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.

Contents

Executive summary

As we rely more and more on information and communication technology, cybersecurity becomes both essential and problematic to our societies. On the one hand, cybersecurity is essential to prevent cyber threats from undermining citizens' trust and confidence not only in the digital infrastructure but in policy makers and state authorities as well. On the other hand, cybersecurity is problematic because enforcing it may endanger fundamental values like equality, fairness, autonomy, or privacy.

The CANVAS project aims to foster value-driven cybersecurity, with respect to European values and fundamental rights. Its first milestone is to consolidate existing knowledge and data related to cybersecurity in four areas, namely the ethical, legal, empirical, and technological domains.

This White Paper summarises currently available empirical data about attitudes and opinions of citizens and state actors regarding cybersecurity. It describes what these stakeholders generally think, what they feel, and what they do about cyber threats and security (counter)measures. For citizens' perspectives, three social spheres of particular interest are examined: 1) health, 2) business, 3) police and national security.

This unique synthesis builds on a variety of sources with both quantitative and qualitative data. For citizens' perspectives, our sources include reports from EU projects and Eurobarometer surveys, as well as additional scientific papers. As for state actors' perspectives, they rely essentially on policy documents, as they are the most relevant data available.

In the general conclusion, we sum up our main findings and suggest four consequent actions:

1. We need to improve awareness about cybersecurity: more information about current risks and concrete measures should be provided to a broader public.
2. We ought to keep a holistic view on all value-related topics: we should not have to choose between (cyber)security and privacy, or any other value.
3. Most found data relates to general issues of security and privacy; therefore, further empirical research is needed to cover other values, but also to investigate specific issues such as in health or business.
4. In line with the Standard Data Protection Model, three new protection goals should be added to the CIA triad (confidentiality, integrity, availability): unlinkability, intervenability, and transparency. Thus, privacy and security can be mutually reinforcing.

Ultimately, working towards value-driven cybersecurity goes beyond adding privacy requirements, although it is a first, significant and welcome step. Both citizens' perspectives and their direct involvement are crucial to enforce fundamental rights in the cyberspace and to contribute to a secure, value-driven information society.

CANVAS White Papers – Overview

In order to summarize the existing literature on the topics and issues that are relevant for the CANVAS project, the CANVAS consortium has created four White Papers as follows:

- White Paper 1 – Cybersecurity and Ethics: This White Paper outlines how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located. The White Paper is based on an extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. For each domain, a systematic literature search has been performed and the identified papers have been analysed using qualitative and quantitative methods. An important observation is that the ethics of cybersecurity not an established subject. In all domains, cybersecurity is recognized as being an instrumental value, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data.
- White Paper 2 – Cybersecurity and Law: This White Paper explores the legal dimensions of the European Union (EU)'s value-driven cybersecurity. It identifies main critical challenges in this area and discusses specific controversies concerning cybersecurity regulation. The White Paper recognises that legislative and policy measures within the cybersecurity domain challenge EU fundamental rights and principles, stemming from EU values. Annexes provide a review on 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.
- White Paper 3 – Attitudes and Opinions regarding Cybersecurity: This White Paper summarises currently available empirical data about attitudes and opinions of citizens and state actors regarding cybersecurity. The data emerges from reports of EU projects, Eurobarometer surveys, policy documents of state actors and additional scientific papers. It describes what these stakeholders generally think, what they feel, and what they do about cyber threats and security (counter)measures. For citizens' perspectives, three social spheres of particular interest are examined: 1) health, 2) business, 3) police and national security.
- White Paper 4 – Technological Challenges in Cybersecurity: This White Paper summarizes the current state of discussion regarding the main technological challenges in cybersecurity and impact of those, including ways and approaches to addressing them, on key fundamental values. It provides an overview on current cybersecurity threads and countermeasures and focuses on ethical dilemmas that emerge when counteracting those threads. It also points to the fact that the cybersecurity community relies much more on interpersonal relations when sharing intelligence and data than in explicit national or supranational regulations. Furthermore, the White Paper presents advanced cryptographic techniques and data anonymization techniques that may help to solve or minimize some of the ethical dilemmas.

All White Papers and additional material are available at the Website of the CANVAS project: www.canvas-project.eu

1. Introduction*

The digitalisation of modern life brings many changes and challenges. As we rely more and more on information and communication technology (ICT), *cybersecurity* becomes both essential and problematic to our societies. On the one hand, cybersecurity is essential to prevent cyber threats from undermining citizens' trust and confidence not only in the digital infrastructure but in policy makers and state authorities as well. On the other hand, cybersecurity is problematic because enforcing it may endanger other fundamental values like autonomy, equality, fairness, or privacy. This is the reason why the CANVAS project aims to foster value-driven cybersecurity.

The first step of CANVAS is to consolidate existing knowledge and data related to cybersecurity in four domains: philosophical-ethical deliberations, legal knowledge, empirical research, and technology development. This White Paper aims at summarising currently available *empirical data on attitudes and opinions* regarding cybersecurity. It is complementary with the three other White Papers dealing respectively with the ethical, legal, and technological domains. Together, these four documents provide an enlightening multi-disciplinary view on current cybersecurity issues with respect to European values and fundamental rights.

In this White Paper, we consider opinions and attitudes of *European citizens and state actors* on cybersecurity, i.e. what they think, what they feel, and what they do about cyber threats and security (counter) measures. As cybersecurity affects ICT applications in every social sphere, an exhaustive evaluation is not feasible. CANVAS focuses on three social spheres of reference, each with its unique types of values conflicts: 1) health, 2) business, 3) police and national security.

Our synthesis builds on a variety of *sources* with both quantitative and qualitative data. For citizens' perspectives, our sources include reports from former EU projects and Eurobarometer surveys, as well as additional scientific papers. We performed a tailored literature search in scientific databases, whose results were then filtered for each social sphere.[1] As for state actors' perspectives, they rely essentially on policy documents, as they are the most relevant data available.

Of course, the proper *interpretation* of any empirical data is delicate. Surveys and polls only give a snapshot of the respondents' answers to carefully crafted questions. Focus groups are more interactive and more instructive, but their participants are fewer and less representative of the general public. Such studies gather attitudes and opinions of particular people in particular places at particular times. If their sampling is adequate, we may generalise theirs results to the population studied, knowing that these results give a partial picture and may evolve over time. That being said, many results exposed in this White Paper reflect findings of large surveys: indeed, several EU projects used a sample of around 27'000 respondents, with about 1'000 citizens from each EU27 member. These results might be influenced by the intrinsic bias towards *privacy* of some of the surveys, especially those focussing on ways to go beyond the traditional trade-off between security and privacy.

This White Paper presents the main findings of most relevant, existing studies. For the sake of brevity, we may speak of, for instance, "the opinion of citizens", even though it would be scientifically more accurate to say "the answers of the respondents to this survey". Moreover, we use the present tense everywhere and specify the date when original data was gathered. For more details, we refer the reader to the original publications where the mentioned data is thoroughly reported and analysed.[2]

---

* This introduction has been written by Florent WENGER and David-Olivier JAQUET-CHIFFELLE (University of Lausanne).

[1] See Appendix A.2: Literature Search Methodology.

[2] See Appendix A.4 References in the end.

2. Citizens on Cybersecurity in general*

In sections 2 to 5, we collate empirical data on EU citizens' attitudes towards cybersecurity. The main issues which are reoccurring in the literature include privacy infringement, data processing, data collection, proportionality, risks, access, control, efficiency, and reliability of the technology. For the purposes of cohesiveness, we consider EU citizens' attitudes towards cybersecurity in general before we present the results for the opinions towards cybersecurity regarding the three focused domains business, health, and national security.

The *Cyber Security Strategy* proposed by the EU in 2013 notes that one of the main challenges in cybersecurity is the fact that cybercrime is high-profit and low-risk, and there is a lack of accountability which criminals often exploit.[3] Cybercrime is now one of the fastest growing forms of crime with more than one million people worldwide falling victim each day.[4] In order to combat cybercrime and increase the efficiency of cybersecurity, the Strategy recommends a coordinated collaborative approach stating that "security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority".[5]

Making a coordinated effort across many sectors to boost cybersecurity with the aim of preventing cybercriminals from intruding into information systems, stealing critical data or holding companies to ransom may significantly reduce the potential of a cyberattack disrupting the supply of essential services we take for granted such as water, healthcare, electricity, or mobile services.[6] However, a coordinated approach will not be successful without public engagement. The Strategy accepts that citizens need to have trust and confidence in the people and businesses which design, control and operate security technologies in order for citizens to adopt and engage with new technology.[7]

The following section provides an overview on empirical research related to attitudes and opinions of EU citizens regarding cybersecurity in general. Therefore, we carried out a research on projects and surveys provided by the EU. It became apparent that the attitudes of citizens regarding cybersecurity are addressed, either to a greater or lesser extent, in many projects. The most relevant points are summarized below. On account of the sufficient number of findings in this research step, an additional literature search was not required (in contrast to the health, business and national security spheres).

2.1 Results from EU Projects and Surveys[8]

It should be noted that the stated EU projects and surveys refer to each other; therefore, the projects will be presented both clustered and in chronological order.

2.1.1 Eurobarometer

Eurobarometer is a regularly published report of the European Commission to survey the public opinion by interviewing around 1,000 respondents per EU member state.[9]

---

* This section has been co-written by Nadine KLEINE (Regensburg University of Applied Science) and Gwenyth MORGAN (Dublin City University).

[3] 'Cyber Security Strategy of the European Union', European Commission.

[4] Ibid., p. 10.

[5] Ibid., p. 12.

[6] Ibid., p. 3.

[7] Ibid., p. 2.

[8] See Appendix A.1: EU projects overview, and A.4 References: EU projects.

[9] http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm

'Flash Eurobarometer 225', conducted in 2008, reveals that 64% of participants fear that organisations may handle their personal data inappropriately.[10] There is consensus that personal data is best protected by medical services, doctors and public institutions and a large majority (82%) believe that data transmission over the web is not sufficiently secure.[11] In respect of citizens' ability to use security technologies, 22% of women answered that they would not know how to install security software on their computers. In respect of the belief that security technologies are effective, respondents who expressed uncertainty about the efficiency of the security oriented technologies were male and from the younger age groups.[12]

'Special Barometer 359', conducted in 2011, reveals that four in ten internet users in the EU use strategies and tools such as anti-spy software to reduce unwanted emails and spam, and/or try to ensure that a transaction is protected by looking out for a security logo or label.[13] One fifth of the internet users change the security settings of their browser to increase privacy and avoid providing the same information to different sites.[14] Other "protection techniques" are cited by less than 15% of Europeans.[15] 22% of internet users change the security settings of their browser to increase privacy and only 12% use a dummy email account.[16] These numbers are very low and appear to be influenced by the security company in charge of the analysis of the data collected, i.e. citizens' opinions vary depending on whether cybersecurity is operated by a public institution or a private institution. For example, 78% of Europeans trust health and medical institutions, 70% trust national public authorities such as tax authorities and social security authorities.[17] 22% trust internet companies such as search engines, social networking sites, and email services.[18] Seven in ten Europeans are concerned that companies may use their personal information for a purpose other than that for which it was originally collected without informing the citizens themselves (e.g. for direct marketing or targeted online advertising).[19] In the event of a cyberattack or information leak, nine in ten Europeans want to be informed by a public authority or by a private company if information held about them has been lost or stolen.[20]

'Special Eurobarometer 423', conducted in 2014 and published in 2015, updates the previous study 'Special Eurobarometer 404' from 2013 about cybersecurity.[21] Simultaneously with an increasing number of internet access (from 72 to 76%), devices (especially smartphones from 35 to 61% and tablets from 14 to 30%) and online activities (e.g. social networks from 53 to 60%, buying goods or services from 50 to 57%), the concerns of EU citizens regarding internet transactions and cybercrime are rising.[22] The most common concerns are about the misuse of personal data (from 37 to 43%) and the security of online payments (from 35 to 42%); only 18% (2013: 23%) of the respondents have no concerns.[23] Asked about their agreement to concrete statements about attitudes to cybersecurity, 89% (2013: 87%) states that they avoid disclosing personal information and 85% (2013: 76%) perceive an increasing risk of becoming a victim of cybercrime. Concerns that personal information is not kept secure by websites are shared by 73% (2013: 70%) and are somewhat lower with regard to public authorities (67%; 2013: 64%).[24] The results of querying a list of concrete cybercrimes show that the majority of internet users

[10] 'Flash Eurobarometer 225: Data Protection in the European Union – Citizens' Perception', p. 5.
[11] Ibid., p. 8, 17.
[12] Ibid., p. 19.
[13] 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union', p. 106.
[14] Ibid., p. 110.
[15] Ibid., p. 135.
[16] Ibid., p. 107.
[17] Ibid., p. 138.
[18] Ibid., p. 141.
[19] Ibid., p. 146
[20] Ibid., p. 151, 154.
[21] 'Special Eurobarometer 404: Cyber Security'.
[22] 'Special Eurobarometer 423: Cyber Security', p. 9, 13, 18.
[23] Ibid., p. 23f.
[24] Ibid., p. 45f.

have growing concerns about different sorts of crimes; they fear identity theft (68%; 2013: 52%), discovering malicious software on their device (66%), being a victim of bank card or online banking fraud (63%, 2013: 49%) and a hacked social media or email account (60%, 2013: 45%).[25] The number of respondents who changed their online behaviour because of security concerns increased since 2013 from 81 to 88% (largest growths: using anti-virus software from 46 to 61%, not opening emails from unknown people from 40 to 49%).[26] Even though only 47% (2013: 44%) feel well informed about the risks of cybercrime, around three in four internet users state to be able to protect themselves sufficiently.[27] In case of becoming a victim of cybercrime, the respondents would, in most cases, contact the police (depending on the sort of crime, between 37% by a hacked social media or email account and 84% in case if identity theft), followed by website or vendor and the internet service provider.[28]

