„Ächtung Digitaler Waffen"

Ein Beitrag für Peira e.V. von Angelika Beer, MdL Piratenfraktion Schleswig-Holstein, Berlin, 28. Juni 2015, es gilt das gesprochene Wort.

Rückblick und Ausblick - Wie komme ich zu diesem Thema:

- Anti Atom Bewegung – gegen Atomwaffen
- Nach dem 2. Golfkrieg der Giftgasangriff auf die Kurden in Halabjah
- Entminungsprogramm Hilfsorganisationen wie Medico International im Grenzgebiet Irak/Iran
- Initiierung der internationalen Kampagne gegen Landminen
- Egal ob als NGO, MdB oder MdEP für radikale Abrüstung und Ächtung aller Massenvernichtungswaffen
- Bis 2013 Vorsitzende des internationalen parlamentarischen Netzwerkes für Konfliktprävention des EWI
- EWI als Mittler zwischen den Supermächten zu Zeiten des Kalten Krieges und eine der ersten, die sich um die Dimension des Cyber Wars gekümmert haben. Für die Menschen ist das viel zu weit weg – deshalb rede ich über Digitale Waffen.
- Für die Piraten sehe ich hier eine besondere Verantwortung: Die digitale Revolution hat Chancen und Risiken. Wir müssen den Wandel vom „Beherrscher des Digitalen" zum Partner des Menschen vollziehen. Bislang profitieren fast ausschließlich die Globalisierer von der DR. Die rasante Geschwindigkeit mach den Menschen Angst. Sie schauen lieber weg, scheuen die Risiken und vergeben so die Chancen. Unsere Herausforderung besteht heute darin, die DR zum Nutzen der Menschen umzuwandeln, und den Risiken entschieden entgegenzutreten.
- Inzwischen haben alle möglichen Institutionen eine Digitale Agenda, die Bundesregierung, die EU… Und alle reden über Cyber Attacken …
- Die Krisen und Kriege nehmen rasant zu, Flüchtlingsströme werden abgewehrt, manch einer sieht angesichts des Konfliktes mit Russland und der Ukraine von der Rückkehr des Kalten Krieges. Die Möglichkeiten eines Krieges mit digitalen Waffen erscheint nachrangig. Das ist fahrlässig. Ich streite heute für eine Regelung in der Charta der Vereinten Nationen zur Ächtung Digitaler Waffen.

- Ich selbst bin weder Völkerrechtler, noch der typische Pirat, also kein Nerd. Deswegen freue ich mich über die Einladung von Peira, heute darüber zu diskutieren und Ideen und Initiativen zu suchen.

D-Waffen – Snowden hat uns mehre Aufgaben mit auf den Weg gegeben

Der Whistleblower Edward Snowden hat uns Menschen vor große Aufgaben gestellt. Die erste war: Wir mussten begreifen, dass die Geheimdienste dieser Welt alles sehen, alles hören, alles speichern wollen. Die USA und ihre Partner-Geheimdienste greifen deswegen jeden Tag die Privatsphäre von Menschen an. Darauf gehe ich später noch ein.

Snowden-Dokumente zeigen nun, dass die Vereinigten Staaten schon 2002 eine NSA-Einheit aufgebaut haben, die auf Attacken gegen die Systeme anderer Länder spezialisiert ist. Deswegen hat Snowden uns Menschen eine zweite Aufgabe gegeben. „Wir müssen einen neuen internationalen Verhaltenskodex schaffen". Er fordert eine D-Waffen-Konvention - in der Tradition der Konventionen gegen atomare, biologische und chemische Waffen (ABC-Waffen).

Digitale Waffen – Krieg im Internet

Cyberkrieg ist in den Köpfen der Menschen zu sehr Weltraum, macht also nicht betroffen. Daher wähle ich als Begriffe: digitale Waffen, bzw. Krieg im Internet. Mein Ziel ist es, persönliche Betroffenheit bei jedem Bürger zu entwickeln und eine klare Sprachregelung zu erreichen. Schließlich ist die gesamte kritische zivile Infrastruktur online, von den Arbeitsabläufen in Krankenhäusern bis zu den Flugleitsystemen für Passagiermaschinen. Nicht zu vergessen: Diese kritische Infrastruktur ist nicht durch internationale Normen oder Abkommen geschützt! Dazu kommt verstärkend die Erkenntnis, dass oft niemand weiß, woher der Angriff kommt und wer hinter der Offensive steckt. (siehe den Hacker Angriff auf den Deutscher Bundestag)

D-Waffen definieren sich nach der Wirkung / der Absicht /der Folgen

Beispiel: **Hammer**

Der Hammer ist ein Arbeitsgerät und ist nicht zu verbieten, wenn er sachgerecht eingesetzt wird. Wird mit dem Hammer aber ein Mord oder Totschlag durchgeführt, wird der Hammer eine Waffe. Es ist also schlechterdings unmöglich, alles zu verbieten, weil es als Waffe genutzt werden könnte.

