SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE

Ethical Vulnerability Research
Automated Methods and Ethical Orientation

M.A. Kaya Cassing
Chair of Ethics of Digital Methods and Technologies,
Faculty of Philosophy and Educational Research
Prof. Dr. Sebastian Weydner-Volkmann

M.Sc. Johannes Willbold
Chair for Systems Security,
Faculty of Computer Science
Prof. Dr. Thorsten Holz

Ethical Vulnerability Research

The research subject of cybersecurity, i.e., information systems, can be found in almost every sector of modern society ranging from economics, science, and politics to personal lives. Hence, they exert a profound impact on society. Therefore, if cybersecurity researchers work on methods to interfere with these systems, it means they work on a method to interfere with aspects of society. While the intention is to improve the security of these systems, it prompts the risk of the researchers introducing insecurity into society by exposing previously unknown security issues. This risk burdens the ethical responsibility to handle the vulnerabilities conscientiously. However, security researchers are not trained nor particularly experienced in ethical discussions, prompting the need for external orientation and support. Although there are already common practices in cybersecurity that attempt to provide an orientation that could be seen as the beginning of applied Ethics of Cybersecurity, they currently need to be improved.

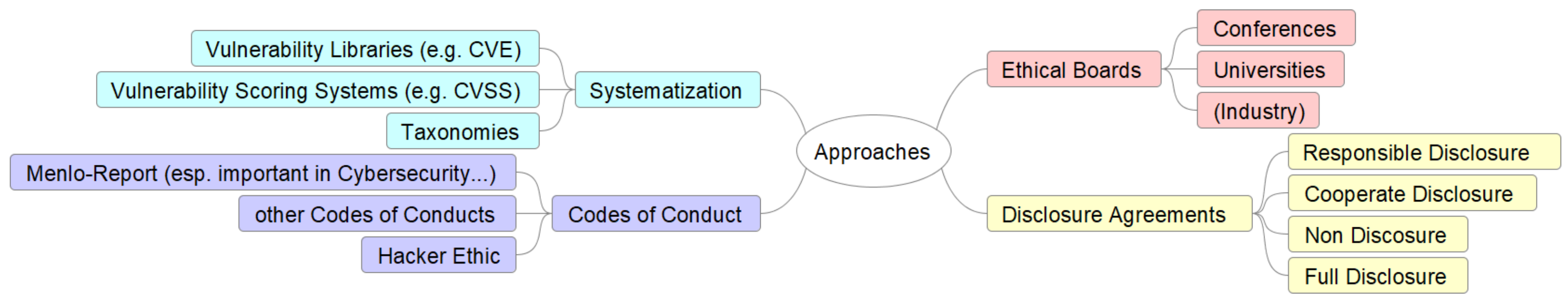
To this end, the project "Ethical Vulnerability Research" supports the development of ethics of cybersecurity through an analysis of the current state of ethical developments in the field from a meta-perspective on the one hand and through drawing parallels of other applied ethics to the ethics of cybersecurity on the other hand. To clarify the practical relevance of the topic, it is helpful to look at a novel and emerging research subfield in cybersecurity, the security of space and satellite systems. The following case study will serve as an example showing the room for improvement of ethical basics in cybersecurity.

Few pieces of technology have a similarly profound impact on our modern society as satellites. These space-born systems became essential parts of our modern lives by providing a plethora of essential and critical services ranging such as telecommunications, global positioning, and Earth observation. Especially in recent years, the number of satellites in orbit has grown exponentially in the wake of the New Space era, which has allowed cheaper deployment of satellites through falling launch costs and sinking development costs through commercial of-the-shelf parts. Despite their critical importance, little academic research has been conducted on space and satellite systems security. The research area only gained traction recently, providing the rare opportunity to observe a novel research area emerging and the ethics that accompany it. Satellite security is an especially interesting topic for ethics due to the long historical separation between the space systems engineering and security community and the prevailing notion of security-by-obscurity in satellite development.

Ethics of Cybersecurity

From an ethical perspective, a crucial step of research is the publication, especially if the research result consists of vulnerabilities (or methods to detect them). Due to the potential of misuse through a third party it can be risky (in some cases) to disclose a vulnerability or a detection method. The researcher has to evaluate whether they disclose a result that could lead to insecurity of the system and in turn to risks for society. In order to make this ethical decision, it could be helpful to have some guidance or instruction. This need of ethical orientation is currently only insufficiently met.