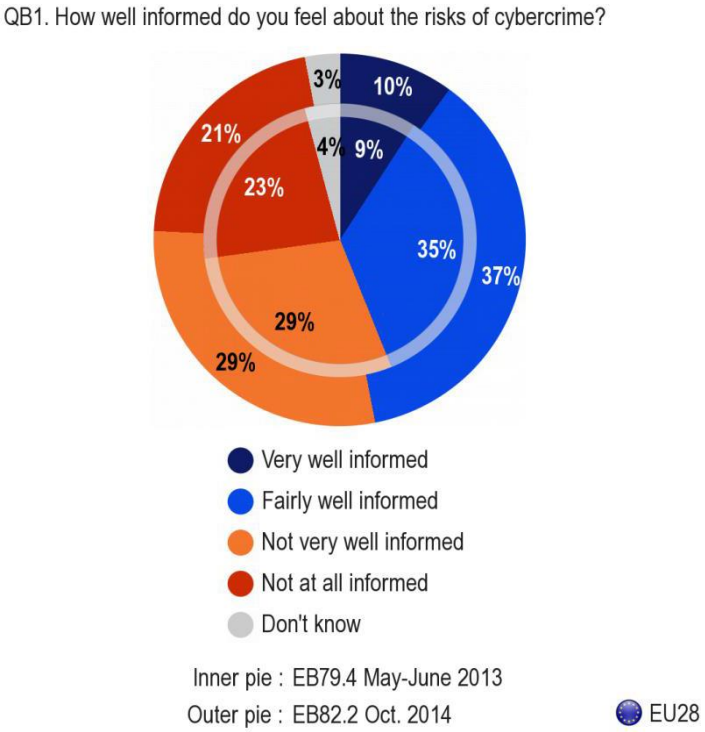

Figure 1: EU citizens and information about cybercrime[29]

In 'Special Eurobarometer 432' from 2015, it becomes apparent that EU citizens perceive cybercrime as a significant threat in general, but they consider themselves also better informed (see Fig. 1): the open question for the (three) most important challenges to the security of the EU was answered by 12% with "cybercrime".[30] By the rating of the five main challenges, cybersecurity was with 80% the third most important internal security challenge; 63% of the respondents believe that cybercrime will increase.[31] For EU citizens, the entities that play an important role in ensuring security against cybercrime are the police (70%), the judicial system (64%), the army (47%) and the citizens themselves (46%) – although only 46% agree that the police are doing enough to fight cybercrime, while 40% do not think so.[32]

[25] Ibid., p. 54f.
[26] Ibid., p. 30.
[27] Ibid., p. 41f, 46.
[28] Ibid., p. 83-93.
[29] Source: 'Special Eurobarometer 423: Cyber Security', p. 41.
[30] 'Special Eurobarometer 432: Europeans' Attitudes towards Security', p. 19.
[31] Ibid., p. 23, 31.
[32] Ibid., p. 38f.

In the most recent report 'Special Eurobarometer 464a' from September 2017, the awareness regarding cybercrime in general increased again: Over eight in ten (87%) respondents see cybercrime as important and this is the case for a majority of respondents in every country. This proportion has increased by seven percentage points since March 2015.[33] However, it is worth noting that the increase in concerns about these threats is steeper than the increase in the proportion of people who have actually been victims of the various kinds of cybercrime.

2.1.2 PRISE and PRESCIENT

Privacy concerns are an issue for EU citizens. For example, according to interview meetings conducted in 2007 within the EU project PRISE (which considered mass surveillance methods in the interests of national security), 85% of EU participants agree that privacy should not be violated without reasonable suspicion of criminal intent and 80% feel that it is unpleasant to be under surveillance stating that "participants in general weigh privacy higher than security".[34] Participants differentiate serious crime from petty crime (e.g. speeding or shoplifting): petty crime is not considered a legitimate reason for privacy infringement whereas serious crime (unspecified) is.[35] The issue of access is again raised in the context of what information is being collected by security companies and what harm could come from the potential misuse of same.[36] The report also notes that EU citizens believe "physically intimate technologies are unacceptable, [the] misuse of technology must be prevented and function creep is not acceptable".[37]

In 2012, PRESCIENT found that the majority of EU citizens lack an adequate understanding of how data processing and security utilities operate, stating that this limits the ability of the individual to "rationally balance each transaction for benefits and consequences".[38] Participants reaffirm the opinion that they are uncomfortable with the idea of being under surveillance.[39]

2.1.3 CONSENT – SMART – RESPECT

The relevant EU projects presented below are all part of the 7th Programme for Research and Technological Development, in which research projects regarding specific thematic areas were generated. The CONSENT, SMART, and RESPECT projects all deal with different perspectives on privacy and new technologies such as security and surveillance, therefore their implications are brought together.[40]

The CONSENT project ran from 2010 until 2013 and attempted to analyse online consumer behaviour by, amongst others, querying consumers' attitudes towards personal privacy.[41] A part of the project was a study ran in 2011 about awareness, values and attitudes of user generated content (UGC) website users towards privacy. With a combination of quantitative and qualitative research, 8,641 individuals from 26 EU countries were questioned.[42] The respondents are "above-average frequency internet users": 87% created an account with a social networking site.[43] Among the reasons why they would not use these accounts, trust issues only plays a minor role (8%), a bigger role among the reasons for deleting the accounts (30%).[44] The types of information that they disclose the most are name (83%), email

[33] 'Special Eurobarometer 464a: Europeans' Attitudes towards Security', p. 5.
[34] 'PRISE D-5.8: Synthesis report – interview meetings on security technology and privacy', p. 20.
[35] Ibid., p. 22.
[36] Ibid., p. 25.
[37] Ibid., p. 33.
[38] 'PRESCIENT D-3: Privacy, data protection and ethical issues in new and emerging technologies', p. v.
[39] Ibid., p. 48.
[40] http://respectproject.eu/research-content/working-packages/consolidation-of-smart-consent-and-respect/
[41] 'CONSENT D-7.3: Synthesised all countries report'.
[42] Ibid., p. 3.
[43] Ibid., p. 3, 15.
[44] Ibid., p. 16-18.

address (79%), and photos of themselves (68%).[45] Nevertheless, the disclosure of personal information is perceived as high risk (5.2 - 6.1 on a scale 1 - 7); for the respondents it is likely to happen that information being shared is used to send you unwanted commercial offers (81%), that it is used without the user's knowledge (74%), and that it is shared with third parties without the user's agreement.[46] 74% are aware that the information they include on a website may be used for other purposes, 53% are changing the privacy settings[47] on UGC websites often or always, 18% rarely or never.[48] Only 11% of the respondents state to always read terms of conditions of a website; the majority rarely or never read them. 89% of those who read them indicate that they do not (fully) understand the privacy policies.[49]

The aim of the SMART project, which ran from 2011 until 2014, was to examine social and legal consequences of adopting automated, "smart surveillance" systems by public bodies.[50] Part of the project was an evaluation of citizens' attitudes towards smart surveillance and privacy via 42 focus group discussions with 353 participants in 14 European countries. The participants showed a high awareness of the current state of surveillance, especially as users of mobile devices and internet services.[51] Individuals, at least in part, are considered as responsible for their own personal (online) data. Surveillance in public places, unlike private places, is mostly accepted, especially if the monitoring is transparent; surveillance for safety reasons is more accepted than for commercial objectives. Dataveillance is perceived as a threat to privacy, even though most participants believe that the recent legal restrictions are sufficient. The acceptance of data sharing and collecting is dependent of the type of data (mostly unacceptable by sensitive data, anonymized data more accepted), the purpose of use (e.g. acceptable by life-saving circumstances), the conducting entity (state actors in general more trustworthy than private actors) and a given consent. The approval of surveillance technologies differs between different types: the more intrusive the technology, the bigger the aversion to it. The concept that more surveillance leads necessarily to more security was opposed by the majority.[52]

Building on the results of CONSENT and SMART, RESPECT explored the European citizens' awareness and acceptance of surveillance systems and procedures, with additional questionnaires and interviews in 28 European countries (5,361 participants) in 2013-2014.[53] It becomes apparent that the majority have knowledge about the different types of surveillance and the reasons for it (especially detection, prosecution and reduction of crime).[54] 23% of the respondents feel secure due to surveillance whereas 37% feel insecure; they perceive a lack of control over their personal information and mistrust government agencies and, to a greater extent, private companies.[55] Surveillance by government agencies is more accepted (just 6%: "not acceptable under any circumstances") than by private companies (16%: "not acceptable under any circumstances"); the approval decreases even more if the surveillance happens without knowledge of the affected people.[56] Moreover, the acceptance is dependent on the location: both CCTV and geolocation surveillance are least accepted in the workplace, most accepted in clinics and hospitals.[57] The risk that information gathered via surveillance could be intentionally misused (6.0 on a scale of 1 - 7) and that that they could be misinterpreted (6.0) are perceived as the highest ones, followed by violation of a person's privacy (5.9) and violation of the citizens' right to control

[45] Ibid., p. 19.
[46] Ibid., p. 20-23.
[47] Change to stricter settings: 79.7%, to less strict settings: 3% (ibid., p. 31).
[48] Ibid., p. 23f, 30f.
[49] Ibid., p. 32f.
[50] 'SMART: Report summary'.
[51] Ibid., p. 8f.
[52] Ibid., p. 9.
[53] 'RESPECT: Periodic report summary 1'.
[54] Ibid., p. 13f.
[55] Ibid., p. 17f, 25.
[56] Ibid., p. 18, 26f.
[57] Ibid., p. 28.

whether information about them is used (5.7).[58] While the majority believe that surveillance takes place often or all the time (depending on the type of technology), only the minority feel well informed and confident about the effectiveness of laws and regulations and just a few respondents changed their behaviour due to surveillance.[59] Social benefits (protection both for the individual citizen and the community) and social costs (limitation of rights, violation of privacy and control over personal data, misuse and misinterpretation, discrimination and stigma) of surveillance are both perceived without balancing them against each other.[60]

2.1.4 SurPRISE – PRISMS – PACT

The EU projects SurPRISE, PRISMS and PACT also belong to the FP7 programme and ran between 2012 and 2015. They aimed to examine the relationship between security and privacy, especially the idea of a "trade-off" between these values.[61] Not only were they all acknowledged in the above-mentioned research of RESPECT, but they also organised a joint final conference about "Citizens' perspectives on surveillance, security and privacy".[62]

Looking at the adoption of security technologies in surveillance and how they are viewed by citizens, the SurPRISE project investigated European attitudes towards the employment of surveillance-oriented security technologies (SOSTs): smart CCTV, deep packet inspection (DPI) and smart phone location tracking (SLT).[63] In 2014, it found that citizens would prefer if SOSTs were evaluated before implementation, paying particular attention to the purpose, appropriateness, cost, and impact of SOSTs.[64] Participants would also prefer verification of what data and information is being collected by SOSTs, be aware of who is responsible of such data and for what purpose the data is being collected.[65] Participants comment on the intrusiveness and usefulness of each SOST: all three SOSTs are considered useful but highly intrusive, with DPI receiving the highest perceived level of intrusiveness (66% of participants).[66] In relation to effectiveness and future use and potential abuse of DPI, 43% of citizens state that DPI is an effective security tool despite 66% feeling uncomfortable with the use of DPI.[67] 84% are worried about the extension and future use of DPI and 70% of participants share the opinion that SOSTs are likely to be abused.[68] 70% are concerned about extensive information collections, 63% fear that information held about them might be inaccurate, near to 80% fear that their personal information might be used against them and 91% are concerned that their information is shared without their permission.[69] 50% of participants disagree with the statement "if you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" with only 34% agreeing with this statement.[70] What is interesting is that 52% of the "nothing to hide" supporters are at the same time concerned that too much information is collected about them, which is contradictory.[71] Some participants also feel that SOSTs are forced upon them.[72]

[58] Ibid., p. 30f.
[59] Ibid., p. 23f, 31.
[60] Ibid., p. 32.
[61] 'SurPRISE: Report summary'. 'PRISMS: Report summary'. 'PACT: Final report summary'.
[62] 'SurPRISE, PRISMS and PACT: Abstract booklet'.
[63] 'SurPRISE D-6.10: Synthesis report', p. i, ii.
[64] Ibid., p. iii.
[65] Ibid., p. iii, iv.
[66] Ibid., p. 27.
[67] Ibid., p. 28.
[68] Ibid., p. 31.
[69] Ibid., p. 33.
[70] Ibid., p. 34.
[71] Ibid., p. 39.
[72] Ibid., p. 51.

In 2014, the PRISMS project explored EU citizens' perceptions of privacy and security issues, gathering data from focus groups and 27,000 respondents (1,000 per EU27 member state).[73] 32% of participants are worried about someone hacking into their computer, 62% of participants feel that it is important that they have the freedom to use the internet anonymously, and 81% state that it is important that they know who has information about them.[74] 80% of participants state that internet service providers (ISPs) selling customer information should not occur and 75% of respondents believe that this practice threatens people's rights and freedoms.[75] Again, citizens distinguish between security technologies and practices operated by public and private sector institutions: citizens have more trust that public authorities will respect citizens' right to privacy and data protection and, similarly to previous studies, citizens oppose covert surveillance practices and secondary use of data, especially for commercial purposes.[76] This study also affirms that citizens seem to present a high level of resistance to private sector actors who collect and process personal data and, while a concern for security decreases resistance, a high level of trust in institutions also decreases resistance.[77]

In 2013, the PACT project examined the European citizens' perception of the relation between privacy, fundamental rights, and security by surveying 27,000 EU citizens (1,000 per EU27 member state) on their attitudes towards scenarios regarding travel, internet service provider, and health.[78] It becomes apparent that the attitudes towards the collection and storage of personal data as well as the access to data are dependent on the specific context. The collection and storage of personal data is rather accepted in the context of traveling (presence of CCTV) and health (storage on devices or systems), but not on internet usage (especially in the long run).[79] The respondents are averse to access to CCTV and internet usage data by the police (especially outside the home country); an EU-wide access to health data is accepted, but for medical personnel only.[80] Moreover, the study shows a correlation between general attitudes towards privacy, surveillance and trust and their chosen preferences, which rejects the trade-off model of security and privacy. For example, a traveling person who is concerned about misuse of data shows weaker preferences towards CCTV cameras than somebody with concerns about misuse of security measures for sexual or racial harassment.[81]

2.2 Discussion and conclusion

The research in empirical studies regarding attitudes and opinions towards cybersecurity seems to show that EU citizens perceive an increasing threat of cybercrime.

There is a number of stated risks (e.g. identity theft, online fraud), but the biggest one by far is privacy violation and loss of data control, especially the misuse of private data. The perception of surveillance depends on different factors: the entity and context of surveillance, the sort of data and the level of transparency about the surveillance methods. Transparent collection of non-intrusive data for security reasons by public authorities meets with the highest acceptance, while non-transparent collection of sensitive data by commercial institutions receives the lowest acceptance. The given consent of the affected citizens is perceived as crucial. There is an awareness about both the social benefits and the social costs of data collection and surveillance. The trade-off model between security and privacy is rejected to a large extent.

