POLICY BRIEF NO. 1

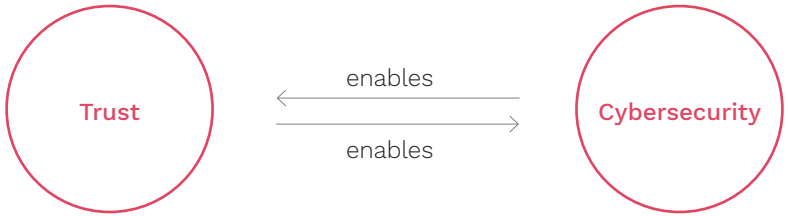
ACHIEVING TRUST IN EU CYBERSECURITY

Prepared by:
Michele Loi and Eleonora Viganó (Universität Zürich Digital Society Initiative DSI)

Trust and cybersecurity

This slidedoc summarizes some essential findings from the interdisciplinary literature on trust and trustworthiness.

It shows that cybersecurity is an essential condition of digital trust. Moreover, it analyses one case in which cybersecurity relies on trust and one case in which it is undermined because of a lack of trust.



- Interpersonal trust
- Trust and trustworthiness
- Moral and non moral elements of trust and trustworthiness
- Trust vs. sanctions

Achieves:

- Confidentiality
- Integrity
- Availability
- Unlinkability
- Intervenability
- Transparency

Trusting someone vs. relying on something

Trust and trustworthiness form positive feedback loops

Interpersonal trust is a more dynamic relation than reliance on mechanisms and systems.
Trust among persons/organizations is dynamic reliance: trustworthy people respond in a special way to people who trust them (Pettit 1995).

Trustworthiness: moral or not?

Trustworthiness can be motivated both morally and non morally.

Trust and reputation
Trustworthy people can be motivated by the desire for a good reputation (Pettit 1995). This motivation is non moral (but not immoral). The more social cooperation relies on trust relationships, the higher the importance of reputation.

Trust and moral obligations
Trustworthy people can be motivated by moral obligations, because accepting trust is similar to promising. When trust expectations are not met, that is often described as a betrayal of trust (Baier 1986).

The dynamic aspect of interpersonal trust

Transparency about the dispositions and performance of agents (persons or organizations) affects the success of «meta-trust» (Baier 1986), our reliance on interpersonal trust to achieve important social goals.

With complete information, only trustworthy types survive.

With no information, selfish strategies are more successful than fair and cooperative ones.

If it is impossible to distinguish trustworthy from non-trustworthy parties, cooperation based on mutual trust cannot develop (Olson 2000).

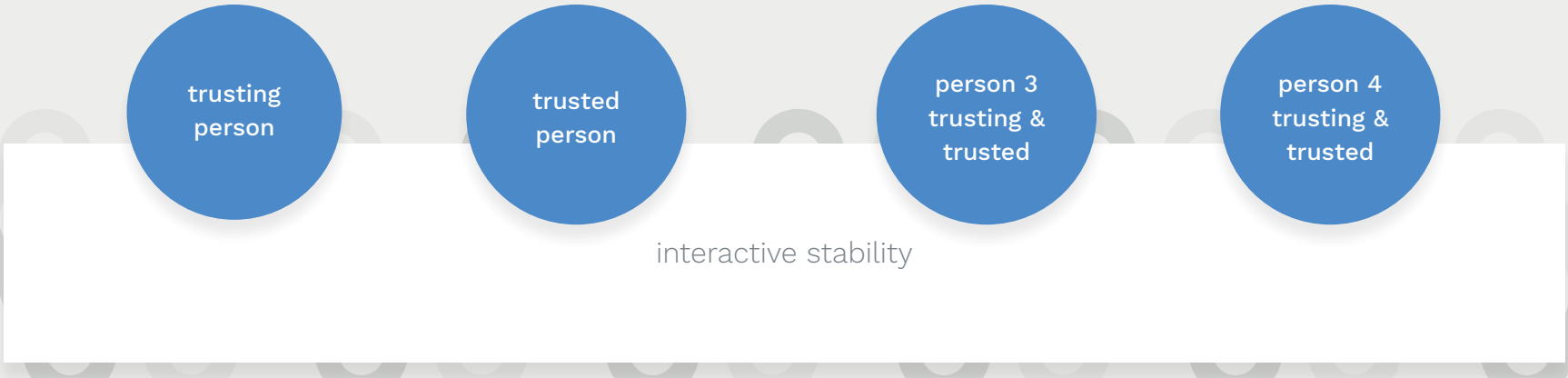
Hence, transparency about dispositions and performance reinforces trust.

