4 SUMMIT VIENNA 2015 IS IS

Extended Abstract

Cyberpeace
Promoting human rights and peaceful use of the Internet

Stefan Hügel

FIfF e.V., Goetheplatz 4, 28203 Bremen, Germany

E-Mail: sh@fiff.de

Tel.: +49 151 17274808

Accepted:

Introduction

Information Technology and Communication Infrastructures – commonly referred to as the Cyberspace – have been in the focus of military institutions and secret services from the beginning. Not only was the Internet originally introduced by U.S. military institutions – it emerged from the Arpanet, named after the Advanced Research Project Agency (ARPA) of the U.S. Department of Defense – it also serves as an infrastructure for military action today, being under surveillance by secret services and military agencies to gather information for cyber- and conventional military means and used for cyber attacks in order to compromise the infrastructure of the percepted enemy.

FIfF has launched the Cyberpeace campaign [1] to address the threats emerging from cyber warfare policies and to push back the colonization of the communication infrastructure by the military and surveillance of the entire population, which, in addition, sets everyone under suspicion. Our goals are non-violent conflict resolution, arms control of cyber weapons and surveillance technology, dismissal of development and use of cyber weapons, the obligation to make IT vulnerabilities public and the promotion of communication infrastructure, which is, by law, secure against surveillance. We want the Internet and all infrastructure to be used in a peaceful fashion and to be protected against military misuse. We want that secure communication be ensured while preserving and promoting human and civil rights.

In order to achieve these goals, we focus on four issues we elaborate on in the following chapters:

- **Rebuilding trust**, which has been seriously affected by the worldwide secret service surveillance recently disclosed. This degradation of trust seriously affects a main resource of political, social and economic cooperation.

- **Condemning offensive action** and promoting non-violent means of conflict resolution by assuring that nations are not willing, and actually cannot, carry out offensive strikes against each others' vital infrastructure, by mutual agreements and control.
- **Securing vital infrastructure** by technical means – building up security provisions, which prevent aggressors from infiltrating computer networks and computer systems, which are vital for the supply of a society with basic services, as energy, health care, communication etc.
- **Preserving political control, democracy and security** by a Cyberpeace initiative on government level, democratic control of the Internet and cyber security strategies and ensuring an demilitarized political language.

This is our framework for the claims we require in our Cyberpeace campaign for a peaceful use of the Internet and all information and communication infrastructures.

Rebuild trust

Our society is based on trust – this is what sociologist Niklas Luhmann pointed out in his book Vertrauen („Trust“) in 1968 [4] – long before the Internet arised to influence our entire life. Luhmann points out, that trust ist essential to reduce the social complexity of our societal environment. This is necessary to enable us to take all the decisions which everyday life requests us to. With a lack of trust, the number of decisions to take would become overwhelming; we would not be able to cope with everyday life. Security expert Bruce Schneier [5] illustrates this convincingly:

„*Just today, a stranger came to my door claiming he was here to unclog a bathroom drain. I let him into my house without verifying his identity, and not only did he repair the drain, he also took off his shoes so he wouldn't track mud on my floors. When he was done, I gave him a piece of paper that asked my bank to give him some money. He accepted it without a second glance. At no point did he attempt to take my possessions, and at no point did I attempt the same of him. In fact, neither of us worried that the other would. My wife was also home, but it never occurred to me that he was a sexual rival and I should therefore kill him.*“

Using Internet services also requires trust – and we are commonly willing to provide this trust, e.g. by calling web sites, often without double-checking their trustworthiness. We often simply rely on our intuition. We call web sites without encryption, trusting, that nobody would eavesdrop on our communication. Also, we do not encrypt our e-mail – nobody would read along and if so, what could possibly happen?

The recent disclosures should have changed our minds. Edward Snowden provided us with the consciousness of world-wide surveillance of the entire communication by secret services [3]. Authors like Josef Foschepoth [2], Professor of history from the University of Freiburg, made clear that modern mail and communication surveillance started from the end of World War II – not only in the eastern states, but also in the Federal Republic of Germany. Currently, an inquiry committee investigates unconstitutional surveillance by the German federal intelligence service (Bundesnachrichtendienst). Austria, as an example, just filed a case due to punishable espionage – formally against the unknown; actually it clearly affects german authorities.

Trust cannot be enforced by political claims – it grows (and vanishes) due to actual action. Nevertheless, political action is necessary to restore trust and to enforce the demands we derive from the second and third issue mentioned above.