[73] 'PRISMS D-10.1: Report on statistical analysis of survey', p. 5.
[74] Ibid., p. 27, 30.
[75] Ibid., p. 35.
[76] Ibid., p. 36.
[77] Ibid., p. 81.
[78] 'PACT: Final report summary'.
[79] 'PACT D-4.2: Survey report', p. 33-36.
[80] Ibid., p. 8.
[81] Ibid., p. 39f, 67.

For most of the respondents, the importance of cybersecurity measures is constantly increasing. The vast majority wants to be informed about cybersecurity risks, but only a smaller part feels sufficiently informed. The trust in authorities which ensure cybersecurity shows a broad range: while trust in public authorities and medical institutions is moderately high, trust in private authorities and commercial institutions is low. In general, trust in sufficient legal restrictions regarding cybersecurity and data protection is very high.

The responsibility for cybersecurity is not just attributed to institutions, but also to the individuals themselves. However, the changes in online behaviour and processing of personal data are not carried through: some security measures, e.g. changing of private settings, are more popular than others, like reading terms of conditions before accepting them.

It appears that the average knowledge about the concrete possibilities and functionalities of cybersecurity measures is deficient. Therefore, more information about cybersecurity risks and concrete measures should be provided for the broad population.

3. Citizens on cybersecurity in health*

The following section provides an overview on empirical research related to attitudes and opinions of EU citizens regarding cybersecurity in health. This includes two main parts: the first step consists of a research on projects and surveys provided by the EU, the second step is an additional research into academic literature. As it became apparent that there are hardly any existing empirical results directly related to attitudes and opinions of EU citizens regarding cybersecurity and the domain of health, it is necessary to take into account partial results of existing surveys which are linked to a greater or a lesser extent to the topic of interest.

3.1. Results from EU Projects and Surveys[82]

It should be noted that the stated EU projects and surveys refer to each other. Therefore, the projects will be presented both clustered and in chronological order.

3.1.1 Eurobarometer

An important survey regarding attitudes towards data is to be found in 'Flash Eurobarometer 225'.[83] In 2008, EU citizens were asked, among others things, about their trust in organisations concerning data protection. They perceive that their personal data is best protected by medical authorities, e.g. medical services and doctors (82%), whereas insurance companies are less so (51%), and private companies, e.g. mail order companies, are the least trustworthy (24%).[84]

In 2010, a part of the survey for 'Special Eurobarometer 341' polled the attitudes towards biobanks. The most preferred group to protect public interest in the use of biobanks are medical professionals (39%), the second one researchers (32%), the third one public institutions (26%).[85] 67% state that researchers should ask for informed consent for every new piece of research (18% "ask for permission only once", 6% "no need to ask for permission").[86] The question "Would you be willing to provide information about yourself to a biobank?" is answered by 46% with yes and by 44% with no.[87] Respondents are mostly concerned about the collection of their personal genetic profile (34%) and personal medical records (33%), while 28 % are not concerned at all about personal information being stored in biobanks. However, 53% agree that the exchange of personal data and biological materials tissue across member states should be encouraged (while 32% opposed).[88]

Another relevant survey is 'Special Eurobarometer 359', conducted in 2011. Being asked which information they consider personal, the respondents name medical information (patient records and health information) as the second most personal (74%) after financial information (75%).[89] Appropriately, the percentage of people disclosing their medical information on the internet is very low at 5% (in comparison: name is 79%, personal photos is 51%).[90] Similarly to 'Flash Eurobarometer 225', the trust in differ-

* This section has been written by Nadine KLEINE and Karsten WEBER (Regensburg University of Applied Science).
[82] See Appendix A.1: EU projects overview, and A.4 References: EU projects.
[83] 'Flash Eurobarometer 225: Data Protection in the European Union – Citizens' Perception'.
[84] Ibid., p. 10f.
[85] 'Special Eurobarometer 341: Biotechnology', p. 144-146.
[86] Ibid., p. 142f.
[87] Ibid., p. 147f.
[88] Ibid., p. 149-152, 151f.
[89] 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union', p. 12, 15f.
[90] Ibid., p. 39f.

ent authorities is addressed: health and medical institutions are deemed the most trustworthy authorities regarding protection of personal data with 78%. In comparison: the second most trustworthy authorities are national public authorities with 70%, the least trustworthy authorities are internet companies (e.g. search engines, social networking sites) with 22%.[91] After being asked whether their specific approval should be required before any kind of personal information is collected and processed, 74% say in every case, and 8% in cases regarding sensitive information such as health information.[92] The vast majority (88%) affirm the request for whether genetic information (e.g. DNA data) should have the same protection as sensitive data.[93]

3.1.2 CONSENT – SMART – RESPECT

According to the CONSENT study from 2011, any disclosure of personal information is considered as risky: sharing of data without knowledge or consent is perceived as riskier (73 - 81%) than personal risks, e.g. fraud or discrimination (23 - 32%). Regarding which types of information they already disclose online, just 1% name medical information.[94]

From the SMART project (2011-2014), it appears that the collection and sharing of sensitive personal data, such as health data, is unacceptable to the majority. However, under certain (especially life-saving) circumstances, the usage of confidential information is deemed acceptable. Moreover, it becomes obvious that the level of acceptance is dependent on the type of technology. Technologies involving the physical sphere, e.g. biometrics, are perceived as especially unacceptable.[95]

The empirical data from RESPECT in 2013-2014 show that the majority feel that they have little or no control over their personal information gathered with surveillance measures, and that there is a big risk of data misuse and misinterpretation.[96] However, we must note that it was not clear in the questionnaire whether personal information included health information.

3.1.3 SurPRISE – PRISMS – PACT

Part of the SurPRISE project was the consultation of EU citizens via workshops and questionnaires, in order to find out their understanding and attitudes towards security and privacy. In 2014, when asked what the core of privacy is, participants of the workshops name sensitive data (e.g. health information, sexual orientation), which should not be intruded upon.[97]

As for the data gathered by PRISMS in 2014, they show that regarding healthcare, there is a high concern about general socio-economic phenomena such as healthcare.[98] Control over personal data (e.g. health) is in general of great importance.[99] Part of the survey was the participants' opinions about scenarios regarding specific security technologies. The first scenario about airport body scanners describes a person whose colostomy bag is detected and who has to explain it to the security staff. The situation is perceived as difficult but acceptable given the security risks; while options for more privacy are discussed, a complete stop of detection is not considered due to security risks.[100] In another scenario, a person receives a letter with doctors' recommendations for flu vaccination based on the government monitoring of internet searches and communication. Hereby, many participants are concerned about government monitoring general internet usage.[101] In a third scenario, a person voluntarily provides a

[91] Ibid., p. 138f.
[92] Ibid., p. 148.
[93] Ibid., p. 203.
[94] 'CONSENT D-7.3: Synthesised all countries report', p. 19.
[95] 'SMART: Report summary', p. 9.
[96] 'RESPECT D-11.3: Synthesised all countries report (quantitative data)', p. 4f.
[97] 'SurPRISE D-6.12: Workshop report'.
[98] 'PRISMS D-10.1: Report on statistical analysis of survey', p. 24.
[99] Ibid., p. 30f.
[100] 'PRISMS D-9.1: Findings from qualitative groups', p. 3-6.
[101] Ibid., p. 22-24.

sample of his DNA to a company for medical research, but then learns that the company has been asked to share the samples with the police for use in criminal investigations. While DNA technologies are considered useful in solving crimes, the idea of sharing such sensitive data make the participants uncomfortable. Therefore, consent for sharing data with the police appears to be crucial; the option to sell this information for profit is widely seen as unacceptable. The uncertainty of what will happen with the information in the future and how the legislation might change plays an important role.[102]

Number	Hypotheses	Findings
H3.1	Respondents prefer a device/system with enhanced health or personal identification information compared to those with only basic health status information.	Reject: Czech Republic, Lithuania Accept : all other countries
H3.2a	Respondents prefer that only doctors and nurses have access to information compared to access also by paramedics	Accept: Slovenia Reject: others
H3.2b	Respondents prefer that only doctors and nurses have access to information compared to access also by paramedics, non-medical emergency personnel or any other state or private institutions.	Accept: all countries
H3.3	Respondents do not prefer device/service that can provide wider access outside their own country (EU/worldwide).	Accept: Austria, Czech Republic, Slovakia, age >65 Reject: all other countries
H3.4	Respondents do not prefer a health-records device/service to which health insurance providers, pharmaceutical companies and researcher could have access.	Accept: all countries
H3.5	Respondents prefer device/service that is free over a device/service that charges a fee per month.	Accept: at the device level Reject: WTP for some data and access options

Figure 2: PACT health hypotheses testing[103]

One of the PACT scenarios was the choice to purchase a device or service for storing health information (see also Fig. 2). In 2013, it becomes apparent that, in relation to other technologies such as CCTV, the storage of health data is mostly accepted. The majority of the respondents would prefer a device or service that allows, in addition to basic health data (e.g. blood group, allergies, diabetic status), storage of personal identification data and data on lifelong health conditions (e.g. asthma, disabilities, cancer), but they oppose to a storage of data relating to all other health conditions and medical history.[104] The perceived trustworthiness of different authorities regarding access to health information is widely ranged, though: an additional access by paramedics is preferred, but not by fire and rescue personnel; the participants are adverse towards non-state actors (e.g. insurance providers, pharmaceutical companies).[105] With more concerns about personal information being accessed by non-medicals and private

[102] Ibid., p. 31, 33.
[103] Source: ibid., p. 65.
[104] 'PACT D-4.2: Survey report', p. 25, 30.
[105] Ibid., p. 27ff.

companies, the preference of storage of medical data becomes weaker.[106] The storage on a device should be accessible across the EU rather than merely in the respective home country – but not worldwide.[107]

3.2 Results from the Academic Literature

Further research in academic literature was performed in two scientific databases with a defined keywords list.[108] The results revealed that most papers related to cybersecurity and health in a broader context do not contain empirical research about EU citizens' attitudes and opinions (beyond the EU projects described above). They engage predominantly with (technical) details of applications, usability of their design and legal guidelines for them. Citizens' concerns were mostly handled as a given fact, but without empirical basis.

However, two topics emerged as relevant regarding cybersecurity and health, both of which deal with specific types of biological data and their electronic handling: biometrics and biobanks.

3.2.1 Biometrics

Biometric technologies for personal authentication can be in some aspects relevant for the health sphere. Two studies were found which surveyed the attitudes of EU citizens towards biometrics: the multilevel-multimethod approach of BioSec[109] in which an attitude survey across Europe took place (204 questionnaires in Finland, Germany, and Spain), and a study about regional differences in the perception of biometric authentication technologies[110] (with 177 questionnaires in the UK).

Although the use of biometric technologies is mostly accepted due to their benefits, e.g. as an authentication method, there are also concerns due to the uncertainty for what exactly (else) the technology will be used for.[111] Especially, the storage of biometrical data, which may include information about physiological condition and health, raises concerns: half of the respondents from the UK are not convinced that their biometric information is stored in a secure way.[112] The cross-European survey shows similar results: while there is no agreement regarding which storage medium is preferred for the data (a central database or a personal smart card), around 33% of the respondents cannot decide or do not want their biometrical data to be stored at all.[113]

3.2.2 Biobanks

As it already became apparent in 'Special Eurobarometer 341', the field of biobanks can be interesting for cybersecurity in health. Two pertinent studies could be found in academic research: a focus group study on biobanks in the information society[114] (18 focus group discussions in Austria, Finland, and Germany) and a multi-method approach about publics and biobanks[115] (with focus groups in the Netherlands and Austria as well as 15,650 questionnaires in EU27 member states, Croatia, Iceland, Norway, Switzerland, and Turkey). Through first degree "snowballing", three other relevant papers were detected: a study of public opinion on the use of tissue samples[116] with 100 questionnaires in the UK, a

[106] Ibid., p. 45f.
[107] Ibid., p. 26, 47.
[108] See Appendix A.2 Literature search methodology.
[109] SANCHEZ, 'BioSec: a European project'.
[110] RILEY et al., 'Culture & biometrics'.
[111] ESCHENBURG et al., 'User acceptance: the BioSec approach', p. 8f. RILEY et al., op. cit., p. 297, 300-303.
[112] Ibid., p. 301.
[113] ESCHENBURG et al., op. cit., p. 9.
[114] SNELL et al., 'From protection of privacy to control of data streams'.
[115] GASKELL et al., 'Publics and biobanks'.
[116] GOODSON and VERNON, 'A study of public opinion on the use of tissue samples from living subjects for clinical research'.

population-based study about perceptions of potential donors in the Swedish public[117] with 2,928 questionnaires, and a paper about attitudes towards biomedical use of tissue sample collections, consent, and biobanks among Finns[118] with 1,195 questionnaires.

The willingness to participate in biobanking by giving personal data through donation of e.g. blood, tissues and body fluids (i.e. including DNA data) is relatively high.[119] The respondents state a broad acceptance of usage especially for research due to the perceived societal benefits.[120] However, the majority would prefer to be informed and asked for consent for every specific use of their data, even though they are aware of the limited possibility to do so.[121] They trust mostly in data security through public and state organisations, but not with private organisations.[122] Not only commercialisation, but also internationalisation of biobanks (especially storage of data) is perceived as risky.[123] The biggest concerns regarding biobanks are the future handling of sensitive data: the uncontrollability of future developments and therefore the possible usage of the stored data (e.g. for discrimination) is viewed very critically.[124]

3.3 Discussion and Conclusion

In the empirical studies found, it becomes apparent that the handling of health data plays an important role. Health data is considered as being an especially sensitive form of personal data. Health data includes every data that provides information about the health condition of a person. In a broader context, it can also include biometrical and genetic data.

The willingness to accept the recording, processing, and storing of health data is dependent on different factors. The transparency about the purposes of personal data and the way it is handled is perceived as crucial. The respondents in the aforementioned studies seem to agree to a certain extent on which authorities can be trusted in dealing with health data: health authorities, especially public institutions, are trustworthy – in contrast to commercial institutions (e.g. health insurance agencies, pharmaceutical companies) which generally are more expected to misuse data. The more databases and networks are connected internationally, the less they are accepted.

Control over own privacy and data is stated important; nevertheless, the majority of respondents are aware of the benefits of electronic records of health information: not just security aspects, but also gained knowledge (e.g. for medical research) is highly appreciated.

