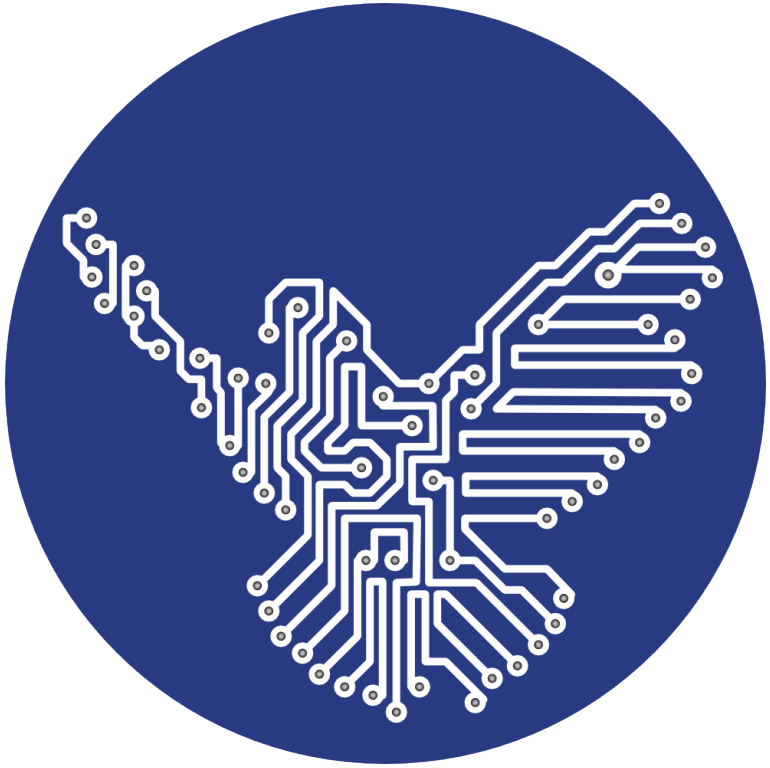
Forum InformatikerInnen
für Frieden
und gesellschaftliche Verantwortung e.V.

Cyberpeace – FIfF-Campaign

Spokespersons:

Sylvia Johnigk, Munich
sylvia.johnigk@fiff.de

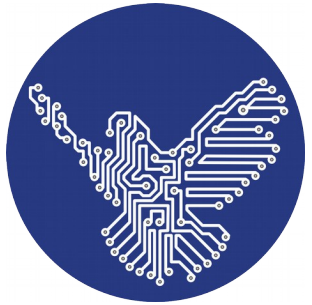
Stefan Hügel, Frankfurt
stefan.huegel@fiff.de



Funded by

stiftung bridge Bürgerrechte in der digitalen Gesellschaft

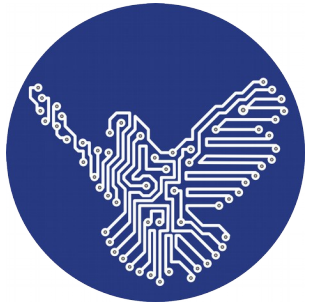
FIfF –
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung



Who we are

- Computer professionals for peace and social responsibility, founded 1984
- About 600 members, headquarters in Bremen
- Ours is a critical view on the social impacts of the use of information technology

FIfF – our Cyberpeace-Campaign



Our cyberpeace campaign

- We have launched our *Cyberpeace* campaign to address the threats emerging from cyber warfare policies

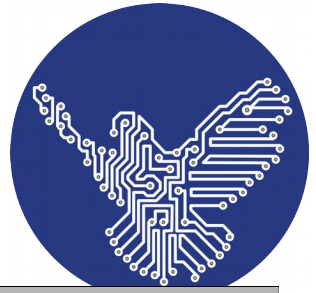
Long-term goals

- Proscription of any kind of cyber warfare
- Guaranteed integrity of Internet that is primarily used peaceful and protected against military misuse
- Prohibition of surveillance of the civil society that is violating the human rights
- Disposing a security doctrine that puts everyone under general suspicion

Short-term campaign goals

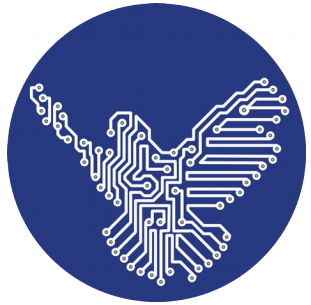
- Arms control of offensive cyber weapons and surveillance technology
- Dismissal of development and use of offensive cyber weapons
- Obligation to make IT-vulnerabilities public
- Communication infrastructures that are, by law, secure against surveillance

