Sylvia Johnigk, Kai Nothdurft

Cyberwarfare

Aufrüstung im Cyberspace als Herausforderung für die Friedensarbeit des FIfF

Dieser Artikel basiert auf einer Gedankensammlung im FIfF-Mitglieder-Wiki[1], an der sich noch mehrere Personen beteiligt haben. Wir wollen die Position des FIfF zum Thema Cyberwar dort weiterentwickeln. Ihr seid alle herzlich eingeladen, Euch daran zu beteiligen.

Wie wird der Begriff Cyberwar verwendet?

Unter *Cyberwarfare* verstehen wir die Kriegsführung mit Computern als Waffen. Computer werden dabei dazu genutzt, militärisch motivierte Angriffe auf andere IT-Systeme durchzuführen (offensive Strategie) oder solche Angriffe mit IT-technischen Mitteln zu erkennen und abzuwehren (defensive Strategie). Da in der politischen und teilweise auch fachlichen Debatte eine verbale Aufrüstung stattfindet, ist es uns wichtig, *Cyberwar* von den Begriffen *Cybercrime* und *Hacktivismus* abzugrenzen, die in der IT-Sicherheit häufig ebenfalls im Zusammenhang mit Angriffen genannt und dabei unter Cyberwar subsummiert werden, denen aus unserer Sicht aber keine militärische Motivation zu Grunde liegt.[2]

Cybercrime umfasst die Begehung von Straftaten, in der Regel mit der Motivation der kriminellen Bereicherung. Unter Hacktivismus verstehen wir das Attackieren von IT-Systemen im Rahmen von politischen Kampagnen z. B. durch zeitweises Lahmlegen mittels *Denial-of-Service*-Attacken oder das Eindringen in Systeme, um geheim gehaltene Informationen der Öffentlichkeit zugänglich zu machen (*Leaken*).

Unter *Cyberespionage* verstehen wir Informationsbeschaffung aus geheimen Quellen mittels Eindringen in IT-Systeme. Diese kann sowohl kriminell-wirtschaftlich (Wirtschaftsspionage) als auch militärisch motiviert sein (Zugang zu militärischen Geheimnissen). Damit kann Cyberespionage, je nach Motivation und Art der ausspionierten Information, zur Cyberwarfare gezählt werden, etwa wenn sie der Vorbereitung eines Angriffs dient.

Cyberwar ist ein sehr wichtiges Thema für das FIfF, das sich kritisch mit den gesellschaftlichen Auswirkungen der IT und insbesondere der Verflechtung von IT und ihrer militärischen Nutzung beschäftigt. Das FIfF wurde vor 27 Jahren von InformatikerInnen gegründet, die die Steuerung von Raketen durch Computer als Bedrohung für die Menschheit identifizierten. Man befürchtete u.a. die Auslösung eines Atomkriegs durch Computerfehler. Inzwischen steuern Computer nicht nur Waffen sondern werden immer mehr selbst zur Waffe. Die Entwicklung von autonomen Kampfrobotern und Drohnen lässt die Grenze zwischen der Waffe und der Technik, die sie steuert, bereits verschmelzen, aber im Cyberwar wird der Computer selbst zur Waffe und dient zur Bekämpfung anderer IT-Systeme, indem Sabotagehandlungen von Angreifern ausgeführt werden. Zum Beispiel können Schadprogramme in die Ziele eingeschleust werden oder Exploits direkt zum Absturz der angegriffenen Systeme führen.

Viele Staaten haben bereits für den Cyberwar spezialisierte militärische Einheiten aufgebaut oder zumindest damit begonnen. Die Einheiten, bestehend aus IT-Spezialisten in Uniform, haben nicht rein defensiven Charakter sondern sind zumindest teilweise auch für Cyber-Angriffe vorgesehen. Neben Russland und China sind vor allem die USA eine treibende Kraft in der digitalen Aufrüstung.