Most worries about potential risks regarding health data concern future developments about who is handling the currently stored data and for what purposes. This lack of confidence is widespread especially with regard to data that contains information about the identity of the data subject.

In the empirical research about cybersecurity in health, it becomes apparent that there are only a few studies dealing with opinions and attitudes of EU citizens. Moreover, the few results that could be found appeared to be focused mostly on attitudes towards (health) data protection and privacy. Other aspects of cybersecurity in health seem merely to play a minor or even no role at all.

---

[117] Kettis-Lindblad et al., 'Perceptions of potential donors in the Swedish public towards information and consent procedures in relation to use of human tissue samples in biobanks'.
[118] Tupasela et al., 'Attitudes towards biomedical use of tissue sample collections, consent, and biobanks among Finns'.
[119] Gaskell et al., op. cit., p. 15f. Goodson and Vernon, op. cit., p. 136. Tupasela et al., op. cit., p. 48.
[120] Kettis-Lindblad et al., op. cit., p. 154. Snell et al., op. cit., p. 299f. Tupasela et al., op. cit., p. 154.
[121] Gaskell et al., op. cit., p. 16. Goodson and Vernon, op. cit., p. 136. Kettis-Lindblad et al., op. cit., p. 151f. Snell et al., op. cit., p. 298f. Tupasela et al., op. cit., p. 48f.
[122] Gaskell et al., op. cit., p. 16f. Snell et al., op. cit., p. 298. Tupasela et al., op. cit., p. 49.
[123] Snell et al., op. cit., p. 298f, 301.
[124] Gaskell et al., op. cit., p. 17, 19. Snell et al., op. cit., p. 300f.

Considering the fact that electronic and digital approaches on health significantly gain importance, more empirical studies going beyond the topics of privacy and data protection would be necessary.

4. Citizens on cybersecurity in business*

In order to capture EU citizens' attitudes towards cybersecurity in the business domain we have used a two-pronged approach. 1) We reviewed and collated empirical data from EU sources including EU cyber security strategy, Eurobarometer and the following EU projects: PRESCIENT, PRISMS, SurPRISE, and PRISE. 2) We did a systematic review of the academic literature.[125]

Cybersecurity utilities are wide ranging so much so that they have been afforded elaborate definitions such as the following: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets."[126] We used this definition as a benchmark with the aim of capturing all relevant empirical data pertaining to EU citizens' attitudes towards cybersecurity utilities from the period 1996 to 2016.

4.1 Results from EU Reports and Projects[127]

4.1.1 Cyber Security Strategy of the EU

This document from 2013 states that in order for businesses and new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need to have trust in businesses and how they operate.[128] However, this is not the case, as a 2012 Eurobarometer survey highlights that Europeans are not confident in their ability to use the internet for banking or purchases because of security concerns.[129] Later surveys, however, indicate increasing awareness of cyber risks, and many are taking action to address these risks. However, there is still considerable variation in the proportions of respondents taking security measures, as highlighted while analysing the results of this survey at country level and by key socio-demographic groups, such as age and level of education (see Section 2.1.1).

4.1.2 Eurobarometer

Lack of trust in privately run businesses is affirmed in 'Special Barometer 359'.[130] In 2013, for example 39% of participants included in this study trust shops and department stores; 32% trust phone companies, mobile phone companies and internet service providers; and 22% trust internet companies such as search engines, social networking sites and e-mail services.[131] Surveillance and monitoring concerns via payment cards, mobile phones or on the internet were also raised, with seven in ten Europeans worried that private companies are using their personal information for a purpose other than originally intended (a process known as function creep), and without informing the citizen (e.g. for direct marketing or targeted online advertising).[132]

While 'Flash Eurobarometer 225' reiterates similar concerns, it also highlights that citizens have the greatest levels of distrust in mail order companies.[133] In 2008, 82% of internet users reason that data

* This section has been written by Gwenyth MORGAN and Bert GORDIJN (Dublin City University).
[125] See Appendix A.2 Literature search methodology.
[126] http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
[127] See Appendix A.1: EU projects overview, and A.4 References: EU projects.
[128] 'Cyber Security Strategy of the European Union', European Commission.
[129] Ibid., p. 2-3 (citing 'Special Eurobarometer 390: Cyber Security').
[130] 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union'.
[131] Ibid., p. 141.
[132] Ibid., p. 204, 146.
[133] 'Flash Eurobarometer 225: Data Protection in the European Union – Citizens' Perception', p. 8.

transmission over the web is not sufficiently secure, with a third of respondents stressing that suspicious persons should be monitored (27%-35%) and one in five (14%-21%) would like stricter safeguards.[134] 92% of Greek and Cypriot respondents who use the internet feel that their personal data is not sufficiently secure, while very few believe that it is (6%).[135] In contrast, 40% of Danish internet users feel transmitting data online is secure and respondents who express uncertainty about the efficiency of the security oriented technologies are male and from the younger age groups.[136]

4.1.3 PRISE

In relation to the potential privacy vs. autonomy conflict, the PRISE project found in 2007 that EU citizens weigh privacy higher than security, while 80% of them feel that it is unpleasant being under surveillance.[137] In relation to the threat of crime and terror, citizens are more accepting of security technology when the risk of crime is increased.[138] In respect of security technology, participants are concerned with its effectiveness and that there is potential for misuse by criminals, commercial interest and governmental institutions.[139] Identifiable information and access are again raised as concerns by EU citizens.[140] They feel that new security tools should be subjected to public scrutiny before implementation.[141]

PRISE concludes that 1) "physically intimate technologies are unacceptable, misuse of technology must be prevented and function creep is not acceptable" and 2) security technologies are more acceptable when there is proportionality between security gain and privacy loss, when security is under strict control (to prevent misuse by the people with access to data) and when privacy infringing security technologies are the last option (previous methods must be measured and found less effective prior to implementing privacy infringing technologies).[142]

4.1.4 PRESCIENT

In relation to security technologies, the PRESCIENT project found in 2012 that new technologies are not understood by the general public and access to new security technology and its uses is invisible to the average citizen – therein is where cybersecurity risks manifest.[143] It revealed that EU citizens have a variety of concerns relating to cybersecurity in business but interestingly, some EU citizens are more concerned than others. For example, data collection, data security, unauthorised or inappropriate use of data, and illegitimate disclosure of intelligence data are issues raised by citizens from Cyprus, Germany, Ireland, Italy, Slovakia. Concerns relating to the disclosure of information on the internet or to third parties regarding the public facility services are raised by Swedish and Latvian citizens. Employer-employee relationships, human resources, monitoring or surveillance of employees in the workplace and employees right to privacy and data protection in the workplace are issues raised by citizens from Belgium, Denmark, Portugal, Slovenia, Sweden, whereas the financial sector in general and the leakage of financial data are raised by Danes and Slovaks. Belgians and Slovenians are concerned with spam and viral marketing and direct marketing and Germans are also concerned with non-public sector and telecommunications. Slovaks too are concerned with the use of loyalty cards and the legitimate use of biometric data, while Danes and Slovenians also have concerns regarding the use of social networking sites.[144] We note that in the United Kingdom between 2007 and 2011 citizens' trust in online companies

[134] Ibid., p. 5, 20.
[135] Ibid., p. 17.
[136] Ibid., p. 19.
[137] 'PRISE D-5.8: Synthesis report – interview meetings on security technology and privacy', p. 20.
[138] Ibid., p. 8.
[139] Ibid., p. 7.
[140] Ibid., p. 8.
[141] Ibid., p. 7, 8.
[142] Ibid., p. 33f.
[143] 'PRESCIENT D-3: Privacy, data protection and ethical issues in new and emerging technologies', p. iv, v.
[144] Ibid., p. 102-138.

decreased by 8% and trust that organisational practices provide sufficient protection of personal information decreased by 5%.[145]

4.1.5 SurPRISE

This project looked at surveillance-oriented security technologies (SOST) including smart CCTV, smartphone location tracking and deep packet inspection (DPI).[146] DPI is the most relevant SOST as 1) it is used in cybersecurity as a packaging filter through which information is scanned for non-compliance, virus, etc.; and 2) it can be used by businesses for internet data mining (the process of collecting and using large sets of data for actions such as choosing the best customers for targeted mailings or analysing a shopping cart), eavesdropping and internet censorship.[147] According to SurPRISE data from 2014, citizens suggest SOSTs should be evaluated before implementation, clarifying their purpose, appropriateness, cost and their potential impact.[148] Participants would like verification on what data is being collected, who is responsible for such data, and for what purpose is the data being collected.[149] SOSTs are considered as useful but highly intrusive and interestingly DPI is perceived as most intrusive.[150] 43% of EU citizens who participated in this study state that DPI is an effective security tool and 66% feel uncomfortable with its use.[151] 84% are worried about the extension and future use of DPI with 70% believing that SOSTs are likely to be abused.[152] 70% are concerned about extensive information collections, 63% fear that information held about them might be inaccurate, near to 80% fear that their personal information might be used against them and 91% are concerned that their information is shared without their permission.[153] 50% of participants disagree with the statement "if you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" with only 34% agreeing with this statement.[154] 52% of the "nothing to hide" supporters are at the same time concerned that too much information is collected about them, which is contradictory.[155]

4.1.6 PRISMS

The PRISMS project found in 2014 that 62% of respondents to the survey think that it is important to be able to use the internet freely and anonymously, and 81% state that it is important that they know who has information about them.[156] It also reaffirms that – as seen in 'Special Barometer 359' – citizens distinguish between security technologies and practices operated by public and private sector institutions. Citizens have more trust that public authorities will respect their right to privacy and data protection when compared to profit-oriented companies; they oppose covert surveillance practices and the secondary use of data, especially for commercial purposes; there is a high level of resistance to private sector actors who collect and process personal data.[157]

[145] Ibid., p. 137.
[146] 'SurPRISE D-6.10: Synthesis report', p. i.
[147] https://docs.microsoft.com/en-us/sql/analysis-services/data-mining/data-mining-concepts
[148] 'SurPRISE D-6.10: Synthesis report', p. iii.
[149] Ibid., p. iii, iv.
[150] Ibid., p. 27.
[151] Ibid., p. 28.
[152] Ibid., p. 31.
[153] Ibid., p. 33.
[154] Ibid., p. 34.
[155] Ibid., p. 39.
[156] 'PRISMS D-10.1: Report on statistical analysis of survey', p. 30.
[157] Ibid., p. 36, 81.

4.2 Results from the Academic Literature

The number of empirical studies we found that directly address attitudes and opinions of citizens regarding cybersecurity in the business domain is surprisingly low. Almost 20 years ago, a small UK study conducted in 1999 focused on the general public's attitudes towards security in an e-commerce environment.[158] 58% of participants say they have not purchased online, of whom 51% say that this was due to insecure communications and 43% say it was due to untrustworthiness of the vendor. 61% are concerned with communications security and 55% worry about the use of personal information by the vendor. 52% mention concerns over vendor authentication and credibility and 33% are concerned with the vendor's vulnerable internal network.[159] Regarding different security safeguards for e-commerce, only 55% attempt this question with an awareness of the following security technologies: data encryption standard (80%); digital/electronic signature 64%; certification authority (50%), secure electronic transaction (42%) and trusted third party (33%).

Although the digital ecosystem has grown considerably since then, the attitudes did not seem to have changed considerably. A more recent study conducted in 2012 in Slovenia gives an illustrative snapshot of how Slovenian citizens view certain cyber processes in terms of safety.[160] Out of 277 participants surveyed, 104 view business data exchange (undefined in the study) as unsafe, 199 view online banking as unsafe, 190 view online shopping as unsafe, and 216 view internet data exchange as unsafe.[161]

4.3 Discussion and Conclusion

The review of EU publications and academic literature reveals that there is little empirical data that in any way significantly relates to EU citizens' attitudes towards cybersecurity in the business domain. Interestingly, EU citizens' attitudes towards cybersecurity in business depends on the type of business and whether that business can be trusted to appropriately use the personal data it collects. Using cybersecurity measures that collect and process personal information, such as DPI, perpetuates the privacy infringement concerns. EU citizens are concerned that private businesses will misuse personal information gathered via security technologies for commercial purposes without the consent of the individual, or that information will be used against them. Access, social networking sites and communications security (in particular internet and e-commerce security) are reoccurring concerns. The trust issue seems to be in congruence with three factors: the institution, be it private or public; the technology; and the person who has access to the security technology or data retrieved.

It would be interesting to study whether the high level of resistance to trusting private businesses with personal information may stem from EU citizens' limited awareness of cybersecurity technologies and their functions. In order to get a better understanding of how EU citizens view cybersecurity in business, further empirical research is required.

[158] Furnell and Karweni, 'Security implications of electronic commerce'.
[159] Ibid., p. 375.
[160] Berknik and Mesko, 'Study of the perception of cyber threats and the fear of cybercrime'.
[161] Ibid., p. 30.