Mutual trust involves reciprocal accountability

Trust in trustworthy agents enables broad networks of mutual trust

Information

trustworthy vs. non-trustworthy



Trust is confidence in another person's virtues

Trust implies a sense of confidence in other people's benevolence, conscientiousness, reciprocity and commitment to justice (Becker 1996).

Trust also has non-cognitive aspects:

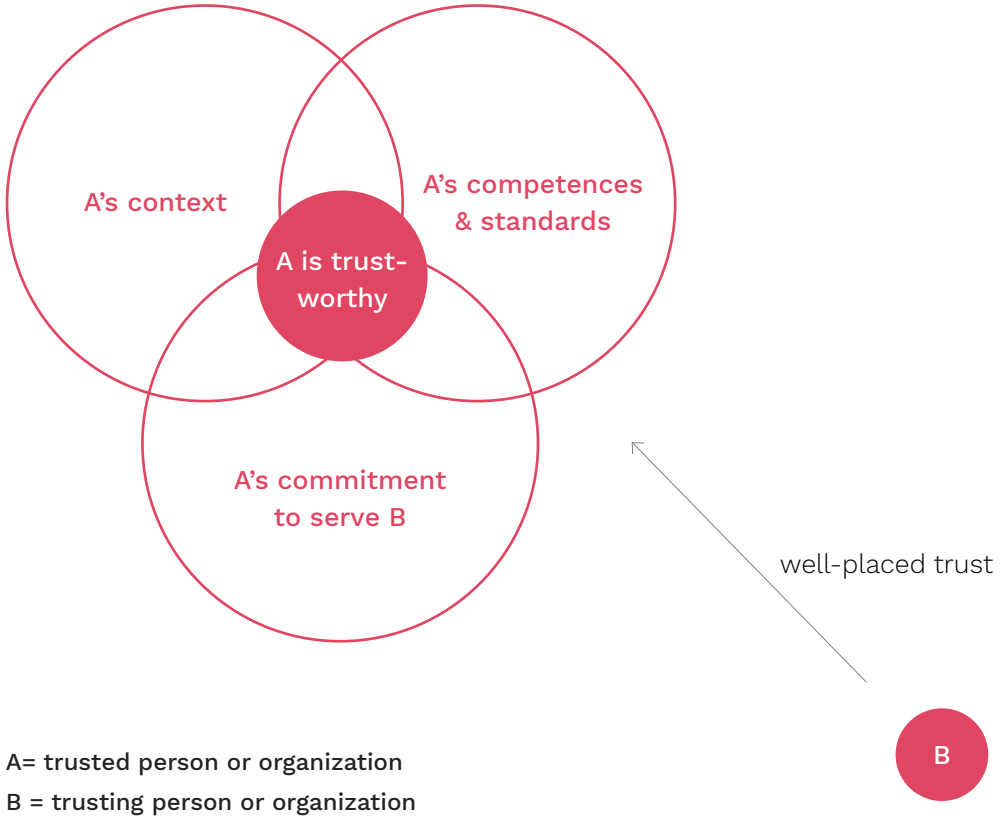
Taking a chance

Trusting someone also means being disposed to take a chance on another's behavior being cooperative when no prediction based on 'utility-maximization' rationality is possible (Held 1968).

Optimism

It requires optimism that the goodwill and competence of another person extends to our interaction with her (Jones 1996), especially when future interactions are foreseen (Olson 2000).

This optimism is not strictly rational, but it is also not foolish. A huge number of experiments has shown that humans can establish relations of mutual trust also in situations in which cooperation appears not to be rationally in each person's interest (Olson 2000).



