# 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.

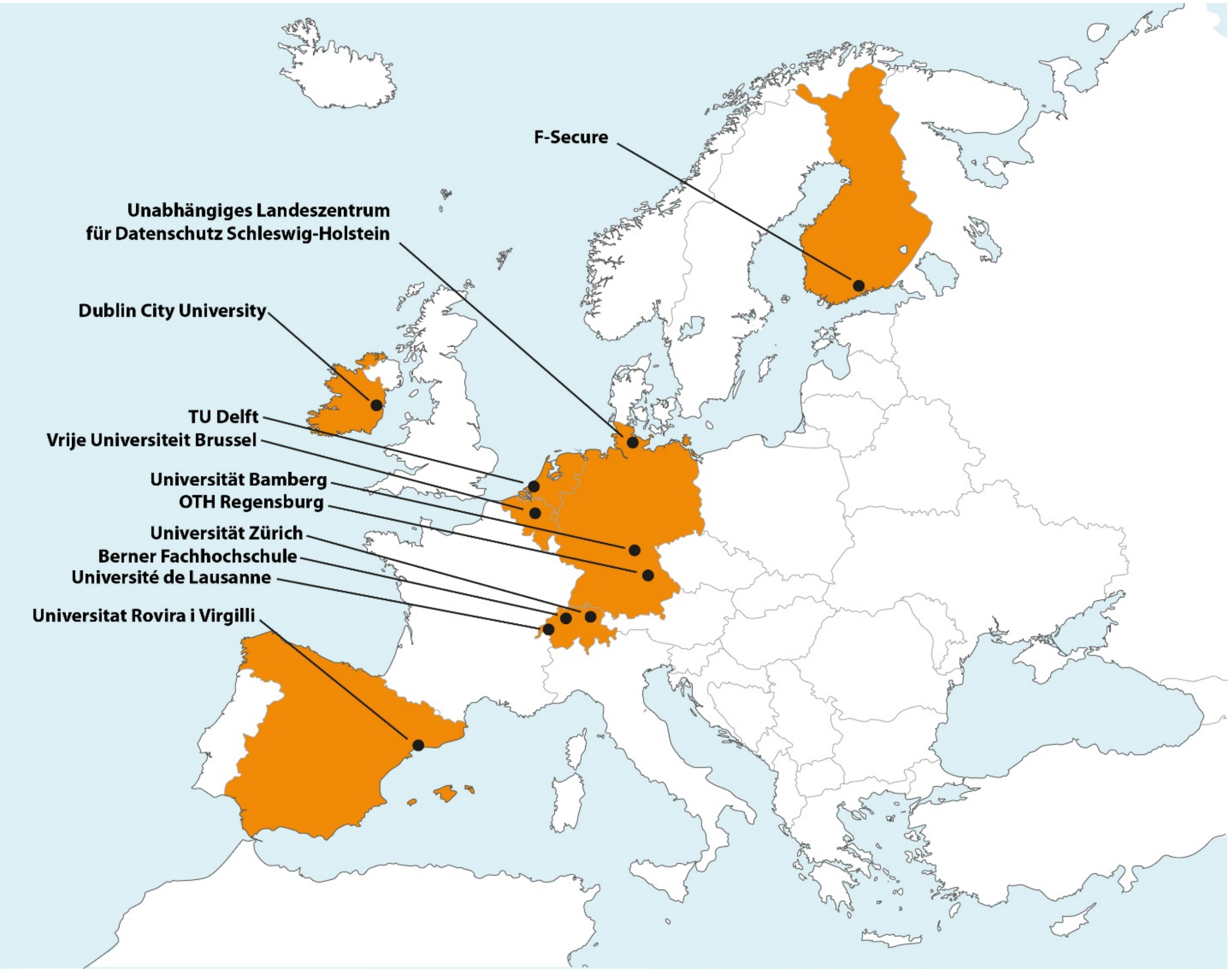
1. **Structure existing knowledge** in ethics, law, empirical and technological research related to cybersecurity.
2. Design a network for **exchanging knowledge** and generating insights across domains (workshops, summarizing conference).
3. **Disseminate** the insights gained in three main output deliverables (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



