Cyberwar & Cyber Defence

Vorbereiten auf die Auseinandersetzung der Zukunft

(BS/Bert Weingarten) Auf der Suche nach einer Definition des Begriffs "Cyberwar" muss man feststellen, dass es weltweit mindestens 840 unterschiedliche Ansätze gibt, um diesen Begriff zu erklären. Diese lassen sich grob in drei Informationslagen gruppieren. Die erste Informationslage beinhaltete Cybercrime Elemente und die Auffassung, ein Cyberangriff wäre einem Cyberwar gleichzusetzen. Die zweite Informationslage beinhaltete die Meinung, einzelne Personen könnten einen Cyberwar führen und die dritte Informationslage vermischte virtuelle und physische Angriffsformen. Die bestehenden Einschätzungen und Meinungen in allen drei Informationslagen sind jedoch nicht zielführend und eine Klassifizierung zur Schwere eines Cyberwars fehlte gänzlich.

Um "Cyberwar" zu definieren, musste als erstes festgestellt werden, was ein Cyberwar definitiv nicht beinhaltet. Hierzu gehören Cybercrime Aktivitäten, die sich direkt gegen Privatnutzer oder Unternehmen richten. Die Historie der multiplen Cybercrime Technologien begann 1990 und erreicht 2010 eine weitere Evolutionsstufe mit der Verbreitung von virtuellen Systemen zur vereinfachten Teilnahme an Cybercrime Netzwerken. Materielle Angriffe, also das Zerstören und die Sabotage von Hardware (z. B. Kabel-, Antennen- und Satellitenverbindungen) sind ebenfalls keine Bestandteile eines Cyberwars solange die Zerstörung oder die Sabotage physisch ausgeführt wird, wie z.B. durch das physische Ausschalten einer Hardwareeinheit, einen Raketenangriff auf eine Vermittlungsstelle oder den Abschuss eines Kommunikationssatelliten.

Davon ausgehend definieren eine Reihe von Wissenschaftlern den Kosovo-Krieg 1999 als den ersten Cyberwar zwischen Staaten, in dem beide Seiten entsprechende Kampfmittel einsetzten. Auch die umfassende Steuerung und Kontrolle des Kriegsgeschehens mittels weltraumgestützter Systeme trat auf NATO-Seite bestimmend hervor, stellt jedoch keine Komponente eines Cyberwars dar, da die eingesetzten Satelliten maßgeblich zur Aufklärung der Lage eingesetzt wurden und nicht zur Manipulation oder Übernahme feindlicher Waffensysteme.

Die Ereignisse in Estland im Jahre 2007 waren beispielhaft für einen erfolgreichen Cyberangriff. Durch konzertierte "Denial of Service"-Angriffe waren Regierungs- und Verwaltungsstellen, ebenso wie die größte Bank Estlands nicht mehr online zu erreichen. Obwohl sich der Angriff auf Krankenhäuser, Energieversorgungssysteme und Notrufnummern in Estland auswirkte, ist der Angriff dem Cybercrime zuzuordnen, da kein Staat nachweislich den Angriff durchführte, sondern allenfalls die Tätigkeit einiger Hacker aus falsch verstandenem Patriotismus duldete.

Cyberwar ist eine Kriegsform zwischen Staaten und/oder "Asymmetric threats", die Cybersoldaten ermöglicht, virtuelle Angriffe gegen Prozessoren, Computer, Systeme oder Netzwerke auszuüben.

Die erste Stufe eines Cyberwars beinhaltet die Ausforschung und die Begrenzung von Zielressourcen. Hierzu gehören beispielsweise der Einsatz von automatisierten Sniffern, Scans und Denial of Service-Angriffe, um Zieldienste zu unterdrücken oder zu stören.

Die zweite Stufe beinhaltet die Infiltration und Manipulation von Daten und Datenverbindungen. Hierzu gehören Beispielsweise Hijacking Sessions, der Einsatz von Trojanern, Würmern und Botnetzen, um zum Zwecke der Informationsgewinnung in fremde Computernetzwerke einzudringen.

Die dritte Stufe beinhaltet die virtuelle Manipulation zur physikalischen Zerstörung von Zielressourcen und Einheiten. Hierzu gehört Beispielsweise die Übernahme oder Zerstörung von zuvor manipulierter Hard- oder Software, von kritischen Infrastrukturanlagen der Energie, Wasser und Informationstechnologie sowie "Manipulated friendly fire" also die virtuelle Manipulation von Freund/Feind-Kennungen, bzw. die virtuelle Manipulation von Zieltechnologie oder Waffen zur Übernahme oder Vernichtung von Zieleinheiten.