A= trusted person or organization
B = trusting person or organization

Trusting trust vs. rational reliance in sanction avoidance

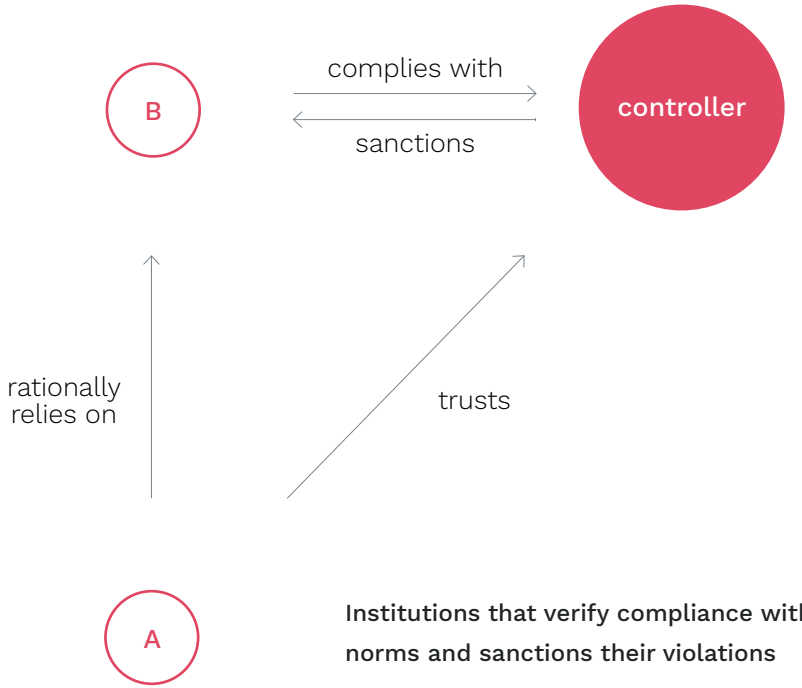
Legal institutions and economic incentives produce a different type of trustworthiness

Reliability can be achieved by institutions that impose sanctions against unreliable parties. These are mechanisms of external accountability.

Rational reliance mitigates the uncertainty and the need to rely on mutual trust.

Rational reliance and trust do not always work well in combination.

The empirical literature shows that sanctions and economic incentives may however crowd out social and moral motivations to be trustworthy (Frey 1994). People can find it harder to achieve a condition of self-reinforcing mutual trust when sanctions against trust betrayal are removed (Frohlich, Norman, and Joe A. Oppenheimer 1996, Ostrom 2000).



Institutions that verify compliance with norms and sanctions their violations

Cybersecurity as an enabler of trust

Elements of cybersecurity

Integrity
(Privacy-relevant) data and services that process such data cannot be modified in an unauthorized or undetected manner.

Availability
Access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner.

Confidentiality
(Privacy-relevant) data and services that process such data cannot be accessed by unauthorized entities.

Trust-enabling mechanisms

Transparency
Relationships based on mutual trust thrive when trustworthy agents (persons and organizations) can be recognized.

Reputation
Reputation systems provide non-moral incentives to be trustworthy.

Non-fabrication
Trust is undermined by unreliable trustworthiness signals.

Privacy (of individuals and groups)
Mutual trust enables and favors the sharing of confidential information. This is only sustainable as long as untrusted parties can be excluded from the information.

Institutions affect citizens' trust in cybersecurity actors

Successful laws, social practices, and social norms sustain rational expectations and emotional attitudes of trust

Actors involved in cybercrime prevention, investigation, and enforcement

National (examples)	EU (examples)
– NIS competent authorities - CERTs266 – Police forces – Cybercrime units – Defense and security agencies	– ENISA – CERT-EU – EP3R – EC3 (Europol) – CEPOL – Eurojust – EEAS – EDA

Countries with national legislative measures on cybersecurity

- Austria (2013)
- Croatia (2015)
- Czech Republic (2015)
- Republic of Cyprus (2012)
- The Netherlands (2014)
- Estonia (2014)
- Finland (2013)
- France (2015)
- Italy (2013)
- Germany (2011)
- Hungary (2013)
- Latvia (2013)
- Lithuania (2011)
- Luxembourg (2018)
- Malta (2015)
- Poland (2013)
- Slovak Republic (2015)
- Spain (2013)
- UK (2016)