5. Citizens on cybersecurity in police and national security*

In order to provide a comprehensive overview of existing empirical data regarding attitudes and opinions of (mainly) European citizens about cyber-related matters of public and national security, we have examined the synthesis papers of the EU projects PRESCIENT, PRISMS, PRISE, and SurPRISE.[162]

5.1 Attitudes towards Privacy

A consensus between European citizens exists that security and privacy are important factors. This is shown by PRISMS in 2014 where 87% of the participants agree upon that "protecting my privacy is very important or important" as well as "taking action against important security risks is very important or important". An even higher consensus is shown (92%) that "defending civil liberties and human rights is very important or important".[163] PRISMS takes this as a first indication that people do not want a trade-off between security and privacy. "This is a first indication for a shared commitment to privacy and security, against a trade-off."[164]

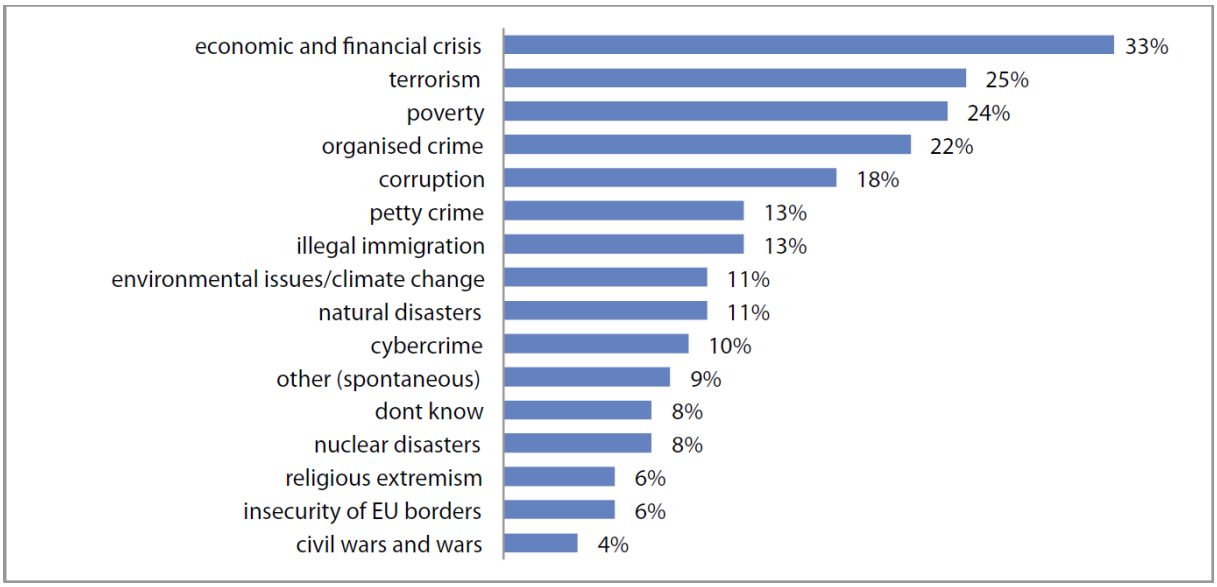

Figure 3: *Europeans' views on greatest challenges to national security in 2011*[165]

This finding, however, is in some tension to the general relevance of cybercrime and other risks directly related to cybersecurity: economic crisis, terrorism and poverty are still considerably higher ranked (see Fig. 3).

* This section has been written by Reto INVERSINI and Endre BANGERTER (Bern University of Applied Science).
[162] See Appendix A.1: EU projects overview, and A.4 References: EU projects.
[163] 'PRISMS D-10.1: Report on statistical analysis of survey', p. 16.
[164] Ibid.
[165] Source: 'SurPRISE D-6.10: Synthesis report', p. 11.

While people do not seem to like the privacy vs. security trade-off situation, it is hard to deny that this trade-off is often present when it comes to concrete measures. In 2015, SurPRISE further discussed the often-cited assumption that the gain of additional security leads to a loss of privacy. "The trade-off model is based on the assumption that the employment of security measures requires privacy intrusion in order to come to a certain level of security. This logic inherently operates as if privacy intrusions would be the only and inevitable option to effectively improve security."[166]

In order to minimize the trade-off in the case of conflicting security and privacy goals, it is important that a good knowledge of the involved technologies and their effectiveness exists.

One of the key findings of PRESCIENT in 2012 has been the fact that citizens often lack understanding of the techniques involved in security measures, especially of security measures deployed on a large scale by state actors such as biometrics. "Thus the consequences of each technology are not necessarily easily comprehensible, or even directly relatable to that technology."[167]

We must therefore conclude that it is not sufficient to define values: adequate and unbiased information need to be supplied, not only to the decision makers but to the citizens as well. For all technically-savvy people it is important to take this into account when implementing value-sensitive technologies. This is not only relevant for state actors but for the private sector as well. It is not sufficient for a security company to say "we adhere to the respective local laws" but it should instead relate to a common set of values for the development and operations of their technology.

The fact that the private sector is a player in this domain as well is reflected by one finding of SurPRISE in 2014, namely the reluctance of many persons against the involvement of the private sector in the domain of surveillance.[168] "Acceptable SOSTs [Surveillance-Oriented Security Technologies] are technologies operated only by public authorities for the sake of the public interest. The participation of private actors in security operations should be limited and strictly regulated."[169]

One of the most often cited attitudes towards privacy is "those who have nothing to hide have nothing to fear", a statement that falsely reduces privacy to a form of secrecy aiming at hiding things.[170]

The authors of PRISE state another interesting fact that the public expects the policy makers to foster a discussion about new technologies before they are introduced, and to state clear limits on the technologies in order to prevent a function creep. This discussion should be as broad as possible.[171] In 2007, the study found a certain ambiguity towards the role of the state and the use of PETs (Privacy Enhancing Technologies). "When it was pointed out that some technologies could prevent investigation of specific crimes such as distribution of child pornography, they gained even less acceptance."[172]

Another important factor described by PRISE was the fact that the public only accepts security measures if they are perceived as effective. This is also valid for all privacy measures. PRISE concludes and recommends a dynamic and regularly reassessed approach when it comes to security and privacy measures: "The implementation of security technologies and legal regulations must therefore be reassessed regularly and precautions for the required flexibility to permit the withdrawal of inefficient and infringing measures and technologies should be taken."[173]

---

[166] 'SurPRISE D-6.10: Synthesis report', p. 47.
[167] 'PRESCIENT D-3: Privacy, data protection and ethical issues in new and emerging technologies', p. iv.
[168] 'SurPRISE D-6.12: Workshop report', p. 29.
[169] Ibid.
[170] Ibid., p. 36.
[171] 'PRISE D-5.8: Synthesis report', p. 32.
[172] Ibid., p. 18.
[173] 'PRISE D-7.6: Concluding conference statement paper', p. 3.

5.2 Country-specific Attitudes

In 2014, SurPRISE asked survey participants how strong they agree with the "nothing to hide" statement. 50% of all participants strongly disagree or disagree with this statement. There is a certain contradiction in the case of Hungary, where only 18% strongly disagreed or disagreed with this statement but where there is a bigger amount of distrust towards its public servants. In the case of Germany, however, these two statements are aligned as Germany disagrees the most strongly with the "nothing to hide" statement (78%). On the other hand, 70% of all participants in SurPRISE share the concern that too much information is collected about a person.[174]

These findings have a strong impact on how citizens see the state as an actor in this domain and may eventually lead towards two basic areas of perception:

- Citizens see the state as a guardian that must protect them against violations of their privacy.
- Citizens see the state as an actor that endangers their privacy.

Which of these two opposites dominates in a society depends on the history and background of a country or society. In 2012, PRESCIENT examined this question based on interviews in 6 European countries (Spain, Hungary, Norway, Germany, Denmark, and Austria). The countries that had confrontations between the state and its citizens (or a part of its citizens) seem to generally have a greater mistrust towards public servants and their use of security technology. On the other hand, the two Scandinavian countries seem to have a higher trust in their institutions.

PRISE stated as well that there are significant differences between nations and their general perception of the state and their trust towards institutions and public servants.[175] In this context, PRISE documented the statement by Norwegian participants in 2007 that directly emphasizes the need for defining and adhering to values: "This is not only something to understand, this is about values."[176]

The question about the involvement of the public and the decision-making has been discussed as well in the PRISE project. There is a common understanding that a public decision is crucial for the acceptance of surveillance technology or more generally privacy-related projects. The question "Who should decide?" is more difficult to answer. Even if – according to PRISE – some countries (Germany and Denmark) would leave the decision to politicians, this should not be taken as a general statement. We believe that this is influenced by the political system (representative democracy vs. direct democracy), as e.g. Switzerland as a direct democracy had several referendums dealing with questions about security and privacy.

Various popular votes that took place in Switzerland provide very interesting and relevant insights on the citizens' attitudes. As opposed to pure surveys, popular votes have legal and societal consequences. One vote concerned the referendum on the introduction of the biometric passport.[177] When the Swiss Federal Council decided to introduce a new passport with biometric elements that are to be stored centrally, the referendum had been taken by various organizations. One of the main concerns of privacy-oriented organizations was the fact that the biometric elements were to be stored in a central database. The topic turned out to be controversial, and the supporters won with a very small margin (50.1% voted yes, 49.9% no).[178]

[174] 'SurPRISE D-6.12: Workshop report', p. 36-37.
[175] 'PRISE D-5.8: Synthesis report', p. 14.
[176] Ibid., p. 28.
[177] https://www.bk.admin.ch/themen/pore/va/20090517/index.html?lang=de
[178] https://www.admin.ch/ch/d/pore/va/20090517/det542.html

Another vote concerned the increases of the electronic surveillance capabilities (e.g., internet and email monitoring, offensive capabilities using Trojans) of Swiss security services.[179] The proposed vote won a support of 66% of the voting population. This is a strong indicator that the benefits of surveillance are perceived to outweigh the associated privacy risks. This conclusion is in line with observations made by Giles and Hartmann:

> *"Although disclosure of the alleged capability and reach of U.S. and allied surveillance mechanisms prompted strident and outraged reportage in some sections of the English-language media, public opinion has not followed suit. Instead, a more balanced and sober assessment of national security needs is leading European states to pass legislation through due democratic process to ensure that internet monitoring of specific threats to security continues unhindered. It follows that active cyber defence in the sense of active measures online in order to prevent and pre-empt threats to national security will continue to be perceived as legitimate, and these measures should be expected to continue unrestrained by the new environment of enhanced public awareness."*[180]

5.3 Attitudes towards Technologies

The SurPRISE project tried, amongst others, to measure the perception of the intrusiveness vs. the effectiveness of so-called surveillance-oriented security technology (SOST). In 2014, SurPRISE analysed the following SOSTs: smart CCTV, deep packet inspection (DPI) and smartphone location tracking (SLT). One interesting finding is that there is a relation in the perception of a technology between its effectiveness and its intrusiveness: "Despite of the differences in particular, the effectiveness and intrusiveness of the SOSTs are interrelated: those technologies perceived as highly intrusive are also perceived as less effective."[181] (see Table below).

Technology	Considered an effective national security tool (*)	Considered an appropriate way to address national security threats (*)	Feeling uncomfortable with the use of the technology
smart CCTV	64%	51%	39%
DPI	43%	about 40%	45%
SLT	55%	about 40%	66%
(*) % of participants strongly agreeing or agreeing that it is an effective technology.[182]			

This is a very interesting finding as, from a technical point of view, DPI was considered as being ineffective for national security compared to SLT and smart CCTV.

When we consider the findings of PRESCIENT and PRISE, a certain part of these findings might be related to the fact that DPI is one of the most complex technologies with a high risk of function creep. However, DPI might be one of the most interesting technologies against certain threats to national security but it is most likely one of the most privacy intruding.

If a state actor decides to do DPI, widely used cryptography is something that hinders this approach. It is interesting to note that none of the examined papers seems to focus on the role of the state when it comes to cryptography ("cryptowars", where states try to enable a decryption of communication or

[179] http://www.bbc.co.uk/news/world-europe-37465853
https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance
[180] GILES and HARTMANN, 'Socio-political effects of active cyber defence measures', p. 36.
[181] 'SurPRISE D-6.10: Synthesis report', p. 29.
[182] Ibid., p. 29, fig. 22.

data by legal measures). The weakening of cryptography would likely have much stronger security and privacy consequences than most of the other invasive technologies.

We believe that not only technologies actively used by actors might endanger some core values but as well the fact that states try to weaken techniques for their own purposes. As von Liechtenstein already pointed out in 2002, this may have a major change in the balance between states and citizens: "The potential of cryptography to reorder citizen/government power relationships is already attracting the close attention of National Governments."[183]

It is important that the public discussion does not only focus on the use of SOST but also on which PETs are available to what extent and if the state does not try to circumvent, ban or weaken such technologies for the broad public for the sake of SOSTs.

One of the most interesting research questions of SurPRISE was about the criteria that should be adopted when introducing new SOSTs. We are going to focus on the most important factors that seem to have a direct relation to potential values that should be considered by state actors. According to SurPRISE participants in 2014, "SOSTs are more acceptable if implemented in a context where information is provided to citizens on: a) where SOSTs are used, b) how SOSTs function, c) for what purpose they have been installed and d) who is in charge of managing the system."[184]

For us, this leads to one of the most important concepts in any democratic state: trust. Trust is something that can only be gained if all participants adhere to a common set of values. This is also proved by a finding of SurPRISE where the relationship between trust and trustworthiness is being shown:

Technology	Security authorities are trustworthy when using the technology (*)	Security authorities do not abuse their power (*)
smart CCTV	36%	22%
DPI	36%	14%
SLT	46%	29%
(*) % of participants strongly agreeing or agreeing that it is an effective technology.[185]		

These values could also be interpreted in a way that the trust is going to be lost quickly if abuse of a technology by a state actor comes to public.

5.4 Conclusions

We have seen that citizens of different countries or with different cultural background differ in their perception of the role of the state and of value-sensitive technologies (e.g., the application of SOSTs). Trustworthiness and transparency of a state seem to be important factors influencing this perception. As SurPRISE clearly points out, it is not only about how safe a technology is, but also how safe is the context in which the technology is used. If citizens see the state more as a guardian of their privacy and security and less as an intruder, they are more likely to accept security measures; this perception is closely related to how much citizens trust their state representatives based on their experience and the history of their society.

[183] VON LIECHTENSTEIN, *Internet und Öffentlichkeit*, p. 182.
[184] 'SurPRISE presentation: Aligning security and privacy. En route towards acceptable surveillance', p. 24.
[185] 'SurPRISE D-6.10: Synthesis report', p. 43, fig. 35.

As Swiss experts in the field, we suggest that, for many technologies, there is an inherent security vs. privacy trade-off, in some cases more pronounced than in others. For instance, in the case of the weakening of cryptography, this trade-off manifests itself strongly. We believe that it is not acceptable to put the privacy of a whole society in danger for the sake of a simpler prosecution of criminals; yet it is undisputed that criminals participating in serious crimes have a limited right to privacy.

There are also security measures where the trade-off is less accentuated, but nevertheless subtle. For instance, consider the collection and analysis of metadata for the discovery of malware flows. On the one hand, the metadata collection has adverse effects on privacy. On the other hand, the detection of infected devices helps restoring the privacy of affected users. We believe that if in this example metadata collection would be forbidden out of, loosely speaking, "naïve privacy concerns", the net effect on privacy would be negative: the damage to privacy caused by undetected malware would be greater than the (forbidden) privacy invasion due to cybersecurity software.

In summary, we believe that it is crucial to gain and maintain a *holistic*, value-based view on all topics and to avoid isolated views on singular problem blocks. A pronounced "privacy first" or "security first" attitude is unlikely to produce beneficial solutions for society. Finding good solutions and trade-offs is a laborious and ongoing process, which requires to assess a multitude of technologies and application scenarios with respect to their effect on the core values of a society.