Definitions



Term	Description
Cyberpeace	By Cyberpeace, we mean peace in Cyberspace in a very general sense: Peaceful use of Cyberspace for the benefit of human kind and the environment. This includes the absence of all acts of Cyberwar, but also the use of the entire communication infrastructure for international understanding.
Cyberspace	Any information and communication infrastructure, hardware or software, public or private, open or restricted. This obviously exceeds the Internet. It might include tools not connected to a network, e.g. if an USB-stick is used for distributing malicious software.
Cyberwar	Any kind of war between nations, as defined in international law, which utilizes services provided in Cyberspace.
Cybercrime	Criminal action, or rather illegal action punishable by law, which utilizes services provided in Cyberspace.
Cyber terrorism	Violent criminal action by non-governmental actors, which seeks to change political systems by causing fear and insecurity. Cyber terrorism is a particular, exceptionally severe type of Cybercrime.
Cyber strike	Martial attack exploiting infrastructure provided by Cyberspace.
Hacktivism	Political activism using services provided by Cyberspace. It does not intend to cause damage and does not use violence.
Online protest	Protest action in Cyberspace, which does not use violence or cause damage. Online protest can include forms of civil resistance.
Cyber weapon	Any software or hardware that can be used to carry out a Cyber strike by exploiting a secret vulnerability. Cyber weapons usually exploit vulnerabilities which are kept secret, and their destructive character arises from the impossibility to mitigate the effects of the exploit. By making the vulnerability public the Cyber weapon is defused.

The heart of our campaign are our cyberpeace claims



- 01 | No offensive or pre-emptive strikes in cyberspace
- 02 | Exclusively defensive security strategy
- 03 | Disarmament
- 04 | No conventional response to cyber attacks
- 05 | Geneva Convention in cyberspace
- 06 | Cyberpeace initiative on government level

07 | Democratic control of the Internet and cyber security strategies

08 | Online protest is not a crime

09 | Well-defined and demilitarized political language

10 | Vulnerabilities must be disclosed

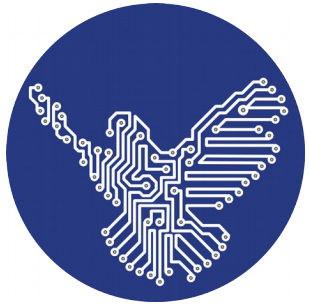
11 | Protect critical infrastructures

12 | Establish cyber security centers

13 | Promotion of (junior) IT experts

14 | Promotion of Open Source

01 | No Offensive or Pre-emptive Strikes in Cyberspace



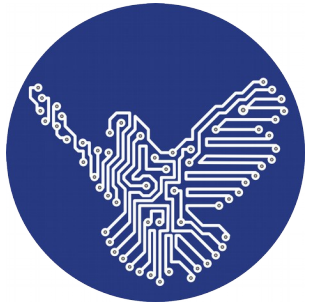
What we call for

- Nations must publicly declare to abstain from offensive, particularly pre-emptive cyber strikes – offensive cyber strikes are generally not considered legitimate
- Economic interests, such as intellectual property rights, are not considered a legitimate reason for war
- Cybercrime, in contrast to cyberwar, must be targeted by means of criminal, not by military law

Motivation

- All nations have the right to defend themselves
- Nations do not have the right to attack or to commit an offensive or pre-emptive strike
- We demand that governments use no cyber weapons for this purpose in any way

02 | Exclusively Defensive Security Strategy



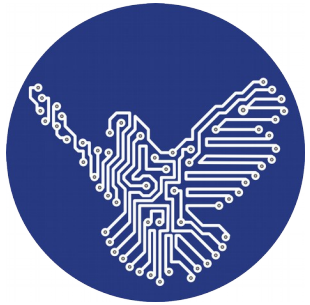
What we call for

- As offensive cyber strikes are not considered legitimate, nations have the obligation to maintain a clearly defensive security strategy concerning cyber strikes
- Nations must commit to neither develop nor use offensive cyber weapons

Motivation

- All nations may develop a security strategy including the use of defensive cyber weapons
- Similarly, all nations have the right to defend themselves
- However, they do not have the right to attack
- We demand that governments neither develop offensive strategies nor use cyber weapons for offensive purposes

03 | Disarmament



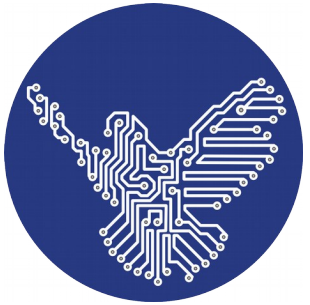
What we call for

- Cyber weapons are a threat to peace and security for all
- We demand that nations and their government disarm, in cyber space as in the “real world“
- This must be accomplished by international treaties
- Although disarmament of (cyber) weapons is highly desirable, keeping such weapons for defensive means is considered legitimate, and so are hacker tools

