Computer science for peace

He is conducting research and teaches on the interface between computer science and peace and conflict research. Professor Christian Reuter explains in the following interview how IT can be used during war and to bring about peace.

Photo: Hessen schafft Wissen – Jürgen Kneifel

Professor Christian Reuter

Professor Reuter, the Council of Science and Humanities is calling for the further structural development of scientific and technical peace and conflict research in Germany. How well prepared are we here in this respect?

We are clearly less well prepared in comparison to peace and conflict research in the political sciences. Greater importance was placed on this field in the past. Scientists were already focussing on dual use issues back in the 1950s and 1960s and thus considering, for example, how they could help to ensure that nuclear power was only used for supplying energy and not also for producing weapons-grade materials. Today, this type of research is underrepresented at German universities. From a structural perspective, this research is currently only permanently carried out at the Carl Friedrich von Weizsäcker-Centre at the University of Hamburg and here at TU Darmstadt. Yet these topics are more current than ever. We should by no means think that things have become more peaceful everywhere. On the contrary, chemical weapons are being used in Syria and international treaties on the disarmament of long-range missiles have just been terminated. Certainly, we are also faced with totally new challenges in cyberspace.

What role do cyberwarfare and cyber forces play nowadays?

Harmful activities taking place between countries in cyberspace are now the norm and cyber forces have become a new pillar of warfare alongside land, air and sea forces, and activities being carried out in space. Many countries and alliances are building up their cyber capacities. This is true for the USA and also for NATO as well as individual countries such as Germany. Money and resources are being invested in this area everywhere and new units and powers are being build up.

What is a cyberweapon exactly?

It is certainly nothing like what we are familiar with from the Star Wars films. The whole situation is much more subtle. Usually, it involves security vulnerabilities in software and hardware combined with code to exploit them. These vulnerabilities are becoming an increasingly valuable commodity. If you want to misuse them for military conflict, you don't notify the manufacturers about them but collect them in your own weapons arsenal. If you have exclusive knowledge about these types of backdoors, you have a decisive advantage for influencing the outcome of a war. Anyone who has been active in cyberspace for a long time can use this knowledge to penetrate IT systems operated by the enemy. This poses a threat not just to military systems but also to civil ones – if, for example, not only the missile base but also an energy supply system becomes the target.

Is it possible to track these types of hostile activities?

In general, we are unable to track them. If somebody launches a rocket, it can be seen on satellite images. However, it has still not been possible to fully understand and trace the hacker attack on the German government in December 2017. It is often not even possible to determine whether these attacks are simply criminal activities or espionage – which although they can be prosecuted under criminal law, would not trigger a war – or whether in cooperation with transnational players they are really intended to provoke a conflict between nations. The whole situation is a little blurred. We are seeing a dangerous normalisation of constant harmful attacks and hybrid conflicts. And this is not exactly promoting trust between countries.

Contact

Science and Technology for Peace and Security (PEASEC)
Prof. Dr. Christian Reuter
Phone +49(0)6151/16–20941
E-mail:
reuter@peasec.tu-darmstadt.de
https://peasec.de

Photo: shock / stock.adobe.com

Amongst other things, the PEASEC is carrying out research into resilient IT-based critical infrastructures.

You have raised the subject of dual use technology. What can you do in computer science to ensure that new, digital technologies are not misused in warfare?

This is not only about assessing the impact of technology or safeguarding infrastructures but importantly also about the conscious design of technology. We need to develop software right from the very beginning that is designed to provide as few opportunities as possible for misuse or use in conflict. However, the dual use problem represents a huge challenge especially in the area of information technology. It is still possible to change software relatively easily and adapt it for purposes other than its originally intended use.

In your institute, computer scientists work together with peace and conflict researchers. How does this work in practice?

Our research is carried out in areas where these two disciplines overlap. On the one hand, we utilise the methods of empirical social research and analyse, for example, the role of new technologies for peace and security. We examine questions such as: How is social media used in conflict situations? What dynamics are created there as a result? What narratives are used to manipulate opinions? We then develop technical solutions on this basis to prevent escalations such as so-called information warfare. For example, we have developed a plug-in for browsers called “Trusty Tweet” that flags up indicators of fake news. We are also working on software that analyses social media data to prevent misuse, such as the tracking of persons, from the outset.

I would imagine that this type of continuous, interdisciplinary cooperation is very demanding.

Yes. It presupposes that researchers can develop a deep understanding for the other field of research. But that’s not all. We have to get to the very heart of the issues together so that we clearly understand which specific points we want to focus on. The process does not begin by focussing on the technical issues. The starting point is always a deficit that has to be analysed in more detail in order to develop possible technical solutions for the benefit of society. At the same time, we also have to gain acceptance in our own relevant specialist fields. This is because we want to be able to introduce our findings into the individual disciplines at the very highest level so that our research becomes visible and others are able to build on it. This usually requires us to go the extra mile once again.

What is it that you would like to achieve in your own specialist field?

As computer scientists, we have a practical influence in this day and age on the whole of life. I would thus like to raise awareness for the fact that our work can also cause damage and we have to place more focus on value-based design in which not only monetary aspects play a role. Software can often result in unintentional developments in the wrong direction. Therefore, we have to learn to actively make decisions and already set the right course during the software development phase so that we can, for example, exclude certain types of use of the software or only provide certain modules in encrypted form. Everyone of us should become aware of these issues.

The interview was conducted by Jutta Witte.
She is a scientific journalist and history graduate.

Background:

Prof. Dr. Christian Reuter is head of the research group of Science and Technology for Peace and Security (PEASEC) at TU Darmstadt that was established in 2017. He is a member of the Department of Computer Science and is also affiliated to the Department of History and Social Sciences. The PEASEC team carries out research into the themes of “Safety-Critical Human-Computer Interaction”, “Information Technology for Peace and Security” and “Resilient IT-based (Critical) Infrastructures”. The group is closely intertwined with the cybersecurity profile area at TU Darmstadt (CYSEC) and the multi and interdisciplinary network IANUS in the Forum for Interdisciplinary Research (FiF) at TU Darmstadt.

https://peasec.de/2020/it-frieden

Latest publication:
“Towards IT Peace Research”:
https://peasec.de/2020/
towards-it-peace-research