6. State actors' cybersecurity strategies*

Cybersecurity is an issue acknowledged widely across Europe and globally. The increasing digitalization permeates the everyday lives of citizens as well as the overall environment in which industry and governments operate. Notably, the NATO countries published in July 2016 a 'Cyber Defence Pledge', which recognizes security threats and reaffirms the support and enhancement of the cyber defences of their national infrastructures and networks.[186]

This section gives an overview on the correlating cybersecurity opinions and presents various state actors strategies to address cybersecurity. State actors are understood here as official governmental institutions at EU and EU member state levels. Furthermore, solution approaches for cybersecurity issues are examined, which not only address the security perspective, but also integrate the data protection perspective. As for the research methodology, only little insight could be drawn from literature and studies. Therefore, our sources consist mostly of legislation, policy documents, official statements and other information directly coming from the above-mentioned state actors.

6.1 Cybersecurity Strategies at the EU Level

Cybersecurity threats are a global issue, a fact that was recognized by the EU and its individual institutions relatively early. Furthermore, it was recognized that this issue can only be dealt with global responses, necessitating international communication, harmonized legislation and effort coming from both the public and private sectors. Nonetheless, cybersecurity matters have a quite complex nature, making a unified approach sometimes difficult. Working towards resolving this difficulty, the European Commission issued a communication addressing Europe's transition to an information society already in 2001. This communication referenced a number of already existing approaches and proposed some further action items in order to protect information and communication infrastructures. It called for a comprehensive policy initiative, a unified definition of cybercrime, more in-depth communication with different stakeholders, and more R&D funding to address such threats. For these goals, the Commission pledged to establish an EU Forum to involve law enforcement agencies, internet service providers, telecommunications operators, civil liberties organizations, consumer representatives, data protection authorities, and other interested parties.[187] The Article 29 Working Party[188] issued an opinion on this communication, welcoming the Commission's stance on this topic, yet asking how individuals' basic rights and fundamental freedoms will be taken into account when adopting measures to combat computer-related crime so that all legitimate interests can be accommodated in the best way possible.[189]

With the drafting of its 'Cyber Security Strategy' in 2013, the EU further detailed its position regarding cooperation and communication related to cybersecurity matters. Thereby, the Commission committed itself to launching a public-private platform on network and information security (NIS) solutions, in order

* This section has been written by Eva SCHLEHAHN (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein).

[186] 'Cyber Defence Pledge', NATO. This pledge entails a general commitment of NATO to allocate adequate resources nationally, foster interaction of stakeholders and improve awareness and understanding of cybersecurity threats overall, including in education and training of NATO and Alliance forces. It is meant to reinforce collaboration and better exchange of best practices across the Alliance, including with the EU.

[187] 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', European Commission, p. 29ff.

[188] The Article 29 Working Party was set up on account of Article 29 EU Data Protection Directive 95/46/EC, which demands the formation of a working group on the protection of individuals with regard to the processing of personal data. It functions as an independent advisory group counselling the European Commission with respect to data protection and privacy issues.

[189] 'Opinion 9/2001', Article 29 Working Party, p. 2f.

to develop incentives for the adoption of secure ICT solutions and for the increase of cybersecurity performance of ICT products used in Europe. This strategy entails further action points to achieve technical guidelines, recommendations, industry standards and general information exchange to enhance cybersecurity, also involving ENISA as well as public and private stakeholders.[190]

More concrete legislative actions followed, such as Directive 2008/114/EC on the identification of European critical infrastructures, or the directive on the security of network and information systems ('NIS Directive'). While the former is aimed at critical information infrastructure protection (CIIP), the latter foresees rules, preconditions, and measures meant to ensure a high common level of NIS across the Union.[191] Furthermore, the European Commission encouraged the EU member states to make the most of the NIS coordination mechanisms enabled by this legislative act.[192] The European Data Protection Supervisor (EDPS) Peter Hustinx commented both the new 'Cyber Security Strategy' and the 'NIS Directive' in an opinion highlighting that a high level of internet security will improve the security of personal information as well.[193] Nonetheless, the EDPS pointed out that there is a threat of cybersecurity measures interfering with individuals' rights to privacy and the protection of their personal data. He called for ensuring that every cybersecurity measure deployed complies with article 52(1) of the 'Charter of Fundamental Rights of the European Union'. Thus, all relevant fundamental rights should be taken into account in the EU's 'Cyber Security Strategy', which includes all its implementing actions.[194] In 2015, the following EDPS in office, Giovanni Buttarelli, further emphasized this demand in a follow-up opinion on the topic of national security in 2015.[195] By that time, the EU has also acknowledged that the protection of individuals' personal information needs to be improved. This is a major reason why the EU triggered its reform process for its data protection framework, while a new regulation on privacy and electronic communications is still underway.[196]

Beyond the 'Cyber Security Strategy' and the 'NIS Directive', the Commission launched a new public-private partnership on cybersecurity with industry to better equip Europe against cyber-attacks and to strengthen the competitiveness of its cybersecurity sector. This action was triggered by various motivations, such as economic considerations (see e.g. the Commission's 'Digital Single Market Strategy'[197]) or the recognition of cybersecurity threats as becoming increasingly significant in the everyday lives of EU citizens. Such recognition may have been expedited by surveys showing this development quite clearly. For instance, the 'Global State of Information Security® Survey', executed by PwC, found that more than 80% of European companies have experienced at least one cybersecurity incident over the last year and that the number of security incidents across all industries worldwide rose by 38% in 2015.[198] The key findings in this survey strongly demand for actions based on this situation, such as:

- Adopting new safeguards for digital business models
- Implementing business-critical threat intelligence and information-sharing programs

---

[190] 'Cyber Security Strategy of the European Union', European Commission, p. 13.
[191] 'Directive (EU) 2016/1148'.
[192] 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', European Commission.
[193] 'Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a "Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace", and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union', European Data Protection Supervisor.
[194] Ibid., p. 4.
[195] 'Opinion 8/2015 on Dissemination and use of intrusive surveillance technologies', European Data Protection Supervisor, p. 3.
[196] The Regulation on Privacy and Electronic Communications (ePrivacy Regulation) is currently in the legislative process. The draft proposal has been made by the European Commission on 10 January 2017. For more information, see: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.
[197] For an overview, see: http://ec.europa.eu/priorities/digital-single-market_en.
[198] 'Global State of Information Security® Survey 2017', PricewaterhouseCoopers.

- Securing the potential of the internet of things (IoT)
- Taking a proactive approach to managing geopolitical threats.

Based on its evaluation outcome, ENISA, founded in 2004, will probably achieve a further mandate to play a crucial role in realizing such actions, mainly by providing information and guidance, e.g. on cyber crisis management.[199] Alongside the European Commission and ENISA, the Cybercrime Convention Committee (T-CY) of the Council of Europe[200] represents the state parties to the Budapest Convention on Cybercrime. The consultation of the T-CY aims at facilitating the effective use and implementation of the Convention, the exchange of information and the consideration of any future amendments. The T-CY has published a number of different assessments and reports on cybercrime.[201] All these institutions at the European level aim at achieving comprehensive and harmonized governance of cybersecurity-related issues, where efforts are undertaken in various areas, such as policy/legislation, finances, and operational measures. Yet, those institutions still struggle with divisive factors on national, pan-European, and extra-European/transatlantic level, mostly caused by diverging willingness of the EU member states to commit resources, lack of clarity regarding the understanding of cybersecurity and cybercrime, and partially significant disparities in governance strategies and focus.

6.2 Cybersecurity Strategies at the National Level

At national level, the EU member states have developed their own cybersecurity strategies, whose goals correlate with those of the EU strategy, with varying detail and focus on specific aspects. For example, Luxembourg's cybersecurity strategy foresees a number of important objectives for the country, plus an additional action plan naming in detail the responsible authorities, as well as the anticipated time frame for realisation. These objectives include strengthening national cooperation (also with the academic and research sphere), increasing the resilience of digital infrastructures, the determination of measures to fight cybercrime, the implementation of norms, standards certificates, labels and frames of references for government and critical infrastructure requirements. Furthermore, this strategy recommends and calls for the information, training, and awareness of cyber risks.[202]

As another example of a larger country, France's cybersecurity strategy focuses on specific details in some areas, such as increasing the security of state information systems (including the development of cybersecurity requirements for public contracting and support), providing local assistance to victims of cyber-malevolent acts, measuring cybercrime, and protecting the digital lives, privacy, and personal data of French citizens. Moreover, France's approach to eliminate and mitigate cybersecurity threats includes operational mechanisms for international administrative assistance and educational measures, the support of security services and products, and knowledge transfer including the education of the general public. However, for the individual objectives mentioned, the French strategy does not provide action items as detailed as the Luxembourg one.[203]

As already mentioned, it proves difficult that many countries still have different understandings of the meaning and scope of both cybersecurity and cybercrime, if they have such a tangible understanding at all. For instance, Spain has a rather strong focus on the country's capability to investigate and prosecute cyber terrorism and cybercrime, yet its cybersecurity strategy does not specify which kind of acts are

[199] See e.g. their overview of recommended publications on that matter: https://www.enisa.europa.eu/topics/cyber-crisis-management?tab=publications.
[200] The Council of Europe (CoE) is not an official EU body, but a human rights organisation that was established in 1949 after World War II. It now comprises of 47 member states, 28 of which belong to the European Union. http://www.coe.int/en/web/about-us/who-we-are
[201] https://www.coe.int/en/web/cybercrime/tcy
[202] 'National Cybersecurity Strategy II', Gouvernement du Grand-Duché de Luxembourg, p. 23ff.
[203] 'French National Digital Security Strategy', 2015, République française, p. 15, 21ff, 26f, 31ff.

considered a cybercrime.[204] As for Croatia's cybersecurity strategy, it provides a definition of cybercrime, yet this definition is rather broad and vague.[205] Thus, there are large differences in the level of detail and commitment made in those national cybersecurity strategies, which will probably take some time and additional pan-European communication as well as harmonization effort for remedy.

Most EU member states have established institutions dedicated to cybersecurity issues such as, for example, the German BSI (Federal Office for Information Security). This institution is tasked with investigating current IT security risks and creates yearly situation reports of the IT security landscape in Germany. It also functions as a cyber defence centre and reporting office for security incidents. Together with another institution, the BBK (Federal Office of Civil Protection and Disaster Assistance), the BSI provides an internet platform for the protection of critical infrastructures.[206] The German operators of critical infrastructures in the sectors of energy, information technology and telecommunications, water and nutrition, are required to report security incidents to the BSI and to demonstrate legal compliance every two years, by providing a detailed protection concept corresponding with the state of the art.[207] Other operators (not active in the aforementioned sectors) can make such reports on a voluntary basis.

Beside institutions like the BSI, many EU countries have expert groups focusing on security incidents, which are organised in computer emergency response teams (CERTs), sometimes also called computer emergency readiness teams or computer security incident response teams (CSIRTs). They are cross-linked globally and across the EU, offering warnings and problem resolution on security issues, especially involving product security teams from the government, commercial, and academic sectors.[208]

National data protection authorities (DPAs) are concerned with cybersecurity issues, too. Article 17 of the current Data Protection Directive 95/46/EC states that "the controller must implement […] measures to […] ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected". This level of security must be reached through the implementation of necessary and suitable technical and organisational measures to protect the personal information of individuals, which will also enhance cybersecurity in general. National data protection laws implement the minimum requirements of this directive in each member state. Moreover, some EU countries felt the need to exceed the requirements of this directive to ensure an adequate protection of their IT landscape. An example of this could be the French Digital Republic Act (Law n°2016-1321 of 7 October 2016). This Act introduces several key amendments beyond the French Data Protection Act of 1978 and other laws, allowing for even stricter rules to protect citizens, e.g. through specific obligations for online platform providers.

With the reform of the European data protection framework, the focus on the security of information technology systems will even deepen. For the private sector, the applicable legal framework is the General Data Protection Regulation[209] (GDPR), coming into force in May 2018. The GDPR requires the implementation of technical and organisational measures necessary and suitable to protect the personal information of individuals. This includes appropriate security measures[210] and the ability to demonstrate compliance with the legal framework.[211] Furthermore, under certain circumstances the responsible controller has to conduct a data protection impact assessment (DPIA, see below).

---

[204] Cf. 'National Cyber Security Strategy', 2013, Gobierno de España, p. 11, 29.
[205] Cf. 'The National Cyber Security Strategy of the Republic of Croatia', p. 16.
[206] See the information website of the BSI:
https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html.
[207] Article 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz or BSIG).
[208] See the information website of the global CERT association platform FIRST (Forum of Incident Response and Security Teams): https://www.first.org/about.
[209] 'Regulation (EU) 2016/679'.
[210] Cf. articles 4 (5), 5 (e) + (f) GDPR.
[211] See e.g. articles 24 (1), 25 (1) + (2), 28 (1) + (3) (e), 30 (1) (g) + (2) (d), 32 (1) GDPR.

Against this background, the national DPAs publish their own statements and opinions on cybersecurity issues to bring in their perspective. In 2015, the French CNIL[212] published an analysis of personal data protection in the context of cybersecurity. It found that privacy is a crucial aspect in the digital era and that a more holistic approach to both cybersecurity and privacy is sorely needed, while baseline security rules are not yet sufficiently established.[213] In 2013, the Italian DPA[214] published guidelines for businesses including recommendations on how to protect their data and the data of their customers and employees.[215] The Information Commissioner of the United Kingdom (ICO UK) also focuses on information security, informing on his website about the relevant technical and organisational measures required by the national and EU data protection frameworks.[216] Moreover, the ICO UK regularly publishes current data security incident trends, covering various issues relating to information security in the cyber domain.[217]

6.3 Solution Approaches

In the sequel, we consider solution approaches proposed and acted upon by state actors at EU and national levels. These solution approaches very often define and/or explain specific working strategies and priorities of state actors. Thereby, they usually make the transfer from theoretical knowledge and statements of state actors to concrete operational or policy-framed legislative actions. We especially focus here on the privacy and data protection perspective, since this domain is increasingly seen as very important to complement the classic security perspective.

With the rise of the digital era and the continuous development of technology, some high-level observations can be made. For instance, the increase of interconnectedness also means an increase of involved actors and recipients of data, i.e. ever greater networks of entities. More data also leads to more possibilities of analysis with big data tools, thus scaling up risks of re-identification of individuals, profiling and disrupted power balances. Furthermore, there is a growing recognition that cybersecurity risks do not only come from the outside, but malicious insiders may cause significant damage as well.[218] In addition, companies as well as governments may be inclined to accept greater risks due to economic or political motivations. Such a stance can lead to the exposure of whole infrastructures to cybersecurity threats. Precisely for these reasons, it is important first not to underestimate cybersecurity risks, then to undertake the necessary measures, and finally to establish the auditability of compliance.