Motivation

- Cyber weapons, like conventional weapons, are a threat to the security of everyone
- Cyber weapons rely on undisclosed vulnerabilities
- Cyber weapons are hard to control since they potentially affect all software systems with specific vulnerabilities, not only the targeted ones

04 | No Conventional Response to Cyber Attacks



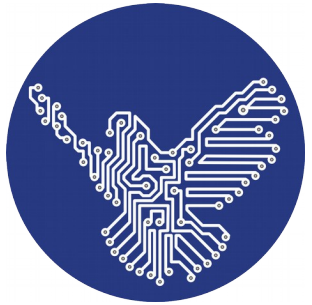
What we call for

- Conventional weapons must not be used in response to a cyber strike

Motivation

- It is impossible to unequivocally attribute cyber strikes to an aggressor
- Responding to a cyber attack with conventional weapons would cause an escalation of forces which might become uncontrollable

05 | Geneva Convention in Cyberspace



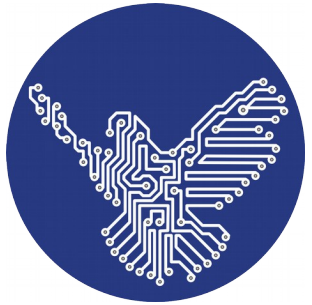
What we call for

- All applicable requirements of the Geneva Convention must be respected in cyberspace as in the “real world“
- Especially, vital infrastructure for the civil population must not be targeted; this might include communication infrastructure if human lives depend on it; this includes so-called collateral damage
- A violation of this principle is considered a war crime
- We demand that nations and their governments commit to common principles agreed upon in international treaties on conflicts

Motivation

- Critical infrastructures are attractive goals to target in wars since their failure fundamentally weakens an enemy
- However, failure of infrastructure seriously affects civil society as well if vital, life-supporting facilities like water supply, energy, health care etc. are attacked

06 | Cyberpeace Initiative on Government Level



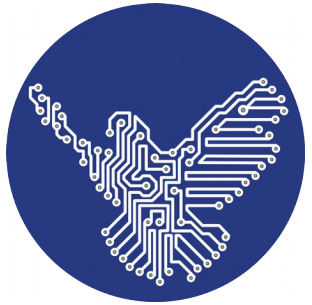
What we call for

- We demand that governments launch an international cyberpeace initiative
- Peace studies and the development of peace-keeping strategies in cyberspace must be promoted on all levels

Motivation

- We consider critical communication infrastructure – cyberspace – a vital basis for the future of mankind
- To endanger this critical infrastructure means to jeopardize our future

07 | Democratic Control of the Internet and Cyber Security Strategies



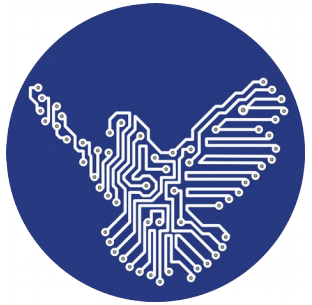
What we call for

- Democratic control must be ensured and separation of powers must be respected
- Parliaments must control cyber security strategies and their implementation; cyber strikes have to be approved by parliament
- Cyber security strategies must be an outcome of legislative democratic decision-making

Motivation

- Today, cyber strategies are developed and implemented secretly
- Transparent cyber security strategies are confidence-building and contravene an arms race in cyberspace

08 | Online Protest Is not a Crime



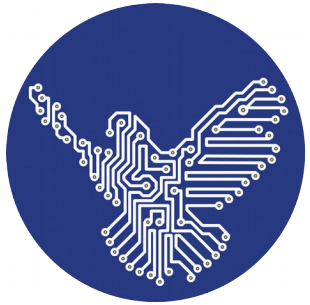
What we call for

- The right to civil resistance and online protest must be respected, assumed that no violence or damage is caused
- Online protest must not be criminalized or serve as a reason to start a war

Motivation

- Information and communication via the Internet nowadays is common practice, akin to a human right
- Protests against some companies can only take place in cyberspace, examples are consumer protests against online services
- To exercise fundamental rights – e.g., free speech or assembly – is not a crime
- It must not serve as grounds for military response or war

