LECTURE NO. 1

CYBERSECURITY (INTRODUCTION)

This lecture focusses on cybersecurity. Why is cybersecurity important? How do insecure networks affect victims of a cyber-attack and the wider society as a whole? This lecture provides students with in-depth knowledge as to what cybersecurity experts do, what cyber-security entails, what technologies are used and what the main limitations are.

The purposes of cybersecurity measures such as surveillance, anti-virus software, regular password changes etc. are discussed. Topics such as (ethical) hacking, penetration testing, employing ex-black-hats, cracking & cybercrime are also briefly introduced and will be further outlined in other lectures.

Learning Goals

Students will learn:

- who cybersecurity is protecting
- the threats to cybersecurity
- who needs cybersecurity
- how cybersecurity penetrates almost every sector of society today

Case Study

No case study provided in this lecture.

Study material

Presentation slides

- Security analysis of confidential data that is publicly exposed
- eHealth and (in)security of health data
- Challenges and moral questions for IT security companies
- Cybersecurity Fundamentals

Literature

- Hermann & Henning Pridohl (2019): Basic concepts and models of Cybersecurity. In: The Ethics of Cybersecurity, Springer

Videos

- Part 1 (Introduction) Security analysis of confidential data that is publicly exposed
- Part 1 (Introduction) eHealth and (in)security of health data
- Part 1 (Introduction) Challenges and moral questions for IT security companies
- Part 2 (Fundamentals) introductory lecture on Cybersecurity

LECTURE NO. 2

ETHICS – THEORIES & CASE ANALYSIS

This lecture is divided into two parts. The first part is on ethical theories, values and principles that can be applied to the field of cybersecurity. Particular attention is given to important ethical theories such as virtue ethics, utilitarianism, deontology and stakeholder theory.

The second part focuses on a method whereby ethical analysis can be systematically applied to case studies. After analyzing different cases with help of this method, students are required to present a case analysis to the group.

Learning Goals

Students will learn:

- the most important ethical theories
- how to systematically apply ethical analysis with help of a method
- practical know-how on conducting ethical analysis

Case Study

Text Generating AI Technologies - The case study involves the release of a new AI text generation model called GPT-2 The latter was only partially released because of concerns about potential malicious use

Study material

Presentation slides

- The Ethics of Cybersecurity Introducing the Terminology
- Cybersecurity Fundamentals
- Ethical Frameworks for Cybersecurity

Literature

- Michele Loi & Markus Christen (2019): Ethical frameworks for cybersecurity. In: The Ethics of Cybersecurity, Springer

Videos

- Part 2 (Fundamentals) The Ethics of Cybersecurity Introducing the Terminology
- Part 2 (Fundamentals) Cybersecurity Fundamentals
- Part 3 (Applying Ethics to Cybersecurity) Ethical Frameworks for Cybersecurity

LECTURE NO. 3

PRACTICING ETHICS IN RESEARCH & INNOVATION

The first half of the lecture will use the results from a paper by Reijers et al. (2018), which outlines the various tools used to practice ethics in research and innovation, critically analyses them and suggests a new approach.

The second half of the lecture introduces an innovative tool, called the Ethics Canvas (see: https://www.ethicscanvas.org/), in relation to one specific, ethically complex and relevant case study about AI. The Ethics Canvas enables to ethically assess case studies with ethical conflicts and potential cybersecurity threats in a step by step fashion.

Learning Goals

Students will learn:

- various tools to practice ethics in research and innovation
- how to apply the Ethics Canvas to assess and analyse ethically complex cases

Case Study

Analysis of the case Text Generating AI Technologies (see lecture 2) by means of the Ethics Canvas tool

Study material

Presentation slides

- Values Conflicts in Cybersecurity
- Ethical Frameworks for Cybersecurity

Literature

- Reijers, W. et al (2018): Methods for practising ethics in research and innovation: A literature review, critical analysis and recommendations. Pre-print downloadable in http://canvas-project.eu

Videos

- Part 3 (Applying Ethics to Cybersecurity) Values Conflicts in Cybersecurity
- Part 3 (Applying Ethics to Cybersecurity) Ethical Frameworks for Cybersecurity
- Part 3 (Applying Ethics to Cybersecurity) A related dilemma regarding autonomous cars

LECTURE NO. 4

CYBERSECURITY AND ETHICS

This lecture provides students with a more in-depth analysis of ethical issues in cybersecurity. To illustrate how ethics and cybersecurity relate to each other, the findings from CANVAS WP1 are used to demonstrate the plethora of value-conflicts that arise in cybersecurity across three key sectors: business, health care and national security.

Students will undertake a systematic ethical analysis of a case study and will be required to present the results of their work to the whole group at the end of the class.