Es bleibt festzustellen, dass sich bislang kein Cyberwar ereignet hat.

Doch eine Vielzahl von Ereignissen der Jahre 2007 bis 2009 erlauben Rückschlüsse auf den Entwicklungsstand und die Weiterentwicklung von Waffen hin zu "Advanced Cyberwar Weapons". So begann die Evolution der Cyberwar Waffen mit der Grundlagenforschung im Jahre 1994 durch das Referat "Information Warfare and Strategy" in den USA. Schon seit den neunziger Jahren arbeiteten Staaten an digitaler Kriegsführung. So kann die erfolgte Aufrüstung und Weiterentwicklung von "Advanced Cyberwar Weapons" in China und den USA seit dem Jahr 2007 als Beginn des "Cold Cyberwar" bezeichnet werden.

Hans-Joachim Otto, Staatssekretär im Bundeswirtschaftsministerium, lässt sich auf der 8. Berliner Sicherheitskonferenz von Bert Weingarten, CEO der PAN AMP AG, die Produkte des Hamburger Unternehmens erläutern.

Foto: BS/Dombrowsky

Es ist davon auszugehen, dass 60 Prozent aller Staaten bis 2014 zumindest eine "Basic-Level" Waffe für den Einsatz im Cyberwar besitzen. Hierdurch wird ein zukünftiger Cyberwar zu einer signifikanten Bedrohung Europas, da heutzutage Staaten und "Asymmetric threats" auch in kürzester Zeit in der Lage sind, Systeme zur Ausführung von Cyber-Attacken zu erwerben. Durch die geringen Entwicklungskosten für Basis-Waffen zur Durchführung eines Online-Angriffes, die sich auf 50.000 bis 100.000 Euro beziffern lassen, sind insbesondere asymmetrische Auseinandersetzungen im Netz vorprogrammiert und finden zwischen der terroristischen Vereinigung Al-Qaida und westlichen Staaten bereits statt.

Insbesondere der Missbrauch des Internets für einen Cyber-Angriff stellt ein hohes Risiko da, da mit Lichtgeschwindigkeit jedes mit dem Internet verbundenen Zielsystems getroffen werden kann. Die hierzu berechnete Vorwarnzeit liegt bei unter zwei Sekunden.

In einer Zeit, in der die tägliche Onlineaktivität eine Selbstverständlichkeit darstellt und die Nutzung von E-Commerce, Online-Banking und Social Networks zum Tagesablauf gehören, wird der tatsächliche Wert und der hohe Nutzen von Daten, Informationen und intakten Netzwerken aller Voraussicht nach erst durch einen Konfliktfall bewusst. Kommt es zu einem Cyberwar, dass heißt zu einem Krieg zwischen Staaten über das Internet, würde dieser letztlich alle miteinander vernetzten Staaten treffen und gravierende politische sowie vor allem ökonomischen Schaden anrichten. Ein internationales Abkommen zur Begrenzung von Cyberwar Waffen ist bereits heute notwendig und sollte dringend von den Vereinten Nationen aufgenommen werden.

Insbesondere unter der Kenntnis der bestehenden Backbone-Netze, die insbesondere Europa und die USA datentechnisch verbinden, gleichen die Internetverbindungen in den USA und Europa "einer Burg mit mehr als 500 Toren". Wenn alle Tore attackiert werden, müssen auch alle verteidigt werden und je mehr Infrastruktur beschädigt wird, desto mehr werden sich die Angriffe auf die vorhandenen und intakten Ressourcen der Teilnetze verteilen und diese im Falle eines Cyberwars belasten. Wenn somit die USA per Cyberwar angegriffen werden, ist damit zu rechnen, dass auch Europäische Teilnetze des Internets tangiert werden. Als Folge von immensen Überlastungen können auch verschlüsselte Verbindungen, die beispielsweise zwischen militärische Einrichtungen im Internet bestehen, zusammenbrechen. Was in militärischen Kreisen als eine gut zu verteidigende Anhöhe gilt, stellt die Netzstruktur Saudi-Arabiens für den Fall eines Cyberwars dar. Anders als in den meisten Staaten haben die Saudis die Möglichkeit, die Internet-Backbones in ihrem Land direkt zu administrieren, in der Kapazität zu begrenzen oder abzuschalten. Gleiches gilt für verschiedene Teilnetze im Land. Damit hält die Regierung ein wirkungsvolles Instrument in der Hand, mit dem sich im Krisenfall eines Cyberwars Schaden begrenzen lässt und nationale Teilnetze nur geringfügig beeinflusst werden.

