Outlining Future Challenges of Cybersecurity – the CANVAS Results

Markus Christen, University of Zürich
Zürich, October 24, 2019
Workshop Overview

16:00 – 16:10  **Introduction** (Markus Christen, University of Zurich)

16:10 – 16:30  **The CONCORDIA network** (Burkhard Stiller, University of Zurich)

16:30 – 17:00  **The CANVAS results** (Markus Christen, University of Zurich)

17:00 – 17:20  **Establishing Global Trust** (Adrian Perrig, ETH Zurich)

17:20 – 17:40  **Outlining Future Challenges for Switzerland** (Reto Inversini, MELANI)

17:40 – 18:15  **General Discussion** (including Florian Schütz, Federal Cyber Security Delegate and Eva May, Office of Economy and Labour of the Canton of Zurich)
Introducing CANVAS
Main Objectives of CANVAS

Advance value-driven cybersecurity by bringing together partners from various scientific traditions – ethical, legal, empirical and technological – that outline problems and solution on how European values and fundamental rights can be integrated into cybersecurity technology.

1. **Structure existing knowledge** in ethics, law, empirical and technological research related to cybersecurity.

2. Design a network for **exchanging knowledge** and generating insights across domains (workshops, summarizing conference).

3. **Disseminate** the insights gained in three main output deliverables (briefing packages for policy stakeholders, reference curriculum for value-driven cybersecurity, MOOC).
CANVAS Consortium

11 partners from 7 European countries.

Focus on three reference domains:

- Health system
- Business
- National Security
Work Package Structure

**WPs 1-4:** Consolidate existing knowledge with a specific focus on the three social spheres under consideration.

**WPs 6-8:** Create three main output deliverables of CANVAS (Briefing Packages, Reference Curriculum, MOOC).

**WP 5:** Integrating unit: management, community built-up and workshop organization.
“Cybersecurity” as an instrumental value

In the technical discourse, cybersecurity is usually seen as an instrument to achieve the following goals with respect to information technology resources, irrespective from the ethical goals associated with using those resources:

- **Availability**: Make sure that information technology resources remain accessible for their users.
- **Confidentiality**: Make sure that only authorized persons can access the content and functionalities of information technology resources.
- **Integrity**: Make sure that the processes and content of information technology resources remain intact.

**Get more**: MOOC on cybersecurity foundations.
Cybersecurity mediates tensions between values

Justice

Care

Nonmalefience

Trust

Privacy

Equality

Cost awareness

Innovation

Efficiency

Autonomy

Cybersecurity

Ü Get more: MOOC on value conflicts in cybersecurity.
Ü Get more: MOOC on cybersecurity in healthcare.
CANVAS Results
Information Source: CANVAS White Papers
CANVAS Briefing Packages (1)

The CANVAS Briefing Packages are a set of **summarized, easily digestible information** on challenges as well as possible, value-driven solution approaches linked to European cybersecurity policy.

Four different Briefing Packages are available, each of them addressing a different challenge in the field of European cybersecurity policy. These challenges are:

- Achieving **Trust** in EU Cybersecurity
- Cybersecurity and the European **Data Protection** Framework
- All **Fundamental Rights** are relevant for Cybersecurity
- Achieving Comprehensive and Consistent EU **Cybersecurity Policies**

Each Briefing Package is downloadable and free to use in English, French and German.
CANVAS Briefing Packages (2)

Each Briefing Package consists of:

- A Policy brief document of 4 pages
- Slide-docs summarizing the topic
## CANVAS: Reference Curriculum

### MOOC

<table>
<thead>
<tr>
<th>MOOC (built-in questions)</th>
<th>Curriculum (with final students presentations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>Vulnerabilities</td>
</tr>
<tr>
<td>Democracy</td>
<td>Ethical hacking</td>
</tr>
<tr>
<td>Law enforcement</td>
<td>Democracy</td>
</tr>
<tr>
<td>Business</td>
<td>Business</td>
</tr>
<tr>
<td>Healthcare</td>
<td>Healthcare</td>
</tr>
<tr>
<td>National Security</td>
<td>National Security</td>
</tr>
<tr>
<td>Cybersecurity in light of EU values</td>
<td>Ethical frameworks</td>
</tr>
<tr>
<td>General data protection regulation</td>
<td>Cybersecurity and EU legal framework</td>
</tr>
<tr>
<td>Value conflicts</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>Ethics general</td>
<td>Ethics general</td>
</tr>
<tr>
<td>Ethical frameworks</td>
<td>Responsible Research and Innovation</td>
</tr>
</tbody>
</table>