Learning Goals

Students will learn:

- ethical issues in cybersecurity
- how ethics and cybersecurity relate
- which key value-conflicts arise in cybersecurity

Case Study

Blocking payment sites in ransomware attacks – There is a political component to blocking payment sites which relates to censorship on the Internet and autonomy. Is this a step in the wrong direction?

Study material

Presentation slides

- Values Conflicts in Cybersecurity
- Ethical Frameworks for Cybersecurity

Literature

- Ibo van de Poel (2019): Core values and value conflicts in cybersecurity. In: The Ethics of Cybersecurity, Springer
- Loi Michele Loi, and Markus Christen (2019): Ethical Frameworks for Cybersecurity. In The Ethics of Cybersecurity, Springer.

Videos

- Part 3 (Applying Ethics to Cybersecurity) Values Conflicts in Cybersecurity
- Part 3 (Applying Ethics to Cybersecurity) Ethical Frameworks for Cybersecurity
- Part 3 (Applying Ethics to Cybersecurity) Running a honey pot for research
- Part 3 (Applying Ethics to Cybersecurity) A related dilemma regarding autonomous cars

LECTURE NO. 5

CYBERSECURITY & EU LEGAL FRAMEWORKS

This lecture covers EU law and policy on cybersecurity. It provides an overview of EU law and policy as it currently stands in relation to cybersecurity. In addition, it identifies the main critical challenges in this area and discusses specific controversies concerning cybersecurity regulation.

Other topics covered include EU soft-law measures, EU legislative measures, cybersecurity and criminal justice affairs, the relation of cybersecurity to privacy and data protection, cybersecurity definitions in national cybersecurity strategies, and brief descriptions of EU values. Students are to conduct a case analysis.

Learning Goals

Students will learn:

- how EU law and policy covers the realm of cybersecurity
- main critical challenges and controversies in cybersecurity regulations

Case Study

Systems administrator discovers confidential information – Report a crime to the police or not?

Study material

Presentation slides

- EU Cybersecurity Objectives and Challenges in Light of EU Values
- Basic Principles of the General Data Protection Regulation
- GDPR Legal Principles and Privacy by Design Strategies
- GDPR Legal Principles and Privacy By Design Strategies

Literature

- Gloria Bonzalez Fuster & Lina Jasmontaite: Cybersecurity regulation in the European Union: The digital, the critical and the fundamental rights.
- Eva Schlehahn: Cybersecurity and the State.
- Josep Domingo-Ferrer and Alberto Blanco-Justicia:
- Privacy-preserving Technologies
- In: The Ethics of Cybersecurity, Springer, 2019

Videos

- Part 3 (Applying Ethics to Cybersecurity) EU Cybersecurity Objectives and Challenges in Light of EU Values
- Part 4 (Technical and Legal Aspects of Privacy) Basic Principles of the General Data Protection Regulation (GDPR)
- Part 4 (Technical and Legal Aspects of Privacy) GDPR Legal Principles and Privacy by Design Strategies
- Part 4 (Technical and Legal Aspects of Privacy) The importance of securing private information of IoT devices

LECTURE NO. 6

ETHICAL ISSUES IN HEALTHCARE

This lecture covers ethical issues that arise in cybersecurity in the health domain. The content includes an overview with regard to the various applications of new (digital) technologies in the health sector, privacy and protection of sensitive data, (informed) consent, the relationship between patients and professionals, patients' autonomy and public welfare, the efficiency of the health system, big data and treatment of people with different needs.

The case study chosen for the second part of this lecture focuses on medical devices and implants.

Learning Goals

Students will learn:

- ethical issues of cybersecurity in the health sector
- the various applications of digital technologies in the health sector

Case Study

Cardiac pacemakers and other implantable medical devices - Digital implants are supposed to have a long lifetime and are required small size to minimize invasive treatment. This often results in weak or missing protection.

Study material

Presentation slides

- Applied Ethics of Cybersecurity in Health Care

Literature

- Karsten Weber & Nadine Kleine (2019): Cybersecurity in health. In: The Ethics of Cybersecurity, Springer
- Loi Michele, Markus Christen, Nadine Kleine, and Karsten Weber. 2019. "Cybersecurity in Health – Disentangling Value Tensions." Journal of Information, Communication and Ethics in Society, May. https://doi.org/10.1108/JICES-12-2018-0095.