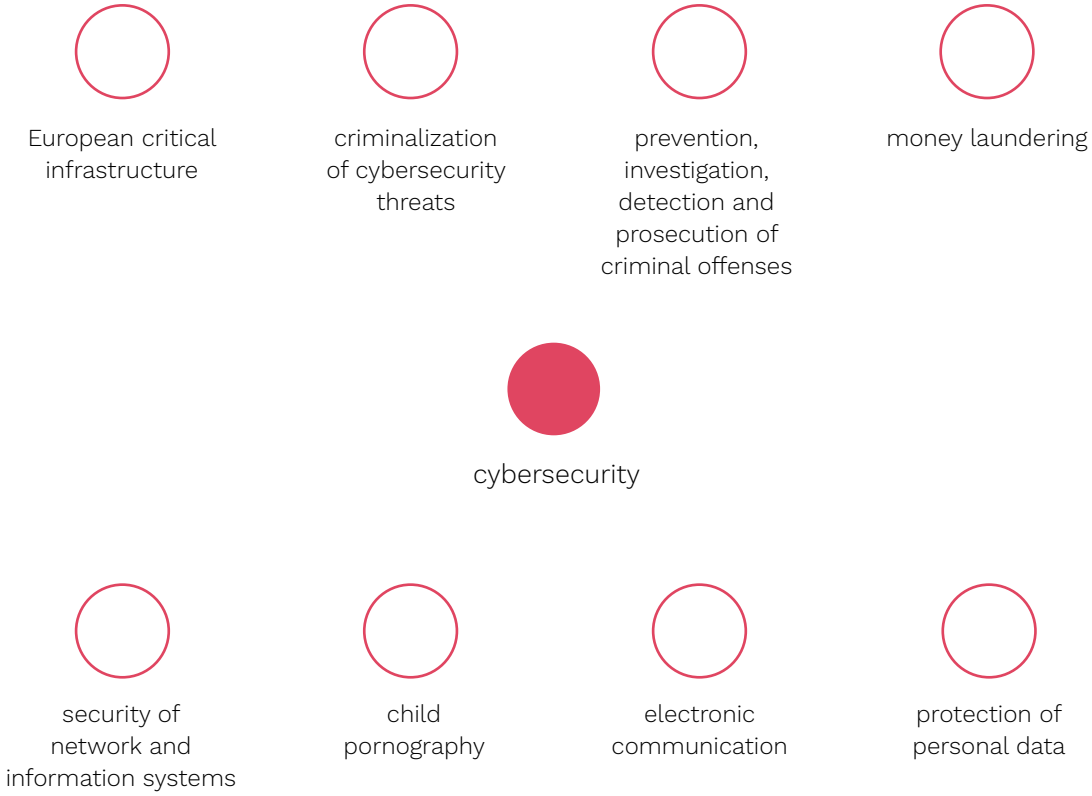
EU legislative measures on cybersecurity

- Proposal of a new Regulation on cybersecurity (12 Sept 2018)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR)
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013
- Directive (EU) 2015/849
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April
- Council Directive 2008/114/EC
- Commission Regulation No 611/2013 of 24 June 2013
- Directive 2016/1148 of the European Parliament and of the Council

Cybersecurity regulation has different facets

EU legislative measures on cybersecurity deal with different aspects of cybersecurity

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR)
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009
- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013
- Directive (EU) 2015/849
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April
- Council Directive 2008/114/EC
- Commission Regulation No 611/2013 of 24 June 2013
- Directive 2016/1148 of the European Parliament and of the Council



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

Often, the best way to detect vulnerabilities is trusting an ethical hacker...

Ethical hacking

Ethical hackers ('white hat' hackers) use the same tools and techniques of malicious hackers in order to test the cyber-defenses of a company, after the company's request and with its permission.