09 | Well-Defined and Demilitarized Political Language



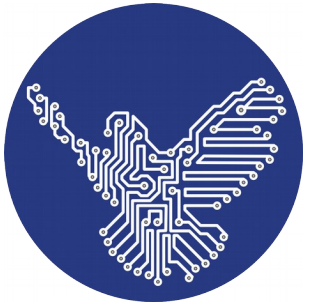
What we call for

- We demand the demilitarization of political speech
- We also demand a clear distinction and definition of wording:
  Cyberwar, Cyber terrorism, Cybercrime, Ethical hacking, Political forms of protest
  (A proposal of definitions is included in this set of slides)

Motivation

- Politics and media frequently use vague language in a misleading fashion, with the potential of escalating conflicts
- As an example, using the term “cyberwar“ suggests that only military solutions are possible

10 | Vulnerabilities Must Be Disclosed



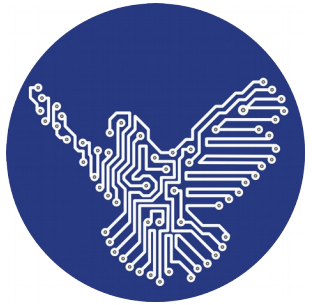
What we call for

- Everyone must disclose vulnerabilities responsibly and within a reasonable timeframe
- Public authorities in particular must protect the integrity of information systems
- This is derived from the fundamental right to IT-systems, whose confidentiality and integrity are to be safeguarded

Motivation

- Today, intelligence agencies seem to exploit (and create) vulnerabilities, eventually withholding them for future use
- These vulnerabilities can be misused for criminal means
- If disclosed, they are likely to be fixed quickly; however, a sufficient timeframe must be provided before public disclosure
- Thus, public awareness and trust in defensive security strategies will be enhanced

11 | Protect Critical Infrastructures



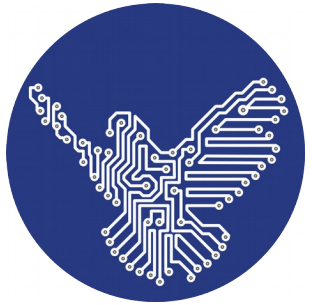
What we call for

- Operators of critical infrastructure must be obliged to protect this infrastructure from cyber attacks
- They must be obliged to implement and operate secure systems
- They must not rely on state authorities or the military for protection
- Wherever possible, critical infrastructure – like nuclear power plants – must be separated from the public Internet

Motivation

- Currently, critical infrastructures are often easy to reach from the Internet
- Since vulnerabilities are unavoidable, they can be attacked
- Security of critical infrastructure must be verified by competent and transparent audits and tests

12 | Establish Cyber Security Centers



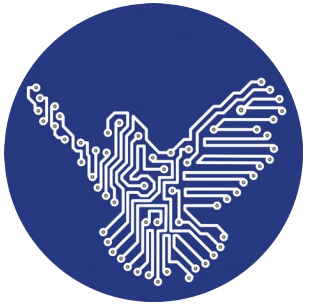
What we call for

- Cyber security centers must be established to deal with cyber threats effectively
- They must be consequently peace-oriented and work in a transparent fashion
- Police, intelligence and military authorities must be operated independently and their information exchange regulated according to democratic principles

Motivation

- Facilities are required which ensure dealing with threats from cyberspace effectively and implement appropriate instruments to provide and enhance cyber security
- Cyber security centers must be organized in a way which preserves fundamental civil and human rights

13 | Promotion of (Junior) IT-Experts



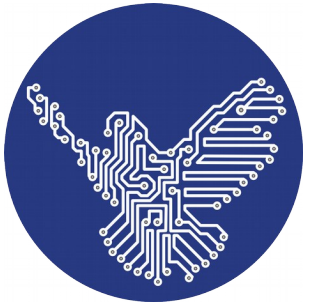
What we call for

- The quality of IT products – particularly with regard to IT security – must be enhanced significantly to reduce their vulnerability
- State authorities and economic enterprises must invest in qualified experts for IT and IT-security in particular
- Academic education must be broadened to cover ethical and political aspects as well as the assessment of technological impact

Motivation

- Today, there is a lack of IT experts and knowledge for effective protection against cyber attacks in Europe
- This lack is intensified because there are IT-experts working at compromising IT systems instead of improving their security
- Currently, instruction covering the impact of technology on society seems to vanish from the curriculum; this development must be reversed

14 | Promotion of Open Source



What we call for

- Open Source software must be promoted and used by public authorities
- It must be preferred particularly for critical infrastructure
- Public authorities must also promote and insist on independent reviews and inspections
- However, care must be taken to avoid an illusion of security

Motivation

- In contrast to proprietary software, Open Source software allows independent inspections and reviews, though it does not guarantee security
- This reduces the probability of back-doors significantly
- In principle, the entire community can conduct these reviews

Discussion

Visit us

Currently in German language only...