European Commission
Horizon 2020 European Union funding for Research & Innovation
TRUESSEC.eu

Deliverable D3.2
Current exemplary discourse dynamics in the field of cybersecurity

WP3

Deliverable

Contract Number:	731711
Project Acronym:	TRUESSEC.EU
Project Title:	"TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe"

Document Identifier:	D3.2
Status:	Final Version

Title of Document:	Analysis of Exemplary Public Discourses on Cybersecurity and Trust
Dissemination Level:	Public

Author(s):	Stefan Reichmann (University of Graz), Martin Griesbacher (University of Graz)
Reviewed by:	Jon Kingsbury (KTN)

Created on:	15 January 2018
Last update:	31 August 2018

CHANGE HISTORY

Date	Change	Author
2018-01-15	Finalization of Research Area Definition and Sampling Strategy	Stefan Reichmann, Martin Griesbacher
2018-03-21	Codebook (first version)	Stefan Reichmann
2018-03-30	Finalization of Objectives and Methodology Sections	Stefan Reichmann, Martin Griesbacher
2018-04-14	Finalization of the Coding Scheme	Stefan Reichmann
2018-06-11	Case Studies completed (first version)	Stefan Reichmann
2018-07-18	Pre-Final Version (for Review)	Stefan Reichmann
2018-07-25	Review Version	Jon Kingsbury
2018-08-31	Implementing Review findings and final version	Stefan Reichmann, Martin Griesbacher

Table of Contents

1 Executive summary

The following report summarizes exemplary case studies of European public discourse in the first half of 2017 with respect to (trust in) ICT products and services and the Internet as an infrastructure, cybercrime and its government-supported counterpart, cyberwar, and issues of privacy and data subjects. The analysed public discourses where located in three geographical regions: The UK (cybercrime), Spain (privacy and data subjects), and Germany (state surveillance). The following meta-topics have been identified, all of which play a significant role in all discourse areas discussed.

- The Internet is not only a space of opportunity but also one of insecurity and risk. "Cybersecurity" addresses the latter aspect. Cybercrime and cyberwar are key elements in the discourse on threats to cybersecurity. In the discussion of upcoming threats to cybersecurity, cybercrime especially but also the handling of personal data by providers of ICT products and services, end-users are frequently addressed as responsible for enhancing overall cybersecurity. This is related to the topic of raising "cyber awareness" and identifying "social engineering" as a tool to combat cybercriminal incidents in the context of an increasingly complex technological world.
- Throughout diverse cybersecurity discourses in the media, esp. regarding privacy and data protection, the topic of the data subject has been identified. The data subject is imagined as the entity to exercise (or the entity entitled to exercise) control over personal data. This construction to some extent allows the detachment of the questions of personal data from the broader issue of a right to privacy. Discussing personal data as separated from persons enables the definition of data processing by different parties as legitimate (or not). In this sense the discourse also shifts from a question of rights (privacy) to a question of property and control over property and allows the implementation of business models.
- A pertaining prominent discourse deals with the ambivalent implications of state security measures. This includes esp. surveillance activities of national security agencies and also the legal access to personal data in police investigations of criminal or terrorist incidents. The main issue here concerns the threat security measures might pose to the general level of cybersecurity because of the use of zero-day vulnerabilities to gain access to incriminating data/digital evidence. By not closing these security gaps in ICT products and services criminals also potentially retain the opportunity to illegally access personal data and to attack and harm digital infrastructures.
- Discourses about "cyber threats" like cybercrime, cyberwar and also cyber surveillance may reduce or enforce trust in huge "regions" of cyberspace (e.g. to what extent are online news trusted). Therefore, strengthening security of different types of ICT products and services alone might be insufficient to create an overall perception of security when prominent discourses simultaneously deal with issues like "fake news", "cyberwar" or "state surveillance".
- Overall there seems to be a high degree of disunity and uncertainty about cybersecurity measures, which shapes an ambivalent "discursive arena" between state, economic/business and civil actors across Europe to create a trustworthy internet.

2 Introduction

2.1 Objectives

Work package three (WP3) of the TRUESSEC.eu-project has been concerned with sociological and cultural factors pertaining to trust in and willingness to use ICT products and services in particular and the Internet infrastructure more generally. While task 3.1 was dedicated to a comprehensive understanding of European public opinions on these matters and therefore relied heavily on representative survey materials (in particular Eurobarometer), task 3.2 sought to deliver a deeper understanding on the structure of media discourse on the Internet, cybercrime/cybersecurity, privacy and data control, and surveillance and the ways these discourses pertain to the spectrum of public opinions described in deliverable 3.1[1].

This deliverable contains three case studies of different public online discourses on the broader issue of cybersecurity and trustworthy information and communication technologies (ICT). It is part of the support studies of the TRUESSEC.eu project, which are aimed towards an interdisciplinary understanding of key aspects of trust and security of ICT products and services. The connected previous deliverable (D3.1: Public Perceptions of Cybercrime and Cyber Security in the EU) collected survey data on this issue to improve the understanding of quantitative differences and priorities in public opinion. This deliverable follows up and is working towards a more qualitative in-depth understanding of central public discourses. Understand cybersecurity is here therefore tackled as not only a matter of technical security features and process but of the public perception and discursive construction of cybersecurity issues.

The aim behind studying public discourse is to gain a deeper insight into public opinion formation and its major influence factors. This has been carried out with special attention towards the topic of trust and trust formation as it pertains to ICT products and services and to the Internet as an infrastructure more generally. However, it was not our intention to understand and assess the impact of these discourses on (potential) audiences. Instead, what we are trying to understand is something more abstract: We want to understand **how discourse on ICT is structured** with respect to **key issues, problems, positions, and actors**. We are aware that media discourse is shaped by a host of factors, not all of which will be adequately taken into account, such as news values, ideologies, and imagined audiences of the selected newspapers. These aspects of news reporting will be reflected on where appropriate, but are not systematically targeted in the present study. The overall aim of the present study is to describe how European values such as transparency and privacy feature in discourse on ICT products and related matters such as cybercrime, data protection and online commerce.

The three case studies presented here focus a) on the issue of responsibility for cybersecurity, b) the role of criminal activities for cybersecurity and c) the issue and public perception of security measures like state surveillance activities.

2.2 Methodology

2.2.1 Overview

The Discourse Analysis (DA) is based on three discourse arenas (privacy/data protection, surveillance/leaks, e-commerce) in three language areas/five countries (German-speaking, English-

[1] Reichmann, Stefan; Martin Griesbacher. (2017). TRUESSEC.eu – Deliverable 3.1.: Public Perceptions of Cybercrime and Cybersecurity in the EU. URL: https://truessec.eu/library.

speaking, Spanish-speaking). For each language area, several (online) news outlets have been selected, each representing a distinct brand of journalism (tabloid, quality newspaper, tech news). The sampling strategy centred on a predefined list of keywords pertaining to the selected discourse arenas (one list per arena which was used for all outlets). This strategy implies that there are (sometimes considerable) overlaps between the three discourse arenas (i.e., discourse on privacy covers state surveillance and vice versa).

Discourse analysis is focused on analyzing topics. A *topos* in this sense is a term (or family of terms/synonyms) which comes up and defines the scope of a discourse. This does not happen by way of formal definitions, however, in particular as the term pertains to public (media) discourses where explicit definitions are seldom found. The meanings of terms are rather constructed in and through public discourse. The aim of the following report is therefore to reconstruct (or, to use a notorious phrase, deconstruct) those meaning constructions. Every time we refer to a concept as a topic in this sense, we use the phrase “the topic/topos of …” and/or put the concept in *italics*.

The sample used in the present study was restricted to the period from 1 January 2017 to 30 June 2017, i.e. six months in total. The analysis focused solely on media discourses on the phenomena of cybercrime, personal data, and surveillance, to the exclusion of e.g. academic discourse, historical discourse, and pop cultural discourse. All of the newspapers included in the sample have a website that includes a search function which was used for the sampling. Given the range of topics and geographical regions, we will settle for a theoretical sampling strategy in combination with stratified sampling to take into account the relative size of the geographical regions and the media coverage of the newspapers involved. The geographical regions and the topics deemed most interesting were selected according to their relative importance based on the findings of the survey analysis.

The Discourse Analysis (DA) is based on three discourse arenas:

(1) privacy/data protection

(2) surveillance/leaks

(3) e-commerce

in three language areas/five countries:

(1) German-speaking

(2) English-speaking

(3) Spanish-speaking

For each language area, several (online) news outlets have been selected, each representing a distinct brand of journalism (tabloid, quality newspaper, tech news). The sampling strategy was centered on a predefined list of keywords pertaining to the selected discourse arenas (one list per arena which was used for all outlets). This strategy implies that there are (sometimes considerable) overlaps between the three discourse arenas (i.e., discourse on privacy covers state surveillance and vice versa). This strategy implies that the selected discourse arenas can be discerned geographically, but not necessarily thematically. Even though there are incidents and corresponding discourse dynamics specific to geographical regions (e.g., the NSA scandal was much more widely covered in the German media due the role played by the German intelligence agency BND), there are therefore many overlaps between discourses. The themes of cybercrime/security and data protection, but also the Snowden revelations cover more than one discourse arena. This is partly due to the structure of these discourses, but it was also already reflected in the sampling strategy. The initial sampling would have included only key words pertaining to the Eurobarometer items most salient for the respective regions (e.g. “surveillance” and related concepts for

Germany). However, that strategy quickly had to be abandoned due to low return rates. Hence, for the UK (e.g.), it was quickly decided to include broader search terms such as “cybercrime” and “cybersecurity” in addition to the initial terms such as “(cyber)fraud” and “e-commerce”.

Discourse in German-speaking media outlets was not translated into English prior to analysis, as all researchers involved in the DA are fluent in German. However, since none of the researchers involved in the DA are fluent in Spanish, the online translator deepL (deepl.com) was used to translate the pieces of discourse found in Spanish-speaking media. The development of the coding scheme was carried out in the English language from the start using coding software MaxQDA 18 for color coding. The entire sample consists of roughly 250 documents (where each document is a newspaper article of varying length). The details of the samples are given below for each of the case studies.

2.2.2 Sampling by Region

Spain

Spain has high levels of concerns about personal data misuse. This might be caused by a higher frequency of reports of data breaches in Spanish news outlets (or at least were frequent prior to the 2017 Eurobarometer survey on data protection[2].

The articles come from the two largest Spanish-speaking newspapers (numbers in brackets indicate the number of articles analysed): El País (1 article) and El Mundo (29 articles), which incidentally were the only two news outlets reasonably available online and which reported reasonably frequently on issues of data protection and privacy. The online search was conducted by relying on those two search terms plus synonyms, e.g. “personal data”, “sensitive data”, “data”, “privacy”, “private sphere”, “data breach” and “data misuse”. The Spanish case study is therefore restricted to the discourse arenas “personal data” and “privacy”.

Since none of the researchers involved in this task are fluent in Spanish, we used online translation software deepL (www.deepl.com) to translate both the search terms so that they could be used in the newspaper websites search functions, and then the articles which were found. The articles were first translated and then selected for fit.

UK

Ireland and the UK both have high levels of concerns about online fraud, and the UK has a high victimization rate (22% of respondents reported in 2017 that they had become a victim of online fraud).[3]

The articles come from the following newspapers (numbers in brackets indicate the number of articles analysed): Evening Press (1 article), Express (5 articles), Insider (1 article), International Business Times UK (11 articles), Metro (1 article), Daily Mail (6 articles), the Daily Mirror (14 articles), the Daily Record (4 articles), the Guardian (8 articles), the Herald Scotland (2 articles), the Independent (9 Articles), the Press and Journal (1 article), the Scotsman (9 articles), the Sun (13 articles), and the Telegraph (12 articles), making 101 articles in total. The articles were searched on the newspapers’ websites according to a list of predefined search terms (fraud, cyberfraud, scam, cyberscam, cybercrime, cybersecurity).