Als logische Konsequenz der Möglichkeit eines künftigen Cyberwars ist es daher dringend erforderlich, eine Europäische bzw. Nato-Strategie zur militärischen Verteidigung des virtuellen Raums der Mitgliedsstaaten aufzubauen. Jeder Mitgliedsstaat sollte sich zudem in Form einer institutionalisierten staatlichen Verteidigung, die sich mit entsprechenden Mitteln auf die Möglichkeit eines Krieges per Internet vorbereitet, für einen kommenden Cyberwar rüsten. Der Ausbau von eigenständiger, militärischer Infrastruktur und die Absicherung nationaler Teilnetze sollten im Fall eines Cyberwars abgeschlossen sein, damit eine effektive Verteidigung erfolgen kann.

Jeder Krieg wird zukünftig mit einem Angriff aus dem Cyberspace beginnen und effektive Gegenmaßnahmen im Cyberwar werden vorbereiteten Staaten vorbehalten sein.

Offensiv in den Wettbewerb

Aufholjagd um die Endgeräte der BOS hat begonnen

(BS/leh) Die Digitalfunk-Entscheidung der deutschen BOS für die Infrastruktur der EADS hat bei Motorola nicht nur Enttäuschungen ausgelöst, sondern auch die ein oder andere organisatorische und personelle Maßnahme nach sich gezogen. Das ist aber schon eine Weile her. Es war anzunehmen, dass die Phase der Resignation schnell überwunden werden kann, das Unternehmen sich seiner tatsächlichen Stärken besinnt und voll konzentriert in den Wettbewerb um die Endgeräte der BOS eingreift.

Obwohl Funkgeräte von Motorola seit Jahrzehnten als eine Klasse für sich gelten und häufig als die Porsches oder Ferraris der Endgeräte bezeichnet werden, geschah jedoch zunächst nichts. Der Wettbewerb zog an Motorola vorbei und gewann eine Ausschreibung nach der anderen. Lediglich in Berlin und Sachsen konnte Motorola kleinere Margen für sich entscheiden. Befasst man sich mit den Ursachen dieser unerwarteten Entwicklung, könnten aus der Sicht eines Außenstehenden folgende Gründe ursächlich sein:

Motorola richtet seine Entwicklungen am Weltmarkt aus und negiert nicht selten individuelle Kundenwünsche (Motorola weiß, was Kunden brauchen).

Motorola ist ein großes Dampfschiff mit vielen Unter-, Zwischen- und Oberdecks und kann im Gegensatz zu Unternehmen, deren Portfolio ausschließlich auf Endgeräteentwicklung und Endgeräteproduktion ausgerichtet ist, oft nicht schnell und flexibel genug auf Kundenwünsche reagieren (Wettkampf zwischen Dampfschiff und Sportboot).

Im Endgerätemarkt hat Motorola die eigene Stärke (wir sind wer) überschätzt und die der Mitbewerber unterschätzt (wer ist das schon).

Vertriebskonzept und Vertrieb werfen Fragen zur Kontinuität, Homogenität und Professionalität auf.