University of Zurich UZH

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

OTH OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

UNIVERSITAT ROVIRA I VIRGILI

ULD

F-Secure

FH Bern University of Applied Sciences

OTTO-FRIEDRICH-UNIVERSITÄT BAMBERG

DCU

TU Delft Technische Universiteit Delft

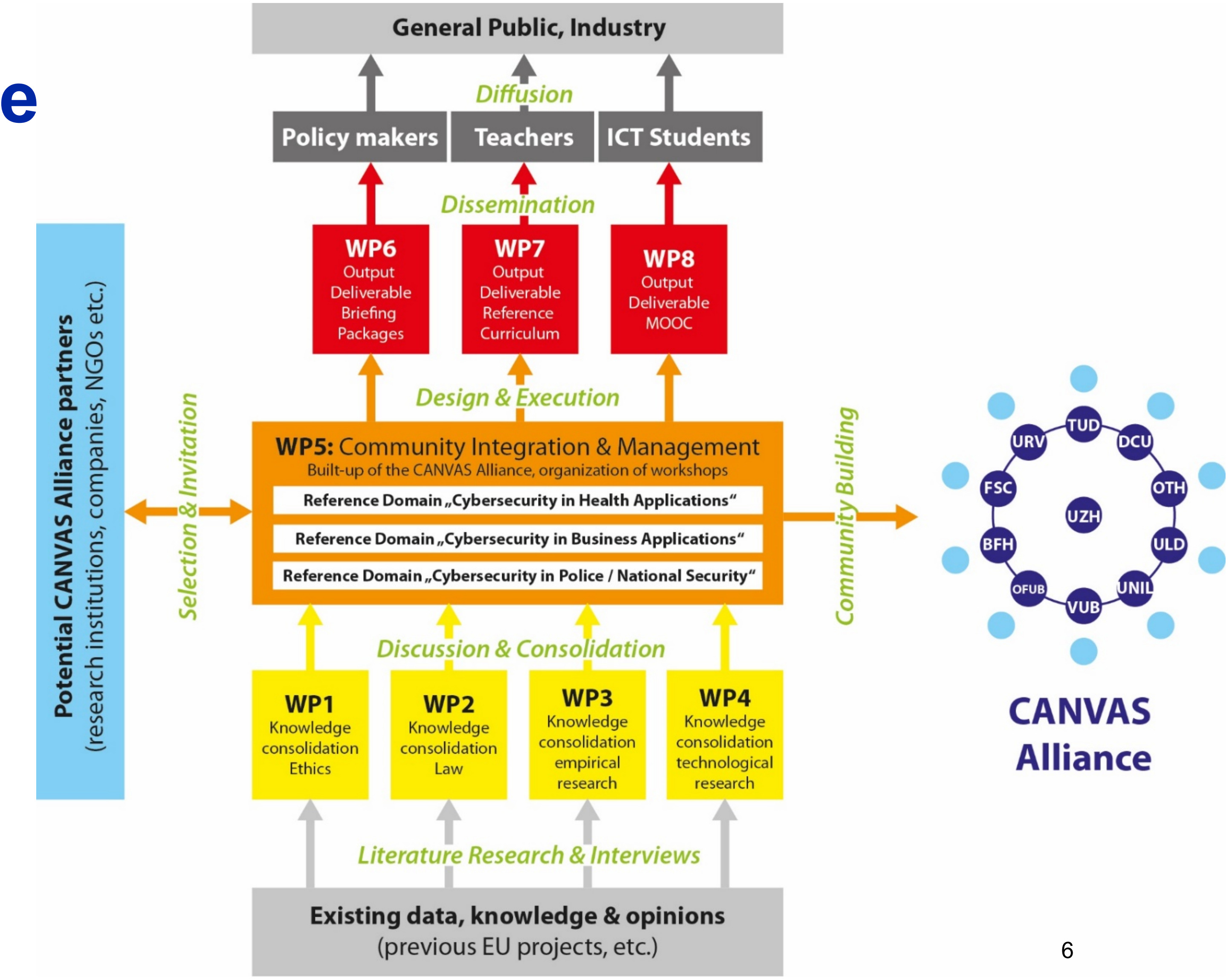
Unil UNIL | Université de Lausanne

# 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.



General Public, Industry

Diffusion

Policy makers | Teachers | ICT Students

Dissemination

WP6 Output Deliverable Briefing Packages

WP7 Output Deliverable Reference Curriculum

WP8 Output Deliverable MOOC

Design & Execution

WP5: Community Integration & Management

Built-up of the CANVAS Alliance, organization of workshops

Reference Domain „Cybersecurity in Health Applications"

Reference Domain „Cybersecurity in Business Applications"

Reference Domain „Cybersecurity in Police / National Security"

Potential CANVAS Alliance partners (research institutions, companies, NGOs etc.)

Selection & Invitation

Community Building

Discussion & Consolidation

WP1 Knowledge consolidation Ethics

WP2 Knowledge consolidation Law

WP3 Knowledge consolidation empirical research

WP4 Knowledge consolidation technological research

Literature Research & Interviews

Existing data, knowledge & opinions (previous EU projects, etc.)

CANVAS Alliance

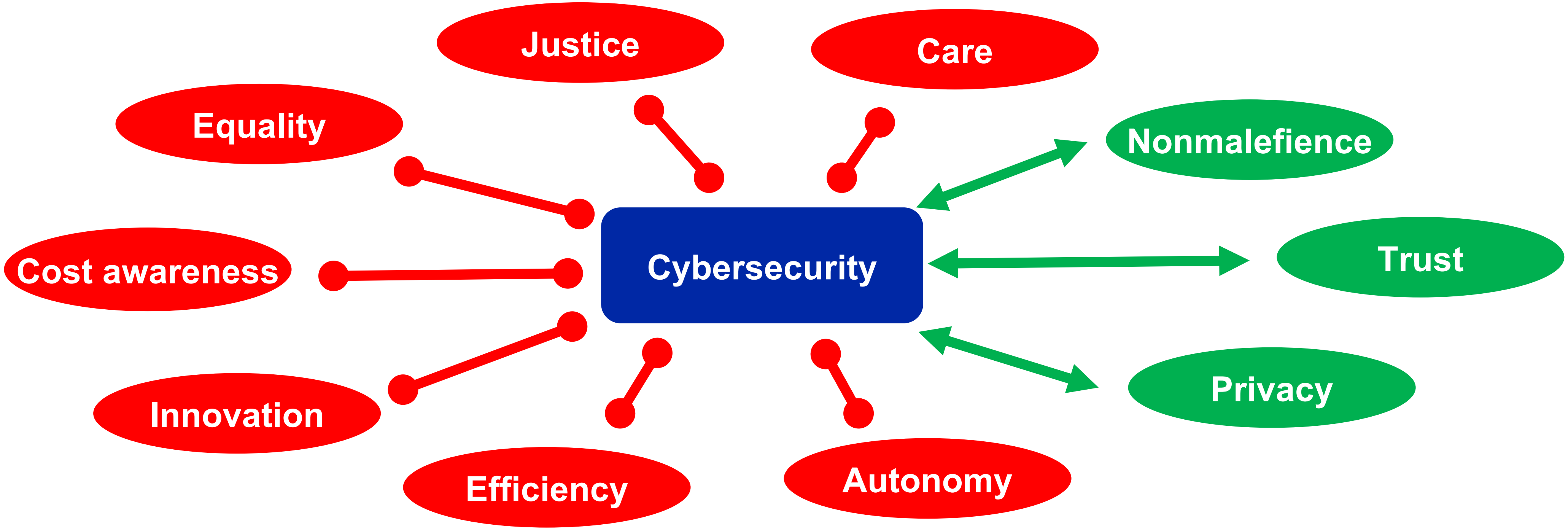
# “Cybersecurity” as an instrumental value

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.