[2] European Commission (2017). Special Eurobarometer 464a: Europeans’ Attitudes towards cyber security.
[3] See European Commission (2017), FN 4.

Germany

Austria and Germany both have high levels of concerns about surveillance. In addition, Germany has had experience with police states in the recent past (in the German Democratic Republic). Germany has been particularly involved in the NSA-espionage scandal revealed by Edward Snowden, with some repercussions for Austria as well. Survey data indicates, that surveillance is a particular important topic in Germany and Austria as the population has the highest reported knowledge about surveillance activities in the aftermath of the Snowden-Case.[4]

The articles come from the following newspapers (numbers in brackets indicate the number of articles analysed): Süddeutsche Zeitung, Germany (91 articles), Chip, Germany (4 articles), Heise (39 articles), Kronenzeitung, Austria (4 articles), making 138 articles in total. The articles were searched on the newspapers' websites according to a list of predefined search terms (surveillance, Edward Snowden, whistleblowing/whistle-blowers). The articles were not translated as the researchers involved are fluent in both German and English. However, in order to be able to present findings in a readable format, the articles selected for closer analysis were translated. This was done in part with the help of online translation software deepL (www.deepl.com) to speed up the process.

As the sampling was restricted to the centre-left of the political spectrum because other eligible news outlets have installed paywalls, the methodology used had to control for political ideology. As a consequence, the aim of the Germany/Austria case study explicitly was not to compare different newspapers' ideologies with respect to surveillance. Rather, the aim was to understand the most general, most fundamental assumptions with respect to surveillance and to reconstruct the prevalent lines of argument from their media representations. In principle, this task could be achieved by relying on a small sample of articles. However, such a strategy runs the risk of producing ad hoc-interpretations. Therefore, the sample used was large (138 articles in total) in order to be able to develop a material-based theory. The approach is similar to that proposed by Glaser and Strauss[5], but we refrained from employing a theoretical sampling strategy which would have integrated analysis and sampling.

As for the interpretation of the material, we employed a strategy that might be labelled "suspension of doubt". We have no way of knowing who the audiences of the news outlets in question are, and we have no way of knowing whether the reported events are in any way factual. It only needs to be assumed that the general public trusts the media in general (it might still be the case that individuals trust some newspapers more than others) and that the general public assumes that what the media report is more or less factual. From this it follows that for present purposes, the question of facticity can be put aside. Instead, the present analysis focuses on the representations of the events reported and on the positions and arguments of the stakeholders involved as they are represented by the media.

[4] European Commission (2015). Special Eurobarometer 431: Data Protection.

[5] Glaser, Barney / Strauss, Anselm (1967). The Discovery of Grounded Theory, Chicago: Aldine.

3 Case Study I: Personal Data and the Rise of the Data Subject (Spain)

3.1 Data Subjects: Privacy and Control

3.1.1 Individuals as Data Subjects: The Limits of Control

The notion of data subject is fundamental to all discussions of data collection, privacy, and control over personal data. It is therefore hardly surprising that a variant of this notion is present in (almost) all the articles sampled here (not restricted to the Spain case). However, the notion largely remains implicit and has to be reconstructed through careful and close interpretations of the material. This is the task of the following section.

In a report published in El Mundo (23 January 2017) readers learn about a data breach by the Spanish employment agency which allegedly uses clear names of clients on its public screens:

> The Andalusian Ombudsman considers that the Ministry of Employment, led by the Minister José Sánchez Maldonado, unjustifiably violates the rights to privacy, confidentiality and security of personal data by airing the names of the unemployed in the offices of the Andalusian Employment Service (SAE). (El Mundo, 23 January 2017)

The above paragraph implicitly acknowledges that there is an individual right to privacy, confidentiality and data security. Additionally, the paragraph says that these rights may be violated by organisations and their data handling procedures. Accordingly, data is something (we don’t learn what exactly they are, though) that can be handled, and this can happen in ways which are appropriate and respecting of individual rights, or it can happen in ways which do not respect individual rights. In any case, the section suggests that there is something about personal data that individuals should legitimately be in control of. This follows from the construction of privacy violations as illegitimate in the above paragraph. The paragraph therefore contains a vivid example of the construction of individuals as data subjects. The next paragraph goes into some detail as to the nature of the data breach in question:

> "It is not acceptable for everyone who is also waiting to see the identity and the person holding the data. When a person makes an appointment, he or she should be assigned a number, which is the one that should appear on the screen," the complainant said in his or her letter.
>
> After receiving the complaint, the Andalusian Ombudsman requested a report from the Management of the Andalusian Employment Service, to explain why it does not offer users a number, as most public bodies do with a "fairly simple" and effective system.
>
> In its reply, the EDC argued that, in view of 'experience gained' and the fact that appointments are issued, in most cases prior to the date of the appointment, it is considered that the jobseeker might 'not know or simply not remember' the number assigned. (El Mundo, 23 January 2017)

The reader learns that the breach concerned a group which is generally considered vulnerable (at least more so than other groups), namely people seeking employment. The *topos* of vulnerability is familiar in discussions of data protection and privacy, as it is usually the transparency of individuals which is juxtaposed with the opacity of data-collecting entities. Depending on the context, the proposed remedies for this situation then involve empowering individuals to gain control over organisations’ data processing activities. The above section further argues that privacy can be a simple matter of process; this suggests that the reverse is also true: privacy breaches are a matter of bad process. The next paragraph fleshes out the legal implications:

> The office of Jesús Maeztu has issued a resolution in which it 'reminds' the Board of the 'obligation to comply with the legal precepts' and recommends that, in coordination with the State Public

> Employment Service – both bodies share offices in the community – technical measures be implemented to guarantee the aforementioned rights in the system of prior appointment.
> The resolution is the result of a complaint filed by a user, who denounced that in all the Employment Offices in Andalusia, when a person comes with their appointment and waits in the room to be called, their surnames and the first initial of their name appear on an electronic screen. (El Mundo, 23 January 2017)

The implicit theory of privacy contained in the above paragraphs can be summarized as follows: Privacy concerns some aspects of an individual's life that, when somehow assessed or measured, turn into "(personal) data" that can be separated from the individual to be processed and shared, and that there are legitimate and illegitimate ways to do so. The notion that personal data can be separated from individuals is reinforced in the following article by El Mundo (7 February 2017) which reports a data breach involving public officials:

> Last January it was announced that the Public Prosecutor's Office is asking for 5 to 16 years' imprisonment for three tax officials, one of them from the Biscay Provincial Council, and two agents of the Civil Guard allegedly involved in one of the branches of the Pitiusa plot, accused of selling personal data of third parties to private detectives, This official was one of more than 70 people arrested in 2012 in an operation carried out in different parts of Spain, and in the provisional conclusions on one of the many pieces of the Pitiusa case, the prosecutor concludes that the defendants collaborated with a network dedicated to the collection, intermediation, marketing and large-scale distribution of confidential personal, labour and tax data of hundreds of people, at least between 2006 and 2012. (El Mundo, 7 February 2017)

In the above case, personal data from "hundreds of people" were distributed and sold in a rather professional way by public officials entrusted with these data. Personal data therefore are imagined as distinct (or distinguishable) from individuals which can develop a life of its own. The section operates on the assumption, now familiar, that there are legitimate and illegitimate ways to handle personal data. This is what justifies qualifying some instances of data processing as legitimate and others as illegitimate.

3.1.2 Constructing Data as Personal

The following two paragraphs reinforce the notion that there are legitimate and illegitimate ways to handle personal data. What is more, it argues that individuals are entitled to their data being handled appropriately:

> The provincial deputy has explained that, after the official was arrested in 2012, the Provincial Council investigated the matter but found no "evidence of any infraction", the member of the Mixed Group Arturo Aldecoa has considered that this type of case generates "mistrust in the public about the security of their data", and the representative of EH Bildu Arantza Urkaregi has also asked Bengoetxea how the Provincial Council guarantees the confidentiality of taxpayer data.
>
> She added that the mechanisms and controls guarantee this confidentiality "regardless of the fact that in a specific case there has been an inappropriate use" of the data. Urkaregi and PP junter Eduardo Andrés have highlighted that "something went wrong" if the Provincial Council investigated the case in 2012, without discovering anything, and that the official is now accused of 12 crimes. (El Mundo, 7 February 2017)

Personal data are constructed as private and as belonging to individuals, which simultaneously reinforces the notion that individuals should have at least some control over their data. The notions of privacy, control over personal data and data subject can therefore be interpreted as co-constitutive, i.e. one would not exist without the others. In other words, data subjects are simply assumed with certain qualities (a right to their data, for example) to argue for rights and obligations. What is striking about these constructions is the approximation of data and property; the notion that something is “private” is very closely aligned with the notion of property. Even though nothing is explicitly said about property by labelling data (something very abstract) as “private”, this conceptualization nevertheless resonates with conceptions of property. Therefore, data and data subjects can even become objects of politics, as can be seen in a report by El Mundo (6 June 2017) which centres on another data breach involving public servants:

> Almost a year has had to pass since the two opposition political groups in Palma City Council, the Popular Party (PP) and the Citizens (Cs) denounced to the Spanish Data Protection Agency (AEPD) the computer tracking of the use of the public parking card of the 13 councillors of these two formations in court ordered by the president of the Municipal Parking Society (SMAP) and councillor for Mobility, Joan Ferrer. And it was yesterday the mayor himself who, at a press conference, announced the opening of a disciplinary file to the management of the municipal company with the imposition, in the first instance, a fine of € 24,000 for these events. Although technicians from the SMAP and the company's contractors, as well as senior officials from the Mobility Department, had the same card that enables free access to all municipal car parks, Ferrer only ordered to track the use that the opposition councillors made of it. The card delivered by SMAP is electronic and includes the holder's personal data. For this reason, the computer systems of the municipal company recorded the movements, entrances and exits of the aforementioned public car parks. (El Mundo, 6 June 2017)

The paragraph discusses an incident revolving around two opposition parties in Palma which became victims of a data breach. Here, “data” are imagined as something that belongs to individuals (otherwise there would be no point in claiming illicit data collection) but can be separated from them and collected on external devices (in this case, an access card). The simple fact that the contents of these cards were used by members of government to reconstruct the whereabouts of members of oppositional parties makes the incident in question one of espionage and surveillance. Both notions are based on the premise that there is such a thing as a (legitimate) data subject which has a right to their data. The article in question thereby reinforces these ideas by relying on them implicitly:

> It happens that these personal passes for the private vehicles of the PP and Cs councillors were given to them without any contract or condition of use. Without having any court order the councillor for Mobility first ordered the computer tracking of the vehicles of the 13 councillors and decided to remove it because they would have made an inappropriate use, under the criteria of the mayor, such as, for example, daily use. (El Mundo, 6 June 2017)

To summarize: There are entities which produce data and which have a legitimate right to these data (data subjects). These data subjects are imagined as somehow being in possession of their data (which makes for legitimate and illegitimate data use) and which therefore have some manner of control over them. Control can be lost and might, in some cases have to be restored by appeal to e.g. individual rights. Therefore, personal data can even be of interest to criminals. Data breaches, readers learn from El Mundo (8 May 2017), are by no means the sole domain of public bodies, though:

> Police alert of new WhatsApp scam promising a year of free Netflix
>
> Through the application multiple hoaxes and scams are viralized. REUTERS
>
> Cyber-criminals ask to enter their telephone number in order to obtain users' personal data
>
> Drug candy, imminent bombings and seven other hoaxes circulating in WhatsApp (El Mundo, 8 May 2017)

The statements above lend credence to the above interpretation of “personal data” as something that can be the object of law and of criminal intent. Data are something of a commodity, on this reading. They are produced by individuals through their actions, and in some cases these data are of interest to third parties who may or may not have legitimate interest in them. Here, the notions of “personal data” and “data subject” (both are only implicitly present) are co-constitutive of the notion “cybercrime” (which also is merely implicitly mentioned above). The section can only credibly speak of cybercrime because personal data are implicitly defined as individuals’ private property.