Videos

- Part 7 (Healthcare) Applied Ethics of Cybersecurity in Health Care
- Part 7 (Healthcare) Rights of patients vs. duty of handling their data properly
- Part 7 (Healthcare) Security and privacy by design for medical implants with cloud access
- Part 7 (Healthcare) Technical solutions and social innovations in medical care
- Part 7 (Healthcare) Consent from patients to use medical data for research and medical care
- Part 4 (Technical and Legal Aspects of Privacy) The importance of securing private information of fitness trackers and IoT devices
- Part 5 (Business) Handling a power outage at a hospital

LECTURE NO. 7

ETHICAL ISSUES IN BUSINESS

This lecture covers ethical issues that arise in cybersecurity in business. It is divided into two parts. The first is theory-based and provides a base level understanding of the problems and threats that arise for businesses in relation to cybersecurity, including the use of cybersecurity reports, ways in which businesses can combat threats in cybersecurity, i.e. through penetration testing and using ethical hackers, the emergence of hacking back between businesses and the problems this can create, managing the insider problem in business through the surveillance of employees, the prohibition of personal devices and usefulness of ethical codes of conduct. The second part of this lecture focuses on the issue of hacking back.

Learning Goals

Students will learn:

- ethical issues of cybersecurity in the business sector
- the various applications of digital technologies in business
- specific threats applying to business
- potentials and problems of hacking back

Case Study

Schwartz' hacking - A security consultant hacked his company's computer system to improve its security but without authorization

Study material

Presentation slides

- Stakeholder Values in Cybersecurity in Business

Literature

- Gwenyth Morgan & Bert Gordijn: A care-based stakeholder approach to ethics of cybersecurity in business.
- Salome Stevens:
  A Framework for Ethical Cyber-defence for Companies.
- Alexey Kirichenko, Markus Christen, Florian Grunow and Dominik Herrmann:
  Best Practices and Recommendations for Cybersecurity Service Providers.
- In: The Ethics of Cybersecurity, Springer, 2019

Videos

- Part 5 (Business)
  Stakeholder Values in Cybersecurity in Business
- Part 5 (Business)
  Ethical issues in day to day business of penetration testers
- Part 5 (Business) Nation-state adversaries, strategies for handling incidents and law enforcement
- Part 5 (Business) Handling a power outage at a hospital

LECTURE NO. 8

ETHICAL ISSUES IN NATIONAL SECURITY

This lecture focusses on national security and the connected ethical issues. Essential public services rely on public ICT networks and are vulnerable to attacks on the internet, and software and hardware failures. The trade-off between the need of privileged access of state actors to ICT services, on the one hand, and values such as freedom and privacy, on the other, is considered, as well as issue of state security versus individual security. This lecture furthermore covers end-to-end encryption, cyber terrorism, cyber warfare, surveillance, profiling and cyber espionage. The second part of this lecture requires students to ethically analyse the Stuxnet case and/or the Iranian hacking back.

Learning Goals

Students will learn:

- ethical issues of cybersecurity in the public sector
- threats to critical infrastructure
- how state security and individual security are contradicting goals

Case Study

Stuxnet - Stuxnet is the cyber weapon that was used to damage Iranian nuclear plants in order to prevent Iran from developing nuclear weapons.
See also **Hacking back**

Study material

Presentation slides

- Political Disinformation, Freedom of Communication and the Role of Epistemic Institutions in Cyberspace

Literature

- Eleonora Viganò, Michele Loi & Emad Yaghmaei: Cybersecurity of critical infrastructures.
- George Lucas: Cybersecurity and Cyber Warfare: the Ethical Paradox of 'Universal Diffidence'
- Reto Inversini: Cyber Peace—and How it can be Achieved
- In: The Ethics of Cybersecurity, Springer

Videos

- Part 8 (Law Enforcement and National Security) Cyber warfare with disinformation and social media as a weapon
- Part 8 (Law Enforcement and National Security) The question whether to engage in activities detrimental to humanity
- Part 8 (Law Enforcement and National Security) Balance between the promise of anonymity and societies need to protect law an order
- Part 8 (Law Enforcement and National security) The definition of cybercrime and forms of online harassment
- Part 5 (Business) Nation-state adversaries, strategies for handling incidents and law enforcement
- Part 6 (Vulnerability Discovery and Disclosure) Risks of full disclosure and regulation of cyber weapons

LECTURE NO. 9

ETHICAL HACKING

The first part of the lecture takes a deeper look into hacking and ethical hacking. The hacker ethics contending that all information should be free and unlimited is discussed, alongside the ethical issues that arise not only for individuals but for businesses too.

For example, some ethical hackers only reveal that they have discovered a vulnerability in a system when there is something to gain recognition from peers or receive a monetary reward. This can create an imbalance of security for individuals and businesses who do not appear to have the means to reward the ethical hacker. Furthermore, the lecture explores the topic of bug bounties and related ethical problems. The second part of this lecture requires students to analyse specific cases.