Condemn offensive action and promote non-violent conflict resolution

Real peace is only possible, if all parties abstain from armament and from attacking each other. Since unilateral measures of disarmament lead to the risk of insufficient defense capacities, bilateral or multilateral agreements must be concluded. These agreements should aim at structural inability to attack and the limitation of military capacity to defense. Strict rules must be agreed upon to protect people, if in spite of focusing military strategies on defense, a conflict might arise. In detail, from our point of view the following demands must be requested [1]:

- **No offensive or pre-emptive strikes in cyberspace.** Of course, each state has the right to defend itself against attacks – cyber attacks as well as conventional attacks. But we reject any kind of offensive attacks, including pre-emptive strikes to circumvent an assumed attack by a potential opponent. We request states to publicly declare to abstain from offensive and pre-emptive cyber strikes and every kind of the offensive use of cyber weapons. Never should economic interests be a legitimate reason for cyber attacks, e.g., assumed violation of intellectual property rights. Governments shall not use cyber weapons for this purpose.
- **Exclusively defensive security strategy.** Although, of course, all nations have the right to defend themselves against attacks, no nation, in our opinion, has the right to attack itself. So states should maintain a clearly defensive cyber strategy; they should publicly commit not to develop nor use cyber weapons for offensive means.
- **Disarmament.** Cyber weapons, as all kinds of conventional weapons, are a security threat to everyone, as they may affect all kinds of infrastructure, vital to human life and well-being. Relying on (undisclosed) vulnerabilities, the effect of cyber weapons is not restricted to the target of an attack. Instead, potentially it affects all systems with the specific vulnerabilities exploited for this attack.
- **No conventional response to cyber attacks.** We do not consider it acceptable, to respond on cyber attacks using conventional weapons. This would cause an escalation of forces which might easily become uncontrollable. In addition, the attacker cannot be easily determined (attribution problem), so the risk of conventional strikes on innocent victims is high.
- **Geneva Convention in cyberspace.** Critical infrastructure facilities, in a war, are attractive targets, since their failure would fundamentally weaken an enemy. However, failure of infrastructure also seriously affects civil society by attacking life-support facilities like water supply, energy, health care etc. This vital infrastructure for the civil population must not be targeted. From our point of view, a violation of this principle should be considered a war crime. We urge nations and their governments to commit to common principles agreed in international treaties. The Tallinn-Manual might be a start, but it would have to be reworked to emphasize the avoidance of the use of force – e.g., conventional responses on cyber attacks are possible according to the Tallinn-Manual, which we reject.

Secure vital infrastructure

Although we prefer all parties in a conflict to abstain from using military force and employ non-violent means of conflict resolution, we must be aware, that defensive military capacity has to be built up to intervene in cases, when short-term non-violent conflict resolution is not possible and a military cyber attack takes place. Additionally, cyber attacks from non-military origins have to be considered, such as cyber crime and cyber terrorism – a threat strongly expanding. Public authorities and business companies will have to meet sufficient security measures, and constantly update them with regard to the evolution of capacity on the attackers' side. The range spans from script-kiddies, hackers, criminals to secret services with virtually unlimited capacity to set up attacks.

The following demands, from out point of view, are preconditions to make secure system operation possible – they do not guarantee it [1].

- **Disclose vulnerabilities.** Cyber attacks often rely on undisclosed vulnerabilities. Vulnerabilties are employed for all kinds of cyber attacks – actual cyber attacks, which aim to destroy the infrastructure of an enemy, and each action, which seeks to prepare for war, as the surveillance by secret service authorities. To accomplish this, public authorities might accept and create vulnerabilities and keep them as a secret for future use. At the same time, these undisclosed vulnerabilities might be misused for criminal means. So we request full disclosure of vulnerabilities – within a reasonable timeframe. We expect that disclosed vulnerabilities will be fixed very quickly. This will enhance public awareness and trust in defensive security strategies.
- **Protect critical infrastructure.** Currently, critical infrastructures are often easily to access from the internet, as they are connected to publicly accessible services. In some cases, it might be reasonable to connect services to the public internet, in order to enhance accessability and quality of public services. Nevertheless, it must be considered, that vulnerabilities are unavoidable in many cases and may be employed to attack by hostile users. So security of critical infrastructure must be verified by competent and transparent audits and tests. 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 even the military. Wherever possible, critical infrastructure – like nuclear power plants – must be separated from the public internet.
- **Establish cyber security centers.** Facilities are required, which ensure to deal with threats from cyberspace effectively and implement appropriate instruments to provide and enhance cyber security. They must be organized in a way which preserves fundamental civil and human rights. So these cyber security centers must be established to deal with cyber threats effectively. They must be consequently peace-oriented and work in a transparent fashion. Separation between police, intelligence and military authorities must be provided.
- **Promote (junior) IT experts.** Today, there is a lack of IT experts and knowledge for effective protection from cyber attacks in Europe. This is even increased due to IT experts working for compromising IT systems instead of improving their security. So the quality of IT products – particularly with regard to IT security – must be enhanced significantly to reduce their vulnerability. Governmental authorites and economic enterprises should invest in qualified