Im Februar 2009 berichtete der SPIEGEL, dass auch die Bundeswehr eine 76 Mann umfassende geheime Cyberwar-Einheit aufbaue, die sowohl defensive als auch offensive Aufgaben habe.[3]

In Deutschland wurde außerdem am 23. Februar 2011 das nationale Cyber-Abwehrzentrum NCAZ gegründet. Hauptzweck des NCAZ soll ein verbesserter Informationsaustausch unter den Strafverfolgern, Militär, Geheimdiensten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sein.

Die Bundesregierung hielt es formal nicht für nötig, ein Errichtungsgesetz verabschieden zu lassen, weil es sich nach ihrer Auffassung beim NCAZ nicht um eine eigenständige Behörde handele. „Dabei sollen alle Mitarbeiter im Abwehrzentrum, unter Wahrung der Zuständigkeit der einzelnen Behörden wie unter Berücksichtigung des Trennungsgebotes zwischen Nachrichtendiensten und Polizei, in ihre jeweiligen Behörden eingebunden bleiben.“[4] Durch die gemeinsame Arbeit wird jedoch aus unserer Sicht eine Vermischung von Strafverfolgung und Geheimdienstaufgaben und zusätzlich noch dem militärischen Bereich gefördert, die de facto das Trennungsprinzip aufweicht und in der Folge zu gefährlichen Machtkonzentrationen führen kann.

US-amerikanische Cyberspace-Strategie

Am 14. Juli 2011 veröffentlichte das amerikanische *Verteidigungs*ministerium eine neue Militärstrategie für das Operieren im Cyberspace.[5] Dieser veröffentlichte Teil der Strategie war entgegen früheren Ankündigungen und Erwartungen[6] zunächst rein defensiv ausgerichtet. Noch im Mai war in Medienberichten diskutiert worden, dass Cyber-Attacken zukünftig von den USA als Kriegsgrund gewertet würden, der auch mit konventionellen Waffen beantwortet werden könnte. Neuere Meldungen und die Tatsache, dass nur Teile der Strategie veröffentlicht wurden, deuten jedoch darauf hin, dass es auch in den USA weiter gehende Überlegungen gibt, die sich sehr wohl mit offensiven Cyberwar-Strategien beschäftigen. So soll das US-Militär bei der Planung des Libyen-Einsatzes im Frühjahr erwogen haben, „in die libyschen Kommunikationsnetze einzudringen,“ um „die daran angeschlossenen Radaranlagen und so die Raketenflugabwehr“ zu stören. Auch für die gezielte Tötung Bin Ladens war erwogen worden, das pakistanische Radar mit einer Cyber-Attacke auszuschalten. „Laut James Andrew Lewis vom *Center for Strategic and International Studies* wollten die USA nicht die

ersten sein, die offiziell Cyberwar-Instrumente einsetzen und damit einen Dammbruch herbeiführen."[7]

Ein Grund dürfte dabei auch die eigene Verletzlichkeit der USA gegenüber Cyber-Angriffen sein, auf die im Strategiepapier vom Juli 2011 mehrfach hingewiesen wird. Diese defensive Schwäche gegen Cyber-Angriffe, die nicht nur die USA sondern alle hochtechnisierten Gesellschaften betrifft, gründet in einer jahrzehntelangen Vernachlässigung der IT-Sicherheit in Architekturen, Design und Implementierung von Netzwerken, Betriebssystemen und Anwendungsprogrammen und setzt sich in Embedded Systems und Steuerungsanlagen fort. Sicherheitsmaßnahmen und Basisschutz müssten für alle mit dem Internet verbundenen Systeme existieren. Stattdessen strotzen die allermeisten Web-Anwendungen vor Sicherheitslücken. Versäumnisse in der Software-Entwicklung wie schlechte Codequalität und fehlendes Testen gegen Sicherheitslücken aufgrund enger Release-Termine und das Sparen an qualifiziertem Personal im Systembetrieb führen zu diesen Sicherheitsrisiken.[8] Die Zentralisierung, Vernetzung (insbesondere über das Internet), Cloud-Computing und der Zugriff über völlig ungesicherte mobile Endgeräte wie Smartphones oder Tablets erhöhen zudem stetig das Risikopotenzial der IT-Systeme und damit die Verletzlichkeit der Betreiber und der gesamten Gesellschaft, in der sie eingesetzt werden.