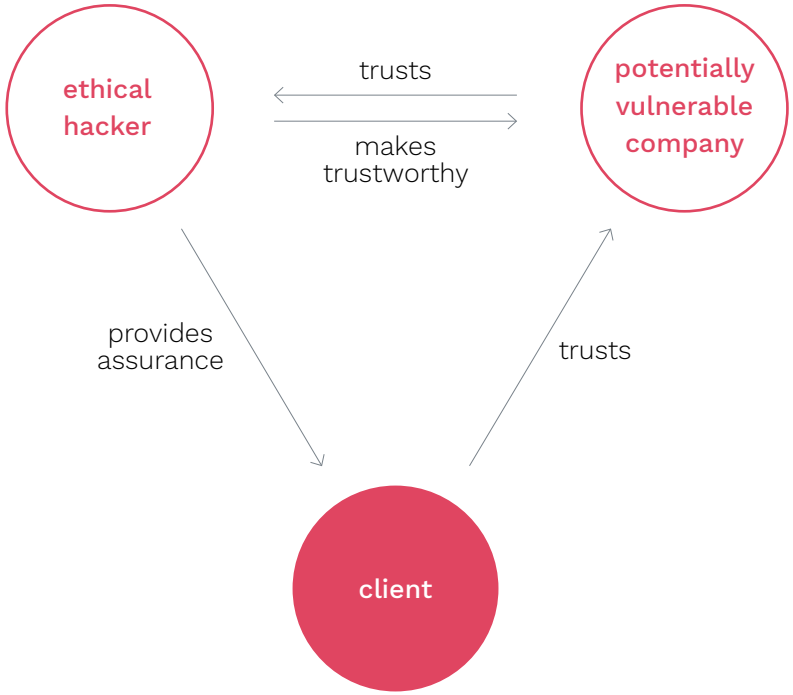
A privacy dilemma

Through penetration testing, an ethical hacker will gain access to the clients' personal data. The risk is that the user will intentionally misuse or carelessly divulge confidential information.

The solution to this dilemma involves finding a hacker you can trust: a trustworthy hacker behaves benevolently, conscientiously and competently.

A vicious trust circle?

- The company is trustworthy only if its cybersecurity provisions are properly tested.
- Penetration testing by an ethical hacker makes the company more trustworthy only if the hacker is also trustworthy.
- How can the company identify trustworthy hackers? And how can the client know this?

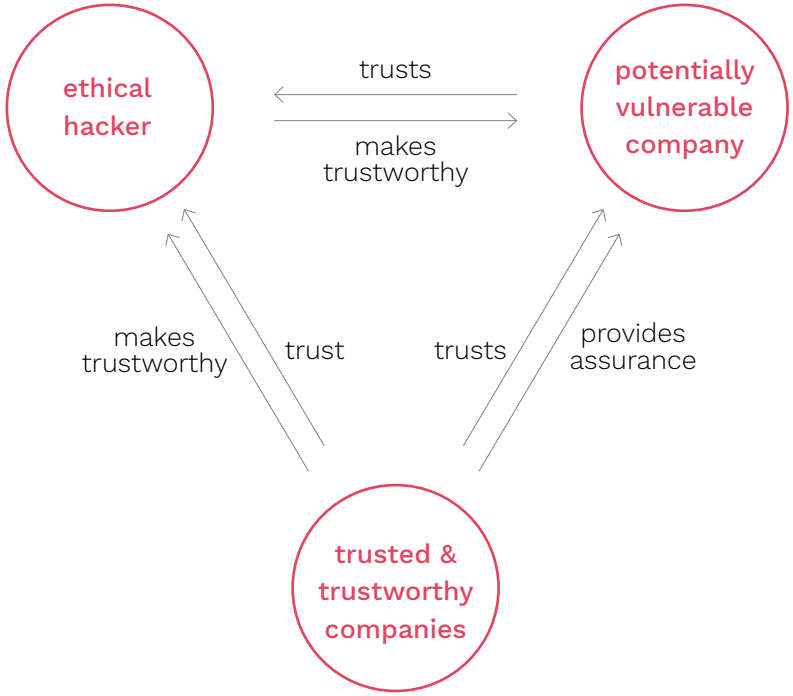


Case-study 1 Ethical hacking and data privacy (2/3)

Trustworthiness trickles down through networks of trust

How does one establish the trustworthiness of an ethical hacker?
It may be difficult to know if a hacker is trustworthy. In practice however trust is more rational if information about ethical hackers flows between companies with similar cybersecurity needs, which trust each other. Clusters of trusted (and trustworthy) companies can share information that indicates that the hacker can be trusted.

