaut, Tausende von Cybersoldaten sollen noch eingestellt werden, aber es gibt offenbar Probleme, genügend Interessierte bzw. Geeignete zu finden.

Wie es in der Ausschreibung der Einsatzleitung (J3) heißt, werden defensive und offensive Ziele verfolgt. Derzeit wird J3 unterteilt in Aktuelle und Zukünftige Einsätze. Letztlich sollen mit einem Auftrag in Höhe von 460 Millionen US-Dollar entscheidende Aufgaben outgesourct und überhaupt eine konsistente Strategie ausgearbeitet werden. Chancen dürften nur große Rüstungskonzerne wie Raytheon, Northrop Grumman oder Lockheed Martin haben. Alles Genauere steht natürlich unter höchster Geheimhaltung.

Insbesondere geht es um die Planung von "cyber fires" und die Bewertung von "cyberspace joint munitions", also um Cyberwaffen, die nach ehemaligen Pentagon-Mitarbeitern und dem neuen Law of War Manual, wie Nextgov.com berichtet[2], auch in Verbindung mit kinetischen Waffen zerstören oder töten können sollen. Man muss also die Waffen und die Munition koordinieren, um die beste oder die gewünschte Wirkung auf den Gegner auszuüben, indem beispielsweise mit einem Cyberangriff das gegnerische Luftabwehrsystem digital manipuliert oder durch einen Zusammenbruch des Stromnetzes lahmgelegt wird, um sicher eigene Flugzeuge fliegen lassen zu können.

Cyberwaffen und das Kriegsrecht nach dem Pentagon

Klar jedenfalls ist, dass Cyberwaffen genauso wie anderen Waffen dazu dienen sollen, töten zu können. Im Law of War Manual[3] (Juni 2015) sind den Cyberoperationen ein eigenes Kapitel gewidmet, auch wenn gesagt wird, dass bislang das Kriegsrecht hier noch in den Anfängen steht. Argumentiert wird, dass Cyberangriffe je nach Art des Angriffs und unabhängig von der Art der eingesetzten Waffen beurteilt werden müsse, allerdings könne es auch Angriffe geben, die keine Parallele zu Angriffen mit kinetischen Waffen haben: "Cyber operations may be subject to a variety of law of war rules depending on the rule and the nature of the cyber operation. For example, if the physical consequences of a cyber attack constitute the kind of physical damage that would be caused by dropping a bomb or firing a missile, that cyber attack would equally be subject to the same rules that apply to attacks using bombs or missiles."

Als Kriegshandlungen würden etwa auch Cyberangriffe gelten, die eine Kernschmelze in einem Atomreaktor auslösen, einen Staudamm über einem bewohnten Gebiet öffnen oder Luftkontrollsysteme stören, die zu Abstürzen von Flugzeugen dienen. Die Beispiele weisen auch darauf hin, was geplant werden könnte. Betont wird hier auch, dass die USA sich das Recht auf Selbstverteidigung in Anspruch nehmen wird, auf einen Cyberangriff, der "Gewalt" anwendet, wie

auf einen anderen Angriff auf das Land zu reagieren, also mit kinetischen Waffen bis hin zu Atomwaffen zurückzuschlagen.

Offiziell sei damit seitens des Pentagon legalisiert, dass Cyberwaffen auch direkt oder indirekt töten können, es kommt halt nur darauf an, ob der Einsatz nach dem Kriegsrecht gerechtfertigt ist oder nicht. So sei das nicht spezifische Verbreiten eines Computervirus nicht legitim, weil hier nicht zwischen militärischen Zielen und zivilen Objekten oder Zivilisten unterschieden wird. Nach Charles Dunlap, Direktor des Center on Law, Ethics and National Security der Duke University, sind Cyberangriffe auch dann nach dem Kriegsrecht erlaubt, "wenn Menschen dabei getötet oder verletzt werden, sofern der vorhersehbare Kollateralschaden nicht im Verhältnis zum erwarteten militärischen Gewinn exzessiv ist". Für Cyberwaffen würden dieselben Regeln wie für Bomben oder Patronen gelten. Eine Malware könne etwa ein militärisches System zerstören, aber auch in Fortsetzung ein ziviles, wenn es sich unvorhergesehen ausbreitet. Das war auch bei **Stuxnet**[1] der Fall.