Das gilt auch für D-Waffen. Ich werde versuchen, der UN Charta folgend, festzustellen, wann ein Virus eine D-Waffe ist/ sein kann. Denn ein Verbot bestimmter Programme löst dieses Dilemma nicht auf, insbesondere unter Berücksichtigung der ständigen Neu- und Weiterentwicklungen.

Art 2(4) UN Charta lautet derzeit:

„Alle Mitglieder unterlassen in ihren internationalen Beziehungen jede gegen die territoriale Unversehrtheit oder die politische Unabhängigkeit eines Staates gerichtete oder sonst mit den Zielen der Vereinten Nationen unvereinbare Androhung oder Anwendung von Gewalt."

Zur Einordnung und Bewertung wähle ich den Wirkungs- oder Folgen orientierten Ansatz (Folgentheorie) Zunächst gilt hier es bei der Einordnung eines Angriffs mit D-Waffen als bewaffneten Angriff auf die Wirkungen und Folgen der Maßnahme zu sehen. Es geht also um die Tötung von Menschen und ganz erhebliche Schäden im betroffenen Land. Insoweit könnte ein Angriff im Internet dann unter den Gewaltbegriff von Art. 2(4) UN-Charta. subsumiert werden, wenn sich seine Wirkungen so darstellen wie bei einem Angriff, der mit klassischen militärischen Waffen durchgeführt wird.

Dann müsste der Art. 2 (4) etwa wie folgt ergänzt werden: „Ein Angriff, der speziell auf die unmittelbare physische Beschädigung materiellen Vermögens bzw. auf die Verletzung oder Tötung von Menschen abzielt, entspricht der Anwendung von Waffengewalt und wird von dem Gewaltverbot erfasst." Unter den Vertretern dieses Ansatzes ist hingegen umstritten, ob demgegenüber Cyberangriffe, die lediglich rein wirtschaftliche oder politische Folgen haben, aus dem Anwendungsbereich des Art. 2(4) UN-Charta herausfallen.

Das **Recht zur Selbstverteidigung** ist in Artikel 51 der Charta der Vereinten Nationen festgelegt und gibt jedem Mitgliedstaat das Selbstverteidigungsrecht gegen einen bewaffneten Angriff, den Art. 2(4) beschreibt.

„Diese Charta beeinträchtigt im Falle eines bewaffneten Angriffs gegen ein Mitglied der Vereinten Nationen keineswegs das naturgegebene Recht zur individuellen oder kollektiven Selbstverteidigung, bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat. Maßnahmen, die ein Mitglied in Ausübung dieses Selbstverteidigungsrechts trifft, sind dem Sicherheitsrat sofort anzuzeigen; sie berühren in keiner Weise dessen auf dieser Charta beruhende Befugnis und Pflicht, jederzeit die Maßnahmen zu treffen, die er zur Wahrung oder Wiederherstellung des Weltfriedens und der internationalen Sicherheit für erforderlich hält."

Jetzt versuche ich eine neuen Definition, bzw. Erweiterung des Begriffes des Angriffs als Grundlage zu Selbstverteidigung nach Art 51 UN Charta:

„Jede Angriffshandlung, die einen „Staat und seine Einrichtungen, seine Souveränität, territoriale Unversehrtheit oder politische Unabhängigkeit in massiver Weise beeinträchtigt und dabei ein im Staatsgebiet des angegriffenen Staates direkte physische Zerstörung verursacht, wobei eine „gewisse Intensität" erreicht wird." Ein solcher „moderner" Angriffsbegriff könnte geeignet sein, auch neue Mittel der Kriegsführung wie D-Waffen zu erfassen. D.h. es würde die territoriale Unversehrtheit kein Argument mehr sein, sondern die Folgen eines Angriffes mit D-Waffen würden in den Mittelpunkt rücken. Ich erinnere hier an mein Beispiel mit dem Hammer.

Hier muss dann die Frage aufgeworfen werden, ob nur ein militärischer Angriff mit massiven Folgen dies auslöst oder nicht auch ein Angriff mit D-Waffen, der nicht unmittelbar zum Tod der Bevölkerung führt, sondern erst in dessen Folge.

Ob dies vor dem Hintergrund der methodischen Ansätze zur Einordnung von Krieg im Internet in die Systematik des Art. 51 UN-Charta greift, ist umstritten. Und es bleiben aus meiner Sicht die **Risiken des Missbrauchs**: Nach dem Angriff auf das world-trade-center, 9/11, haben die USA unverzüglich den Krieg gegen den Terror erklärt. Und die NATO hat den Verteidigungsfall nach Artikel 5 ausgerufen, und zwar nur wenige Stunden nach dem Angriff.