From the client perspective:
Companies who know that a company belongs to a cluster that is a network of trust have reasons to trust the company will adopt appropriate cybersecurity practices (e.g. hiring trustworthy ethical hackers), especially if associates are known to share best practices. Other indicators of trustworthiness can be certifications, including self-certification schemes.



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

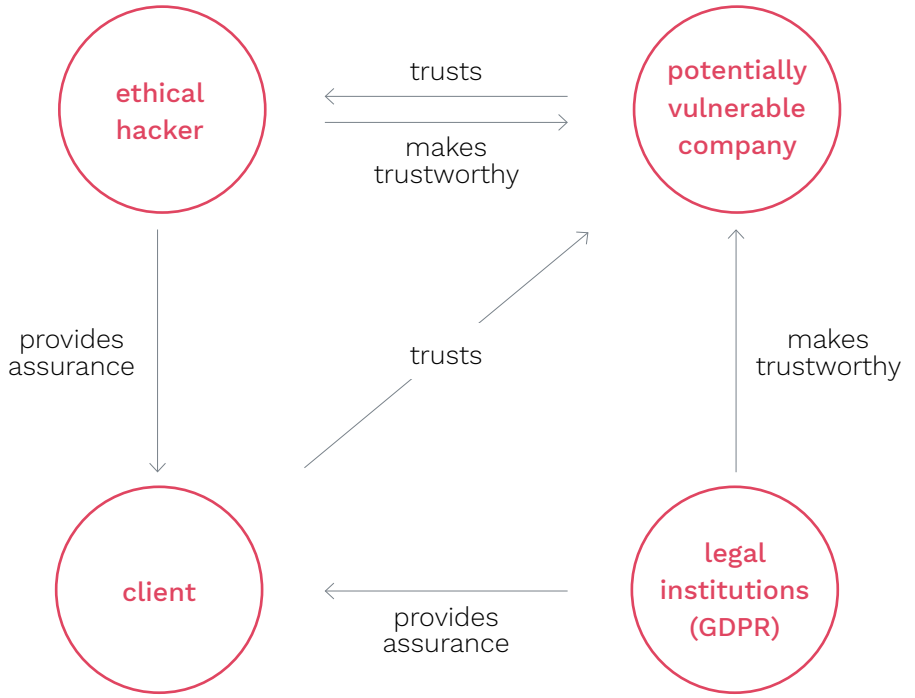
What is the role of legal institutions?

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.



Case study 2 Governments using zero-day exploits (2/3)

A cyber-arms race in which the need of security reduces trust

A new way to attack and spy enemies

Zero-day exploits are a form of weapon, as they can disrupt computers and their network as well as they can give access to relevant information. Governments buy zero days in order to attack or spy other countries or opponents.