3.1.3 Data Subjects as Political and Economic Entities

El País (5 June 2017) states the dimensions of the problem of (unwanted) data collection:

> The study we are conducting with our colleagues has identified and is investigating a major risk unknown to most of us: more than 70% of mobile applications transmit personal data to tracking companies such as Google Analytics, Facebook's Graph API or Crashlytics. Very few applications make their privacy policy public and, if they do, it is usually through extensive legal documents that a normal person does not read, much less understand. (El País, 5 June 2017)

Here, the reader encounters a familiar theme. The article presents risks (probabilities) which are allegedly “unknown to most of us”. The scale of the problem is alarming, to be sure; apparently, 70% of mobile apps do transmit personal data to companies while their owners remain largely ignorant. However, the paragraph only suggests that this should be worrisome to users; it does not contain any information as to why it should be problematic that apps collect and transmit personal data. This is only comprehensible if the notions of personal data as private property and of the individual as data subject are accepted. The next line is telling as it refers to privacy policies, echoing a feeling which arguably is familiar to many non-expert users of digital technologies: that of being overwhelmed (or in other cases simply bored) by the “legalese” of privacy statements which causes many people to just skip them (and accepting them anyway). The paragraph is overtly sympathetic towards users who do not understand privacy policies, but is not entirely without condescension (“extensive legal documents that a normal person does not read, much less understand”), thereby reinforcing the users-as-ignorant stereotype.

El Mundo (29 March 2017) reports plans by the US administration to effectively nullify privacy safeguards:

> Internet service providers in the US will be able to sell their users' data
>
> The bill that eliminates privacy safeguards on the web
>
> The FBI's face recognition program is malfunctioning and racist.
>
> The U.S. Congress has passed a bill that eliminates the online privacy safeguards imposed by former President Barack Obama and will allow Internet service providers to sell user data, such as search histories or locations, the bill, to be endorsed in the next few days by President Donald Trump, repeals a regulation that Democrats had drafted for the Federal Communications Commission (FCC) that required providers to obtain permission from their users before selling their data. (El Mundo, 29 March 2017)

The language used suggests that the author(s) of the article are writing in favour of strong privacy laws. This is suggested by the use of the term “safeguard” in the second line. This framing of privacy suggests that privacy is the status quo which needs to be protected from illicit intrusions. The US legislation discussed in the article is thereby constructed as an assault on privacy as something inherently positive. The suggested commercialization of privacy further underscores the idea that privacy is fundamental and valuable and should not be commodified by opening up the possibility of selling personal data. The new legislation is here presented as effectively nullifying the idea that users are data subjects.

> Republicans have always viewed the regulation as over-regulatory and its rule will allow providers like Verizon, Comcast and AT&T to use their users' data by default to compete on an equal footing with Google and Facebook in the $83 billion online advertising business. (El Mundo, 29 March 2017)

Both the above paragraphs testify to the idea that data subjects are (also) political and economic entities. What happens to personal data and how it is used, is therefore the legitimate object of political and legal deliberation, as this has implications for market competition. Here, personal data take on an economic and political dimension as well:

> These companies had opposed the Obama administration's attempts to protect users' privacy and felt it was unfair that Google and Facebook should have different rules than theirs. Online privacy advocates such as the executive director of the Centre for Digital Democracy, Jeffrey Chester, told The Washington Post that with this project, "Americans will never be safe from having their personal data stealthily examined and sold to the highest bidder. Civil rights associations said the repeal of this rule will allow the uncontrolled dissemination of personal data, such as browsing history, which may reveal religious beliefs, ideologies, sexual orientation, health status or geographical information of users. (El Mundo, 29 March 2017)

If personal data have economic value (at least to some), it is equally the case that they have political implications for the individual, as human rights organizations point out. What is more, personal data can travel and cross borders:

> Data is transferred across national borders, often to countries whose privacy laws are of dubious confidence. (El País, 5 June 2017)

It is worthwhile to note that even though data are introduced as the property of the individual (which makes it problematic if other entities want to commodify them), data can be entirely separated from the individual and "transferred across national borders". This makes the call for (re)empowering individuals comprehensible.

3.1.4 Data Subjects as Worthy of Protection

The following article in El Mundo (22 May 2017) was published almost exactly a year before the GDPR came into force (25 May 2018). It deals with the GDPR from the perspective of consumer protection. Its tone is therefore much less optimistic than that of many other news items sampled where users are usually imagined as in need of education in order to assume their full responsibility for and control over their personal data. Rather, it constructs an opposition between users and "large companies" with respect to their interests in data collection and processing:

> The danger of not complying with the GDPR in time
>
> PROGRESSIVE REGULATION. Protect the user against large companies
>
> This is the date marked in red on the online privacy calendar as the end of the European adaptation period to the General Data Protection Regulation (GDPR). A rule that will penalize companies that handle their consumers' confidential information in an unsecured manner will impose millions in fines for the illegitimate use of the same data and will oblige firms to publicly report any attack suffered that has put their database at risk. The opposite of what the golden-haired man, Donald Trump, is proposing in the United States, where the president and his henchman at the FCC (AjitPai) want to

> free the telco from any responsibility for the use of their customers' personal data and even allow them to sell it to third parties without their consent. (El Mundo, 22 May 2017)

Privacy norms and privacy regulations are introduced as a means to protect the consumer. The latter is thereby interpreted as an entity worthy of (legal) protection where the GDPR is an appropriate means (a “progressive regulation”, readers are informed). The positive characterisation of the GDPR is juxtaposed rhetorically with the (bad) example of US legislation which serves to weaken (rather than strengthen) individual privacy rights. The article goes on:

> IN A HURRY. Seven out of ten companies may not arrive on time
>
> European regulations, like all those coming from Brussels, are a headache for companies across Europe, unable not only to implement the policy and technical changes required, but also to understand the law itself. A study published this week by NetApp highlighted this issue: more than 70 percent of organizations say they have some degree of concern about complying with the regulations within the stipulated time frame, but more serious is the palpable lack of knowledge about the GDPR in the business community: Germany is the best informed territory on the subject, yet only 17 percent of respondents say they understand the new regulations in their entirety. (El Mundo, 22 May 2017)

The article is overtly critical of the GDPR because, the argument goes, the new regulations will do more to harm businesses than to help consumers. In fact, if critics are right, the GDPR will not only cause high fines and reputational damages for businesses, it might also actually hamper net neutrality by “favouring large operators over seemingly irrelevant users”:

> RISKS. Not only economic, but also reputational damages
>
> If the worst omens are confirmed according to the adoption of the GDPR, companies will face not only millions of euros in sanctions, but also a loss of reputation that will further challenge privacy policies in Europe. That would give the advocates of the free use of personal data on the Internet wings.
>
> It will also help the advocates of ending the Net neutrality by favouring large operators over seemingly irrelevant users to the commercial proposals of commercial operators and, ultimately, it will also help the advocates of ending net neutrality through favouring large operators over seemingly irrelevant users. (El Mundo, 22 May 2017)

The article offers an argument which runs very much counter to the familiar narrative encountered in a GDPR context which centres on empowering consumers. Here, possible adverse effects for consumers are put into the foreground: Enforcing the GDPR, the argument goes, would cause reputational damages to European businesses of such a magnitude that it would effectively render the arguments of privacy opponents (or conversely: advocates of data trade) cogent.

In an article already analysed above (El Mundo, 31 January 2017), readers learn a lot about what makes data personal:

> 3. Need to report gaps. The amounts of the penalties are substantially increased and can reach up to 4% of total annual turnover, but the current document does not yet make it clear where, how and what needs to be reported. As a security incident is not easy to detect and investigate and obviously delays the reporting of it, this whole part needs to be clarified. As for us, the people and individuals who are so concerned, the regulation strengthens the definition of personal data which will be broader and will include identifiers such as: genetic, mental, cultural, economic and social identity. And not only that: obtaining consent must be clear and will require an affirmative response. A big step forward towards the proper use and protection of our fingerprint. (El Mundo, 31 January 2017)

The article deals with the responsibilities the GDPR puts on businesses when it comes to collecting and processing personal data. The language used to refer to personal data is telling here, as it underscores the notion that personal data are in some sense the property of the individual. Notice the term “fingerprint” in the last sentence. The section does not make any concrete reference to data processing activities. The reader does not learn what it might mean for a company to process personal data, but nevertheless learns that concerns about personal data are in order (“the people and individuals who are so concerned”). Personal data are introduced as individual “identifiers”, i.e. as information which can serve to (uniquely) identify individuals. Contrary to the article above, the above section employs a different construction of users-as-worthy-of-protection. This time, privacy legislation is interpreted as empowering both consumers and companies, thereby introducing the notion of consumer responsibility through the backdoor.

3.1.5 Constructing the User as Responsible: The Dilemma of Personal Data Collection

A *topos* which popped up frequently in the all three case studies (UK, Austria/Germany, and Spain) is that of individual responsibility. Consumers or end-users of digital products and services are imagined in some sense or other to be in control of what happens to their data and who are therefore responsible (at least to a degree). End-users are frequently referred to as subjects which are (supposed to be) in control of “their” data:

> "This information is among the most intimate in a person's life. Consumers must be able to control what companies do with them," said Natasha Duarte of the Centre for Democracy and Technology. (El Mundo, 29 March 2017)

Recall that data are frequently imagined as the data subject’s property (after all, this is what makes data “personal”). Control over data is therefore what ultimately guarantees privacy.

In an opinion piece by Eduardo Esparza in El Mundo (19 January 2017), we learn that it is in the hands of consumers to control their personal data:

> Privacy and data protection on the Internet are in the hands of consumers
>
> Technology has made our lives exceptionally easy. Now we can do business with the bank from home without queuing and paperwork, we can write and talk to a friend on the other side of the world through mobile applications, social networks or from the computer. We can search for information, buy all kinds of products, set up a business without having to pay the rent of a shop, work from home.... and more and more personal information is being stored on the Internet. (El Mundo, 19 January 2017)

The introductory paragraph to this opinion article gives an overtly positive, even optimistic characterization of the possibilities associated with the Internet. The paragraph is written entirely from a first-person-perspective, though in plural form. This suggests that the reader should empathize with the views expressed here. Speaking in terms of “we” and “us” reduces distance to what is being said. The other aspect of the paragraph which is striking lies in the characterization of the functions digital technologies serve. The aim of the paragraph is to represent these technologies as positive and helpful (though possibly disregarding other, more negative aspects). Rhetorically, this prepares the ground to introduce a notion of responsibility on the part of the user/consumer who (supposedly) gets so a lot from the Internet in exchange for very little in return. Readers only learn in the last line that there might be a problem with this situation: “[…] more and more personal information is stored on the Internet”. Since this information (it is assumed) belongs to the individuals in question (at least to a certain degree), this in principle beneficial situation produces a dilemma which is then resolved by appeal to individual responsibility. The familiar story goes something like this: ICT products and services are in general beneficial, but they only work if individuals are willing to share their data. Since there are many entities which would make illegitimate use of these data, individuals need to be reminded of their responsibility over their data. Only if individuals assume responsibility can they enjoy the benefits of the Internet.

> In this sense, can we be sure that our personal data is sufficiently protected? Cybercrime is a reality. According to the latest study on cybercrime in Spain carried out by the Secretary of State for Security, last year alone a total of 60,154 criminal acts were carried out on the Internet, of which 67.9% were computer frauds (swindles) and 16.8% were threats and coercion. In 2015, this type of crime left a total of 46,860 victims of cybercrime in our country. (El Mundo, 19 January 2017)

Tellingly, the above paragraph uses the passive voice when talking about personal data protection. The juxtaposition of this passive voice with the survey data of cybercrime incidents prepares the ground to confer responsibility on the individual. If – the paragraph suggests – the problem of cybercrime is real (which the sheer numbers suggest it is), and if one cannot be sure whether others (e.g. organisations handling personal data) can sufficiently provide for their safety, then it is plausible to assume that said responsibility should fall onto individuals. Again, the paragraph contains a variant of the dilemma sketched above. The “responsibilization” of individuals is made still more plausible by reference to changing dynamics in the field of cybercrime:

> Traditionally, banks have invested large amounts of time and money in data protection and fraud prevention, and every time a customer makes a transaction, technology tracking is carried out to warn of any anomalies that may occur, compared to the usual patterns of behaviour.