Constructing an Alliance for Value-driven Cybersecurity

This overview chart outlines the main components of the CANVAS massive open online course (MOOC) and the CANVAS Reference Curriculum for value-driven cybersecurity. All material of the Curriculum as well as access to the MOOC is provided on: www.canvas-project.eu
Canvast Reference Curriculum – Example (1)

Lecture 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? (question sheet and answer sheet)
CANVAS Reference Curriculum – Example (2)

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

Literature (In: The Ethics of Cybersecurity, Springer, 2019)
- 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

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
- 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

Ü Get access: https://canvas-project.eu/results/reference-curriculum.html
CANVAS MOOC

The massive open online course (MOOC) transports the main insights of CANVAS to a broad public.

In particular, it provides a comprehensive overview of the central principles and challenges in the fields of cyber security, privacy and trust.

Concrete case studies from health, business and national security spheres are presented. Technical, legal and ethical perspectives on the issues are included.

Ü Get access:
https://mooc.canvas-project.eu/
New CANVAS book

This collection occupies a vast chasm between these extremes, offering intelligent, considered reflections on ethical issues in cybersecurity at a general level, while assuming a degree of understanding on the part of the reader. I must say that I am very excited to see this in print.

Reviewer 1

The book is timely and about pressing issues of which little has been said. The book has a lot of merit for its structure, the topics addressed, and the quality of each individual article.

Reviewer 2
1 Introduction .................................................. 1
Markus Christen, Bert Gordijn, and Michele Loi

Part I Foundations
2 Basic Concepts and Models of Cybersecurity ................. 11
Dominik Herrmann and Henning Pridohl
3 Core Values and Value Conflicts in Cybersecurity: Beyond
Privacy Versus Security .................................. 45
Ibo van de Poel
4 Ethical Frameworks for Cybersecurity ....................... 73
Michele Loi and Markus Christen
5 Cybersecurity Regulation in the European Union: The Digital,
the Critical and Fundamental Rights ..................... 97
Gloria González Fuster and Lina Jasmontaitė

Part II Problems
6 A Care-Based Stakeholder Approach to Ethics of Cybersecurity
in Business .................................................. 119
Gwenyth Morgan and Bert Gordijn
7 Cybersecurity in Health Care ................................ 139
Karsten Weber and Nadine Kleine
8 Cybersecurity of Critical Infrastructure ...................... 157
Eleonora Viganò, Michele Loi, and Emad Yaghmaei
9 Ethical and Unethical Hacking ................................ 179
David-Olivier Jaquet-Chifflotte and Michele Loi

10 Cybersecurity and the State .................................. 205
Eva Schleich
11 Freedom of Political Communication, Propaganda and the Role
of Epistemic Institutions in Cyberspace ................... 227
Seumas Miller
12 Cybersecurity and Cyber Warfare: The Ethical Paradox of
‘Universal Difference’ .................................. 245
George Lucas
13 Cyber Peace: And How It Can Be Achieved .................. 259
Reto Inversini

Part III Recommendations
14 Privacy-Preserving Technologies ............................ 279
Josep Domingo-Ferrer and Alberto Blanco-Justicia
15 Best Practices and Recommendations for Cybersecurity Service
Providers ....................................................... 299
Alexey Kirichenko, Markus Christen, Florian Grunow, and Dominik Herrmann
16 A Framework for Ethical Cyber-Defence for Companies .... 316
Salome Stevens
17 Towards Guidelines for Medical Professionals to Ensure
Cybersecurity in Digital Health Care ....................... 331
David Koepp
18 Norms of Responsible State Behaviour in Cyberspace ........ 347
Paul Meyer

Appendix ...................................................... 361
National research projects to come (Switzerland)

Creating an integrative framework for solving ethical and legal dilemmas in cybersecurity (project reached second round). Partner: University of Lausanne