Das Sicherheitsniveau der meisten Systeme ist für die potenziellen Schäden, die bei einer Manipulation, Sabotage oder Kompromittierung entstehen können, viel zu gering, da in der Vergangenheit IT-Sicherheit häufig hinter anderen Kriterien wie erweiterter Funktionalität, Kosten oder Bequemlichkeit zurückgestellt wurde. Eine der fünf im Strategiepapier genannten Initiativen soll das Sicherheitsniveau der militärischen wie zivilen IT-Systeme verbessern – ein Ziel, das sicherlich nicht kurzfristig zu erreichen ist.

Was wird als Angriff gewertet?

Das DoD (*Department of Defense*) betrachtet in seinem Strategiepapier sehr unterschiedliche Formen von Bedrohungen im Cyberspace, unterscheidet aber aus unserer Sicht zu wenig zwischen durch Cyberwar, Cybercrime und Hacktivism motivierten Angriffen. Neben *Denial-of-Service*-Attacken auf die militärischen Netzwerke und angeschlossenen Systeme oder Angriffen auf zivile Einrichtungen mit Sabotagecharakter – Infrastrukturen wie Energieversorgung, Verkehrsinfrastrukturen – werden auch Manipulationen oder der Diebstahl von Informationen als Bedrohung der nationalen Sicherheit angesehen. Der Diebstahl von geistigem Eigentum schwäche demnach die technologische Vormachtstellung. Aber auch sonstige Wirtschaftsspionage wird als Bedrohung angesehen, weil dadurch die ökonomische Stärke der USA beeinträchtigt und damit die USA insgesamt geschwächt wird.

In den Monaten, bevor die Strategie veröffentlicht wurde, kam es vermehrt zu spektakulären Hacking-Aktivitäten und Cyber-Attacken, die für die USA eine Herausforderung darstellten und auch allgemein als Eskalation der Bedrohungen der IT-Sicherheit wahrgenommen werden können:

1. Im Juni 2010 wird der *Stuxnet-Wurm* entdeckt, bei dem es sich um eine völlig neue Klasse von Schadsoftware handelt. Da der Wurm seine Schadroutinen nur bei einer sehr speziellen Art von Steuerungssystemen ausführt (*Simatic S7* von Siemens) und dabei sehr gezielte Veränderungen in der Steuerung vornimmt, und weil Iran von Infektionen besonders stark betroffen war, wird angenommen, dass der Wurm speziell für die Sabotage von Zentrifugen in der iranischen Urananreicherungsanlage in Natanz entwickelt wurde.[9] Die Entwicklungskosten liegen im 7-stelligen Dollarbereich. Die Urheberschaft ist bisher unbekannt, wird aber wegen des Ziels und der Höhe der eingesetzten Mittel bei israelischen und/oder US-amerikanischen staatlichen Stellen vermutet.

2. In 2010 werden von Wikileaks mehrere für die US Regierung problematische Dokumente enthüllt: am 5. April ein Video zu Luftangriffen von US-Kampfhubschraubern in Bagdad, bei denen gezielt Zivilisten – u.a. auch Reporter – getötet wurden, im Juli die *Afghan War Diaries*, 76.911 Dokumente über den Krieg in Afghanistan, und am 28. November 250.000 US Botschaftsdepeschen (*Cables*).

3. Als Solidaritätsmaßnahme für Wikileaks wurde ab Ende 2010 von den lose organisierten Netzaktivisten von Anonymous die *Operation Payback* gestartet. Es handelte sich dabei um zeitlich begrenzte, aber erfolgreiche DDoS Attacken mit einem Tool namens *Ionenkanone*. Die Attacken richteten sich u.a. gegen Visa, Mastercard und Paypal, weil diese keine Zahlungen an Wikileaks mehr transferierten. Die Web-Dienste der betroffenen Unternehmen waren dadurch zeitweise nicht mehr erreichbar.

4. Die Hackergruppe *Lulzsec* drang in mehrere Server (u. a. Sony, Nintendo, die US Fernsehsender Fox und PBS, die Website des US-Senats) ein und stellte kopierte Daten demonstrativ ins Internet, darunter auch sensible personenbezogenene Informationen.[10]

5. Im März 2011 wurden durch eine Hacking-Attacke, hinter der ein ausländischer Geheimdienst vermutet wurde, 24.000 geheime Dateien des Pentagon entwendet.[11]

6. Unbekannte aus dem Umfeld von Anonymous erlangten im Juli Zugriff auf fünft GB Daten der NATO.[12]

7. Am 18. März 2011 gab die Sicherheitsfirma RSA bekannt, Opfer einer APT-(*Advanced Persistance Threat*) Attacke geworden zu sein. Dabei wurden Firmengeheimnisse über das Produkt *Secure ID Token*, das zur 2-Faktor Authentisierung genutzt wird, entwendet.[13] Am 21. Mai 2011 wurde in Server des US-Rüstungskonzerns Lockheed Martin eingebrochen, wobei Informationen aus dem vorangegangenen RSA-Hack genutzt wurden.[14]

Alle genannten Vorfälle würden nach der Doktrin als Cyber-Bedrohungen gewertet, die die nationale Sicherheit der USA gefährden.

Mit der sehr weiten Definition von Bedrohungen geht aber eine gewisse Beliebigkeit einher, was alles als militärischer Angriff gewertet werden kann, aus dem möglicherweise auch militärische Gegenaktionen legitimiert werden sollen.

Der IT-Sicherheitsexperte Bruce Schneier warnt zu Recht vor verbaler Hochrüstung und davor, zu schnell Angriffe auf die IT-Sicherheit als Cyberwar-Aktivität zu werten:

> *„And just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar."*[15]

Die breite Definition von Bedrohungen, unabhängig von der Motivation und Organisation des Angreifers, lässt mit ihrer Beliebigkeit theoretisch auch die Taten einer Einzelperson, etwa eines pubertierenden *Scriptkiddies*, das eine Malware ausprobiert, als Kriegsgrund zu. Sie könnte sogar als ungesetzlicher Kombattant eingestuft werden. Bei den Bedrohungen wird nicht unterschieden, ob militärische oder zivile Systeme angegriffen werden. Wenn Gleiches auch für die Offensive gilt, entsteht ein großes, neues Risiko für die Zivilbevölkerung der angegriffenen Länder. Im Cyberwar verschwimmen die Grenzen zwischen militärischen und zivilen Zielen weiter, und die Schwere und Häufigkeit von Kollateralschäden bei der Zivilbevölkerung wächst.

Besonders kriminell motivierte Angriffe kommen sehr häufig vor. Wenn davon auch nur ein Bruchteil als kriegerischer Akt eingestuft wird, herrscht Dauerkrieg. Die Subsummierung kann auch durch eine Konkurrenz zwischen Strafverfolgungsbehörden und Militär motiviert sein, wer für Cyber-Attacken zuständig ist, wer zu deren Bekämpfung finanzielle Mittel bekommt, wessen Methodiken der Gegenmaßnahmen angewendet werden. Schon beim *Krieg gegen den Terror* wurde vergeblich versucht, Kriminalität militärisch zu bezwingen.

Es gibt durch die Beliebigkeit von Bedrohungen in der Strategie auch keine erkennbaren Maßstäbe, ob es sich um eine völkerrechtlich legitimierbare Verteidigung nach einem tatsächlich erfolgten Angriff handelt. Im Zweifelsfall werden technische Details als Geheimsache unter Verschluss gehalten (werden müssen), womit sie sich jeglicher Prüfung durch unabhängige Instanzen entziehen, ob ein militärische Gegenschläge rechtfertigender Angriff überhaupt stattgefunden hat.