Learning Goals

Students will learn:

- what differentiates hacking from ethical hacking
- which issues arise out of either
- who benefits from bug bounties and which ethical problems arise out of them

Case Study

Anonymous hacking ISIS - Some of ISIS' accounts on social networks were shut down by Anonymous to contrast ISIS' criminal activity but such acts make terrorist groups harder to monitor.
See also **Schwartz' hacking**

Study material

Presentation slides

- Hanno Böck on Ethical dilemmas from a technical perspective

Literature

- David-Olivier Jacquet-Chifelle & Michele Loi (2019): Ethical and unethical hacking. In: The Ethics of Cybersecurity, Springer

Videos

- Part 5 (Business) Ethical issues in day to day business of penetration testers
- Part 6 (Vulnerability Discovery and Disclosure) Crowdsourcing vulnerability discovery to improve security
- Part 6 (Vulnerability Discovery and Disclosure) Principles, examples and difficulties of responsible disclosure
- Part 6 (Vulnerability Discovery and Disclosure) Communicating vulnerabilities to third parties
- Part 6 (Vulnerability Discovery and Disclosure) Ethical dilemmas from a technical perspective

LECTURE NO. 10

CYBERSECURITY & DEMOCRACY

This lecture focusses on cybersecurity and democracy, covering the impact of cybersecurity on democratic decision making. How can bots, trolls and sock-puppets compromise security by undermining civic integrity? Hacking democratic societies is covered as well as exploiting cybersecurity in politics such as using technologies to tamper with voter registration, access voting machines, manipulate storage and transmission of results and influence election outcomes or strategic misinformation.

There are two case studies for this lecture: the first is on Text Generating AI Technologies, which are relevant for democracy because they can contribute to the spread of misinformation and the second one regards hacking criminal organizations such as terrorists groups.

Learning Goals

Students will learn:

- how cybersecurity impacts democratic decision making
- how hacking democratic societies works
- how politics exploit cybersecurity

Case Study

Text Generating AI Technologies - This case features an interesting new development in AI and its anticipated effects on cybersecurity.
See also **Anonymous hacking ISIS**

Study material

Presentation slides

- Political Disinformation, Freedom of Communication and the Role of Epistemic Institutions in Cyberspace

Literature

- Seumas Miller (2019): Freedom of political communication, propaganda and the role of epistemic institutions in cyberspace. In: The Ethics of Cybersecurity, Springer
- Paul Meyer (2019): Norms of Responsible State Behaviour in Cyberspace. In: The Ethics of Cybersecurity, Springer

Videos

- Part 9 (Cybersecurity and Democracy)
  Political Disinformation, Freedom of Communication and the Role of Epistemic Institutions in Cyberspace
- Part 9 (Cybersecurity and Democracy)
  Trust in the computing stack and its impact on democracy
- Part 9 (Cybersecurity and Democracy)
  The problem with autonomous decisions

LECTURE NO. 11

HANDLING VULNERABILITIES

The first part of this lecture considers the problem of finding and selling zero-day vulnerabilities and explores related ethical issues. It is the prospect of gaining substantial amounts of money to find and sell zero-day vulnerabilities. The buyer could be a well-intentioned individual to a malicious individual, group or agency.

This lecture explores the possible use of vulnerabilities as weapons, also employed by governments. The second part of this lecture gives students the opportunity to debate both for and against the motion: “Paying Security Researchers Millions of Dollars for Zero-Day Exploits is a Recipe for Disaster”.

Learning Goals

Students will learn:

- how finding and selling zero-day vulnerabilities works
- ethical considerations on the practice
- how they can be used as weapons
- how governments take advantage

Case Study

Selling vulnerabilities - The case study is about a security researcher’s decision regarding where to sell a software vulnerability that he discovered: on the gray market or the black market or to the software vendor?

Study material

Presentation slides

- Hanno Böck on Ethical dilemmas from a technical perspective

Literature

- Alexey Kirichenko, Markus Christen, Florian Grunow and Dominik Herrmann (2019): Best Practices and Recommendations for Cybersecurity Service Providers. In: The Ethics of Cybersecurity, Springer
- European Commission. “What is a data breach and what do we have to do in case of a data breach”. European Commission (see link at the bottom of this page)
- Schwartz, Matthew. “Uber Fined $1.2 Million in EU for Breach Disclosure Delay”. Bank Info Security (see link at the bottom of this page)

Videos

- Part 6 (Vulnerability Discovery and Disclosure) Risks of full disclosure and regulation of cyber weapons
- Part 6 (Vulnerability Discovery and Disclosure) A case of responsible disclosure in a scientific publication
- Part 6 (Vulnerability Discovery and Disclosure) Principles, examples and difficulties of responsible disclosure
- Part 6 (Vulnerability Discovery and Disclosure) Communicating vulnerabilities to third parties