Many institutions within the EU, at both national and European levels, recommend taking initial steps for IT systems and networks with the definition of processes, the close monitoring of their execution, supplemented by preventive and reactive measures compliant with the state of the art.[219] This includes the consideration of information security best practices and standards, such as ISO, COBIT, or ITIL. From a data protection perspective, the above-mentioned technical and organisational measures often correlate and their implementation should be much more prevalent in many areas and sectors. Equally

[212] Commission Nationale de l'Informatique et des Libertés (National Commission on Informatics and Liberties).
[213] Cf. the CNIL's '36th Activity Report 2015', p. 14ff.
[214] Garante per la Protezione dei Dati Personali (Guarantor for the Protection of Personal Data).
[215] 'Privacy: working with business – Ten corporate best practices to improve your business'.
[216] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
[217] Such as cryptographic flaws (e.g. failure to use HTTPS), exfiltration of data, key-logging software, phishing, cyber security misconfiguration (e.g. inadvertent publishing of data on website), loss/theft of an only copy of encrypted data or the loss/theft of an unencrypted device, diverse DDoS and others. These examples come from the July-September 2016 period: https://ico.org.uk/action-weve-taken/data-security-incident-trends/.
[218] Cf. the assessment with study references in 'ENISA Threat Landscape Report 2016', p. 46ff.
[219] This is also reflected in the private sector, reacting to the governmental encouragement. See e.g. the recommendations of the industry-driven European Cyber Security Organisation (ECSO) in its 'European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private-Partnership (cPPP)', p. 26ff.

essential are *data protection by design* and *by default* efforts, including a DPIA before any IT system deployment.[220] For the DPIA, many national DPAs in the EU have developed different approaches.[221] Yet, some of these approaches have shortcomings with regard to the protection of the fundamental rights of individuals by reducing the assessment to a mere risk-based approach. However, this viewpoint does not sufficiently represent both data protection issues and cybersecurity matters.

In Germany, all national data protection supervisory authorities have acknowledged a unified approach named Standard Data Protection Model, which has a strong fundamental rights underpinning.[222] It is based on protection goals which can be derived directly from the applicable data protection framework. This protection goal based approach provides a more tangible concept to identify and implement measures needed to protect information related to individuals, while those measures are also useful to enhance cybersecurity. According to article 35(7) GDPR, the DPIA is required to provide at least:

> *"(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
>
> *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
>
> *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
>
> *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."*

Such an assessment requires the responsible entity to take into account the whole processing lifecycle, including all data, formats, IT systems, processes and functions.

	Data security	Data protection
Focus	Serves the interest of the data processing entity	Serves the interest of the concerned person (data subject)
Function	Protects against the loss of confidentiality, integrity and availability	Protects against technical determinism, intransparency and unjustified linkage of data/ processes/events related to an individual
Measures	IT security measures also realise data protection	Data protection measures also realise data security
Scope of application	Related to automated data processing	Related to all types of data processing

Figure 4: *A comparison of data security and data protection*

In the IT security domain, the processing lifecycle is usually looked at from a risks assessment standpoint, while some classic protection goals are taken into account as well (see also Fig. 4). This approach is called the classic CIA triad (for the protection goals *confidentiality*, *integrity*, and *availability*) and is commonly used by IT security experts to conduct assessments. However, these protection goals do not cover all data protection requirements, since the classic IT security perspective is driven by the desire of the controller to protect business data and assets. Data protection, however, goes further than that, due to

[220] As already demanded at the EU level by the EDPS in its action plan in 'The EDPS Strategy 2015-2019', p. 17ff.
[221] See e.g. the ICO UK or the French CNIL (methodology handbook):
https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/
https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual.
[222] 'The Standard Data Protection Model', German Data Protection Authorities.

its fundamental rights status, primarily considering the perspective of the individual (the data subject). Therefore, the classic IT security approach needs to be extended to a more holistic viewpoint, striving for tangible operational measures that protect not only business models, but also the fundamental rights of individuals in relation to privacy and data protection.

To close this gap and help with the translation of complex legal requirements into functional requirements, an extension of the original methodology has been made in the above-mentioned Standard Data Protection Model.[223] Originally developed in Germany[224], it provides a methodology which is directly based on the GDPR and is thus useable all across the EU. Briefly summarized (see also Fig. 5), three additional data protection goals supplement the IT security focused ones, namely: *unlinkability* (data minimisation), *intervenability*, and *transparency*.

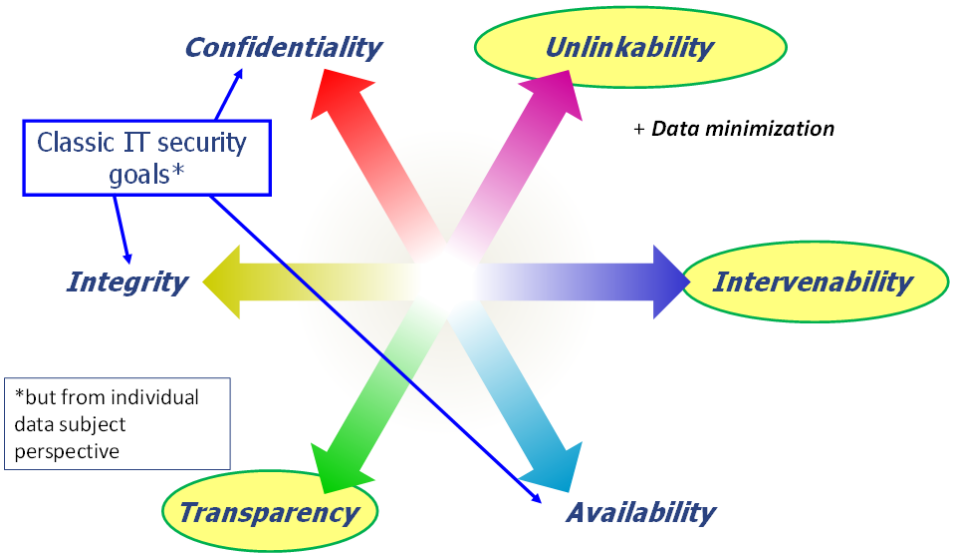

Figure 5: The six data protection goals of the SDM

These additional, privacy-focused goals can be used together with the classic IT security goals to assess and evaluate data protection and data security objectives and risks. Therein, they can be mapped exactly to the (often rather vague and broad) legal requirements of the European data protection framework. This approach is strongly aimed at determining the needed operational measures to resolve data protection issues, but which have the potential to enhance cybersecurity as well. Therefore, it may be a candidate methodology to receive more widespread recognition internationally, besides the efforts of the above-mentioned IT security and cybersecurity focused institutions to raise the prevalence of already known security standards.

[223] For the direct linkage of the individual protection goals to the requirements of the GDPR, see ibid., p. 23ff.
[224] HANSEN, JENSEN and ROST, 'Protection goals for privacy engineering'.

7. Conclusion*

As a general conclusion, we will summarise our main findings and suggest consequent actions. Let us first remember that people's attitudes and opinions are by definition *subjective*. Perceived risks may not fully match real threats. Likewise, known security measures may not be the only ones in use, nor necessarily the most adequate. Moreover, these results might be influenced by the intrinsic bias towards *privacy* of some of the surveys, especially those focussing on ways to go beyond the traditional trade-off between security and privacy.

For citizens, the biggest risk associated to cybersecurity generally seems to be privacy violation and the loss of data control. People seems to trust more public authorities than private entities with their personal data. They also perceive the increasing threat of cybercrime. They feel insufficiently informed about cybersecurity risks, which highlights the need to improve *awareness*: more information about current risks and concrete (counter)measures should be provided to a broader public.

In the health sphere, citizens are especially sensitive to the handling of their health data. Consent and trust for the recording, processing, and storing of such data depend on the context. In the business sphere, citizens are also concerned with privacy infringements. There is a lack of trust in private businesses regarding the use of personal data, as well as a concern with internet and e-commerce security.

In the police and national security sphere, there is diversity in the perception of the role of the state and of value-sensitive technologies such as DPI. Citizens find national security measures more acceptable if they view the state as a guardian rather than an intruder, which depends on their experience and their country's history. Security technologies and their application scenarios should be carefully assessed before seeking public acceptance. However, we should not have to choose between (cyber) security and privacy, or any other value. We ought to keep a *holistic view* on all value-related topics.[225]

Overall, most found data on citizens' perspectives relates to general issues of security and privacy. The *cyber* component of security is often not emphasized in the studies. *Further research* is therefore needed to cover other values, but also to investigate specific issues such as cybersecurity and health, or cybersecurity in business. Besides, longitudinal surveys could study the influence of news stories on public opinion. For instance, what are acceptance levels of personal data collection before, during, and after privacy scandals (e.g. Snowden's revelations)?[226]

As for state actors, their attitudes and opinions are known to us mainly through policy documents. There already are EU institutions aiming to achieve comprehensive and harmonized governance of cybersecurity-related matters. But divisive factors still remain across member states, namely lack of clarity in understanding of cybersecurity and cybercrime, disparities in governance strategies and focus, as well as diverging willingness to commit resources.

Does an attitude towards privacy leads to an attitude towards cybersecurity? The protection of personal information can also improve cybersecurity. For example, using a VPN when connected to a public hotspot (in an airport, in a hotel or in a shopping centre) prevents the communication to be eavesdropped by other users at this hotspot. In particular, personal identifying information is not visible anymore. Therefore, using a VPN can be seen as an attitude towards privacy. A VPN also prevents the interception and the stealing of the passwords at the hotspot. From this point of view, it is also an attitude towards cybersecurity. Thus, privacy and some aspects of (cyber)security can be mutually reinforcing. However, a VPN can also be used to lure content providers about the actual geolocation of a user. This is a way to circumvent location dependant DRM and intellectual properties. Such a use of a VPN is an

* This conclusion has been written by Florent WENGER and David-Olivier JAQUET-CHIFFELLE (University of Lausanne).

[225] Cf. PAVONE et al., 'A systemic approach to security: beyond the tradeoff between security and liberty'.

[226] 'PACT D-4.2: Survey report', p. 2. 'PRISMS D-10.1: Report on statistical analysis of survey', p. 84.

attitude against some particular cybersecurity measures. This example illustrates how an attitude can protect privacy and at the same time be an attitude both *towards* and *against* cybersecurity: the use of a VPN prevents some personal identifying information leakage and protects certain cybersecurity assets while endangering some others. Cybersecurity is too vague or too broad to be considered as a monolithic entity. It needs to be contextualized in order to assess the impact of a particular attitude, measure or action. Eventually, according to the Standard Data Protection Model, three new *protection goals* should be added to the CIA triad (confidentiality, integrity, availability): unlinkability, intervenability, and transparency.

Ultimately, working towards value-driven cybersecurity goes beyond adding privacy requirements, although it is a first, significant and welcome step. Both citizens' perspectives and their direct involvement are crucial to enforce fundamental rights in the cyberspace and to contribute to a more secure, value-driven information society.

Appendix

A.1 EU Projects Overview

See also A.4 References: EU projects

Project	Description	Duration	Countries in survey
CONSENT	*Consumer sentiment regarding privacy* It sought to examine how consumer behaviour and commercial practices are changing the role of consent in the processing of personal data.	2010-2013	Austria, Bulgaria, Czech Republic, France, Germany, Ireland, Italy, Malta, Netherlands, Poland, Romania, Slovakia, Spain, UK[227]
PACT	*Public perception of security and privacy* Its goal was to carry out a root and branch review of public perception of privacy and security, to collect empirical evidence, and to translate research into a privacy framework and a decision support system.	2012-2015	27 EU member states
PRESCIENT	*Privacy and emerging sciences and technologies* It aimed to identify and assess privacy issues posed by emerging sciences and technologies and to contribute to the development of new instruments for the governance of science and technology.	2009-2012	Austria, Bulgaria, Czech Republic, Denmark, France, Germany, Hungary, Italy, Latvia, Lithuania, Malta, The Netherlands, Poland, Portugal, Romania, Slovenia, Spain, Sweden, UK
PRISE	*Privacy enhancing shaping of security research and technology* It provided guidelines and support for security solutions with a particular emphasis on human rights, human behaviour and perception of security and privacy.	2007-2008	Austria, Denmark, Germany, Hungary, Norway, Spain
PRISMS	*Privacy and security mirrors* It analysed the traditional trade-off model between privacy and security and worked towards a more evidence-based perspective for reconciling privacy and security, trust and concern.	2012-2015	27 EU member states
RESPECT	*Rules, expectations and security through privacy enhanced convenient technologies* It addressed the role of surveillance systems and procedures in preventing and reducing crime, tracking evidence, and improvement of crime and acts of terrorism prosecution.	2012-2015	Austria, Bulgaria, Czech Republic, Germany, Italy, Malta, the Netherlands, Romania, Slovakia, Slovenia, Spain, Sweden, UK[228]

[227] Only 14 out of the 26 surveyed countries had respondent numbers which were sufficient for a meaningful quantitative analysis by country.

[228] For only 13 out of the 28 surveyed countries (EU plus Norway), the number of respondents met the required target quota to be representative.

Project	Description	Duration	Countries in survey
SMART	*Scalable measures for automated recognition technologies* It examined the social and legal consequences of adoption of automated, "smart surveillance" systems by public bodies.	2011-2014	Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Norway, Romania, Slovakia, Slovenia, Spain, the Netherlands, UK
SurPRISE	*Surveillance, privacy and security* A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.	2014-2015	Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland, UK

A.2 Literature Search Methodology

We searched for additional papers in two scientific databases, namely Scopus and Web of Science Core Collection.[229] We started from the cybersecurity-related references found with the validated keyword set identified in the bibliometric study of CANVAS Work Package 1 (see White paper 1 for details).

Then we refined these base results to obtain the empirical studies with the attitudes and opinions of European citizens on cybersecurity. After merging final results and removing all duplicates, this search yielded 1,131 unique references.