> These measures have led to a change in strategy and cyber-criminals are now attempting to gain control of personal data through users' passwords or by accessing sensitive information in their social networking accounts. Therefore, while financial institutions focus on building their own defences, they may be neglecting the fact that it may be their own clients who are unknowingly weakening them. (El Mundo, 19 January 2017)

The first of the above paragraphs serves to certify that the organisations involved in handling personal data (in this case, banks, where trust traditionally plays a huge part) are doing their part of the job. A similar argument was already encountered several times in the UK use case. Responsibility on the part of individual users is here constructed as necessitated by growing complexities. In fact, readers learn, it is the very measures banks have put into place to protect their customers’ data which have led cybercriminals to pursue other strategies geared more towards individual users as opposed to IT infrastructures. In a different article (El Mundo, 31 January 2017), the responsibilities of companies are acknowledged:

> When we talk about Digital Transformation and the large amount of personal and confidential data we handle in companies, we must be aware of the responsibility and challenges in the face of possible attacks and security breaches. In many cases we feel as if we are dancing with wolves' and - bearing in mind the entry into force of regulations that come on top of this dance such as the European Data Protection Regulation and the NISS - companies will have new obligations that affect the processing of data, and will increase people's privacy. […] (El Mundo, 31 January 2017)

Incidentally, the very strategies deployed by banks and other institutions in the name of cybersecurity also account for a certain diversification in the attack strategies (El Mundo, 19 January 2017):

From phishing attacks to data security breaches, the nature of the potential threat is, unfortunately, so varied that bank defence methods alone can no longer combat it. Privacy and data protection are being passed on to consumers for a number of reasons:

> On the one hand, poor customer data management practices can significantly increase the frequency and scope of attacks. A Dashlane study shows that the average Spaniard has 92 Internet accounts registered with the same email account and, taking into account Telesign's study, according to which 54% of people use five passwords or less for their online activity, a scammer can control a large part of a person's data relatively easily. On the other hand, the exponential growth of the dark web, where personal data can be sold anonymously, means that there is an attractive market for both opportunists and organized scammers. (El Mundo, 19 January 2017)

In the following paragraph, a notion of the Internet as a common good is invoked to justify the responsibility accorded to individuals:

> In the case of banks and businesses, it is virtually impossible to avoid damage to their reputation and potential loss of customers if they are not adequately supported in cases of identity theft. For customers, the confidence in the security provided by their bank and the lack of awareness of identity theft crimes means that they do not take responsibility for their actions on the Internet. So, in a world increasingly dependent on the Internet, it is everyone's responsibility to try to protect it. (El Mundo, 19 January 2017)

The above paragraph strikes familiar chords: confidence (of users in organisations), responsibility (of users for their personal data), and awareness (which needs to be raised). An interview with Tim Berners-Lee (dubbed the “father of the Internet” in the headline) in El Mundo (13 March 2017) links, in much the same vein as the above paragraph, the themes of privacy and trust when it comes to the Internet:

> In an open letter written for the foundation that watches over the improvement and availability of the WWW, Berners-Lee is concerned about "three new trends" that he considers that "we have to calm down so that the web can reach its authentic potential as a tool that serves humanity".(El Mundo, 13 March 2017)

What is particularly striking is the notion that the Internet should be a tool that serves humanity. The author of the above opinion piece echoes the same conviction when he argues that “it is everyone’s responsibility to protect it [the Internet]”. Both articles argue from a perspective of alienation which either needs to be reversed (Berners-Lee) or prevented (Esparza).

> The three issues he [Tim Berners-Lee] points to are the control of personal data, fake news and the opacity of politics. Berners-Lee points out that the lack of control over our personal data on the Internet creates "an effect on freedom of expression and prevents the web from being used to explore important issues" As regards fake news and opaque politics, he points out that "those with bad intentions can play a key role in spreading disinformation for their political or financial benefit" and wonders if it is democratic "that political advertising allows a campaign to say conflicting and totally opposite things to different groups".(El Mundo, 13 March 2017)

Staying with Berners-Lee’s opinion for a little while, we learn that there are three basic threats to the openness of the Internet which prevent it from reaching its true potential: control over personal data, fake news, and the opacity of politics. The third of these will be discussed later (see section …). Fake news is especially poignant when it comes to individual responsibility, because its exercise depends very much on having adequate and complete information. In total, Berners-Lee seems to be less optimistic than Esparza (the author of the opinion article about users’ responsibility) about according Internet users more responsibility. The next section (El Mundo, 19 January 2017) echoes the familiar *topos* of education as the future domain of banks:

> So perhaps it is time for financial institutions to look beyond the threat and see the challenge as a potential opportunity. To begin with, they could educate consumers about the risks and the measures they can take to protect themselves. While some financial institutions may wonder if this is their role,

> given the amount of money they lose because of fraud, perhaps the question banks should ask themselves is whether they can afford not to address the problem. (El Mundo, 19 January 2017)

Bank customers and users of apps are constructed as ignorant here, as potential targets of educational interventions. Recall that earlier, the same article had introduced “individualized” cybercriminal activity as a direct consequence of increased corporate security measures. Similar to Berners-Lee’s opinion, the article argues that empowerment (according end-users more responsibility) is a matter of better information (which is problematic given the existence of fake news). When that information is framed in terms of education, however, this creates resp. reinforces the notion of a power gap between banks and customers (after all, education involves a social status difference). The construction of users as responsible agents therefore depends, to an extent, on the construction of users as ignorant. The difference between the two articles discussed here seems to lie in the fact that one is inclined to accord users more responsibility, while the other argues that first a few problems outside the scope of individual influence need to be tackled. For banks and other businesses, there obviously is more at stake than the fight for a free Internet:

> By enabling people to make better security and fraud prevention decisions, backed by relevant and knowledgeable support when something goes wrong, banks can improve their reputation with customers. As a result, it would increase the customer's emotional affinity and loyalty to his bank, and reduce the amounts borne by the banks in relation to fraudulent activities. (El Mundo, 19 January 2017)

Education encourages responsibility which translates (more or less) directly into reputation and loyalty. Banks, the author argues, therefore have a stake in educating customers. Interestingly, while acknowledging that the surge in cybercriminal activities targeted at end users is a direct result from better IT security measures (a displacement effect) it remains silent on possible displacement effects due to behavioural changes of users. Arguably, when users change their behaviour and become more aware of risks, cybercriminal may change their attack strategies as well. Taking responsibility, the author goes on, may strengthen users’ emotional affinities which could, given due attention, be a factor in strengthening brand value as well.

The rest of Tim Berners-Lee’s opinion piece reads:

> Through the WWW Foundation, Berners-Lee is carrying out a five-year plan to improve this situation, although it already points out that the situation of Internet freedom has not stopped getting worse in the last six years and that two thirds of the population live in countries where there is censorship and where criticism of institutions can be condemned. (El Mundo, 13 March 2017)

In addition to fake news threatening freedom on the Internet, there are regions where there is downright censorship. However, given the role fake news and disinformation played (and will continue to play) in world politics, this is issue is Berners-Lee’s focus:

> Fake news are given a lot of attention since Donald Trump's victory, whether it's the blame for having played a role in his victory through platforms like Facebook, or whether it's simply pointed out as a problem of the giants of the world of technology. They are already taking action, but it seems that the effect of disinformation on the Internet is becoming increasingly clear and, ironically, difficult to deal with. (El Mundo, 13 March 2017)

The last paragraph provides a hint at the magnitude of the problem. Fake news, readers are reminded, are so endemic that they might have already begun to influence democratic processes. Information on the Internet is therefore a prime concern for those who want the Internet to serve humanity (and not merely a few special interest groups).

3.1.6 Data Collectors as Responsible and Trustworthy Agents

Concerning trust and reputation, banks are often cited as among the most trustworthy actors on the Internet (at least among businesses):

> Second, banks are generally among the most trusted brands in data security for consumers; according to Symantec's 2015 Privacy Status Report, 66% of respondents trusted banks for their personal data, and only hospitals and health care providers exceeded them in confidence by 69%. However, according to the Brand Generosity Report, 75% of those surveyed said that one of the attributes that they value most about banks is transparency and honesty, but the sector is hardly moving in this direction, since according to this study these features barely achieve a score of 2.80 out of 10. This means that there is already a great deal of goodwill and brand value on the part of customers towards financial institutions and that, at the moment, they are not being sufficiently strengthened. (El Mundo, 19 January 2017)

Effectively, the above section says that if anyone can be trusted on the Internet, it is banks. In addition to former statements made in the same article about the need to educate consumers, the thrust of the article becomes a little clearer: While banks and possibly other businesses are in fact well trusted and therefore should be seen as trustworthy (a non-sequitur, but this remains covert), users are described as untrustworthy and in need of education and training, because their behaviour on the Internet essentially makes them a liability for themselves (their own data and money) and for institutions such as banks. If consumers already trust banks, these institutions should then build upon said trust by expanding their services resp. data management activities:

> It is clear that it is important for customers to protect information, so banks should transform their proposals and take advantage of it. For example, if a bank extends its reach into consumers' lives by offering secure data storage services to help individuals protect their fingerprint, the sense of trust can only grow. There will come a time when this will make the decision to change banks more difficult, an opportunity too good to ignore. (El Mundo, 19 January 2017)

> This situation should be seen as a source of opportunity for the banking community. An opportunity to help customers protect themselves (and automatically protect the bank) and for financial institutions to put their organisation at the centre of more areas of people's lives, thus avoiding customer traffic and fostering more ingrained and long-lasting customer relationships. (El Mundo, 19 January 2017)

The paragraph begins by reinforcing two ideas: One, that information is an asset ("For whom?", one might ask) and two, that asset needs to be protected. This protection is further argued to be in the consumers' best interest (again: "Why?"). What this amounts to is only covertly stated in the second paragraph: The goal of enhanced consumer protection through enhanced consumer responsibility is to have "more ingrained and long-lasting customer relationships". The responsibility of consumers is therefore part of a larger strategy to enhance business for banks: If consumers believe that they should protect their information, then this can in turn be monetarized by banks through offering them the means to do so. Furnishing a notion of consumer responsibility thereby serves merely to introduce novel kinds of business models. Responsible agency is therefore nothing more than a driver of innovating business models: constructing consumers first as responsible for their data and then as worthy of protection opens up the space to commodify said protection. This commodification is cast in overtly positive terms ("An opportunity to help customers protect themselves"), but the reader is left to wonder: If consumers are indeed responsible, active agents of their own data, why would they need banks to take care of that for them?