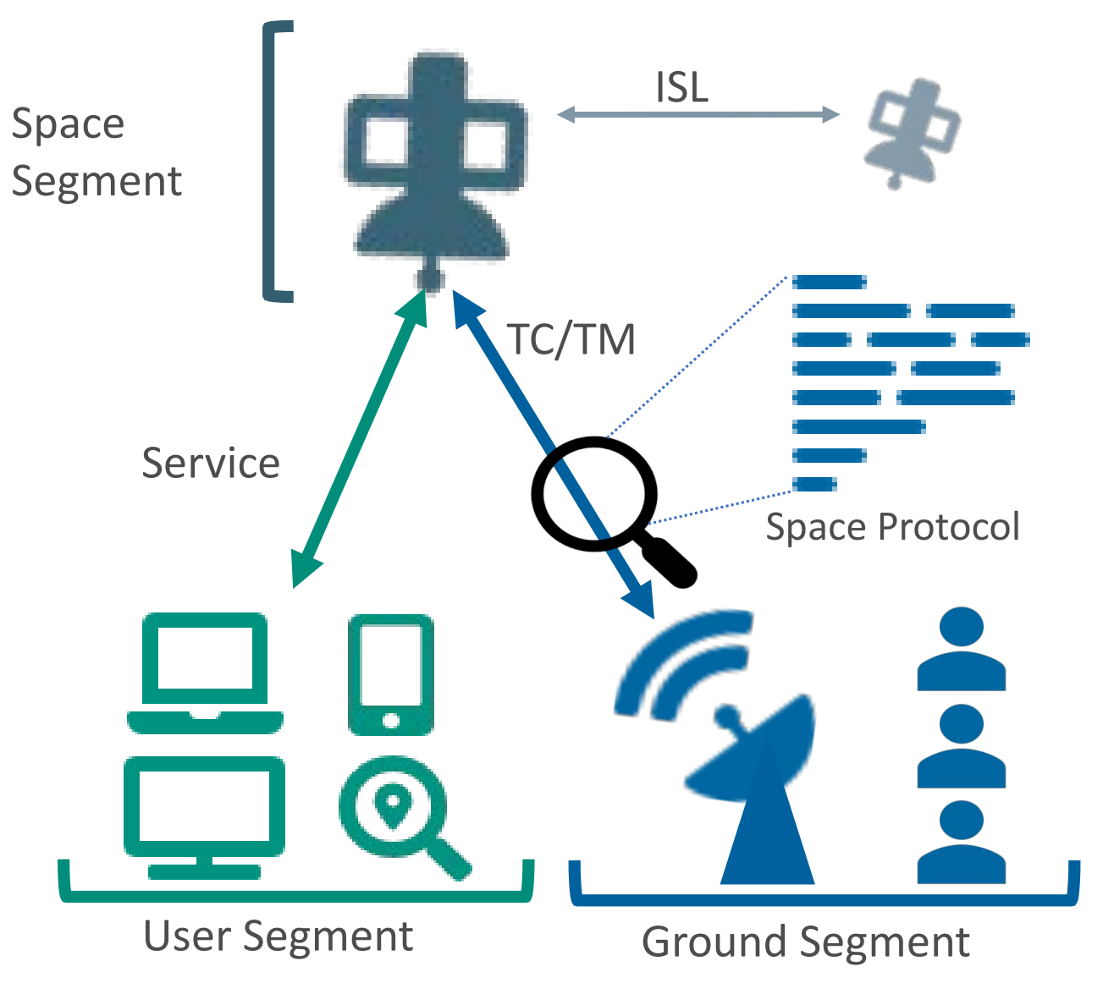
However, there are some approaches for handling vulnerabilities ethically, that could be seen as a beginning of Ethics of Cybersecurity.



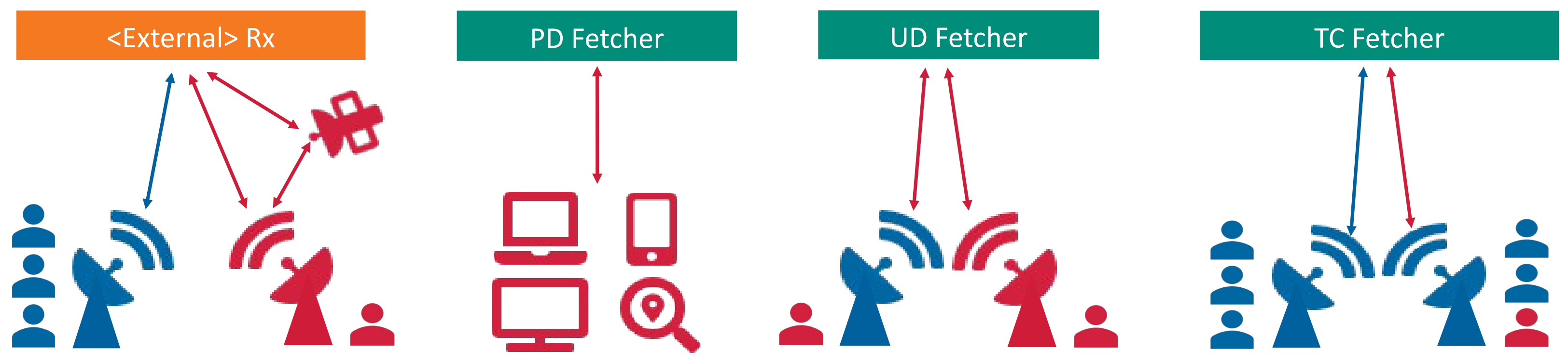
A closer look at these approaches shows that each has different application problems in certain situations. Some examples: The agreements (like Responsible Disclosure) are not applicable if the vulnerability is not fixable, the Codes of Conducts are very abstract and hence not leading to specific guidance. The systematization of vulnerabilities is helpful for technical aspects, but does not involve ethical criteria. The (recently) formed committees at the conferences refer to codes of conducts (esp. Menlo-Report) and therefore have similar problems as the codes themselves. The overall problem is a missing holistic concept. The process of developing and establishing an Ethics of Cybersecurity is complicated by a large number of stakeholders involved, the lack of attribution of responsibilities and accountability and the lack of ethical competence in cybersecurity. There is a lot of work to be done until there is an ethical basis for orientation which satisfies all stakeholders.