Es geht mir also zum einen um Änderungen an der UN Charta und zum Anderen nicht darum, bestimmte Programme sondern **definierte Ziele zu verbieten.**

Beispiele: Ein A 400M ist durch Programmierfehler abgestürzt, der modernste Russische Kampfpanzer wird bereits per digitalen Befehlen abgefeuert, polnische Passagiermaschinen bleiben am Boden nach einem Angriff mit D-Waffen.

Das führt zu dieser Fragestellung: Was geschieht, wenn diese Programme durch einen digitalen Angriff übernommen oder zum Absturz gebracht werden? Wenn also Panzer selbstständig angreifen oder sich die Motoren aller Flugzeuge eines Typs plötzlich abstellen?

Hier gibt es eine **Grauzone und es herrscht Rechtlosigkeit**. **Eine Art Genfer Konvention für den Krieg im Internet müsste als erstes definieren, welche Rechner nicht angegriffen werden dürfen:**

zum Beispiel die Computer in Krankenhäusern, Altenheimen oder bei der Flugsicherung. Es geht also um die Frage von **Leben und Tod**! Der US Angriff mit STUXNET auf das Iranische Atomprogramm hat kein Menschenleben gekostet, aber angeblich eine Verzögerung erreicht. Ein Angriff auf die zivile, kritische Infrastruktur wie z.B. Krankenhäuser, Wasser- oder Elektrizitätswerke hätte aber enorme – auch letale – Auswirkungen und ein Angriff auf die Flugsicherheit eines Landes gefährdet alle Menschen im Luftraum und an den möglichen Absturzstellen.

Auch hierzu wenige Beispiele: Die IT-Spezialisten zählen, wie oft sich bekannte Schadsoftware, die in einem fremden System eingeschleust wurde, beim Heimat-Server, also dem digitalen Hauptquartier, meldet.

Im März 2014 etwa wurden die Schädlinge vor allem in einer Weltregion immer aktiver: Osteuropa. Auf dem Maidan in Kiew kämpften zu dieser Zeit die Ukrainer um die Zukunft des Landes, und Russland besetzte die Halbinsel Krim. Nur ein paar Monate später attackierten auffällig viele kanadische Rechner Ziele im Nahen Osten. Die Vermutung liegt nahe, dass israelische Hacker Anlagen in Nordamerika für sich arbeiten ließen, um die Luft- und Bodenoffensiven im Gaza-Streifen durch Cyber-Operationen zu begleiten. Die israelische Armee (IDF) erklärte schon vor drei Jahren: „Der Cyberspace wird genutzt, um Angriffe und Geheimdienstoperationen durchzuführen." Und das neueste Beispiel: Die Webseite des Führungsstabes der litauischen Armee wurde angegriffen und die Meldung veröffentlicht, dass die Militärübung „Saber Strike" dazu diene, die Annexion von Kaliningrad vorzubereiten.

Deshalb rede ich über die **Ächtung der Anwendung von D-Waffen**, zumindest für spezifische, besonders zivile Ziele und kritische Infrastruktur.

Zur Erinnerung: Chemische Waffen kamen vor allem im Ersten Weltkrieg zum Einsatz. Ihre schreckliche Wirkung führte ab 1928 zu einer Ächtung durch das Genfer Protokoll. 1975 kam ein Abkommen dazu, das die Entwicklung, Produktion und Lagerung von biologischen Kampfstoffen wie Anthrax verbietet. Und jetzt brauchen wir dringend eine vergleichbare Konvention für D-Waffen.

Die Forderung gibt es schon länger:

Seit Jahren drängte Russland immer wieder auf internationale Regeln für offensive Cyber-Waffen. Die USA sperrten sich lange dagegen, das bisherige Kriminalrecht genüge, hieß es in den Staaten. Nachdem US-Präsident Barack Obama 2009 neue Abrüstungsgespräche mit Russland verkündet hatte, änderten die USA ihre Haltung, kamen mit Russland ins Gespräch und richteten **2013 einen Kommunikationskanal** ein, über den Moskau und Washington schnell, diskret und direkt über ihre Cyber- Unterfangen reden konnten. Im Herbst vergangenen Jahres einigten sich dann auch Russland und China auf ein Abkommen, allerdings mit anderen Schwerpunkten.

Aus Furcht vor einer Cyber-Aufrüstungsspirale forderte Bundeskanzlerin Merkel bereits 2011 ein internationales Abkommen zur Bekämpfung von Cyber-Angriffen und Internet-Kriminalität.