3.2 Data Collection, Data Storage, and Data Processing

3.2.1 Personal Data as Correlates of (Data) Processing

An article in El País (5 June 2017) makes several comments on the way personal data are processed:

> An application not only collects data for use on the mobile phone itself. For example, maps send your location to a server managed by the app creator to calculate the directions from your location to your desired destination.
>
> The application can also send data anywhere. Like websites, many mobile programs are written combining various functions, pre-coded by other manufacturers and companies, in what are called "third-party libraries". These libraries help manufacturers track users' interests, connect to social networks, and make money by showing ads and other items without having to write them from scratch. (El País, 5 June 2017)

This time, data processing does not refer solely to some state-bureaucratic process but rather to something applications do in the name of companies. The presentation of the issues creates an image of an increasingly transparent mobile phone user (but only transparent for unnamed “servers” which underscores the imagery of a loss of control over personal data. The data collection process is presented as, in some instances, necessary for the apps to function properly. Still, this is described as happening in a way which makes it very difficult, if not impossible, for end-users to determine what exactly happens to their data, emphasizing the implied sense of a loss of control. If anything, this is exacerbated in the next section:

> However, apart from their valuable help, most libraries also collect sensitive data and send it to their servers or to another outside company. The most competent library creators are able to create detailed digital user profiles. For example, one person may give permission to one application to know its location, and another may give access to their contacts. In principle, both are separate permissions, one for each application, but if the two use the same third-party library and share different pieces of information, the library creator can connect those fragments.
>
> Users will never know, because applications don't have to tell them about the program libraries they use. In addition, very few applications make their privacy policy public and, if they do, it is usually through extensive legal documents that a normal person does not read, much less understand. (El País, 5 June 2017)

The two paragraphs are rife with allusions to the technical capabilities of companies and the ways these might be used against the end-users’ best interests. The capabilities of data collectors are described in a way reminiscent of state surveillance activities, which is remarkable insofar as the end-user would suspect that it is not the primary job of mobile apps to collect data (which happens, but is merely incidental to some other goal). Privacy policies are discussed here not as a means to enlighten and empower the end users, but rather to confuse them and conceal certain activities. This is the point of departure of the study described in the article, which is to empower users and give them real control (as opposed to pseudo-control), as the reader learns in the next paragraph:

> The purpose of our study is to make known how much data may be being collected without users knowing it, and to give users more control over their data. To get a picture of what data is being collected and transmitted from mobile phones, we have developed our own free Android app, called Lumen Privacy Monitor. The application analyses the traffic sent by apps to reveal which applications and services over the Internet actively collect personal data. (El País, 5 June 2017)

The above paragraph describes the aim of the author’s research project. What is interesting for present purposes is the framing of privacy and transparency it contains, because it can be suspected that the construction of these issues as found in media discourses subtly influences public opinion. The approach is to develop an app that monitors data traffic on mobile phones. The overarching narrative is one of user empowerment and of (re)gaining control:

> Because Lumen's goal is transparency, a phone user can see in real time what information is collected by the applications they have installed and with whom they share that information. We try to show the details of hidden application behaviour in an easy to understand way. Research is also important, so we ask users if they allow us to collect some data about what Lumen sees their applications doing, but they don't include any personal or privacy sensitive data. This exclusive access allows us to study how mobile apps collect personal data from the user and with whom they share it on an unprecedented scale. (El País, 5 June 2017)

It remains to be seen whether it helps users when they are able to monitor the data traffic their apps create. In any case, the target of interventions is the user, not (as could be imagined) the companies making and using those apps. Nowhere in these paragraphs are these practices (openly) questioned. This suggests that ultimately, it falls upon the user to manage their own data and to (re)gain control. Transparency therefore does not mean abolition. The goal is not, strictly speaking, to control data collection, but rather for users to be aware of the kinds of data collected about them.

> In particular, Lumen tracks which applications are running on the user's terminal, whether they are transmitting privacy sensitive data from the phone, to which Web sites they send it, the network protocol they use, and what kind of personal information each application sends to each site. Lumen analyses app traffic on the same terminal and removes any information related to the person's identity before sending them to us for study. For example, if Google Maps records a user's GPS location and sends the specific address to maps.google.com, Lumen tells us, "Google Maps found a GPS location and sent it to maps.google.com," but not where that person actually is. (El País, 5 June 2017)

The app developed by the project is then used to analyse the data collection activities of other apps. The next two paragraphs give a drastic description of the extent of the problem:

> Trackers are everywhere.
>
> Since October 2015, more than 1,600 people have used Lumen, allowing us to analyse more than 5,000 applications. We discovered 598 websites that were probably tracking users for advertising purposes, including social network service providers such as Facebook, large Internet companies such as Google and Yahoo, and Web marketing companies that operate under the umbrella of Internet service providers such as Verizon and Wireless.
>
> We found that more than 70% of the applications we analysed connected with at least one tracker, and 15% connected with five or more. One in four trackers collected at least one device identifier, such as the phone number or the terminal's unique 15-digit IMEI number. Unique identifiers are crucial for Internet tracking services because they allow different types of personal data provided by different applications to be connected to a particular person or device. Most users, including those with a command of privacy, are unaware of these hidden practices. (El País, 5 June 2017)

The above paragraphs hint at the extent of the problem. Supposedly, “[t]rackers are everywhere”, which means that the scale of the problem is arguably quite large. Seeing as how it is very difficult (if not impossible) for users to assess if and when their behaviour is being tracked, such numbers serve a double function: On the one hand, giving numbers literally fleshes out an otherwise intractable phenomenon. On the other hand, the phenomenon of data tracking is normalized and rationalized by assigning numbers. If something is countable, it loses some of its otherworldly character. Thereby, the otherwise abstract phenomena of personal data collection and personal data use are given a somewhat more tangible form.

> More than just a mobile problem
>
> Tracking users via their mobile devices is only part of a larger problem. More than half of the tracking applications we have identified also work through the web pages. Thanks to this technique, called "inter-device tracking", service providers can create a much more complete profile of one's image on the Internet. (El País, 5 June 2017)

Tracking, readers are reminded, is a problem which should be familiar from another domain, namely websites tracking user behaviour through e.g. cookies. Technically, the section informs readers, it is now possible to combine user profiles from different sources. This is arguably the alternative meaning of transparency, where users become increasingly transparent for websites and Internet companies. Such a blunt statement does sound alarming, but the problem seems to be even worse, as the following paragraph suggests:

> On the other hand, each monitoring site does not have to be independent of the others. Some are owned by the same legal entity, while others may be taken over in future mergers. For example, Alphabet, Google's parent company, owns several of the tracking domains we investigate, including Google Analytics, DoubleClick or AdMob, and collects data from more than 48% of the applications we analyse through them. (El País, 5 June 2017)

It seems that tracking is not a marginal problem confined to obscure, insignificant brands. Rather, the names given in the paragraph are some of the Big Players on the Internet. Also, these activities supposedly surpass national jurisdictions:

> The laws of the users' countries of origin do not protect their identities on the Internet. We have found that data is transferred across national borders, and often ends up in countries whose privacy laws are of dubious confidence. More than 60% of the connections to tracking sites are made with servers located in the United States, United Kingdom, France, Singapore, China and South Korea, six countries that have implemented mass surveillance technologies. Government agencies may have access to the data on these sites, even if users are in countries with stricter privacy laws, such as Germany, Switzerland or Spain. (El País, 5 June 2017)

The paragraph utters the additional worry that traditional instruments of consumer protection are ineffective when it comes to data collection. And it is not just companies who might be interested in those data, as suggested above: In many cases, data collected end up in countries with either less-than-strict privacy laws or with government surveillance programs already in place.

As will be elaborated on in the UK case study, children are imagined as users who are particularly vulnerable:

> Even more worrying is that we have observed the presence of trackers in applications intended for children. When we analysed 111 children's apps in the lab, we found that 11 of them were filtering the MAC address, a unique identifier of the wireless router to which they were connected. This is a problem, because it is easy to search the Internet for physical locations associated with specific MAC addresses. Collecting private information from children, including where they are located, their accounts and other unique identifiers, is a potential violation of the Federal Trade Commission's rules for protecting children's privacy. (El País, 5 June 2017)

And as if the above sections were not enough to be deeply worrying, the author suggests that the study may have been too small to catch the full extent of the problem:

> A simple glimpse
>
> Although they include many of the most widely used Android apps, our data is a small sample of users and applications and therefore probably represents a small set of all possible crawlers. Our findings may only be scratching the surface of what is thought to be a much larger problem spanning multiple regulatory jurisdictions, devices and platforms. (El País, 5 June 2017)

The article in El País then goes on to connect issues of privacy with issues of transparency:

> People being more willing to pay creators to use the applications might be helpful, but it doesn't solve everything. We found that, while paid applications often contact fewer tracking sites, they also track users and connect to third-party tracking services.
>
> The key lies in transparency, education and a strong legal framework. Users need to know what information related to them is being collected, who is collecting it, and what it is being used for. Only then can we as a society decide what protections are needed and put them into practice. Our findings, as well as those of many other researchers, can help turn the tables and track the trackers. (El País, 5 June 2017)

The problem, the reader learns, lies in the fact that transparency is ambiguous. It can either refer to the users becoming increasingly transparent to companies and state bureaucracies (which is the overarching theme of the present article), or it can refer to the data collection (and processing) activities of organisations being made transparent. What is interesting is that here, much like in many other discussions of transparency, the term remains more or less undefined. Given its inherent ambiguity, this is rather surprising. It does not ask for a limitation of data collection activities, but merely for data collection to be transparent so that users can at least comprehend what organisations know about them. Nowhere does the section question the legitimacy of data collection activities, though. Data collection is taken at face value, as something all of us have to live with. Knowing what data collectors know about us is a prerequisite for adequate control, the last paragraph argues. The overarching narrative of the article therefore does not question data collection in general. Rather, it states that data collection has positive effects and negative effects, and in order to enjoy the former, it is necessary to control the latter.

Having discussed personal data collection at length from the perspective of the end user, we now turn to personal data processing from organisations' point of view. Personal data processing will have to change due to the GDPR, the following piece from El Mundo (31 January 2017) argues:

> 1. Audit vs. risk analysis. It will be the company's responsibility to carry out the risk analysis and establish the controls and measures it will put in place to comply with the regulations. Besides, you'll have to document it. We are moving from a reactive to a proactive audit vision, in which the company is responsible. Before, you only complied and now you have to comply and show that you are complying. (El Mundo, 31 January 2017)

The paragraph discusses issues of responsibility. While it will be shown below how users are constructed as responsible by Spanish media, the above section talks about responsibilities of organizations. Clearly, businesses (and not their customers) are the object of regulation introduced through the GDPR. While users are constructed as data subjects with responsibilities and some degree of control over their data, businesses and other organizations (the entities which collect and process personal data) are imagined as entities which have to be regulated in some form and which therefore can be forced to comply with regulations.

> 2. Implementation of the figure of the DPO. Spanish companies that comply with certain requirements - mainly those that carry out periodic and systematic large-scale data monitoring or manage data considered sensitive - will have to appoint or hire a data protection officer (DPO). A study by the

> International Association of Privacy Professionals (AIPP) conducted in April 2016 indicated that it will affect 28,000 businesses including public sector institutions. Experts warn that there is a shortage of professionals in this field, as well as in the entire cybersecurity industry. In the fight for talent there is a job opportunity for our young people and other professionals who want to turn their careers around. (El Mundo, 31 January 2017)

The second paragraph talks about data processing. The activities associated with data processing are described as requiring increased monitoring under the GDPR. Even here, the reader is reminded that there is a shortage of competent professionals ("fight for talent"), which puts the burden of education upon the workforce. Even where the overt topic is the responsibility of companies, the pressure is entirely on individuals.

> Individuals and companies are in luck. We must both focus all our efforts on protecting our most important asset: information. Slowly but surely, 2018 is just around the corner. (El Mundo, 31 January 2017)

Tellingly, the last paragraph talks about "individuals and companies", which supposedly "are in luck". (It is not explicated in any detail why that might be.). Individuals are the entity supposedly protected by the GDPR, while companies are those most affected by the new regulation. On the face of it, citing the two in one breath is incomprehensible. At a second glance, however, the short section contains a familiar theme: While overtly acknowledging that the GDPR will impact data processing activities of companies, it also covertly states that individuals will also be made responsible, if in a very different way. The section further suggests that information is "our most important asset". While that may be fairly obvious for businesses, it is less obvious in what sense information can be an asset to individuals given current legislation. In any case, the section underwrites the assumption that ultimately, individuals and businesses share the same interests.