**Ü Get more:** MOOC on cybersecurity foundations.

# Cybersecurity mediates tensions between values



Justice

Care

Equality

Nonmalefience

Cost awareness

Cybersecurity

Trust

Innovation

Privacy

Efficiency

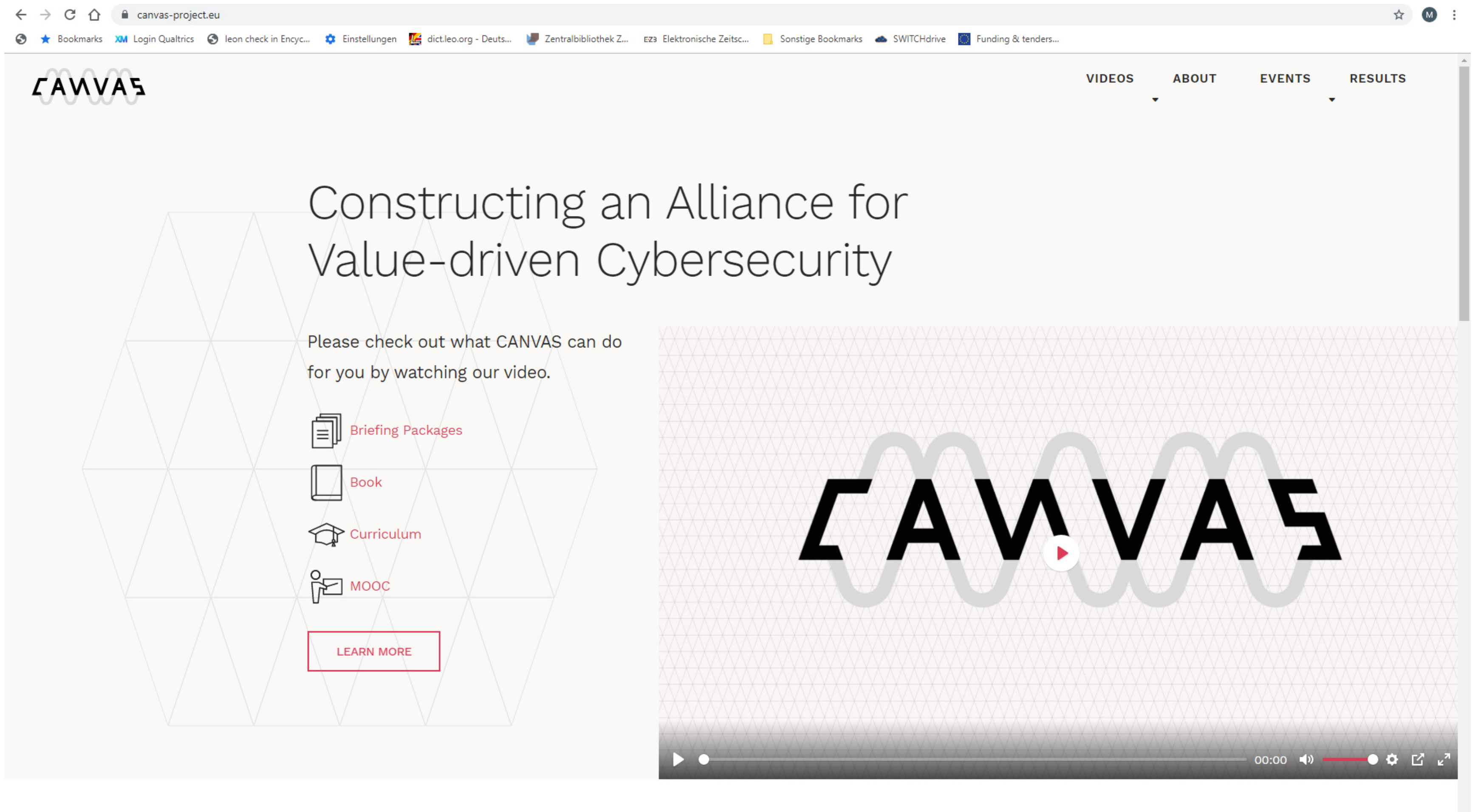
Autonomy

**Ü Get more:** MOOC on value conflicts in cybersecurity.

**Ü Get more:** MOOC on cybersecurity in healthcare.

# CANVAS Results

# Entry-page: www.canvas-project.eu



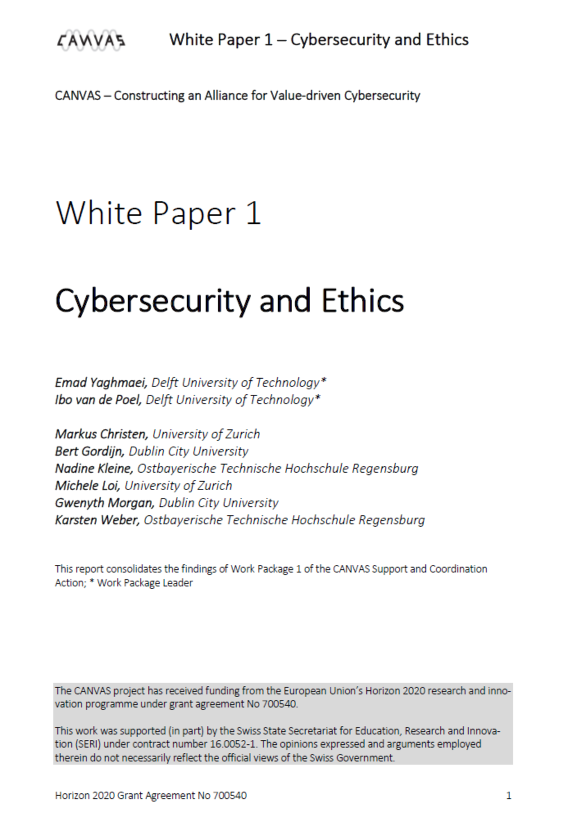
Constructing an Alliance for Value-driven Cybersecurity

Please check out what CANVAS can do for you by watching our video.

- Briefing Packages
- Book
- Curriculum
- MOOC

LEARN MORE

# Information Source: CANVAS White Papers



White Paper 1 – Cybersecurity and Ethics

CANVAS – Constructing an Alliance for Value-driven Cybersecurity

White Paper 1

Cybersecurity and Ethics

***Emad Yaghmaei,*** *Delft University of Technology**
***Ibo van de Poel,*** *Delft University of Technology**

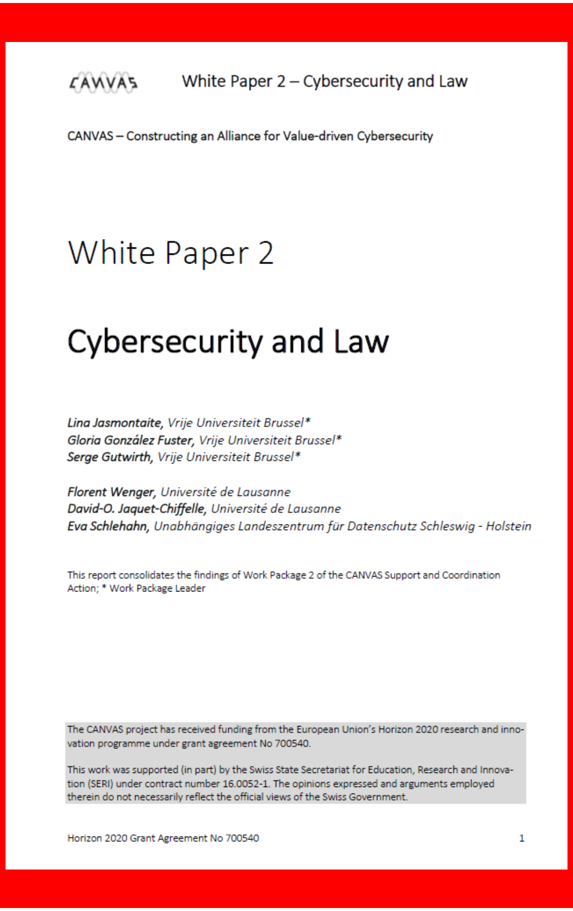
***Markus Christen,*** *University of Zurich*
***Bert Gordijn,*** *Dublin City University*
***Nadine Kleine,*** *Ostbayerische Technische Hochschule Regensburg*
***Michele Loi,*** *University of Zurich*
***Gwenyth Morgan,*** *Dublin City University*
***Karsten Weber,*** *Ostbayerische Technische Hochschule Regensburg*