The opposite of dynamic reliance

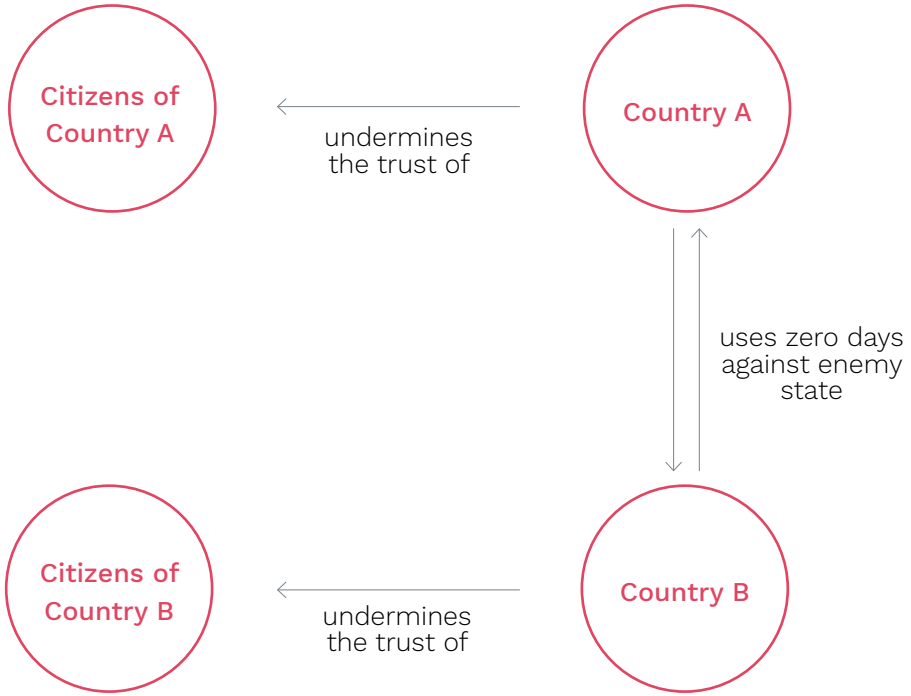
If each government seeks for vulnerabilities of other countries, in order to protect itself, in the long-run each country will be less secure. The search for “cybervulnerabilities” of the other countries makes relationships of trust among countries impossible.

Numbers are positive expected outcomes for national defense (e.g. savings in traditional defense expenditure, in millions of $).

	Country B	Exploit	Do not exploit
Country A	Exploit	-100,-100	100,-300
	do not exploit	-300,100	30,30

Trustworthiness externalities of using zero-days exploits (3/3)

If governments keep the zero-day exploits they know in secrecy, can their citizens trust them? Can governments be relied on not to use them to monitor their citizens?



Securing trust in cybersecurity: challenges

Commercial trade-offs (utility vs. security)

- Security and data protection are costs for data driven businesses.
- Arms race for offensive strategies
- Consumers do not want the usability costs associated with heightened cybersecurity
- Companies increasingly rely on vulnerable IT

Enforcement trade-offs (privacy vs. security)

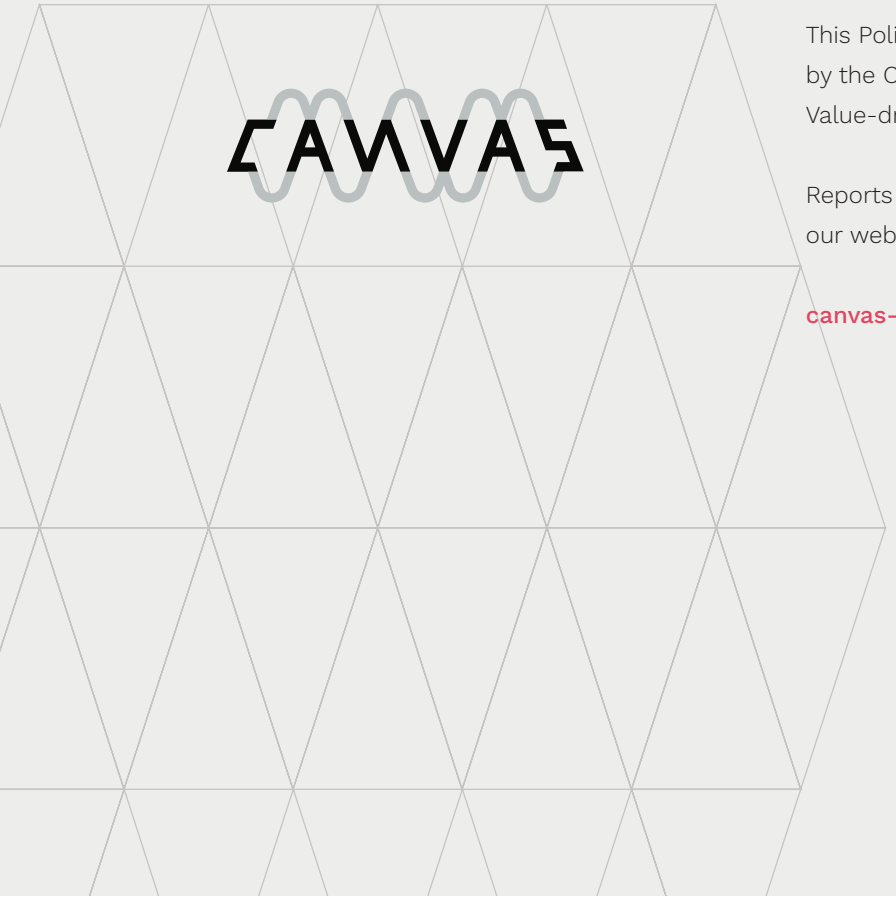
- Infringement of privacy
- Intrusiveness of security tools challenging privacy
- Vulnerabilities sold on grey and black markets to governments
- Lawful access exploits can be loopholes for malicious parties
- Many cybersecurity measures rely on surveillance
- Risk of misuse
- Offensive measures can weaken security for everyone