3.2.2 Illegal Data Collection: What is a Data Breach?

The following section discusses three articles (El Mundo, 8 and 16 May 2017, and El Mundo, 9 February 2017) to analyse how the notion of a "data breach" is constructed in Spanish media. The first article discusses an incident of such a data breach and one way personal data might be obtained illicitly:

> The message in question states that 'Netflix is giving away a year's free subscription'. It comes with a fake link that hides its appearance because it contains the name and image of the video service.
>
> The hoax has spread quickly in the application thanks to the strategy of asking to forward the message to ten user contacts. Once this step is completed, the cybercriminals ask victims to enter their phone number in order to obtain the supposed free accounts on the popular video platform. (El Mundo, 8 May 2017)

The article discusses a case of phishing for personal data on WhatsApp (this incident might therefore also be labelled a case of "smishing"). The perpetrators used a fake prize (a free Netflix subscription) to trick users into giving away their phone number. What makes this a case of illicit data collection, as opposed to the forms of data collection discussed at length above? After all, there are many instances of websites or mobile apps collecting personal data, often without the data subject's consent or with consent hidden in some elaborate privacy policy (e.g., Facebook has been accused of doing this in the past). Here, the reader is supposed to think that this is a case of illicit data collection, through the use of terms such as "hoax" and "cybercriminals" (after all, crime is defined as an illicit or even illegal activity). The next two paragraphs expand on this theme by suggesting that the activity in question is an empty "promise":

> Behind these promises, according to police reports, lies a dangerous scam aimed at obtaining the user's personal data and telephone number. It is recommended that you do not click on the link that accompanies the message, which would also expose you to malware infection on the phone you use, according to the law enforcement account.
>
> With this hoax, WhatsApp records its second episode in less than a week, as another fake was recently released, warning that there were only 530 new accounts left in the messaging service, as well as that it would become paid. Police again used their Twitter account to warn about this problem. (El Mundo, 8 May 2017)

The following article (El Mundo, 9 February 2017) reports the illegal use of personal data by the Catalan National Assembly to conduct surveys prior to the Independence Referendum.

> ANC calls for donations to pay 250,000 euro fine for illegal use of data
>
> The Catalan National Assembly (ANC) has called for the collection of the nearly € 250,000 it has been fined for illegally using personal data in the survey it conducted before 9 November.
>
> "We don't believe in coincidences. This embargo comes after the extraordinary mobilization of the 6-F[the demonstration in support of Mas before he testified before the judge] and its international repercussions, which has increased the pressure on the State," argues the pro-independence organization. […] (El Mundo, 9 February 2017)

The story itself is not important for present purposes. Here, it only matters what readers learn about illegal data use. What is relevant for the present purpose is again the way the above paragraphs introduce – explicitly and implicitly – the notion of illegal (or illicit) data collection (data breach). The above paragraph is more explicit as it labels the personal data (the reader does not learn what data exactly) collected by the ANC as illegal. Since the incident is politically loaded (it happened in the context of the Catalan independence referendum, apparently), reference to "illegal" activities might be motivated by other considerations. In any case, there seems to be two basic kinds of data collection activities: Those that are licit or legal, and those that are illicit or illegal.

An article in El Mundo (16 May 2017) covers supposedly illicit data processing activities by Spanish tax authorities:

> The Data Protection Authority concludes that the ATC uses tax data legally
>
> Requires corrective measures from the ATC in data retention and password management
>
> The Catalan Data Protection Authority (APDCat) has concluded that the Catalan Tax Agency (ATC) "does not process identifying data, or tax data, that has been obtained irregularly or illegally".
>
> This is clear from the audit commissioned from the APDC at by the Regional Ministry of Vice Presidency and Economy and Finance of the Generalitat following the declarations of former Senator Santi Vidal regarding the fact that the ATC could have tax data on taxpayers and that they could have been obtained illegally, informed the Generalitat in a statement. (El Mundo, 16 May 2017)

Apparently, the public authority dealing with tax data was charged with somehow misusing these data but then cleared. To be more precise, the section states that the tax agency does process (personal) data, but none of these data has been obtained illegally. The report acknowledges, however, that the Spanish tax authority has problems when it comes to managing these data and that it might have been retaining them illegally. The reader is left with some unease regarding apparently opaque data collection practices. What is striking here is the way the article talks about the authority's misguided behaviour, but leaves out individual tax payers and how they might be affected.

> The audit adds that the ATC has these data "exclusively for the exercise of its functions", and does not use them for incompatible purposes or functions that are not attributed to it, in accordance with article 4.2 of Organic Law 15/1999 of 13 December on the protection of personal data.
>
> However, the APDC at points out that there are certain circumstances related to the processing of personal data by the agency that "do not comply" with the provisions of the data protection regulations, and therefore it requests corrective measures in certain fields. (El Mundo, 16 May 2017)

The authority supposedly was less than careful at complying with data protection regulations.

> Specifically, and with regard to the ATC's handing over to the State Agency of the Tax Administration of data on large families or persons with disabled dependents for the purpose of making personal income tax deductions, the Authority considers that the role of the ATC in the processing of this data, which it does at the request of the Aeat, should be regulated "specifically".
>
> For this reason, the ATC will sign an agreement with the Ministry of Labour, Social Affairs and Families to commission the processing, which will clearly specify the role of the Catalan tax office in the processing of this information.

Regardless of whether the allegations voiced here are true, the article fuels suspicions that personal data are not always handled with appropriate care. In any case, personal data are imagined as something to be handled by authorities (and possibly other organisations), and that there are (better or worse) standards to do so. The article thereby reminds readers that personal data are being collected (though it does not specify what these are) and that this might impact individuals.

3.2.3 Big Data, Privacy, and Convenience

Why are personal data collected? What happens when they are collected, and what purpose does data collection have with respect to consumer needs? The first article comes from El Mundo (26 April 2017) and deals with a new product by e-commerce firm Amazon:

> What should I wear? Whatever Amazon says!
>
> Alexa, Amazon's artificial intelligence, has learned to see and her first job will be to judge how we dress. The e-commerce giant today announced Echo Look, a closet camera that takes full-body photos and videos using voice commands and displays the results on the phone. (El Mundo, 26 April 2017)

What is striking here is the way the familiar *topos* of (consumer) (ir)responsibility is constructed here. Amazon’s Echo Look is introduced as a device which is designed to help users in finding appropriate outfits to wear. The headline is telling in this respect because it suggests that users should wear “Whatever Amazon says”. If empowerment is the overt theme of many public discourses concerning personal data, this is a case of taking away responsibility from consumers and according it to a big data-fuelled device. Although not explicitly argued in the text, it echoes themes that are familiar from other articles in the sample, namely a notion of increased complexity which Amazon’s device is supposed to cure. While overtly empowering users to take care of more important things than wardrobes, it simultaneously takes away responsibility from them. Additionally, the device collects a huge amount of data:

> These photos and videos can be saved to have a historical archive of the combinations that have been used or sent to friends with a couple of clicks on the screen. The device can also help you choose between two different dresses or garments by analysing the image and comparing the options with the latest trends. (El Mundo, 26 April 2017)

Here, the notion of empowerment pops up again: “The device can also help you choose…”. Incidentally, the paragraph reinforces aestheticist-hedonistic values by suggesting that it is somehow important to dress according to “the latest trends”. The next paragraph tells readers that the device is designed to supplement the shortcomings of “traditional mirrors”:

> The camera includes a depth sensor that is capable of isolating the subject, slightly blurring the background like a camera with a small depth of field and thus better highlighting the person being photographed. One of the advantages over a traditional mirror is that it allows you to see how your clothes look from any angle. (El Mundo, 26 April 2017)

Amazon was careful enough to think of privacy-conscious users, though:

> The proposal complements Amazon's growing collection of Echo devices but, like the company's speakers, is currently available only in the U.S. The price of the device is $200 and for the most privacy-conscious users in the bedroom it includes a button on the side that completely blocks listening and recording. For Amazon, in any case, this device could become a valuable source of personal data with which to refine product recommendations within its store. (El Mundo, 26 April 2017)

Only in the last sentence does the reader learn what might be considered Amazon’s actual motivation, namely to sell a means of additional data collection. The tone of the article suggests that trading off privacy for a little convenience is the right thing to do.

Banking is the subject of the next article (El Mundo, 30 May 2017):

> From the individual to the context in modern banking

> In these times when Big Data has become a hackneyed term almost meaningless, there is one type of company that really exemplifies what it means to know everything about its customers: banking. (El Mundo, 30 May 2017)

> Through our financial habits, we can know everything: from our customs and hobbies, to the location of our home and work, the challenge now is that it is not our actions that tell us how we are, but our friendships. (El Mundo, 30 May 2017)

This sounds terribly alarming, even though the paragraph is written in a very matter-of-factly tone. Notice how the headline suggests that banks literally give away money without asking anything in return. No wonder they need to install some way to approve their beneficial’s trustworthiness. The collection of data about us might impinge on our friends and families as well:

> Analysing our friendships to give us money

> A good example of this - and not the only one - is Banco Santander, a financial institution that is working on what they call data science scoring to understand how our environment influences our quality as a banking customer. "We want to go beyond the individual and understand how our social relationships can be good indicators when granting a loan or securing a certain product," the bank's sources explain to this journalist. (El Mundo, 30 May 2017)

The *topos* of trust and trustworthiness are introduced in the next section, though now not from the consumers’ vantage point:

> The aim is to find out if we can be trusted on the basis of our usual transfers (if we have a couple in trouble to whom we usually lend money, if our family is going through a bad time, if we have regular transfers from relatives that complement our salary, etc.) Contextual data that will condition our

> personal financial situation when this technology is definitively integrated into the core of the bank. (El Mundo, 30 May 2017)

The paragraph develops a particular notion of trustworthiness which puts it very close to reliability: If a person reliably pays their bills they can be trusted. This involves very personal aspects of people’s lives, such as whether they are able to support themselves or whether they receive regular financial aids. On the face of it, this description of possibilities must sound alarming to readers. Nevertheless, the next paragraph starts by describing the benefits:

> The benefits in this new way of scoring seem obvious, while the entity will have much more information about us to rely on and that, at times, can cover those dark spots that many have in their accounts. However, the risks of taking this social scoring to the extreme are also clear. From a lax or too light-hearted analysis based on these social relationships, to the eternal dilemma of privacy. (El Mundo, 30 May 2017)

The paragraph seems critical of social scoring by banks at first glance. However, it is clear from the penultimate sentence that the author is generally in favour of social scoring, as it remains unexplained what is meant by “extreme”. Up to which point, one might ask, would it be okay to score clients, and when does it become illicit? Recall that what is licit and illicit is a matter of (social) construction and negotiation. The last sentence is also revealing in this regard, as it fleshes out a different aspect of the same dilemma: If one uses Big Data for social scoring, one better do it “all the way down”, because a “lax or too light-hearted” analysis runs the risk of arriving at the “wrong” conclusions about the data subjects. The last paragraph (finally) addresses some of these questions:

> Is it really legitimate for our bank to know who our partner is or to qualify our friends because of their importance to us - even if we don't want to? To what extent does this Big Data become a Big Brother who knows everything about us? Taking advantage of all our personal data seems like a different matter when third parties enter the equation. (El Mundo, 30 May 2017)

3.2.4 Constructing Personal Data as Endangered

Spanish daily newspaper El País (5 June 2017) reports the following story on the way mobile apps can be used to collect personal data of mobile phone holders and track them. The article is written by an academic who studies data collection activities. Therefore, the article is not typical of daily news articles on any subject. On the other hand, it has become customary for many newspapers (in particular “quality” newspapers) to regularly invite experts to write on various issues of public interest. In any case, the analyses summarized here do not aim to understand the viewpoint of any specific social group, be they journalists, “experts”, “end-users” or what have you. As before, it is based on the much simpler hypothesis that people in Spain, much like everywhere, read newspapers and form opinions based, among other things, on what they read. Therefore, any and all news items on personal data and data protection are potentially relevant here. The analysis deals with imaginations of the rather very elusive area of personal data. How are personal data and surrounding issues described and contextualized? In what ways are personal data envisioned by newspapers?

> More than 70% of mobile applications transmit personal data to tracking companies.
>
> Our mobile phones can reveal a lot about us: where we live and work; who our family, friends and acquaintances are; how we communicate with them (and even what we communicate), as well as our personal habits. With all this information stored on the devices, it's no wonder that users take steps to protect their privacy, such as using personal identification numbers or access codes to unlock their phone. (El País, 5 June 2017)

The framing the article chooses in the first paragraph is interesting, insofar as it is (or seems to be) quite far removed from constructions of the end-user as ignorant which should be familiar from the UK case. Even though the paragraph starts by acknowledging the (quite large) dimensions of the problem, it is written in a confident and rather empowering tone. Users are imagined here as capable agents and knowledgeable controllers of their own data, which creates an altogether optimistic image of data protection. The article goes on to explain the way these apps work when collecting personal data:

> When Internet users install a new Android or iOS application, it asks the user for permission before accessing personal information. Overall, this is positive. In addition, some of the information collected by these applications is necessary for them to function properly. For example, a mobile map would be much less useful if you could not use GPS data to find a location.
>
> But, once the app has permission to collect that information, it can share your data with whomever its creator wants, allowing third-party companies to track where you are, how fast you're moving, and what you're doing. (El País, 5 June 2017)

The applications the article talks about are mundane, and it can be assumed that a large proportion of the population has installed at least a few such apps on their phones. This, in conjunction with the above description of their mundane workings, creates a rather worrisome atmosphere, suggesting that one’s personal data are unsafe. The language employed in the two paragraphs is telling, as it invokes opacity (of the data collection process) by reference to e.g. “third-party companies”. The first paragraph of the article (top of the page) is telling as well, as it begins with the suggestion that “our phones can reveal a lot about us”. The phrase suggests that information about individuals is usually hidden in some way or other and that this is the default case. Unless individuals use digital devices, this information can remain hidden. Only when devices such as smartphones are employed does data collection become an issue (of course, the matter is not that simple, as there are other possible means of surveillance). However, with virtually everyone using digital technologies in some way, this might no longer be the default option.

> It is difficult to know what users can do about it. Preventing sensitive information from leaving the phone may affect the operation of the application or the user experience. An application may refuse to work if it cannot load advertising. In fact, blocking ads is detrimental to application developers by depriving them of a source of income to support their work with programs that are generally free to users. (El País, 5 June 2017)

Eventually, data processing and collection are matters of user experience. This suggests that users can influence the amount of data collected and processed only to a very limited extent, insofar as this impinges on the functionalities of their devices or apps. The argument is familiar and has the structure of a trade-off (in fact, two trade-offs are mentioned in the above paragraph). Lest users agree to data collection they won’t be able to reap the benefits of digital technologies. What remains covert, however, is the fact that there is a difference between the amount of data collection necessary for devices to work and the factual amount of data collected. In many cases, there is a possibility to restrict data collection.

4 Case Study II: Cyberspace as a "Crime Problem"[6] (UK)

4.1 Cyber Threats: Key Issues and Incidents

4.1.1 Attacks on Financial Institutions and their Customers

Attacks on financial institutions are frequently reported and are therefore (presumably) quite frequent in the UK (and not just the UK, of course). The frequent breaches serve to highlight the (apparent) need for more and better cybersecurity measures with consequences for SMEs, corporations, financial institutions and individuals in terms of (a lack of) skills and threats. The Insider (02 March 2017) makes a connection to the complexity of banks' IT systems. However, large incidents reported and actually named are few.

The UK version of the International Business Times (07 May 2017) reports an initiative by UK-based bank Barclays to "help tackle online crime". The initiative is based upon a three-pronged approach: information, tools and tips (ibid.). The strategy seems to involve empowering customers to take control over e.g. daily withdrawal limits. As far as cooperation with LEAs goes, employees would be given access to a police hotline (ibid.). Additionally, Barclays launched an awareness campaign and a toll for digital self-assessment. All these measures move the intuitional cybersecurity systems in the background and point towards an individualization of responsibility. The article mentions a tension between confidence in and knowledge about digital technologies, a tension which seems to be at the heart of Barclays' strategy. The reason for the reported rise in cybercriminal activity is hypothesized to lie in this "safety gap". Again, cybersecurity is framed as a largely individual issue. Tellingly, the article closes with a statement of Barclays' CEO which constructs cybercrime as a national resilience issue. The use of an exclusive "we" in his statement ("we all need to boost our digital safety levels") suggests two things: one, cybercrime is a matter of having a national "edge", and two, the responsibility to reach that "edge" is a thoroughly individual responsibility.

The same newspaper reports about a new kind of malware supposedly targeting UK-based financial institutions. The malware (The International Business Times speaks of a Trojan) attacked "a slew of private banks, wealth management firms, investment companies and insurance businesses" (28 April 2017). Online news outlet Metro (23 January 2017) reports a "major cyber attack" which targeted three banks (Lloyds, Halifax, and Bank of Scotland). The attack itself was a Distributed Denial of Service Attack (sending large numbers of automated but fake requests in order to crash websites with the aim of collecting a ransom). According to Lloyds, no accounts were compromised and customers were supposedly able to access their accounts after one failed login. The largest cyberattack in the UK was targeted against Tesco Bank (November 2016), which left 20 000 customers robbed. MPs argued that incidents such as this one (with considerable individual harm) call, not for more empowerment (i.e., individual responsibility), but rather for more scrutiny and accountability on the part of financial institutions (ibid.)

4.1.2 Perpetrators, Culprits, and Victims: Cybercriminals in the Press

How are incidents of cybercrime such as fraud (and other financial crimes) reported in the British press? How are these incidents framed by different newspapers? In what ways do European values feature in these framings?

[6] The title is inspired by the work of David Wall, who described the "Rise of the Internet as 'crime problem'", see Wall, David (2011). Criminalising cyberspace: the rise of the Internet as a 'crime problem', in: Jewkes, Yvonne / Yar, Majid: Handbook of Internet Crime, Routledge.

On April 12, 2017, the Daily Mail reports on a cyber scam that hit the Santander bank. The article is about the way the bank denies responsibility in the form of impersonal letters to scammed customers. As the Daily Mail largely follows a personalizing, informal style of reporting, the article about the Santander cyber scam highlights the perspective of the fraud victims (i.e., Santander's customers) and demands the bank take responsibility. The article contains hints at its (imagined) target audience when it portrays Santander as an impersonal institution with apparently incomprehensible policies, whereas the article sympathizes with the scam victims and empathizes with them through emphasizing their helplessness and the responsibilities of Santander.

An incident that is frequently reported by the Sun, the Daily Mirror, and the Daily Express concerns former Premier League football player Nile Ranger's conviction for banking fraud. These newspapers adopt a personalizing style of reporting which focuses on the personality and biography of this particular perpetrator. In most cases of cybercrime, the perpetrators are unknown and do not lend themselves easily to this style of reporting. In such cases, the mentioned news outlets focus on the perspective of their (imagined) audience. This is especially visible in reports about online fraud such as banking scams where these outlets frequently take position for their targeted audience. In general, trust among their readership in institutions such as banks, but also IT infrastructure in general, is described by these outlets to be low (sometimes by reference to survey data). The Nile Ranger case is particularly telling of the personalizing reporting style of media outlets such as The Sun and Express, especially since other newspapers do not even mention the case. Here is a description of the incident published by Express (24 May 2017):

> Ex-Newcastle United striker Nile Ranger jailed for online bank fraud
>
> FORMER Premier League footballer Nile Ranger has been jailed for eight months after plotting to swindle more that £2,000 from a family doctor's bank account.
>
> Nile Ranger has been jailed after plotting to swindle more that £2,000 from a doctor's bank account
>
> The ex-Newcastle United striker got hold of the personal bank details of Dr Diana Bloss and transferred £2,090.23 into a friend's account before moving it into his own.
>
> Ranger, 26, a former England Under 19 international who now plays for League One Southend United, obtained the details of the GP's online HSBC account and transferred the money into the Santander account of his unwitting friend, Philippe Kane.
>
> The footballer tricked Mr Kane to allow the stolen cash to be transferred from the victim into his account then into Ranger's account.
>
> Co-conspirator Aseany Duncan, who got hold of the details of Dr Bloss, along with more than 500 potential victims' personal details, paid for a night at a Premier Inn with girlfriend, Reanne Morgan, and bought a takeaway with the cash. (The Express, 24 May 2017)

The entire article is written in a fallen-hero-kind of jargon, which is invoked in the first line ("ex-Newcastle United striker Nile Ranger…"). The piece is interesting insofar as it presents a rare occasion to examine reports about cybercriminals (even though Ranger's case is not very interesting from a technical or a sociological perspective). Additionally, it offers some details about the attempted fraud. The Sun (11 January 2017) offers a much more personalizing, emotional account of the case, focusing on the people involved rather than on the details of the case:

> FOOTIE FRAUDSTER Former Newcastle United footballer Nile Ranger admits swindling vulnerable woman out of £2,000 in online banking fraud
>
> Ranger signed a contract to stay at Southend United until summer 2020 in December

> FORMER premier league star Nile Ranger admitted swindling a vulnerable woman out of £2,090 in an online banking fraud today.
>
> Ranger, 25, obtained the bank details of his victim and transferred the money from her account.
>
> The cash was paid into the bank account of a man described as an "innocent third party".
>
> Dressed in a green bomber jacket and jeans, the former Newcastle Utd striker admitted conspiracy to defraud but denied money laundering when he appeared at Wood Green Crown Court.
>
> The prosecution said they would not be seeking a trial against Ranger on the money laundering charge. (The Sun, 11 January 2017)

What is particularly striking is the way the jargon of the article asks its readers to empathize with the fraud victim ("swindling vulnerable woman out of £2,000"). In general, the article follows a rather informal reporting style. The reference to Ranger's exterior might serve to describe him as somehow disrespectful of the court (because he failed to show up in formal clothing), underlining his criminal intent.

A Sun article following Nile Ranger's conviction (23 May 2017) testifies to their personalizing brand of journalism:

> He has been in trouble since the age of 15, when he was sent to a Young Offenders Institute for his part in a street robbery in London.
>
> Since becoming a professional footballer, he has been involved in a host of incidents, including posing with a replica gun, being charged with being drunk and disorderly, being fined by the FA for making homophobic comments, being fined for causing criminal damage and being found not guilty of rape. (The Sun, 23 May 2017)

Cybercrime is here (meaning The Sun) portrayed as an issue largely resulting from individual pathologies. While it may be that Ranger has the biography of a young offender, these biographical details have nothing in particular to do with cybercrime, but they do ask the imagined readers to distance themselves from Ranger.

4.1.3 Identity Theft: How to steal Personal Data

One of the most common cybercrimes targeted at individuals is identity theft, whereby individuals are tricked into giving away personal data such as bank account or credit card details which are then used to make purchases in that person's name. The social engineering tactics behind it are especially problematic as they seem to reinforce the role of the individual in tackling cybercrime. The Daily Mail (31 March 2017) reports a particular case of identity theft that makes do largely without IT:

> Criminals are also turning to a more basic method of attack, with fraud committed at cash machines jumping by almost a third to £43.1million.
>
> There have been increased reports of 'distraction thefts' at cash machines, with criminals also tampering with ATMs to trap people's cards.
>
> This enables them to get their hands on the card and the PIN number.
>
> This has allowed criminals to brazenly walk into shops and make purchases with stolen cards. (The Daily Mail, 31 March 2017)

This short paragraph includes a representation of social engineering techniques which are not restricted to IT. This alludes to a blurring of boundaries between online and offline crime: Personal data can be unwittingly given away offline as well. This dimension of cyberfraud invokes a rather basic notion of individual responsibility.