This report consolidates the findings of Work Package 1 of the CANVAS Support and Coordination Action; * Work Package Leader

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Horizon 2020 Grant Agreement No 700540 1



White Paper 2 – Cybersecurity and Law

CANVAS – Constructing an Alliance for Value-driven Cybersecurity

White Paper 2

Cybersecurity and Law

***Lina Jasmontaite,*** *Vrije Universiteit Brussel**
***Gloria González Fuster,*** *Vrije Universiteit Brussel**
***Serge Gutwirth,*** *Vrije Universiteit Brussel**

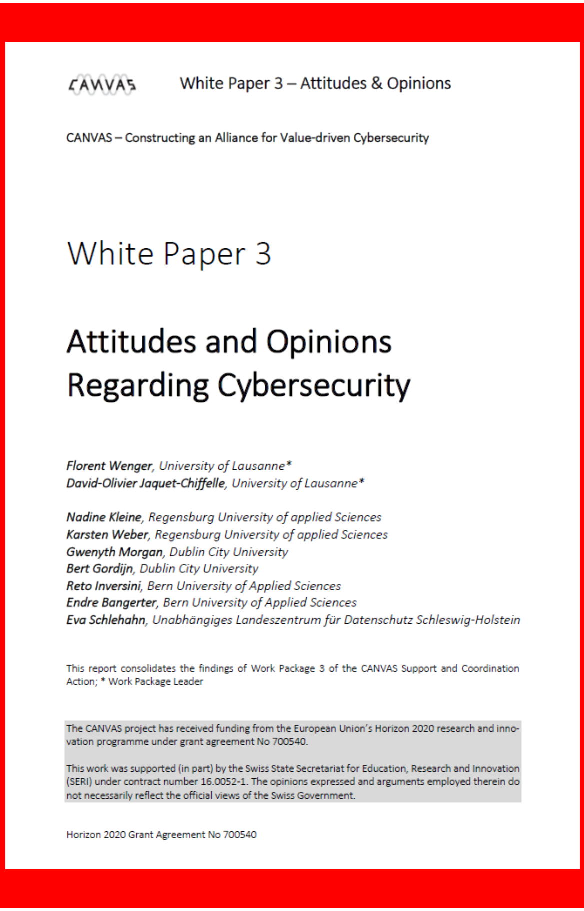
***Florent Wenger,*** *Université de Lausanne*
***David-O. Jaquet-Chiffelle,*** *Université de Lausanne*
***Eva Schlehahn,*** *Unabhängiges Landeszentrum für Datenschutz Schleswig - Holstein*

This report consolidates the findings of Work Package 2 of the CANVAS Support and Coordination Action; * Work Package Leader

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Horizon 2020 Grant Agreement No 700540 1



White Paper 3 – Attitudes & Opinions

CANVAS – Constructing an Alliance for Value-driven Cybersecurity

White Paper 3

Attitudes and Opinions
Regarding Cybersecurity

***Florent Wenger***, *University of Lausanne**
***David-Olivier Jaquet-Chiffelle***, *University of Lausanne**

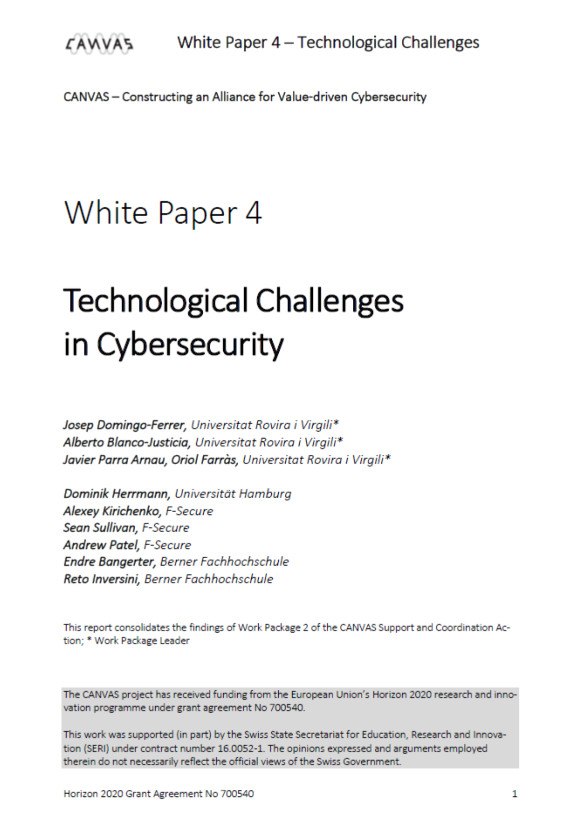
***Nadine Kleine***, *Regensburg University of applied Sciences*
***Karsten Weber***, *Regensburg University of applied Sciences*
***Gwenyth Morgan***, *Dublin City University*
***Bert Gordijn***, *Dublin City University*
***Reto Inversini***, *Bern University of Applied Sciences*
***Endre Bangerter***, *Bern University of Applied Sciences*
***Eva Schlehahn***, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*

This report consolidates the findings of Work Package 3 of the CANVAS Support and Coordination Action; * Work Package Leader

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Horizon 2020 Grant Agreement No 700540



White Paper 4 – Technological Challenges

CANVAS – Constructing an Alliance for Value-driven Cybersecurity

White Paper 4

Technological Challenges
in Cybersecurity

***Josep Domingo-Ferrer,*** *Universitat Rovira i Virgili**
***Alberto Blanco-Justicia,*** *Universitat Rovira i Virgili**
***Javier Parra Arnau, Oriol Farràs,*** *Universitat Rovira i Virgili**

***Dominik Herrmann,*** *Universität Hamburg*
***Alexey Kirichenko,*** *F-Secure*
***Sean Sullivan,*** *F-Secure*
***Andrew Patel,*** *F-Secure*
***Endre Bangerter,*** *Berner Fachhochschule*
***Reto Inversini,*** *Berner Fachhochschule*

This report consolidates the findings of Work Package 2 of the CANVAS Support and Coordination Action; * Work Package Leader

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Horizon 2020 Grant Agreement No 700540 1

# 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:

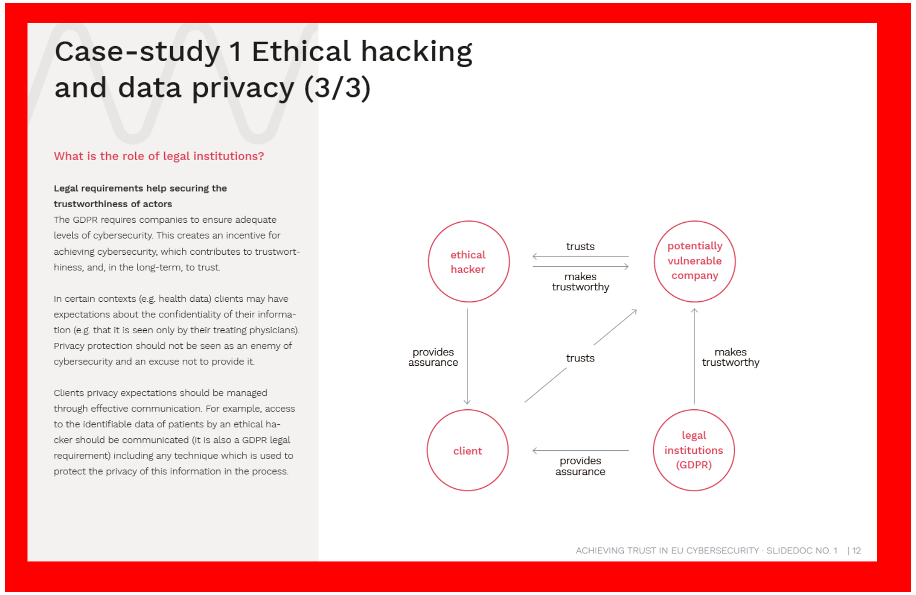
- Achieving **Trust** in EU Cybersecurity
- Cybersecurity and the European **Data Protection** Framework
- All **Fundamental Rights** are relevant for Cybersecurity
- Achieving Comprehensive and Consistent EU **Cybersecurity Policies**

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**



## Case-study 1 Ethical hacking and data privacy (3/3)

What is the role of legal institutions?

**Legal requirements help securing the trustworthiness of actors**
The GDPR requires companies to ensure adequate levels of cybersecurity. This creates an incentive for achieving cybersecurity, which contributes to trustworthiness, and, in the long-term, to trust.

In certain contexts (e.g. health data) clients may have expectations about the confidentiality of their information (e.g. that it is seen only by their treating physicians). Privacy protection should not be seen as an enemy of cybersecurity and an excuse not to provide it.

Clients privacy expectations should be managed through effective communication. For example, access to the identifiable data of patients by an ethical hacker should be communicated (it is also a GDPR legal requirement) including any technique which is used to protect the privacy of this information in the process.

ACHIEVING TRUST IN EU CYBERSECURITY · SLIDEDOC NO. 1 | 12

Constructing an Alliance for Value-driven Cybersecurity

POLICY BRIEF NO. 3

## ALL FUNDAMENTAL RIGHTS ARE RELEVANT FOR CYBERSECURITY

### Maintaining a comprehensive approach to fundamental rights protection in EU cybersecurity

When the European Commission puts forward cybersecurity policy and regulation proposals, their evaluation is often focused on their compatibility with the right to protection of personal data and the right to respect for private and family life. Indeed, in the digital environment, the right to data protection and privacy are among the most relevant concerns. Yet, while still recognizing the significance of these two rights enshrined respectively in Articles 8 and 7 of the Charter of Fundamental Rights of the European Union (EU Charter), policy makers should consider a wider range of fundamental rights that are or may be affected by EU cybersecurity policies and regulatory measures.

Policy makers should consider a wider range of fundamental rights that are or may be affected by EU cybersecurity policies and regulatory measures.

#### European primary law proclaims protection of EU values and fundamental rights

According to Article 2 of the Treaty of the EU, '[t]he Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities'. These EU values are determined by the principles of pluralism, non-discrimination, tolerance, justice and equal treatment of men and women and they are further detailed in the EU Charter. Additionally, the EU Charter foresees a wide array of fundamental rights enjoyed by EU citizens and residents, including but not limited to the right to a fair trial, freedom of thought, freedom of expression and information, rights to property, education and to an effective remedy. These values and rights must be reflected in EU regulatory measures.