This dissertation project aims to contribute to the formation of Ethics of Cybersecurity. In order to do this it focuses on the current development in the field from a meta perspective and compares the developments of other applied ethics (like bioethics, ethics of nanotechnology or medical ethics). Results of this analysis may enable researchers to critically adapt known structures, to identify challenges at an early stage, and - if applicable - offer innovative, simple and sustainable solutions.

Case Study – Satellite Security

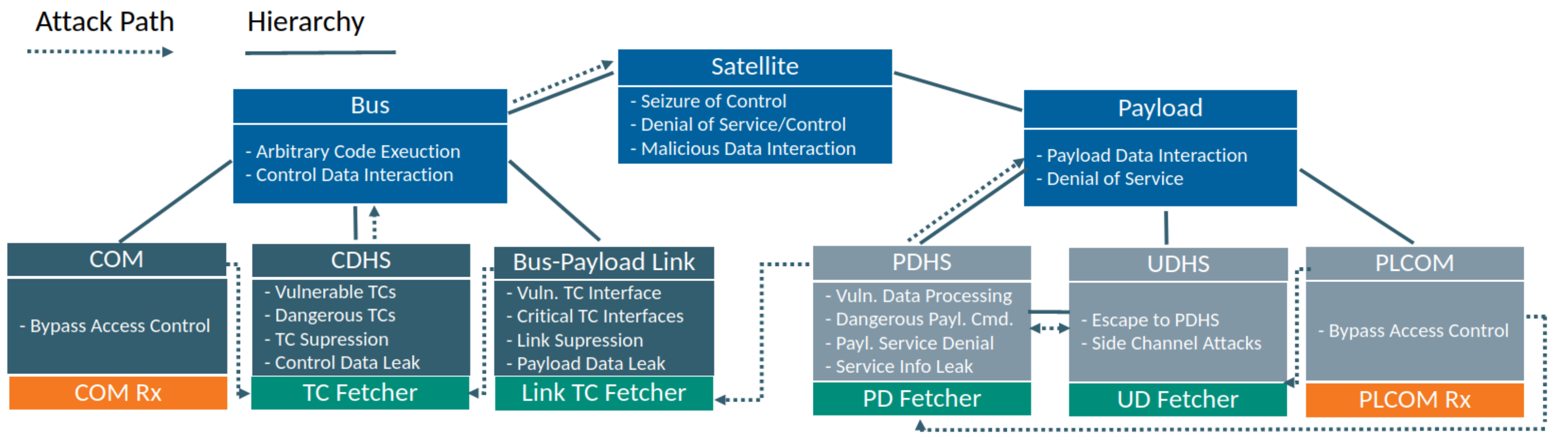


Satellites are essentially remote-controlled space-born embedded devices. Despite their similarity with terrestrial embedded devices and the shared research challenges, satellites prompt several novel challenges due to their remoteness, often outdated hardware, and potentially hard-to-fix/architectural vulnerabilities. Additionally, their position in orbit allows attackers with adequate radio to exploit vulnerabilities.



Research in this young field has focused on exploration and systematization. First, the explorative research identified severe issues such as missing traffic protection of command traffic on small satellites and trivial vulnerabilities in satellite firmware. The systematization then categorizes knowledge i.e., through attacker models (Figure above) and threat taxonomies (Figure below), providing standard terms and terminology for future research.

Further, an essential part of our work on satellite firmware was acquiring firmware. However, traditionally manufacturers act as "gate-keepers" (Pavur et al., 2020), prohibiting meaningful research on this topic. We handeled this through *Non-Disclosure Agreements* with manufacturers and extended discussions with developer teams on how we perform *Coordinated Disclosures* if we identify vulnerabilities. Despite these efforts, a common understanding, such as the *45-90 days coordinated disclosure*, has not yet been established.



Funded by:
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Project partners:
Fachhochschule Dortmund
University of Applied Sciences and Arts
technische universität dortmund
RUB

Further partners:
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY