Unsere Ziele

Cyberpeace ist der Gegenentwurf zur militärischen Kolonialisierung des Cyberspace. Es gilt, die einstmals viel beschworene Rolle der globalen Netze für Friedensstiftung und Völkerverständigung wiederzubeleben. Dafür setzt sich das FIfF ein.

Deshalb fordert das FIfF:

- die Ächtung jeglicher Cyberkriegführung
- die ausschließlich zivile Nutzung der öffentlichen Kommunikationsnetze
- die Unterbindung einer menschenrechts- und verfassungswidrigen Ausspähung der Zivilgesellschaft
- die Abkehr von einer Sicherheitsdoktrin, die alle Menschen unter Generalverdacht stellt
- die Entflechtung von Militär und Geheimdiensten sowie deren zivilgesellschaftliche Kontrolle

Mit unserer Kampagne Cyberpeace machen wir Druck auf die Politik, diese Forderungen umzusetzen.

Erreichen wollen wir:

- das Ende der umfassenden Überwachung
- den Verzicht auf die Entwicklung und den Einsatz offensiver Cyberwaffen
- Rüstungskontrollbestimmungen für Cyberwaffen und Überwachungstechnologien
- den Schutz der zivilen Informationsgesellschaft
  - durch eine internationale Kooperation bei der Untersuchung von Cyberangriffen
  - durch eine Veröffentlichungspflicht für IT-Schwachstellen
  - durch eine angemessene Ausstattung ziviler Einrichtungen zum Schutz der IT-Infrastrukturen

In vierzehn Forderungen haben wir unsere Standpunkte zu Cyberpeace formuliert:

⇒ *cyberpeace.fiff.de/Kampagne/WirFordern*

Mitmachen!

Wir brauchen eine breite politische Bewegung, um das Wettrüsten im Cyberspace zu beenden. Unterstützen Sie unsere Kampagne, informieren Sie sich, tragen Sie unsere Botschaft weiter, machen Sie mit:

⇒ *cyberpeace.fiff.de/Kampagne/Mitmachen*

Stiftung bridge unterstützt und fördert die Kampagne. Partner sind Campact, der CCC, die Humanistische Union, die Kooperation für den Frieden u.a.

Das FIfF

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. ist ein Zusammenschluss von Menschen, die sich kritisch mit den Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen. Das FIfF wurde 1984 im Umfeld der Friedensbewegung gegründet. Neben dem Engagement in vielen anderen Problembereichen der Informationsgesellschaft ist die Verstrickung der Informatik in das Militärgeschäft Kernthema des FIfF.

Anschrift:	Geschäftsstelle FIfF e.V. Goetheplatz 4; 28203 Bremen
Telefon:	+49 (0) 421 - 33 65 92 55
E-Mail:	fiff@fiff.de
PGP:	3920 68D5 E07D 48AF 0B64 313E BCDB 77F3 BACF B3D0
Web:	fiff.de und cyberpeace.fiff.de

Das FIfF finanziert sich aus Spenden und Mitgliedsbeiträgen, um unabhängig zu bleiben.

Spendenkonto bei der Bank für Sozialwirtschaft (BFSW)

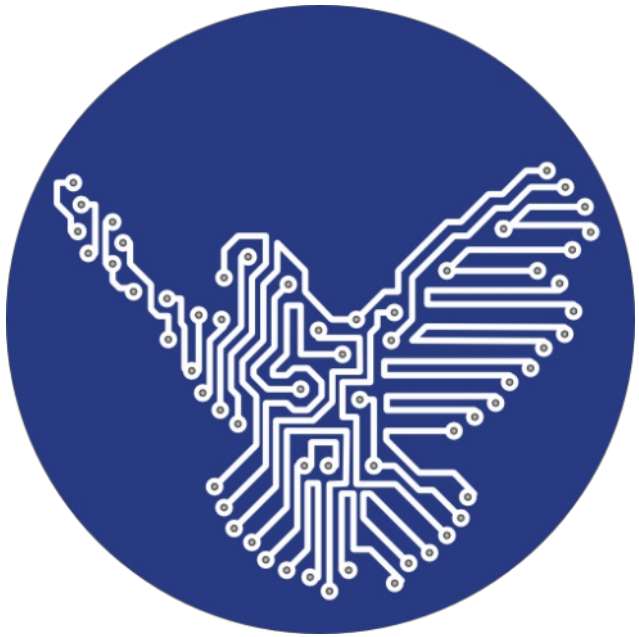
IBAN:	DE79 3702 0500 0001 3828 03
BIC:	BFSWDE33XXX

Für Spendenbescheinigung:
bei Überweisung Adresse als Verwendungszweck angeben

ViSdP: Stefan Hügel Design und Layout: ideal.istik.de

cyberpeace

cyberpeace.fiff.de



eine Kampagne des

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

Spionageziel Cyberkrieg

Die weltweite Ausspähung der Kommunikation über Telefon und Internet ist bereits ein massiver Bruch unserer Grundrechte. Aber sie dient nicht allein der Überwachung. Sie ist ein entscheidender Teil der gegenwärtigen militärischen Doktrin, die sich hinter dem Begriff Cyberkrieg verbirgt.