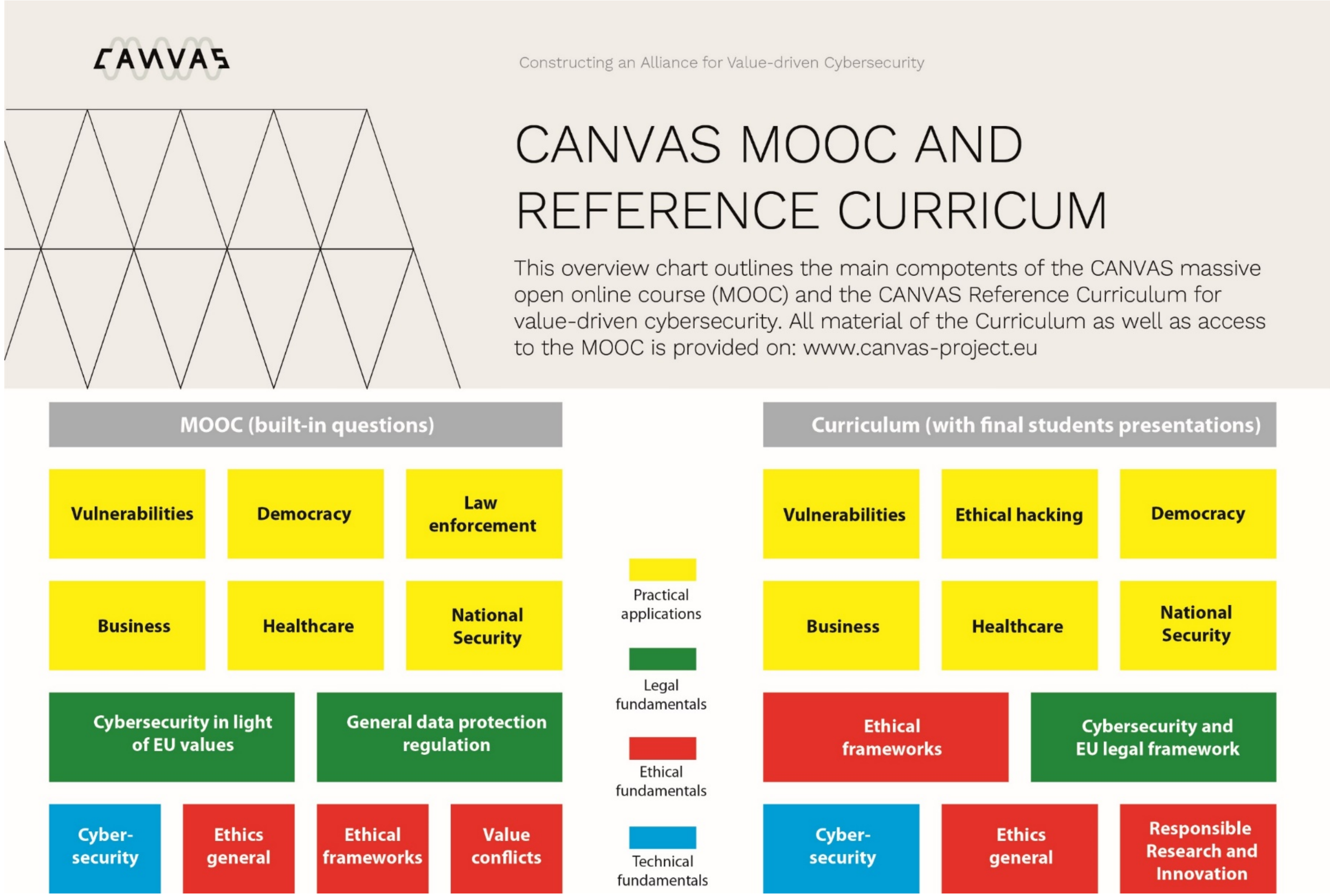
#### Step 1: Recognise challenges of protecting fundamental rights on EU level in the digital environment

EU policy documents and legislation in the cybersecurity area recognise that any measures taken with respect to the protection of EU citizens, society as well as information systems and infrastructure, should be developed in accordance with the commitment to

# CANVAS:

# Reference Curriculum

# MOOC



Constructing an Alliance for Value-driven Cybersecurity

## CANVAS MOOC AND REFERENCE CURRICUM

This overview chart outlines the main compotents 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

**MOOC (built-in questions)**

- 🟨 Vulnerabilities
- 🟨 Democracy
- 🟨 Law enforcement
- 🟨 Business
- 🟨 Healthcare
- 🟨 National Security
- 🟩 Cybersecurity in light of EU values
- 🟩 General data protection regulation
- 🟦 Cyber-security
- 🟥 Ethics general
- 🟥 Ethical frameworks
- 🟥 Value conflicts

**Curriculum (with final students presentations)**

- 🟨 Vulnerabilities
- 🟨 Ethical hacking
- 🟨 Democracy
- 🟨 Business
- 🟨 Healthcare
- 🟨 National Security
- 🟥 Ethical frameworks
- 🟩 Cybersecurity and EU legal framework
- 🟦 Cyber-security
- 🟥 Ethics general
- 🟥 Responsible Research and Innovation

🟨 Practical applications

🟩 Legal fundamentals

🟥 Ethical fundamentals

🟦 Technical fundamentals

# CANVAS 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

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

**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:**

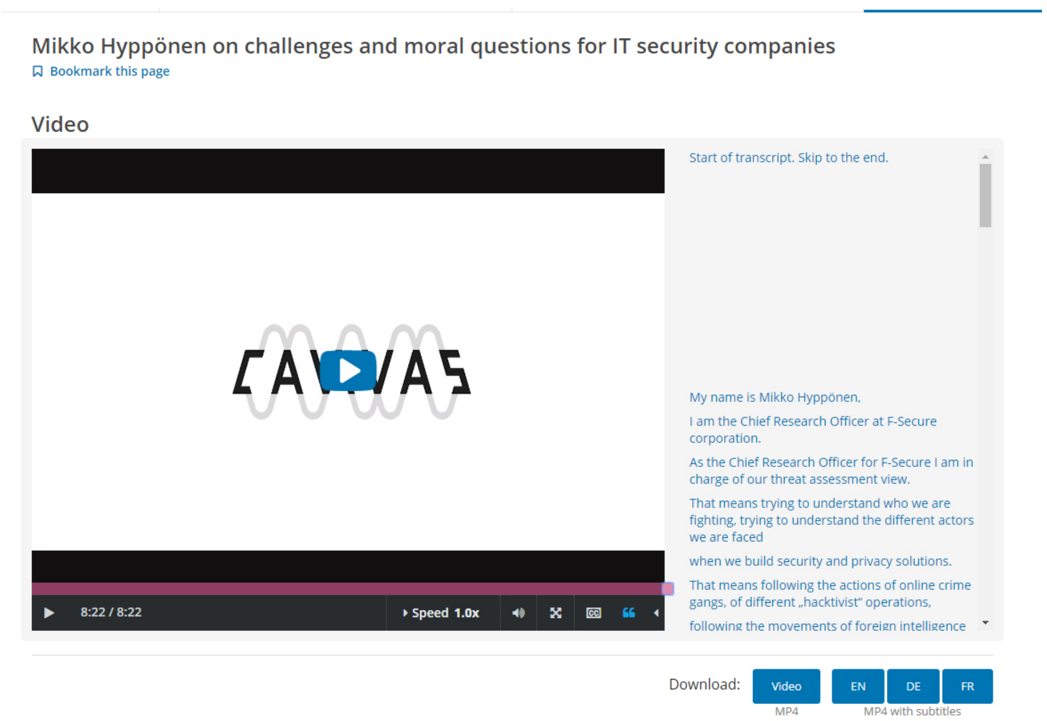
- Part 3 (Applying Ethics to Cybersecurity) EU Cybersecurity Objectives and Challenges in Light of EU Values
- Part 4 (Technical and Legal Aspects of Privacy) Basic Principles of the General Data Protection Regulation
- Part 4 (Technical and Legal Aspects of Privacy) GDPR Legal Principles and Privacy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

# 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.



Mikko Hyppönen on challenges and moral questions for IT security companies

Video

Start of transcript. Skip to the end.

