Jürgen Altmann, Francesca Vidal:

Ethics of cyber warfare

The Internet has opened up tremendous new possibilities for the exchange of information. It has become one pillar of modern life. It is a global network that has to be available continuously for the functioning of economy and policy as well as private households. At the same time it constitutes a fragile infrastructure that can be disturbed – or used for malicious purposes. The principal possibilities range from manipulation or deletion of data to interference with critical infrastructures. Criminals attack servers and plant worms or viruses on computers to draw money from others' accounts or to spy on secret information. Hackers invade networks for protesting.

Even though such actions often require deep knowledge and considerable sophistication, they are dwarfed by far by state preparations for cyberwar. The US has declared cyberspace the fifth domain of military operations, beside land, sea, air and outer space. Other countries follow this precedent.

Whereas protection and defence against cyber attack is clearly legitimate, preparations for cyber offence raise many problems and can become very dangerous. Attacks in cyberspace can have direct consequences in the real world. Indirectly they can lead to counter-attack by real weapons. Cyberwar and its links to real-world war present challenges for security policy and international law, as can be seen in a developing body of academic and practical literature and differing approaches, still in flux, by various countries.

New possibilities of warfare also pose questions with respect to ethics. Here the issues are not only ethical assessment of virtual attacks and the consequences in reality, but also consequences that military preparations for cyber warfare can have on the civilian use of the Internet. Other aspects are: How could the infrastructure of ubiquitous communication be used malevolently? How do different countries deal with the problem of (national and international) security in cyberspace?

To shed light on such questions to do with the ethics of cyber warfare, the present issue of the International Review of Information Ethics presents four articles.

In his paper "*Cyber War: Will it define the Limits to IT Security?*" Ingo Ruhmann shows that cyber warfare is one part of military information operations that have a long tradition. Existing gaps in civilian information security and insufficient law enforcement, in particular due to the international character of the Internet, are being used as arguments for offensive military preparations. They are directed against a very broad range of potential adversaries, including civilians and allies. IT security is increasingly moved from the civilian to the military domain. Surveillance, espionage and IT system manipulations – alleviated by forced co-operation by the IT industry –violate legal and ethical principles and undermine the foundations of a civil information society.

Also Ute Bernhardt's essay "*Google Glass: On the implications of an advanced military command and control system for civil society*" deals with the modification of civil society through wide-spread information and communication technology and the ethical implications. She describes the possibilities of using augmented reality at the example of Google Glass. Military uses of head-mounted displays and networking of soldiers have a twenty-year history. Civilian uses, in particular in co-ordinated groups with central supervision, open new possibilities for observation by police or intelligence, for crimes and their rehearsals, and for terrorist attacks. Since incorporating countermeasures against criminal uses would be difficult and convincing arguments for legitimate uses in the civilian sphere have not been made, Google Glass-like systems pose the question whether IT professionals can ethically approve the work on such systems at all.

In his paper "*Uma análise sobre a política de informação para a defesa militar do Brasil: algumas implicações éticas*" (*An analysis about the information policy for the military defence of Brazil: some ethical implications*) Bruno Nathansohn analyzes the development of the Brazilian defence information policy particularly in regions of Brazil's geostrategic importance. The Brazilian government faces a dilemma between international cooperation based on a multilateral perspective on the one hand, and the threats to its information infrastructure arising from this cooperation on the other. The fragility of the Brazilian information infrastructure is due to the

ISSN 1614-1687

lack of an appropriate information policy that could and should support the role of the country in the international power system. The paper deals with these issues as related particularly to cyber warfare from an ethical and legal perspective.

The article "*Creating a secure cyberspace – Securitization in Internet governance discourses and dispositives in Germany and Russia*" written by David Gorr and Wolf Schünemann deals with the emerging policy field of Internet governance in general and the challenge of cybersecurity in particular from a political science perspective. After some theoretical reflections on the structural difficulties that the regulators of cyberspace 'naturally' face they present the social-constructivist concept of securitization in order to explain how the internet is frequently constructed as a security problem by societal actors in different countries as well as on the international level. Finally, they illustrate their observations by a comparative analysis of cybersecurity discourses and dispositives in Germany and Russia.

All in all these articles add important considerations to the on-going debate on the ethics of cyber warfare. We want to thank the authors, but also the anonymous reviewers who contributed much to the preparation of this special issue.