In Ihrem Auto arbeiten bis zu 1.500 Prozessoren, viele davon mitverantwortlich für Ihre Fahrsicherheit. – Wie wichtig ist Ihnen die Sicherheit dieser Computersysteme?

Überwachungssysteme wie XkeyScore oder Prism spähen nicht nur aus – automatisiert sammeln sie auch Information über Sicherheitsschwachstellen der Computersysteme in ihrem Suchraster und erproben Angriffsmöglichkeiten. Das Ausspionieren dient auch der Vorbereitung gezielter Angriffe auf Computer und Computernetzwerke. Die Mittel sind u.a. Computerviren und Trojaner sowie Einbruchswerkzeuge für bekannte Sicherheitslücken, sogenannte Exploits. Ziele sind die Computersysteme der UNO, der EU-Kommission und ziviler Organisationen. Ziele sind auch Unternehmen, öffentliche Versorgungssysteme und schließlich wir als Privatpersonen.

Ziviler Flugverkehr ohne Flugsicherung, Flugleitsysteme, Satellitennavigation ist heute undenkbar. Dahinter steht eine hochkomplexe digitale Infrastruktur. – Wie wichtig ist Ihnen die Sicherheit dieser Computersysteme?

Um sich die Arbeit zu erleichtern und um Sicherungssysteme zu umgehen, werden auf Betreiben von Geheimdiensten Hintertüren in Computersysteme eingebaut. Geheimdienste „motivieren“ IT-Unternehmen mit unterschiedlichen Mitteln zur Kooperation. Sie kaufen sich auf dem Schwarzmarkt Kenntnisse über unbekannte Sicherheitslücken und die dazu maßgeschneiderten digitalen Einbruchswerkzeuge ein. Und sie schaffen sich bei Bedarf die Schwachstellen selbst.

Informationsgesellschaft als Geisel

Unsere Zivilgesellschaft ist bereits heute in hohem Maße auf ein sicheres Funktionieren von Computern und digitale Kommunikationsnetzen angewiesen. Die Geheimdienste arbeiten jedoch erfolgreich daran, die Sicherheit und Zuverlässigkeit dieser Systeme auszuhebeln.

Ein nächster Schritt sind Cyberwaffen, die eigens dafür entwickelt werden, unmittelbaren Schaden zu bewirken und damit auch militärische Ziele zu verfolgen. Computerviren wie Stuxnet sind solche Cyberwaffen. Sie werden durch staatliche Stellen als Schadsoftware verbreitet. Die Freilassung dieser sabotierenden oder zerstörenden Programme in unsere Kommunikationsnetze kann umfangreiche und unkontrollierbare Kollateralschäden in zivilen Systemen nach sich ziehen.

Das Chemiewerk in Ihrer Nachbarschaft wird von Computern gesteuert. Von staatlichen Stellen verbreitete Schadsoftware kann, wie das Beispiel Stuxnet demonstriert hat, solche Systeme sabotieren. – Wie wichtig ist Ihnen die Sicherheit dieser Computersysteme?

Die NSA und ihre Verbündeten agieren nicht allein: Weltweit rüsten Geheimdienste und Militärs für den Cyberkrieg auf, um Computer und Internet mit verdeckten Mitteln stören und kontrollieren zu können. Nicht anders operieren auch das Kommando Strategische Aufklärung der Bundeswehr und der BND.

Cyberangriffe sind Kriegshandlungen

Geheimdienste wie die NSA sind zugleich Kampfunterstützungseinheiten der Militärs. Die NSA mit ihrem Milliardenbudget beschäftigt die vermutlich am besten ausgerüstete Hackertruppe der Welt. Sie führt bereits heute einen versteckten Cyberkrieg gegen Freund und Feind.

Internet, Stromnetz, Wasserversorgung und öffentliche Verkehrsmittel werden durch Computersysteme gesteuert. Sie sind lebenswichtige Infrastrukturen für die Zivilgesellschaft. In einem Cyberkrieg sind sie attraktive Angriffsziele. – Wie wichtig ist Ihnen die Sicherheit dieser Computersysteme?

Cyberangriffe von Militärs und Geheimdiensten sind auch nach Überzeugung von Sachverständigen der NATO Kriegshandlungen. Cyberangriffe könnten konventionelle militärische Reaktionen provozieren. Wer Cyberkriegsattacken durchführt, beschwört erhebliche Eskalationsgefahren herauf und gefährdet die internationale Sicherheit.

Cyberkrieg – vom Ausspähen bis zum Angreifen von Computersystemen – ist nicht, wie uns gern glauben gemacht wird, eine „saubere“ Kriegsführung, sondern eine hochgefährliche Entwicklung für ein friedliches Zusammenleben auf dieser Welt. Diese betrifft uns alle.

cyberpeace

eine Kampagne des FIfF