My name is Mikko Hyppönen,

I am the Chief Research Officer at F-Secure corporation.

As the Chief Research Officer for F-Secure I am in charge of our threat assessment view.

That means trying to understand who we are fighting, trying to understand the different actors we are faced

when we build security and privacy solutions.

That means following the actions of online crime gangs, of different „hacktivist“ operations,

following the movements of foreign intelligence

**Ü Get access:**
https://mooc.canvas-project.eu/

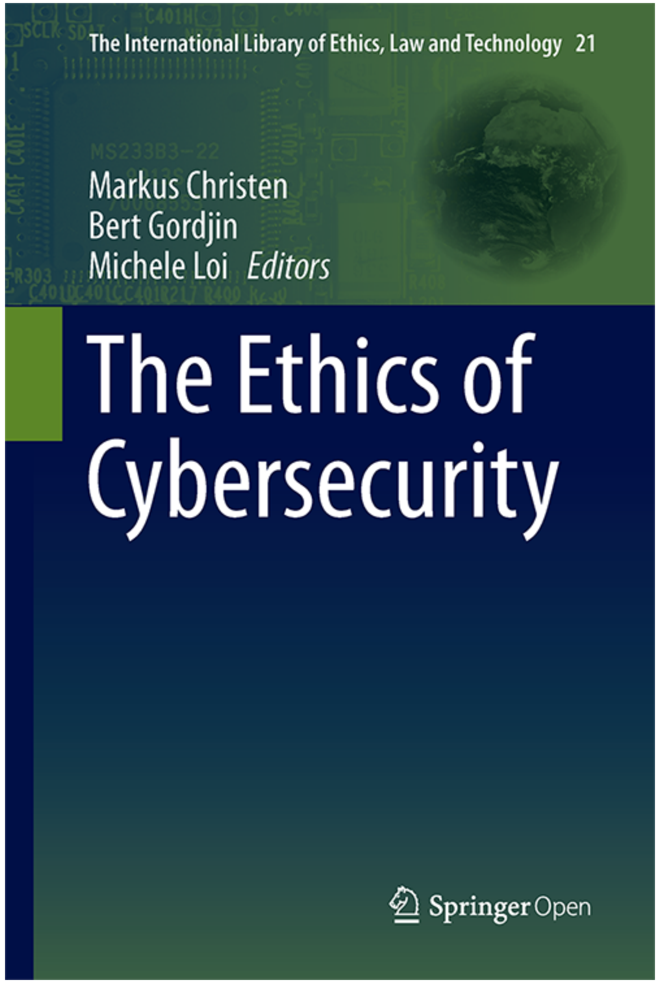
# New CANVAS book

*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**

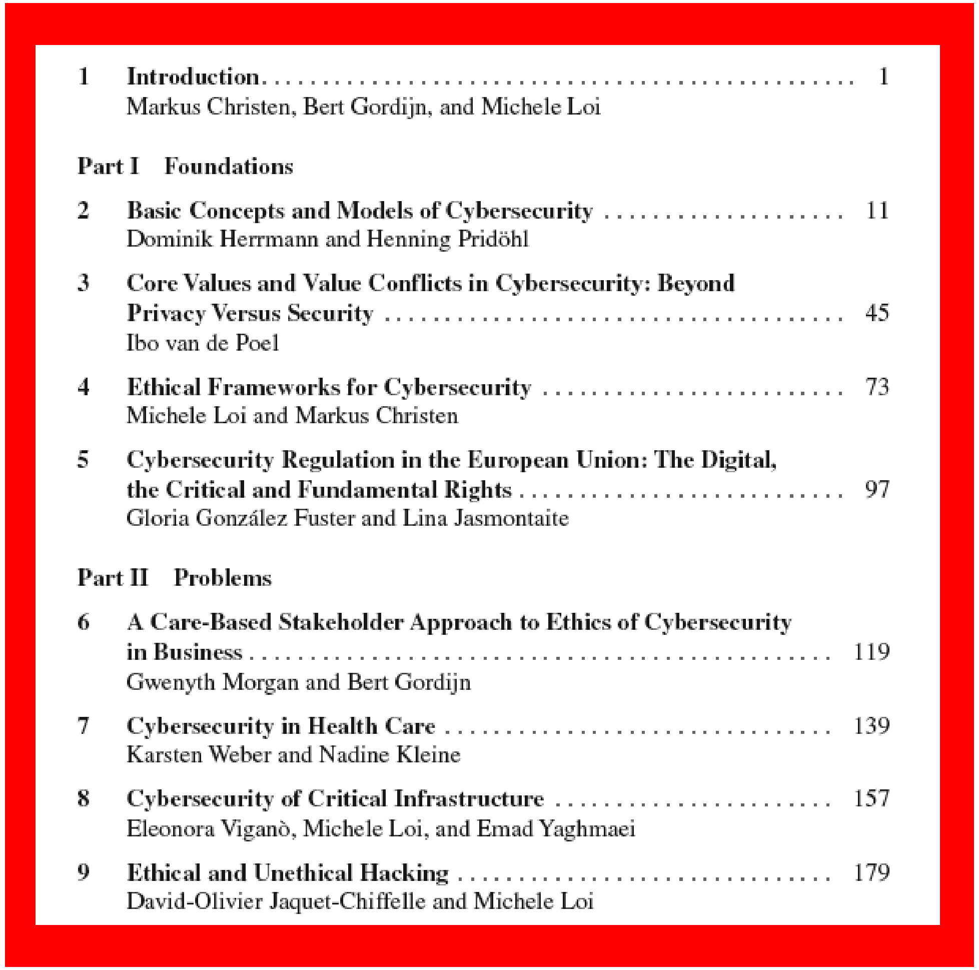


The International Library of Ethics, Law and Technology 21

Markus Christen
Bert Gordjin
Michele Loi *Editors*

The Ethics of Cybersecurity

Springer Open



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 Pridöhl

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 Jasmontaite