Nun aber scheint alles anders und vor allem besser zu werden. Von September bis Mitte November war Motorola mit einem großen Truck auf einer deutschlandweiten Roadshow unterwegs. An Bord des Trucks zeigte man in mehr als 25 Städten die neuesten Produkte und Lösungen und demonstrierte Kundennähe und vor allem eine produktbezogene Kundenorientierung. Ein neuer Vertriebschef wurde installiert, um die Dinge zu ordnen und zu richten. Beim Branchentreff für Professionellen Mobilfunk und Leitstellen in Köln war Motorola nach Jahren der Abwesenheit erstmals wieder selbst und gleich mit der größten Standfläche auf der PMRExpo 2009 präsent. Neben zahlreichen Entwicklungen und Lösungen des Unternehmens fand insbesondere das neue eigens für die speziellen sicherheitskritischen Anforderungen der deutschen BOS entwickelte Funkgerät MTP850 reges Interesse und Zuspruch. Das Gerät, das erstmals im Mai auf dem TETRA World Congress 2009 in München vorgestellt wurde, verfügt über eine FMS-Status-Applikation, mit der taktische Kurzinformationen zum Aufenthalt von Einsatzkräften oder Einsatzfahrzeugen automatisch und ohne verbale Kommunikation an die Leitstelle übermittelt werden. Darüber hinaus versendet das FuG MTP850 eine akustische/verbale Quittung durch Drücken der Sendetaste – ein Leistungsmerkmal, das sich schon im Analogfunk als effizient und effektiv bewährt hat. Das Gerät verfügt zudem über eine eingebaute Totmann-Alarmschaltung. Außerdem bietet das FuG MTP850 zahlreiche weitere Vorteile, die zu mehr Effizienz beitragen. Ein neuer und belastbarer 12-PIN-BOS-Zubehöranschluss stellt sicher, dass Zubehörteile jederzeit zuverlässig mit dem FuG MTP850 verbunden sind. Das Gerät verfügt über eine Sendeleistung gemäß ETSI Klasse 3L (1,8W) und eine erhöhte Empfängerempfindlichkeit. Damit sorgt das Gerät speziell im Direkt-Modus für eine verbesserte Reichweite und Durchdringung, sowohl innerhalb von Gebäuden wie auch in stark bebauten Gebieten. Die zertifizierte Ende-zu-Ende-Verschlüsselung mit SIM-Karte gemäß BSI-Anforderung sorgt für eine sichere Übertragung von Sprache und Daten und den direkten Zugriff auf Datenbanken durch einen integrierten WAP-Browser, sofern dieser Dienst von der TETRA-Infrastruktur zur Verfügung gestellt wird.

Erste konkrete Erfolge nach der neuen Ausrichtung von Motorola zeichnen sich am Horizont ab. Der Freistaat Thüringen bestätigte die Bestellung von mehr als 5.000 TETRA-Digitalfunkgeräten inklusive Zubehör und Serviceleistungen. Im Einzelnen umfasst der Auftrag die Lieferung von über 2.000 Mobilfunkgeräten CM 5000 und MTM 800E sowie erstmals die Auslieferung von mehr als 3.000 Handfunkgeräten des Typs MTP850.

Partner im Nahen Osten

Beziehungen zwischen Deutschland und Israel

(BS) Seit der Gründung des Staates Israel haben sich die Handelsbeziehungen zu Europa und besonders Deutschland immer weiter vertieft. Gleichzeitig gilt Israel als einer der Garanten für wirtschaftliche Stabilität im Nahen Osten. Seit drei Monaten ist nun Inon Elroy der Direktor des Israel Trade Center an der israelischen Botschaft in Berlin. Der Behörden Spiegel befragte ihn zu dem aktuellen Stand der Handelsbeziehungen sowie zur unterschiedlichen Arbeitsweise und Beschaffenheit der jeweiligen Industrien. Das Interview führte der Chefredakteur des Behörden Spiegel, R. Uwe Proll.

Behörden Spiegel: *Was sind die Schwerpunktaufgaben des Trade Center of Israel?*

Elroy: Unsere Aufgaben ergeben sich aus unserer Struktur. So sind wir einerseits dem israelischen Ministerium für Industrie, Handel und Arbeit und andererseits direkt der Botschaft – und damit dem Außenministerium – unterstellt. Wir sehen uns entsprechend als die Augen und Ohren der israelischen Industrie in Deutschland. Wir sind dicht am deutschen Markt, verfolgen die Neuigkeiten und können dadurch unserer Industrie Möglichkeiten zur Beteiligung aufzeigen. Gleichzeitig öffnen wir den Industrievertretern Türen und bieten ihnen Kontakte, über die ein israelisches Unternehmen so nicht verfügen würde.

Behörden Spiegel: *Israelische Firmen wenden sich also über Sie an den deutschen Markt?*

Elroy: Zumindest die kleineren. Wir haben natürlich auch Global Player, die ihre eigenen Kontakte und Beziehungen nutzen. Aber wir bieten allen Firmen, deutschen sowie israelischen, unsere Dienste an.

Behörden Spiegel: *Bevor Sie nach Deutschland kamen waren Sie in Frankreich akkreditiert. Gibt es Unterschiede zwischen diesen beiden Märkten?*

Elroy: Die Aufgaben unseres Büros in Deutschland stellen eine größere Herausforderung als in Frankreich dar. Zum einen ist die Landschaft in Deutschland von dezentralen Strukturen geprägt. Dies erfordert einen Austausch mit vielen verschiedenen Partnern aus verschiedenen Regionen. Ein weiterer Aspekt ist der höhere Industrialisierungsgrad Deutschlands, das vor allem auch ein höheres Potential und Forschungskooperationen bietet. Deutschland ist auch ein Zentrum internationaler Leitmessen. Diese Tatsache erhöht das Interesse israelischer Unternehmen an Deutschland und dementsprechend die Inanspruchnahme unserer Dienstleistung.