Jeder Cyber-Angriff könnte damit sogar den Vorwand für das Ausrufen eines militärischen Bündnisfalls liefern.

Birgt schon die militärische Bewertung aus der Defensive erhebliche Risiken, so ist die offensive Cyberwar-Kriegsführung aus mehreren weiteren Gründen äußerst kritisch zu sehen.

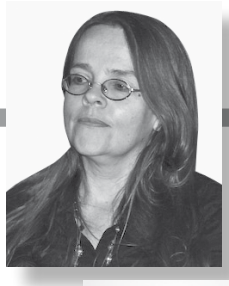
Wer ist der Angreifer?

Schon das korrekte Identifizieren des Gegners wird im Cyberwar zum Problem, wie auch das DoD erkannt hat (Problem der *Non-Attribution*):

> *„Cyber is also an attractive weapon to our adversaries because it is hard to identify the origin of an attack and even more difficult to deter one. A keystroke travels twice around the world in 300 milliseconds. But the forensics necessary to identify an attacker may take months. Without establishing the identity of the attacker in near real time, our paradigm of deterrence breaks down. Missiles come with a return address. Cyber attacks, for the most part, do not." (William Lynn, Deputy Secretary of Defense*[16]*)*

Halbwegs versierte Angreifer nutzen für Cyber-Attacken nicht den eigenen Computer sondern infizieren den PC eines (bis dahin unbeteiligten) Dritten mit Malware und übernehmen dadurch die Kontrolle darüber. Der so übernommene PC wird ab diesem Zeitpunkt bei Bedarf durch den Angreifer ferngesteuert. Der kompromittierte PC wird zu einem *Zombie* als Ausgangspunkt für den eigentlichen Angriff. Dieses Verstecken des Angreifers hinter einem kompromittierten PC lässt sich noch mehrfach iterieren, indem der erste befallene PC einen weiteren befallen PC fernsteuert usw.

Oft werden solche Zombie-PCs mit anderen infiltrierten PCs zu einem Bot-Netz zusammengeschaltet, in dem mehrere befallene Rechner von einem Controlserver gemeinsam gesteuert werden. Dadurch können dann auch *Distributed-Denial-of-Service*-Angriffe (DDoS-Attacken) ausgeführt werden. Der Angreifer steu-



Sylvia Johnigk und Kai Nothdurft

Sylvia Johnigk studierte Informatik an der TU-Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit, arbeitete fünf Jahre in der Forschung am Thema Informationssicherheit und acht Jahre bei einem Finanzdienstleister als IT-Security Consultant in Frankfurt am Main. Seit Mitte des Jahres 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensiblisierung spezialisiert hat.

Kai Nothdurft studierte Informatik an der Uni Bremen und beschäftigte sich schwerpunktmäßig mit Datenschutz und IT-Sicherheit. Nach dem Studium arbeitete er fünf Jahre als Freiberufler im Schulungs- und Consultingbereich. Seit 1999 arbeitet er als IT-Sicherheitsbeauftragter für ein großes deutsches Versicherungsunternehmen.

ert dabei eine große Menge an Zombie-PCs, was es zum Beispiel ermöglicht, angegriffene Systeme durch Überlastung zusammenbrechen zu lassen.

Will man aber die Quelle solcher Angriffe identifizieren und sucht in Logfiles nach der Quell-IP, so stößt man zunächst nur auf die Zombie-PCs und muss in deren Logfiles nach weiteren Spuren suchen, von wo aus diese kontrolliert wurden – ein zeitaufwendiges und oft auch erfolgloses Unterfangen. Damit wird es aber sehr schwer, die eigentliche Quelle des Angriffs zu ermitteln. Ein militärischer Gegenschlag kann, wenn überhaupt, nicht zeitnah erfolgen oder man riskiert dabei, den „Falschen" zu erwischen.