In a second phase, we filtered these 1,131 references for each of our three social spheres of reference (health, business, police and national security) by following these steps:

1. Filtering by title and abstract:
   - If no abstract was available, the first page of the paper was skimmed for relevance.
   - Inclusion criteria: empirical studies focusing on EU citizens' attitudes or opinions regarding cybersecurity, English papers between 1996 and 2016.
   - Exclusion criteria: empirical studies about non-EU citizens, non-English papers, papers outside of 1996-2016.
   - After removing 27 non-English papers, 1,104 papers remained. Among them, we found 22 specific references for health, 23 for business, and 16 for police and national security.
2. Full paper analysis:
   - The specific papers found were read. Among them, four empirical studies were in any significant way related to EU citizens' attitudes or opinions about cybersecurity in health, two were relevant for business, and one for police and national security.
3. Snowballing:
   - We checked the bibliographies of the specific papers analysed. Each contributor, being an expert in the field, also used its overview knowledge of the relevant literature. Snowballing yielded four additional empirical studies for the health sphere.

The fact that only very few papers have been found points to a clear research need. The results of this literature search are included in the above sections: 3. Citizens on cybersecurity in health, 4. Citizens on cybersecurity in business, 5. Citizens on cybersecurity in police and national security.

[229] https://www.scopus.com/ – https://www.webofknowledge.com/

A.3 Abbreviations

BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (German Federal Office of Civil Protection and Disaster Assistance)
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CNIL	Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)
CoE	Council of Europe
CSIRT	Computer Security Incident Response Team
D-	deliverable (document produced for an EU project)
DPA	Data Protection Authority
DPI	Deep Packet Inspection
DPIA	Data Protection Impact Assessment
EC	European Community
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
EU	European Union
FIRST	Forum of Incident Response and Security Teams
FP7	7th Framework Programme for research and technological Development
GDPR	General Data Protection Regulation
ICO UK	Information Commissioner of the United Kingdom
ICT	Information and Communication Technologies
IoT	Internet of Things
ISP	Internet Service Provider
IT	Information Technology
LEA	Law Enforcement Agency
NATO	North Atlantic Treaty Organization
NIS	Network and Information Security
OJ	Official Journal of the European Union. (It contains two series: L for legislation, C for information and notices.)
PET	Privacy Enhancing Technology
PwC	PricewaterhouseCoopers
R&D	Research and Development
SET	Secure Electronic Transaction
SLT	Smartphone Location Tracking
SOST	Surveillance-Oriented Security Technology
T-CY	Cybercrime Convention Committee (of the Council of Europe)
UGC	User Generated Content

A.4 References

NB: titles of must-read references are highlighted in **bold** print (with or without *italics*).

Books and articles

BERKNIK, Igor and Gorazd MESKO (2012): Study of the perception of cyber threats and the fear of cyber-crime. *Proceedings of the 7th International Conference on Information Warfare and Security*

(ICIW2012), University of Washington, Seattle, USA, 22-23 March 2012, p. 27-35 (ISBN 978-1-908272-29-4)

ESCHENBURG, Felix, Jani LYLYKANGAS, Nicole KRÄMER, Veikko SURAKKA, Heide TROITZSCH, Kimmo VUORINEN and Gary BENTE (2005): User acceptance: the BioSec approach. *Biometric Technology Today*, 13(7), 2005, p. 8-10 (https://doi.org/10.1016/S0969-4765(05)70369-6)

FRIEDEWALD, Michael, J. Peter BURGESS, Johann ČAS, Walter PEISSL and Rocco BELLANOVA (eds.) (2017): ***Surveillance, privacy and security: citizens' perspectives***[#] Oxon, Routledge, 2017 (PDF version available for free) (http://www.tandfebooks.com/doi/book/10.4324/9781315619309)

FURNELL, S.M. and T. KARWENI (1999): Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research*, 9(5), 1999, p. 372-382 (https://doi.org/10.1108/10662249910297778)

GASKELL, George, Herbert GOTTWEIS, Johannes STARKBAUM, Monica M. GERBER, Jacqueline BROERSE, Ursula GOTTWEIS, Abbi HOBBS, Ilpo HELÉN, Maria PASCHOU, Karoliina SNELL and Alexandra SOULIER (2013): Publics and biobanks: pan-European diversity and the challenge of responsible innovation. *European Journal of Human Genetics*, 21(1), 2013, p. 14-20 (https://doi.org/10.1038/ejhg.2012.104)

GILES, Keir and Kim HARTMANN (2014): Socio-political effects of active cyber defence measures. 2014 6th International Conference on Cyber Conflict (CyCon 2014) (https://doi.org/10.1109/CYCON.2014.6916393)

GOODSON, M. L. and B. G. VERNON (2003): A study of public opinion on the use of tissue samples from living subjects for clinical research. *Journal of Clinical Pathology*, 57(2), 2003, p. 135-138 (https://doi.org/10.1136/jcp.2003.9886)

HANSEN, Marit, Meiko JENSEN and Martin ROST (2015): Protection goals for privacy engineering. Security and Privacy Workshops (SPW), IEEE, 2015, p. 159-166 (https://doi.org/10.1109/SPW.2015.13)

KETTIS-LINDBLAD, Åsa, Lena RING, Eva VIBERTH and Mats G. HANSSON (2007): Perceptions of potential donors in the Swedish public towards information and consent procedures in relation to use of human tissue samples in biobanks. A population-based study. *Scandinavian Journal of Public Health*, 35(2), 2007, p. 148-156 (https://doi.org/10.1080/14034940600868572)

PAVONE, Vincenzo, Elvira SANTIAGO GOMEZ and David-Olivier JAQUET-CHIFFELLE (2016): A systemic approach to security: beyond the tradeoff between security and liberty. *Democracy and Security*, 12(4), 2016, p. 225-246 (https://doi.org/10.1080/17419166.2016.1217776)

RILEY, Chris, Kathy BUCKNER, Graham JOHNSON and David BENYON (2009): Culture & biometrics: regional differences in the perception of biometric authentication technologies. *AI & Society*, 24(3), 2009, p. 295-306 (https://doi.org/10.1007/s00146-009-0218-1)

SANCHEZ, Orestes (2005): BioSec: a European project. *Biometric Technology Today*, 13(6), 2005, p. 9 (https://doi.org/10.1016/S0969-4765(05)70347-7)

SNELL, K., J. STARKBAUM, G. LAUß, A. VERMEER and I. HELÉN (2012): From protection of privacy to control of data streams: a focus group study on biobanks in the information society. *Public Health Genomics*, 15(5), 2012, p. 293-302 (https://doi.org/10.1159/000336541)

TUPASELA, Aaro, Sinikka SIHVO, Karolna SNELL, PA JALLINOJA, Arja R. ARO and Elina HEMMINKI (2010): Attitudes towards biomedical use of tissue sample collections, consent, and biobanks among Finns. *Scandinavian Journal of Public Health*, 38(1), 2010, p. 46-52 (https://doi.org/10.1177/1403494809353824)

[#] This reference is a must read to get an overview of the most relevant findings.

VON LIECHTENSTEIN, Alfred (2002): *Internet und Öffentlichkeit.* Vienna, WUV Universitätsverlag, 2002 (ISBN 978-3-85114-667-7)

EU projects

See also A.1 EU Projects Overview

CANVAS: constructing an alliance for value-driven cybersecurity: https://canvas-project.eu

CONSENT: consumer sentiment regarding privacy: http://www.consent.law.muni.cz/

'CONSENT D-7.3: Synthesised all countries report'[#]: Public deliverable, February 2013 (not available online)

PACT: public perception of security and privacy: http://www.projectpact.eu

'PACT D-4.2: Survey report'[#]: Public deliverable, 20 June 2014: http://www.projectpact.eu/deliverables/wp4-data-analysis/d4.2/D4.2.pdf/view

'PACT: Final report summary': http://cordis.europa.eu/result/rcn/181728_en.html

PRESCIENT: privacy and emerging sciences and technologies: http://www.prescient-project.eu

'PRESCIENT D-3: Privacy, data protection and ethical issues in new and emerging technologies'[#]: Public deliverable, 16 May 2012: http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_Deliverable_3_Final.pdf

PRISE: privacy enhancing shaping of security research and technology: http://www.prise.oeaw.ac.at Supported by PASR (preparatory action on the enhancement of the European industrial potential in the field of security research)

'PRISE D-5.8: Synthesis report – interview meetings on security technology and privacy'[#]: Public deliverable, April 2008: http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf

'PRISE D-6.2: Criteria for privacy enhancing security technologies': Public deliverable, 2008: http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf

'PRISE D-7.6: Concluding conference statement paper': Public deliverable (no date): http://www.prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf

PRISMS: privacy and security mirrors: http://prismsproject.eu

'PRISMS D-10.1: Report on statistical analysis of survey'[#]: Public deliverable, 16 October 2015 (not available online)

'PRISMS D-9.1: Findings from qualitative focus groups': Public deliverable, 29 October 2013: http://prismsproject.eu/wp-content/uploads/2014/01/PRISMS-D9-1-Focus-Groups-Report.pdf

'PRISMS: Final report summary': http://cordis.europa.eu/result/rcn/191772_en.html

RESPECT: rules, expectations and security through privacy enhanced convenient technologies: http://respectproject.eu

'RESPECT D-11.3: Synthesised all countries report (quantitative data)'[#]: Public deliverable, 19 May 2015 (not available online)

'RESPECT: Periodic report summary 1': http://cordis.europa.eu/result/rcn/153820_en.html

[#] This reference is a must read to get an overview of the most relevant findings.

[#] This reference is a must read to get an overview of the most relevant findings.

SMART: scalable measures for automated recognition technologies: http://www.smartsurveillance.eu

'SMART: Report summary': http://cordis.europa.eu/result/rcn/178069_en.html

SurPRISE: surveillance, privacy and security: http://surprise-project.eu

'SurPRISE D-6.10: Synthesis report'[#]: Public deliverable, February 2015: http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesis-report.pdf

'SurPRISE D-6.12: Workshop report': Public deliverable, December 2014: http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.12-Workshop-report.pdf

'SurPRISE presentation: Aligning security and privacy. En route towards acceptable surveillance'. Sara Degli Esposti, Vincenzo Pavone and Elvira Santiago: Joint conference of SurPRISE, PRISMS and PACT, Vienna, 13-14 November 2014: http://surprise-project.eu/wp-content/uploads/2014/11/Degli-Esposti_Aligning-security-and-privacy-en-route-toward-acceptable-surveillance.pdf

'SurPRISE, PRISMS and PACT: Abstract booklet' *Citizens' perspectives on surveillance, security and privacy: controversies, alternatives and solutions*. Joint final conference, Vienna, 13-14 November 2014: http://surprise-project.eu/wp-content/uploads/2014/11/Booklet_Final.pdf

'SurPRISE: Report summary': http://cordis.europa.eu/result/rcn/171903_en.html

Other surveys

'Flash Eurobarometer 225: Data Protection in the European Union – Citizens' Perception'
Analytical Report, The Gallup Organization (for the European Commission), 2008
http://ec.europa.eu/commfrontoffice/publicopinion/flash/fl_225_en.pdf

'Global State of Information Security® Survey 2017'
PricewaterhouseCoopers International Limited (PwCIL)
http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

'Special Eurobarometer 341: Biotechnology'
Report, TNS Opinion & Social (for the European Commission), 2010
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_341_en.pdf

'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union'
Report, TNS Opinion & Social (for the European Commission), 2011
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf

'Special Eurobarometer 390: Cyber Security'
Report, TNS Opinion & Social (for the European Commission), 2012
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf

'Special Eurobarometer 404: Cyber Security'
Report, TNS Opinion & Social (for the European Commission), 2013
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_404_en.pdf

'Special Eurobarometer 423: Cyber Security'[#]
Report, TNS Opinion & Social (for the European Commission), 2015
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

[#] This reference is a must read to get an overview of the most relevant findings.

'Special Eurobarometer 432: Europeans' Attitudes towards Security'
Report, TNS Opinion & Social (for the European Commission), 2015
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_en.pdf

'Special Eurobarometer 464a: Europeans' Attitudes towards Security'
Report, TNS Opinion & Social (for the European Commission), 2015
http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171

Legislation and Policy Documents

European Union

'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'
European Commission, Communication COM/2000/890 final, Brussels, 26 January 2001
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890

'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace'#
European Commission, Joint communication JOIN/2013/1 final, Brussels, 7 February 2013
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union'
[2016] OJ L 194/1 (NIS Directive)
http://data.europa.eu/eli/dir/2016/1148/oj

'ENISA Threat Landscape Report 2016'#
European Union Agency for Network and Information Security (ENISA), January 2017
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

'European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private-Partnership (cPPP)'
European Cyber Security Organisation (ECSO), June 2016
http://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

'Opinion 8/2015 on Dissemination and use of intrusive surveillance technologies'
European Data Protection Supervisor (Giovanni Buttarelli), Brussels, 15 December 2015
https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf

'Opinion 9/2001 on the Commission Communication on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime"'
Article 29 Working Party, WP 51, 5 November 2001
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp51_en.pdf

'Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a "Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace", and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union'
European Data Protection Supervisor (Peter Hustinx), Brussels, 14 June 2013
https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC'

[2016] OJ L 119/1 (General Data Protection Regulation)
http://data.europa.eu/eli/dir/2016/1148/oj

'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'
European Commission, Communication COM/2016/410 final, Brussels, 5 July 2016
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410

'The EDPS Strategy 2015-2019'[#]
European Data Protection Supervisor, Publications Office of the EU, Luxembourg, 2015
https://doi.org/10.2804/35559

Other (non-EU)

'36th Activity Report 2015'
Commission Nationale de l'Informatique et des Libertés (CNIL), France
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_2015_gb.pdf

'Cyber Defence Pledge'
North Atlantic Treaty Organization (NATO), Press release (2016) 124, 8 July 2016
http://www.nato.int/cps/en/natohq/official_texts_133177.htm

'French National Digital Security Strategy'
République française, France, 2015
https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/

'National Cyber Security Strategy'
Gobierno de España, Spain, 2013
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

'National Cybersecurity Strategy II'
Gouvernement du Grand-Duché de Luxembourg, 2015
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

'Privacy: working with business – Ten corporate best practices to improve your business'
Garante per la Protezione dei Dati Personali, Italy
http://www.garanteprivacy.it/documents/10160/2416443/Privacy%3A+working+with+business-vademecum.pdf

'The National Cyber Security Strategy of the Republic of Croatia'
Official Gazette No 108/2015, Zagreb, 7 October 2015
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf

'The Standard Data Protection Model: a concept for inspection and consultation on the basis of unified protection goals'
German Data Protection Authorities, Kühlungsborn, 9-10 November 2016
https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html
See also: https://www.datenschutzzentrum.de/sdm/

[#] This reference is a must read to get an overview of the most relevant findings.