junior experts for IT in general and IT security in particular. Academic education must be broadened to cover ethical and political aspects as well as the assessment of technological impact.

- **Promote Open Source.** In contrast to proprietary software, open source software may allow independent inspections and reviews. This reduces the probability of back-doors significantly. In principle, the entire community can conduct these reviews. So open Source software should be promoted and used by governmental authorities. It should be preferred particularly for critical infrastructure. Governmental authorities should also promote independent reviews and inspections. Nevertheless, we have to be aware, that open source is not the solution to all our security challenges – it is not sufficient, that it is virtually possible to inspect systems and find its vulnerabilities – reviews must be conducted in practice by competent reviewers, and sufficient resources must be granted to achieve the effort necessary. But still, there is no guarantee to eliminate all vulnerabilities critical to confidentiality, integrity and availability of the systems.

Preserve democratic political control

The demands mentioned before need sufficient attention on the political level. Organisational and legislative measures must be taken to promote confidentiality, integrity and availability, bring forward democratic control and civil rights such as free speech, and, last but not least, take care of appropriate political language [1].

- **Cyberpeace initiative on government level.** From our point of view, the cyberspace – viz. all kinds of critical communication infrastructure – is a vital basis for the future of mankind. So to endanger the integrity of this critical infrastructure means to jeopardize our future. A cyberpeace initiative must be launched to preserve the confidentiality, integrity and availability of the communication infrastructure. Peace studies and the development of peace keeping strategies in cyberspace should be promoted.
- **Democratic control of the Internet and cyber security strategies.** Today, cyber strategies are developed and implemented secretly. Meanwhile, only transparent cyber security strategies can be confidence-building measures and counteract an armament race in cyberspace. So democratic control and separation of powers are required. Parliamentary approval for cyber security strategies and its implementation must be mandatory. Cybersecurity strategies should be an outcome of legislative democratic decision-making. They have to be controlled by a division of powers.
- **Online protest is not a crime.** Information and communication via the internet nowadays is common practice. So to exercise fundamental rights – e.g., free speech – must not be considered a crime. Especially, it must not serve as a reason for military response or war as well. Examples are consumer protests against online services. The right for civil disobedience and online protest has to be respected. Online protest must not be criminalized or even serve as a reason to start a war.
- **Well-defined and demilitarized political language.** Finally, politics and media frequently use vague language with the effect of potential escalation of conflicts. E.g., using the term

„cyberwar“ might suggest, that only military solutions are possible. Cybercrime, in contrast to cyberwar, must be targeted by means of criminal law, not by military; this has to be reflected in political language.

We consider these four fields – trust, non-violent conflict resolution, securing vital infrastructure and democratic political control – an appropriate framework to achieve cyberpeace. We are convinced, that this framework and the demands will help us to take the political decisions to reject the military colonization, promote peace and human and civil rights in cyberspace.

Acknowledgments

The framework and the claims cited in this paper are a result of collaborative work in the Cyberpeace campaign team.

References and Notes

1. FIfF e.V.: Forderungen zum Cyberpeace. *FIfF-Kommunikation* **2014**, *4*, 62-65.
2. Foschepoth, J.: *Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik*; Vandenhoeck & Ruprecht: Göttingen, Bristol, Germany, U.S.A., 2002
3. Greenwald, G.: *No place to hide. Edward Snowden, the NSA, and the U.S. Surveillance State*; Metropolitan Books: New York, U.S.A., 2014
4. Luhmann, N.: Vertrauen; 4th ed.; Lucius & Lucius: Stuttgart, Germany, 2000
5. Schneier, B.: *Liars & Outliers. Enabling the Trust that Society needs to Thrive*; John Wiley & Sons: Indianapolis, U.S.A., 2012