Auf der Angreiferseite ist durch das geringe Entdeckungs- und Vergeltungsrisiko die Hemmschwelle zum Ausführen eines Cyber-Angriffs geringer als für einen konventionellen Angriff.

Da die Identifizierung des Angreifers so problematisch ist, kommen bei Sicherheitspolitikern bestimmt auch bald wieder Wünsche nach einer zwangsweisen Identifizierung und Vorratsdatenspeicherung als einfache politische Antworten auf dieses Problem auf. Dem muss entgegengesetzt werden, dass sich Cyber-Soldaten oder gewiefte Kriminelle eben fremder, gestohlener Identitäten oder in letzter Instanz dann doch Anonymisierern bedienen.[17]

Verstärkung der Tendenz zur asymmetrischen Kriegsführung

Die Cyber-Strategie der USA erwähnt auch, dass das Land sich in einer technologischen Führungsposition befindet. Wird aber ein offensiver Cyber-Krieg gegen technologisch weniger entwickelte Gegner geführt, werden diese womöglich mit einfachen Guerilla-Aktionen reagieren. Durch die Aufrüstung im Cyberspace wird so die Tendenz zur asymmetrischen Kriegsführung verstärkt. Wenn das gegnerische Militär technologisch überlegen ist, werden primitive Gegenmaßnahmen in Form von bspw. Sprengstoffattentaten auf zivile Einrichtungen attraktiver.

Militärische Geheimhaltung schadet auch der eigenen Zivilgesellschaft

IT-Sicherheit ist bisher noch ein Sicherheitsbereich, der nicht staatlich kontrolliert und nur wenig reglementiert wird. Versuche der USA in der Vergangenheit, z. B. Kryptografie-Exporte zu beschränken, scheiterten, da sich dies als negativ für die eigene Wirtschaft herausstellte.

Wissen über Sicherheitslücken (*less than Zero day exploits*) geheim zu halten, um sie im Cyberwar zum Angriff nutzen zu können, ist gefährlich, da es auch die eigene Wirtschaft gefährdet, die die gleichen Betriebssysteme und Anwendungen einsetzt wie der Gegner, den man angreifen möchte. Dieses Dilemma wurde von der NSA als *Equity Issue* identifiziert. Es handelt sich um ein *Dual-Use*-Problem, dass man Sicherheitslücken als militärischen Vorteil geheim halten kann, dann aber auch die eigenen Unternehmen und Zivilisten gefährdet, oder sie veröffentlicht und damit auch dem „Gegner" hilft, seine IT-Sicherheit und damit Cyber-Verteidigungsfähigkeit zu verbessern.[18] In ein vergleichbares Dilemma laufen staatliche Institutionen auch, wenn sie im Rahmen der Strafverfolgung Sicherheitslücken geheim halten, um damit PCs von Verdächtigen mit einem Staatstrojaner kompromittieren zu können.

Kriminelle erlangen Wissen schneller als die Öffentlichkeit, daher entstehen sehr schnell auch volkswirtschaftliche Schäden. Da sich viel Geld damit verdienen lässt, wird solches Wissen nicht nur an offizielle Stellen verkauft, ganz davon abgesehen davon, dass es auch in staatlichen Institutionen Kriminelle gibt. Es gibt viel zu viele Lücken und daher Möglichkeiten, diese zu entdecken, als das man das Problem kurz- oder mittelfristig unter Kontrolle bringen könnte.