Doch die Realität sieht anders aus:

Die **NATO** hat auf ihrem Gipfel im September 2014 „Cyberabwehr als eine zunehmend wichtige Aufgabe" festgestellt und: Cyber-Attacken könnten auch als Angriffe gewertet werden, die den Artikel 5-Fall in Gang setzen – also den NATO Bündnisfall und damit die kollektive Verteidigung der Allianz. Und: Moderne Streitkräfte müssen heute über Cyber-Waffen verfügen, um handlungsfähig zu sein. Dabei entscheide die Strategie darüber, ob sie defensiv oder offensiv eingesetzt werden". Die Grenze ist also fließend. Und diese Grauzone ist gefährlich – wir bewegen uns in einer fließenden Grenze zwischen Krieg- und Nichtkrieg. Und keiner der staatlichen Akteure hat ein wirkliches Interesse, diesen Zustand zu beenden. Wir dürfen nicht länger zulassen, dass diese Strategien jahrelang abgekoppelt von demokratischen Entscheidungsprozessen weiterlaufen. Auch während der lettischen Ratspräsidentschaft wurde am 25. Und 26. März in Berlin über Cyber- Verteidigung diskutiert.

Hier wurde eine engere Zusammenarbeit zwischen dem Sicherheits- und Wirtschaftssektor in Europa angemahnt, um allen Bedrohungen und Risiken umfassend und gemeinsam zu begegnen. Entscheidungen wurden aber auch nicht getroffen.

Experten berichten, dass heute weltweit etwa **50 Staaten** auch offensive Kapazitäten haben. Solche Cyberfähigkeiten werden dabei in die jeweiligen militärischen Strategien integriert. Das kann von der Manipulation oder Ausschaltung militärischer Kommando- und Kommunikationsstrukturen bis hin zu Angriffen auf die zivile Infrastruktur reichen.

Und der **Europäische Rat** hat letzte Woche vereinbart bis Juni 2016 eine neue Sicherheits- und Verteidigungsstrategie zu erarbeiten, die den aktuellen Herausforderungen wie hybriden Konflikten und Cyber-Security Rechnung trägt

Es gibt also Bewegung in der Frage, allerdings nicht im gemeinsamen Bestreben, eine völkerrechtlich verbindliche Regelung und Verbot für D-Waffen zu erreichen.

Ist ein Minimalkompromiss erreichbar?

Ein Minimalkonsens scheint sich abzuzeichnen. Zumindest sehr viele Juristen und Techniker glauben, dass so eine Einigung einen Minimalkompromiss umfassen könnte, der nicht auf die D-Waffen zielt, sondern auf die Angriffsziele. So könnten sich die Staaten einigen, bestimmte Ziele nicht anzugreifen (wie Krankenhäuser und Schulen) oder Dritte zu schützen – wie bereits jetzt durch das offen gezeigte Rote Kreuz - oder nur bestimmte Arten von D-Waffen nicht einzusetzen. Ein generelles Verbot, wie es etwa die Chemiewaffenkonvention vorsieht, erscheint ihnen als wenig wahrscheinlich.

Bei konventionellen Waffenverträgen achten die Vertragsparteien selbst oder eine internationale Organisation darauf, dass niemand gegen sie verstößt. Dazu kontrollieren sie Fabriken, Lager, Militärbasen. Im Falle von D-Waffen würde eine Inspektion bedeuten, das komplette Internet nach Schadprogrammen zu durchsuchen. Dafür müssten private Firmen und staatliche Stellen ihre Netze für Dritte öffnen. Die Geräte und Server von Privatpersonen müssten zugänglich sein - und das alles unverschlüsselt. Ein Datenschutz-Super-Gau, der bestimmt nicht im Sinne von Edward Snowden wäre.

Die strategisch-militärische Brille absetzen!

Wenn wir die strategisch-militärische Brille absetzen und auf das Thema als normale Bürger schauen, wird klar, was **das Ziel aller Anstrengungen sein muss:** sichere Daten, sichere Infrastruktur, ungestörter Betrieb unserer alltäglichen Einrichtungen. Die Verringerung unverschlüsselter Datenmengen wird zu weniger Cyber-Verbrechen und weniger Cyber-Spionage führen, was gut ist für die Sicherheit der Menschen und der Staaten, denn Whistleblower Edward Snowden sagte schon kurz nach seinen Enthüllungen, dass richtig genutzte Verschlüsselung gegen die NSA helfe. Die Menschen müssten nicht nur begreifen, was die Geheimdienste alles sehen, hören, speichern wollen, sondern auch anfangen, sich zu wehren.

Wenn wir alle uns also für eine UN Konvention gegen Digitale Waffen einsetzen, dann können wir das Ziel erreichen. Dass dies geht hat die internationale Kampagne gegen Landminen gezeigt. Minen sind geächtet – und die Kampagne hat den internationalen Friedensnobel Preis erhalten.