Wie auch immer das Kriegsrecht beurteilt wird, so wird offenbar und wenig erstaunlich im Pentagon daran gedacht, Cyberwaffen zu entwickeln, die eben tödliche Folgen haben können. Das eben ist auch mit "cyber joint munitions" gemeint. CyberCom-Sprecherin Kara Soules wollte gegenüber Nextgov zwar nicht sonderlich präzise werden, aber erläuterte, es gehe dabei um die Beurteilung des Erfolgs einer Waffe gegenüber einem Ziel. "Cyber fires" habe eine breitere Bedeutung und könne "für offensive und defensive Ziele benutzt und so gestaltet werden, dass sie Effekte im und durch den Cyberspace schaffen". Das ist ziemlich dunkel, lässt aber alles offen.

Noch freilich ist völlig offen, was ein entfesselter Cyberwar mit den unbekannten Waffenarsenalen, die die hochgerüsteten Staaten besitzen - nach den USA gehören zu den hochgerüsteten Cyberwarstaaten außer sie selbst Russland, China, Israel, Iran und Nordkorea, Europa kann man offenbar vergessen -, an Folgen haben wird. In den USA glaubt man daran, dass das Cyberkommando auch im Cyberspace Präzisionsangriffe führen wird, während die Gefahr bestünde, dass die Gegner keine Rücksicht auf Kollateralschäden nehmen. Aber man kann natürlich auch mit dem Konzept eines sauberen Kriegs schnell mal Kriege führen.

Von Florian Rötzer gerade zum Thema Stadt erschienen: Smart Cities im Cyberwar[4].

---

[1] **Stuxnet** ist ein Computerwurm, der im Juni 2010 entdeckt und zuerst unter dem Namen RootkitTmphider beschrieben wurde.[T 1] Das **Schadprogramm** wurde speziell zum Angriff auf ein System zur Überwachung und Steuerung (SCADA-System) der Firma Siemens – die Simatic S7 – entwickelt. Dabei wurde in die Steuerung von Frequenzumrichtern der Hersteller Vacon aus Finnland und Fararo Paya in Teheran eingegriffen. Frequenzumrichter dienen beispielsweise dazu, die Geschwindigkeit von Motoren zu steuern.

Solche Steuerungen werden vielfach in Industrieanlagen wie Wasserwerken, Klimatechnik, Pipelines usw. eingesetzt. [T 2]

Da bis Ende September 2010 der **Iran** den g**rößten Anteil der infizierten Computer besaß**[T 3] und es zu außerplanmäßigen Störungen im iranischen Atomprogramm kam, lag es nah, dass Stuxnet hauptsächlich entstand, um die Leittechnik der Urananreicherungsanlage in Natanz[1] oder des Kernkraftwerks Buschehr[2] zu stören.

Die hochversierte Programmierer-Gruppe und Auftraggeber sind unbekannt.[T 4] Jedoch gab das US-Justizministerium im Juni 2013 bekannt, dass es Ermittlungen gegen den ehemals zweithöchsten Offizier der USA und späteren Stuxnet-Projektleiter General James E. Cartwright einleitete.[3] Die Behörde vermutet, dass Cartwright im Jahr 2010 Details zu Stuxnet an die New York Times weitergab, was mutmaßlich zur Enttarnung des 50 Millionen Dollar teuren Sabotage-Programms führte.[4]

Anhang

Links
[1]

https://www.fbo.gov/utils/view?id=185ca85709407f796ae81cb348f167bb
[2]

http://www.nextgov.com/cybersecurity/2015/11/lethal-virtual-weapons-real/123417/
[3]

http://www.dod.mil/dodgc/images/law_war_manual15.pdf
[4]

http://www.westendverlag.de/buecher-themen/programm/florian-roetzer-smart-cities-im-cyberwar.html#.Vemzx5fpX6t