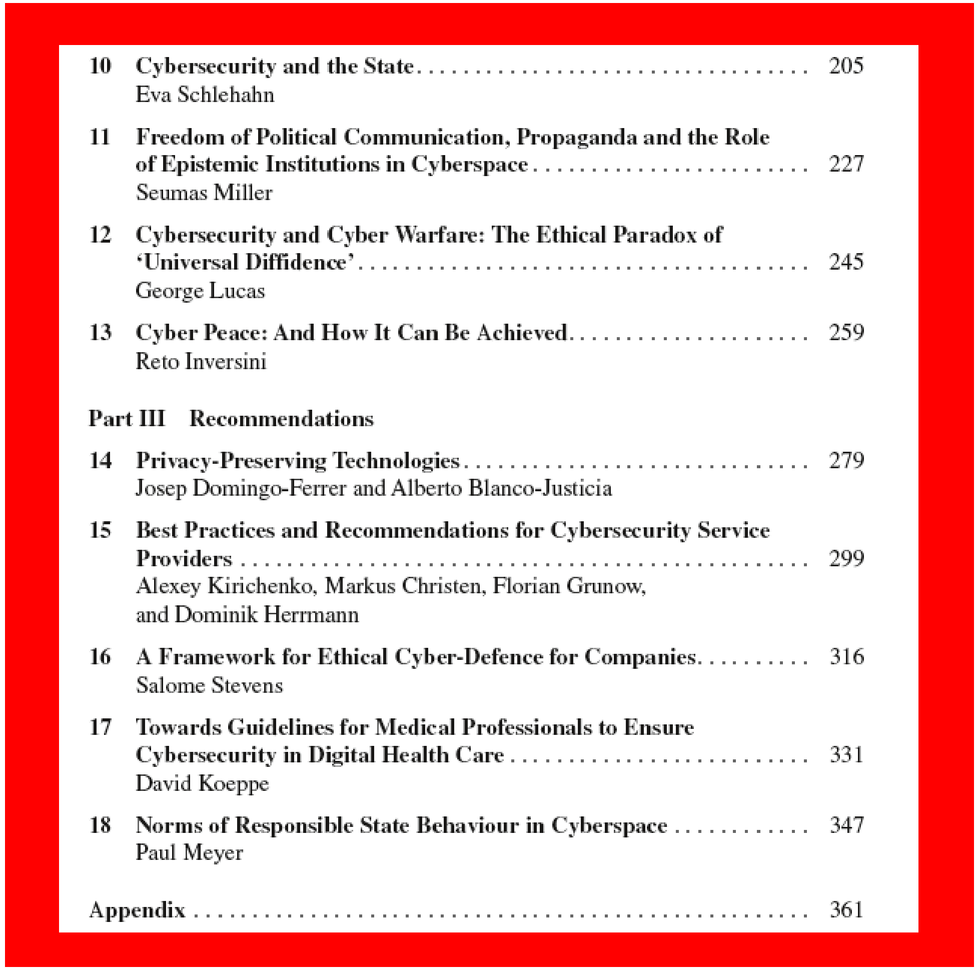
**Part II Problems**

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-Chiffelle and Michele Loi



10 **Cybersecurity and the State** . . . . . . . . 205
Eva Schlehahn

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 Diffidence'** . . . . . . . . 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 Koeppe

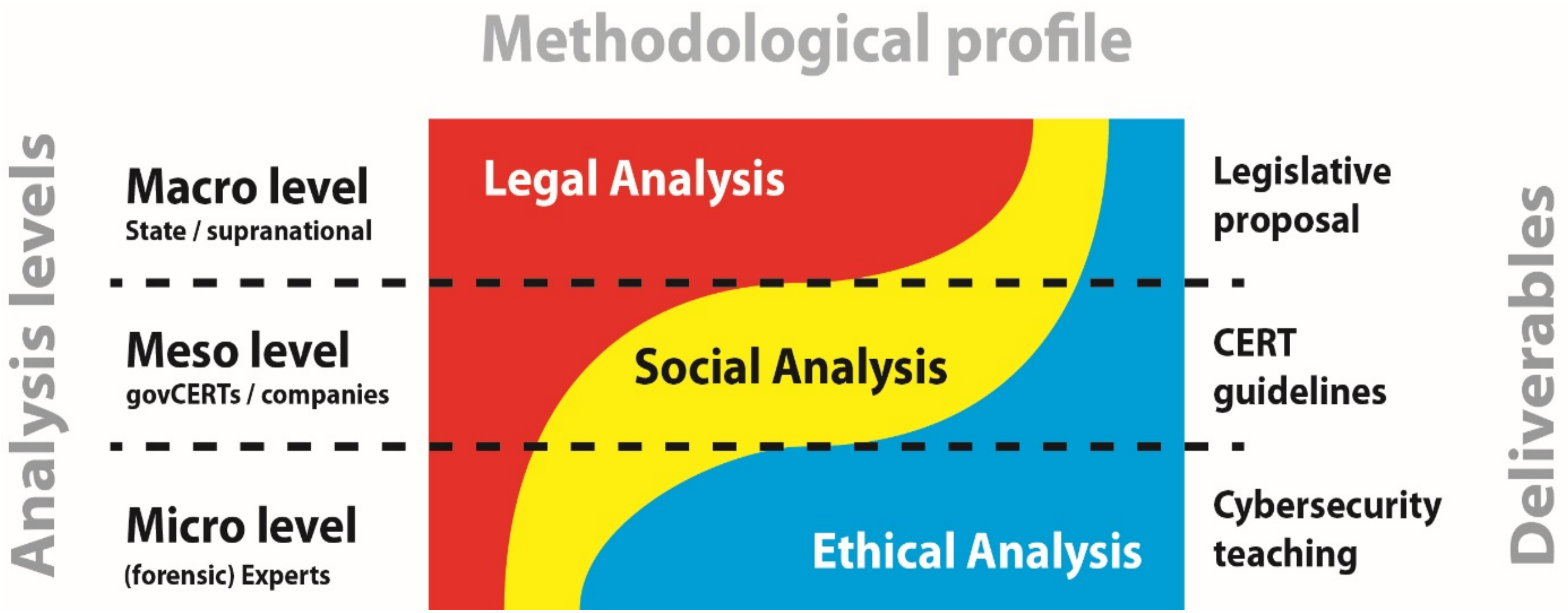
18 **Norms of Responsible State Behaviour in Cyberspace** . . . . . . . . 347
Paul Meyer

**Appendix** . . . . . . . . 361

**Ü Preliminary version:** CANVAS website / in print December 2019.

# 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


Methodological profile
Analysis levels
Macro level
State / supranational
Meso level
govCERTs / companies
Micro level
(forensic) Experts
Legal Analysis
Social Analysis
Ethical Analysis
Legislative proposal
CERT guidelines
Cybersecurity teaching
Deliverables