Regulatory trade-offs (complexity vs. security)

- Difficult actor allocation for cybersecurity incidents
- Legal and factual frame conditions often unclear
- Rapidly developing technology
- Cybersecurity is a very complex global issue
- Varying and unforeseeable impact of events

Challenges explored in Jasmontaite et al 2017

Where more info can be found



This Policy Brief is based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity).

Reports of the CANVAS work have been published on our website:

canvas-project.eu

The objective of CANVAS is to bring together stakeholders from key areas of the European Digital Agenda to approach the challenge how cybersecurity can be aligned with European values and fundamental rights.

The following slide directly points to those of our White Papers which address in detail the challenges of cybersecurity.

Bibliography: cybersecurity challenges (CANVAS)

Ethical challenges

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Legal challenges

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Technological challenges

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter, and Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” SSRN Scholarly Paper ID 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Bibliography

Trust – general – philosophical

- Held, Virginia. 1968. “On the Meaning of Trust.” Ethics 78 (2): 156–59.
- Baier, Annette. 1986. “Trust and Antitrust.” Ethics 96 (2): 231–60.
- Pettit, Philip. 1995. “The Cunning of Trust.” Philosophy & Public Affairs 24 (3): 202–25.
- Becker, Lawrence C. 1996. “Trust as Noncognitive Security about Motives.” Ethics 107 (1): 43–61.

Trust – general - social science

- Frey, Bruno S. 1994. “How Intrinsic Motivation Is Crowded out and In.” Rationality and Society 6 (3): 334–52.
- Ostrom, Elinor. 2000. “Collective Action and the Evolution of Social Norms.” The Journal of Economic Perspectives 14 (3): 137–58.
- Frohlich, Norman, and Joe A. Oppenheimer. 1996. “Experiencing Impartiality to Invoke Fairness in the N-PD: Some Experimental Results.” Public Choice 86 (1): 117–35. https://doi.org/10.1007/BF00114878.

Trust – online – digital

- Erlich, Yaniv, et al. 2014. “Redefining Genomic Privacy: Trust and Empowerment.” PLOS Biology 12 (11): e1001983.
- Etzioni, Amitai. 2017. “Cyber Trust.” Journal of Business Ethics, July. https://doi.org/10.1007/s10551-017-3627-y.
- Chakravorti, B., Bhalla, A., Chaturvedi, R.S., 2018. The 4 Dimensions of Digital Trust, Charted Across 42 Countries. Harvard Business Review.

Project facts

Project coordination and contact:
PD Dr. sc. ETH Markus Christen
University of Zurich (UZH),
Digital Society Initiative
Rämistrasse 66, 8001 Zürich

Slidedocs version:
Version 1.0, March 2019

Project duration:
Sept. 2016 – Aug. 2019

Partners:
The CANVAS Consortium consists of 11 partners (9 academic institutions and 2 partners outside academia) located in 7 European countries.

Funding:
1.57 Mio. €, of which 1 Mio. € is funded by the European Commission and the remaining part emerges from the Swiss State Secretariat for Education, Research and Innovation.

Funding notice for CANVAS

Co-funded by the Horizon 2020 programme of the European Union

The CANVAS project (Constructing an Alliance for Value-driven Cybersecurity) 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