Cyber-Demonstrationsrecht – Digitale Aktionsformen und Hacktivismus

Die in der Medienberichterstattung viel beachtete Aktivistengruppe Anonymous würde nach der US-Strategie als nationale Bedrohung eingestuft. Im Gegensatz zu von staatlichen Institutionen durchgeführten Angriffen machen sie ihre Aktivitäten publik und kündigen sie sogar an. Bei den Aktionen von Anonymous handelt es sich auch weniger um Hacking zur Sabotage oder Spionage als vielmehr um einen Online-Protest im Rang zivilen Ungehorsams, der in die kriminelle Ecke gedrängt und als Terrorismus diffamiert werden soll. Bei der Nutzung des DDoS-Tools *Ionenkanone* wurden die betroffenen Server nur vorübergehend für einen kurzen Zeitraum lahmgelegt. Die Aktionen wurden zum Teil sogar vom eigenen PC aus vorgenommen, waren also nicht einmal vollständig anonym und einige Aktivisten bekamen in der Folge entsprechende Repressalien zu spüren. Solche Aktionen gleichen politische Sit-Ins oder Blockaden zu Demonstrationszwecken. Sie müssten eher als ziviler Ungehorsam eingeordnet werden denn als Terror oder gar Angriff in einem Cyberwar. Da inzwischen viele Organisationen sehr stark, einige sogar ausschließlich im virtuellen Raum in Erscheinung treten und agieren, muss auch die Kritik und Auseinandersetzung bis hin zum gewaltfreien Widerstand im Cyber-Raum legitim werden.

An ethische Grenzen stoßen solche Aktionen allerdings, wenn dabei wichtige Grundrechte verletzt oder gar Menschenleben gefährdet werden. So hat die Hackergruppe Lulzsec mehrfach sensible personenbezogene Daten von Servern, in die sie eingedrungen waren, kopiert und im Internet veröffentlicht, etwa die Kundendaten von Sony.

Conclusio

Für das potenzielle Schlachtfeld im Cyberspace wurde eine neue gefährliche Rüstungsspirale in Gang gesetzt. Sie zieht ihre Motivation aus dem Auf- und Ausbau von militärischen Cyberwar-Einheiten, der hohen Verletzlichkeit der *digitalen* Gesellschaften mit ihren global vernetzten IT-Systemen und dem vermeintlich geringen Risiko für den Angreifer, identifiziert und für sein Tun sanktioniert zu werden. Es ist höchste Zeit, dass die in Gang gesetzte Rüstungsmaschinerie wieder gestoppt wird. Das FIfF als Teil der Friedensbewegung ist in besonderer Weise gefordert, seine fachliche Expertise dafür zu nutzen. Die folgenden Forderungen sollen zu einer Deeskalation und Vermeidung von Cyber-Kriegen beitragen:

Forderungen des FIfF

1. **Verzicht auf Erstschlag und Offensive im Cyberspace: Staaten sollen öffentlich darauf verzichten, Cyber-Waffen präventiv oder zum Angriff einzusetzen.**
2. **Reine defensive Sicherheitsstrategie: Staaten sollen sich verpflichten, keine Offensivwaffen für den Cyberwar zu entwickeln oder gar einzusetzen.**
3. **Digitale *Genfer Konvention*: Für die Zivilbevölkerung lebenswichtige Infrastrukturen wie Wasserversorgung, Gesundheitsversorgung, etc. dürfen nicht angegriffen werden. Eine Verletzung dieses Grundsatzes soll als Kriegsverbrechen gelten.**
4. **Anerkennung eines Grundrechts auf zivilen Ungehorsam und Online-Protestformen im Internet: Derartige Aktionen dürfen nicht kriminalisiert werden geschweige denn als Kriegsgrund herhalten.**
5. **Wirtschaftliche Interessen, wie ein Verstoß gegen *Intellectual Properties*, sind kein legitimer Kriegsgrund.**
6. **Konventionelle Waffen dürfen nicht als Antwort auf eine Cyber-Attacke eingesetzt werden.**
7. **Staatliche Stellen müssen zur Offenlegung von Schwachstellen verpflichtet werden (ableitbar aus dem Grundrecht für Integrität, das der Staat schützen muss).**
8. **Betreiber kritischer Infrastrukturen müssen verpflichtet werden, sich selbst zu schützen, bzw. IT-Systeme sicher zu gestalten, zu implementieren und zu betreiben, anstatt nach dem Staat oder gar Militär zu rufen. Kompetente, transparente Prüfungen und Tests müssen Voraussetzung für eine Betriebserlaubnis sein. Wir fordern Entnetzung und Dezentralisierung kritischer Infrastrukturen (wie z. B. DE-CIX).**
9. **Abrüstung der politische Sprache: Klare Trennung von Cyberwar, Cyberterror, Cybercrime, ethical Hacking, politischen Protestformen.**
10. **Demokratische Kontrolle, Gewaltenteilung, Parlamentsvorbehalt für Cyber-Sicherheitsstrategien und deren Umsetzung.**
11. **Transparenz beim Aufbau jeglicher „Cyber-Zentren".**
12. **Klare friedenspolitische Ausrichtung der Cyber-Zentren.**
13. **Die Trennung von Polizei und Geheimdiensten und Militär in Cyber-Abwehrzentren muss gewährleistet werden.**
14. **Cyberpeace-Initiative: Verpflichtung zur Förderung von Friedensforschung zur Entwicklung von Strategien zur Befriedung des Cyberspace.**