Behörden Spiegel: *Wenn wir schon von den Märkten sprechen, welche Auswirkungen hatte die Finanzkrise auf Israel?*

Elroy: Die Auswirkungen auf die israelische Wirtschaft spiegeln sich besonders in der Abwertung des Dollars und dem Nachfragerückgang der Exportmärkte wieder. Israelische Unternehmen haben in den letzten Jahren verstärkt in Immobilien investiert. Der Einbruch auf den Immobilienmärkten hat auch diese Unternehmen getroffen und die Geldbeschaffung sowie Tilgung erschwert.

Behörden Spiegel: *Im Gegensatz zu Deutschland kann Israel allerdings kaum auf einem inländischen Markt setzen. Es ist einfach zu klein. Hat diese Exportabhängigkeit gerade in der heutigen Situation Auswirkungen?*

Elroy: Deutschland ist die dominierende Exportnation in Europa. Allerdings haben israelische Firmen tatsächlich eine andere Grundeinstellung als deutsche. Unsere Unternehmen wollen von Anfang an auf den internationalen Markt, da sie wissen, dass das Geld nicht in der Heimat liegt. Der weltweite Nachfragerückgang hat natürlich Auswirkungen auf den israelischen Arbeitsmarkt.

Behörden Spiegel: *Es wird dabei viel von einer Zusammenarbeit zwischen Lehre und Industrie in Israel gesprochen. Wie eng sind die Verknüpfungen?*

Elroy: Es existiert ein reger Austausch zwischen Forschung und Industrie. Zusätzlich fördert der Staat den „Kno-How" Transfer durch den Einsatz verschiedener Instrumente und Programme. Dies ist notwendig, bei einem Land mit der weltweit größten Relation von Wissenschaftlern per Einwohner. Viele Hochschulen haben eigene Technologietransfergesellschaften gegründet, die potentiell erfolgreiche Projekte noch vor der Patentanmeldung prüfen. Die Anmeldung von Patenten ist mittlerweile fast zu einer eigenen Industrie in Israel geworden. In anderen Fällen gehen die Unternehmen gezielt auf Forscher zu, damit diese ihre Anstrengungen in eine bestimmte Richtung legen – eine Richtung die natürlich für die Firma interessant werden könnte.

Behörden Spiegel: *Welche israelischen Branchen sind Ihrer Ansicht nach besonders für Deutschland von Interesse?*

Elroy: Israel ist ein technologieorientiertes Land mit Schwerpunkten im Bereich Telekommunikation, IT, Naturwissenschaften und der Automobilindustrie. Besonders hervorzuheben ist auch der gesamte Bereich der Sicherheitstechnologien, etwa die Grenz- und Flughafensicherheit. Unsere Produkte werden besonders vom so genannten Homeland-Security-Markt beschafft. Aber auch im Bereich E-Health ist Israel weit voraus. Wenn man etwa die politische Diskussion um die elektronische Gesundheitskarte betrachtet, dann will Deutschland dieses Projekt vorerst aussetzen, um die Debatte dann erneut zu beginnen. In Israel sind wir da schon weiter und können dann in zwei Jahren mit konkreten Erfahrungen aufwarten.

Behörden Spiegel: *Welche Rolle spielt der deutsche Markt dabei für Israel?*

Elroy: Deutschland ist nach den USA und China der drittgrößte Exportpartner und unser wichtigster Handelpartner in der Europäischen Union. Vorteilhaft für den Handel ist, dass Isarael sowohl mit der EU als auch mit Deutschland Handelsverträge geschlossen hat, so dass beispielsweise keine doppelte Besteuerung stattfindet. Aber auch wir sind für Deutschland nach Saudi-Arabien der wichtigste Haupthandelpartner im Nahen Osten. Wobei man bedenken muß, dass Saudi-Arabien vor allen Dingen Öl und Benzin exportiert, während Israel über keine nennenswerten Rohstoffe verfügt. Von daher würde ich die industrielle Kooperation zwischen Deutschland und Israel schon als bedeutend empfinden.

S036_BS01_Allg_Schulz