Our Goals

Cyberpeace is a countermodel to the military colonisation of cyberspace. The objective of cyberpeace is to revive the once commonplace idea that our global networks should promote peace and international understanding, which is part of the FIfF's mission.

FIfF therefore makes the following demands:

- to condemn each and every form of cyber warfare
- communications networks exclusively for civil purposes
- to end and prevent mass espionage, which is incompatible with human and constitutional rights
- to step back from a doctrine of security, which labels everyone a suspect
- to untangle military command and secret services and reinstating civil control over both

Our cyberpeace campaign puts pressure on politics to put our demands into effect.

We want to attain:

- the end of blanket surveillance
- renouncement of the development and deployment of offensive cyber weapons
- the protection of civil society via
  - international cooperation in the investigation of cyberattacks
  - mandatory disclosure of IT vulnerabilities
  - adequate funding of civil institutions enabling them to protect their IT infrastructures.

Our positions with respect to cyberpeace are formulated in these fourteen demands :

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

How to participate!

A broad political initiative is needed to end the cyber arms race. Please support our campaign, get yourselves and others informed and motivated, spread our message. Get involved:

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

The bridge foundation supports and provides funding for the campaign. Partners are Campact , the Chaos Computer Club e.V., Humanistische Union e.V., Kooperation für den Frieden and others.

About FIfF

We are a convention of people who take a critical stance towards the consequences of the deployment of informatics (computer science and related fields) and information technology in our society. The FIfF originated in 1984 as a part of the peace movement. Besides many other problematic aspects of information society, the interconnection between IT and the military business has been a main focus of FIfF.

Address:	Geschäftsstelle FIfF e.V. Goetheplatz 4; 28203 Bremen
Phone:	+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 and cyberpeace.fiff.de

FIfF is funded from donations and membership fees to remain independent.

Account for Donations
at Bank für Sozialwirtschaft (BFSW)

IBAN:	DE79 3702 0500 0001 3828 03
BIC:	BFSWDE33XXX

For donations receipt
please state your address as reference
in your bank transfer formular.

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

cyberpeace

cyberpeace.fiff.de

a Campagne by

Forum of
Computer Scientists and IT-Professionals
for Peace and Social Responsibility

The Goal of Global Espionage: Cyberwar

The global eavesdropping on human telecommunications on the internet and the phone network is already a massive violation of civil liberties. But its goals go beyond mere surveillance: it is an integral part of the current military doctrine known as cyberwar.

In your car, there are upto 1,500 microprocessors at work. Many of these are security relevant. How much do you value the security of these computer systems?

The computer systems used for spying on us, like XKeyScore and Prism, are capable of detecting vulnerabilities in every computer system that gets caught in their dragnet surveillance. These systems pave the way to automated attacks. Surveillance is then followed by manipulation of systems with viruses and trojans, exploits are weaponised. Computer espionage and attacks are directly related. The targets: computers used by the UN, the EU commission and civil organisations. Other targets are private companies, public infrastructure and finally private individuals.

To operate more efficiently and subvert security systems, secret services work to have backdoors integrated in computer systems, and by various means "convince" IT companies to cooperate. They buy knowledge about undisclosed vulnerabilities as well as tailor-made exploits on the black market. If they can, sometimes the secret services introduce the vulnerabilities themselves.

Civil aviation would be impossible without air traffic control, aircraft guidance systems, satellite-assisted navigation. This is made possible by a highly complex digital infrastructure. How highly do you rate the security of these computer systems?

Civil Information Society Taken Hostage in Cyberwar

Civil society is highly and increasingly dependent on working computers, and on the internet. Meanwhile, spying agencies do everything they can to undermine the security and dependability of such systems.

Cyberweapons are the next step. Their purpose is to effect direct damage and pursue military goals. Computer viruses such as Stuxnet are cyberweapons. They are being distributed by state agencies to distribute malware. In the wild, these programs built for sabotage and destruction may cause large-scale, uncontrolled collateral damage in civil systems.

Nor are the NSA and their allies acting alone: there is a worldwide rush for armament in the computer domain. Throughout the world, secret services and military commands are ramping up on covert means for sabotaging and owning computers and the internet. The "Command for Strategic Intelligence" of the German Bundeswehr and the BND operate in much the same way.

The chemical plant in your neighbourhood is controlled by computers. State malware is able to sabotage systems, as the Stuxnet example has showed. How much do you value the security of these computer systems?

Cyber Attacks as Acts of War

Secret services such as the NSA double as combat support units for the military. The NSA, with its billion-dollar budget, is the best-equipped hacker army of the world. It wages a cyberwar against friend and foe alike.

Cyber attacks by military forces and secret services are acts of war, also according to NATO experts. Cyber attacks could provoke conventional military reactions. Whoever perpetrates them conjures up major dangers of escalation and endangers international security.

The Internet, the power grid, water supplies as well as public transport systems are controlled by computers and present highly attractive targets for military attacks in cyberwarfare. At the same time, these are vital infrastructures for civil society. How highly do you rate the importance of the security of these computer systems?

Cyberwar – ranging from computer espionage to attacks on computer systems – is therefore not a harmless or "clean" form of warfare as one would have us believe. It is a highly perilous development as far as our peaceful coexistence is concerned. It concerns us all.

cyberpeace

a Campagne by FIfF