Anmerkungen

1 *http://wiki.fiff.de/CategoryCyberwarfare. Login-Daten erhaltet Ihr über die Geschäftsstelle.*
2 *Eine gefährliche Analogie wäre auch, IT-Sicherheitstools mit Waffen gleichzusetzen. In dieser Logik wäre ein Programmierer, der solche Tools herstellt, ein Rüstungsbetrieb, befänden sich Massenvernichtungswaffen (Botnetze) in den Händen von kriminellen Zivilisten.*
3 *http://www.spiegel.de/netzwelt/tech/0,1518,606096,00.html*
4 *http://de.wikipedia.org/wiki/Cyberabwehrzentrum*
5 *http://www.defense.gov/news/d20110714cyber.pdf – Department of Defense: Strategy for operating in Cyberspace*
6 *http://www.heise.de/security/meldung/Bericht-USA-wollen-Hacker-angriffe-zum-Kriegsgrund-erklaeren-1253088.html*
7 *http://www.heise.de/newsticker/meldung/Bericht-US-Regierung-erwog-Cyberwar-gegen-Libyen-1362698.html*
8 *Schlecht konfigurierte und nicht gehärtete Betriebssysteme, unzureichend gesicherte Netze, keine oder fehlerhaft konfigurierte Intrusion Detection Systeme, mangelnde Überwachung dieser Systeme sind nur eine kleine Auswahl von Sicherheitslücken, mit denen sich die Liste erweitern lässt.*
9 *Ein Foto auf der Webseite des iranischen Präsidenten Ahmadinedschad von einem Besuch in Natanz zeigt ein Steuerungs-Panel für die gleiche Anzahl von Zentrifugen, die mit Stuxnet manipuliert werden.*
10 *http://www.heise.de/security/artikel/LulzSec-ausser-Rand-und-Band-1261669.html*
11 *http://www.spiegel.de/politik/ausland/0,1518,774553,00.html*
12 *http://www.spiegel.de/netzwelt/web/0,1518,775811,00.html*
13 *http://www.heise.de/security/meldung/RSA-Hack-koennte-Sicherheit-von-SecurID-Tokens-gefaehrden-1210245.html*
14 *http://www.heise.de/security/meldung/Hacker-steigen-bei-Lockheed-Martin-ein-1251902.html*
15 *http://www.schneier.com/blog/archives/2007/06/cyberwar.html*
16 *Remarks at Stratcom Cyber Symposium William J. Lynn http://www.defense.gov/speeches/speech.aspx?speechid=1477*
17 *Auch das DoD fördert das TOR-Projekt und Sicherheitsbehörden und Militärs nutzen TOR selbst.*
18 *http://www.softsecurity.com/news/blog-posts/dual-use-technologies-and-the-equities-issue.html*