This personalization can also be observed in an article published by the Evening Press (2 March 2017):

> Detective Inspector Iain McPhail, of the Economic Crime and Financial Investigation Unit, said: “I would urge people to always be on your guard when you are contacted by email or by telephone by someone claiming to be from your bank, supplier of goods to your business or indeed any other company such as an electricity supplier, and especially if the call involves transferring money, providing or confirming your bank details.
>
> “I cannot emphasise enough, if you have the slightest doubt, attend your bank in person or highlight it to other members of your business.
>
> “Do not provide your details over the telephone or the computer. (The Evening Press, 2 March 2017)

Financial crime is here constructed not as something targeted at financial institutions, but much more frequently at individuals. The scams usually work in the same way, either via unsolicited calls or unsolicited emails/text messages/visits where someone claims that they are from the victim’s bank and asks for login details. The Sun (3 January 2017) offers advice on how to deal with social engineering, albeit in a style that is characterized by innuendo and simultaneously offering understanding for somewhat illicit activities:

> Tony Anscombe reveals the very dirty tricks cyber-crims use to target innocent people
>
> "Cybercriminals love to target people when their guard is down or if they are doing something that they would prefer to hide – such as viewing adult content websites.
>
> "A tactic that cybercriminals sometimes take is to publish an adult website offering users directly downloadable apps and encouraging the user to use the apps. (The Sun, 3 January 2017)

This paragraph offers an example of co-construction of end-users and criminals. The first sentence uses sexual language (“dirty tricks”) to describe criminals, which is then countered by a description of users as “innocent”, allowing readers to identify with “innocent” targets while simultaneously opening space for legitimate contempt. The second paragraph describes a supposedly typical attack strategy, “to target people when their guard is down”, which serves a double purpose: On the one hand, it serves to rhetorically exculpate the Sun’s readers, as it gives credence to the notion that nobody can be attentive and alert all the time. On the other hand, it alludes to the somewhat illicit habits of its readers and offering a somewhat apologetic framing which simultaneously sounds preachy no less. Presumably, people would be very vulnerable to cybercriminals indeed whilst visiting “adult content websites”. In any case, the paragraph is telling as to how the Sun imagines its readership.

The Daily Mail (31 March 2017) offers a familiar explanation for why cybercriminals increasingly target individuals:

> Efforts by lenders to bolster their IT defences against hackers have simply encouraged fraudsters to bombard individual customers with scams, according to Financial Fraud Action UK.
>
> Despite investing millions in tackling fraud, losses from fraud rose last year as banks became less effective at preventing scams.
>
> Losses from fraud on cards and credit cards jumped by 9 per cent to £618million last year – while total fraud including online scams – increased 2 per cent to £768.8million.

> High street banks are losing the battle against fraud as criminals switch tactics to directly target customers (The Daily Mail, 31 March 2017)

This paragraph suggests a simple displacement mechanism which causes more efforts by financial institutions (but also other businesses) to simple lead criminals to target individuals instead of these institutions. Although rarely stated this openly in the corpus we studied, this does entail a certain rhetorical exculpation on the part of the end-users. A different interpretation could say that the paragraph rather calls for more individual responsibility, not less, even though it does not do so openly.

4.1.4 Data Breaches in the British Media: Property not Privacy

When discussing cyber fraud and cyber scams, issues of personal data (mis)use are seldom put into the foreground in the case of the UK. Data breaches do occur frequently, but when they are discussed, this usually does not happen with an eye towards privacy as a fundamental right.

The Express writes (14 January 2017):

> Cyber-attackers target security company used by British police to download personal data
>
> HACKERS who breached systems at secretive Israeli security firm Cellebrite might have got their hands on sensitive personal data held by British police forces. (The Express, 14 January 2017)
>
> That the term “hackers” is written in capital letters should not be alarming, as this is a technique frequently employed by mid-market and tabloid news outlets. The section suggests that hacking is illegal, especially when targeting the police. What the data in question are is explained in more detail below:
>
> Hackers have targeted secretive Israeli security firm Cellebrite
>
> At least 28 UK police forces are known to use Cellebrite’s UFED device to controversially download photos, text messages, emails and other data from the mobile phones of suspects.
>
> The UFED is a laptop-sized device that can be plugged into phones, bypass passcodes and download material in an easily readable format.
>
> But Cellebrite, which has offices in London, San Francisco and Sydney, has been targeted by cyber-attackers and the information obtained by the British police might have fallen into the wrong hands. (The Express, 14 January 2017)

While the article is overtly about a data hack targeted at a security firm, it also contains a representation of data collection practices of police forces as questionable (as hinted at by the use of the term “controversial” in the second paragraph). The rather mild form of critique readers might get from this is counteracted, however, by the last paragraph which asserts that “information obtained by the British police might have fallen into the wrong hands”, covertly acknowledging that the police is in fact “the right hands” for personal data. This paragraph can therefore be read as reinforcing a particular imagination of surveillance activities as rightful or (to say the least) necessary. The next paragraph explains in a little more detail why the police hold personal data:

> British police hold personal data they download from suspects' devices
>
> I can’t say whether UK force data is vulnerable at the moment because we are still analysing the dump
>
> Joseph Cox

> Secretive Cellebrite is rumoured to have been brought in by the FBI to help get around the refusal of Apple to help access a new iOS8 encrypted phone belonging to Syed Farook, who carried out the 2015 mass shooting in San Bernardino, California.
>
> The 900 gigabytes of Cellebrite data, leaked to the technology news site Motherboard, includes email and communications from UK police forces and also includes “technical information, evidence and logs”. (The Express, 14 January 2017)

What is implied here (but not really explained in any detail) is the now wide-spread practice of online raids. Interestingly, the term “vulnerabilities” in the second paragraph is not associated with the personal (and possibly sensitive) data of “suspects” (who, after all, are suspected and not convicted of having committed a crime). Again, a very subtle way of reinforcing the idea that surveillance is at least necessary.

> It is not yet clear what information the hackers may have obtained
>
> Peter Sommer, a professor at Birmingham university’s school of computing and digital technology, said the devices were unlikely to be sending large quantities of suspects’ data to the company.
>
> He told The Times: “There’s no reason the police would be sending routine material, but mobile phone information keeps changing, particularly in the way the encryption has to be overcome.”
>
> Human rights watchdog Privacy International has condemned the widespread downloading of personal data from mobile phones as it emerged that officers routinely use broad warrants obtained for searching a suspect’s house to access the data. (The Express, 14 January 2017)

In the above paragraph the reader learns a bit more about outsourcing practices of the British police and how these might have something to do with the data breach. After all, it was not the Police’s IT systems which were hacked but rather those of a sub-contractor. In any case, the incident would seem to be a very good example of a data breach, and the way these are imagined in the news. The example is unique in the sense that it was not ordinary citizens’ data that were leaked but rather data of suspects, who occupy an inferior social position. The practice of online raiding is criticized by human rights organizations:

> Human rights watchdog Privacy International has condemned the widespread downloading of personal data from mobile phones as it emerged that officers routinely use broad warrants obtained for searching a suspect’s house to access the data.
>
> It said examinations were not always for crime types classified as “serious” prompting concerns that personal data of suspects of petty crimes, as well as any related data from their friends and family, is being stored. (The Express, 14 January 2017)

The last paragraph reports on the possible extent of data collection practices by the police. Readers are informed that the data leaked were with a high probability not confined to serious crimes at it seems to be common practice to obtain general warrants even in cases of petty crimes. The two paragraphs provide an indication of the extent of data collection, if only at close reading.

The Express (20 May 2017) tells a story about the frequency of data breaches and offers strategies how ordinary citizens can protect themselves:

> Now, experts have revealed simple measures people can take to protect themselves from harm – starting with never giving away personal information online.
>
> Everyday thousands of people freely tap in their address, their name, their occupation and other invaluable data – when companies offer deals on the internet.
>
> But this is being used against people time and time again.

> Raj Samani, Chief Scientist McAfee, warned people about their digital tattoo.
>
> He said: “Trying to rid of it is expensive and painful - and it leaves a scar.
>
> “What you need to think is if the worst was to happen and data was leaked are you going to be ok?
>
> “My kids know they should lie when they are asked to give information.
>
> “Us as consumers need to be aware.” (The Express, 20 May 2017)

The excerpt revolves around a theme that is very common in news articles about cybercrime and cyberfraud, namely the theme of empowerment and (individual) responsibility (which are discussed at length below, “Constructing the Users as Ignorant”). The language used in the first section is typical for mid-segment to tabloid-style news outlets: “experts have revealed simple measures people can take” is a prime example of co-construction, in this case of users-as-ignorant and of users-as-empowered (and, possibly, of experts). The term “simple measures” enforces responsibility, because it suggests that what stands between citizens and criminals is not necessarily expert knowledge but stuff so simple that everybody can (and should) do it – victimization becomes a matter of not wanting to protect oneself. The first paragraph thereby also includes a moralizing element – protection is easy, so the blame is on the potential victims. This gives the recurring theme of raising awareness a moral edge.

> Mr Simani highlighted the Ashley Maddison scandal in which the names given to a confidential website were leaked.
>
> He said: “The site listed people searching for affairs.
>
> “That was people openly giving their data – telling them they were married and they want to have an affair.
>
> “There were lawyers providing Ashley madison [sic!] divorces services. (The Express, 20 May 2017)

The above section gives further credence to the interpretation offered above. Overtly, the section offers one example of a typical cyberscam where not-so-innocent people were tricked into giving away their personal data. This suggests, covertly, that data leaks are very often the fault of those harmed, for they were simply being careless or inattentive or, as in the case above, were engaged in less-than-decent behaviours when they thought they were incognito.

> “If it asks you for data what do you do?”
>
> Mr Simani is urging businesses to regularly update their software, and educate their staff on how to spot a phishing email.
>
> However, he said people in general must be more aware, and stop giving out their personal information. (The Express, 20 May 2017)

Personal information is key in cybersecurity. This is a common conception, and it underscores the responsibilities of individuals. After all, who else would be in a position to take care of your personal data? Websites then seem to demand an unnatural amount of awareness from their users, as awareness is usually the default cybercrime fighting strategy on offer.

> He said: “This is not cyber crime - it’s crime
>
> “This is not cyberwar – it’s war.
>
> “We don’t rob banks with guns we use USB sticks and malware.
>
> “We need to change perceptions around this.” (The Express, 20 May 2017)

The "need to change perceptions" around cybercrime can be filed in the "awareness" folder. The language used in the paragraph – short-and-to-the-point sentences with juxtaposition – suggest urgency and determination, both seem to be targeted at individuals who need to be made aware in language as plain as possible that there is nothing short of a war going on in cyberspace. And as if to underscore the crucial part played by individuals, the next section reads:

> WannaCry ransomware held data hostage from users
>
> A common misconception, tech experts say, is that the victims of huge malware attacks are large corporations with endless cash, and while that may be true, hackers are more frequently using everyday people to get to them.
>
> Sanjay Ramnath, Vice President, Security Products and Business Strategy at Barracuda, said attacks are being more sophisticated.
>
> He said: "When they have information on you that is when it is dangerous.
>
> "They can customise an attack specifically for you.
>
> "They are extremely sophisticated."
>
> Setting your password, as 'password' is also a huge no-go. (The Express, 20 May 2017)

The WannaCry attack on Britain's National Health Service was one of the largest cyberattacks on British soil in recent history (it hit other countries and institutions as well, though). The interesting part is the second paragraph, where individual readers are urged to take seriously their individual risk. The paragraph works by juxtaposing individuals and corporations. Now it is certainly correct to say that even though many cyberattacks are directed at large organisations (e.g. banks), it is in many cases individual customers who suffer. The paragraph, however, offers a slightly different (and therefore more interesting) morale: It frames individuals as the gateways for cyberattacks against corporations, warning that it is ultimately individuals who are victims. After all, a bank does not have money of its own but rather takes care of its customers' money, right?

4.2 From Cybercrime to Cyberwar

The Scotsman (23 March 2017) reports plans by the finance ministers of the UK and Bangladesh to cooperate more effectively in tackling cybercrime, thereby stressing (and reinforcing) the fundamental role played by the financial sector and simultaneously echoing the theme of downsizing public spending. Thus, the article's headline reads

> Clear command and control needed in cyber-crime war. Clear lines of accountability are vital in the fight against cyber-crime. (The Scotsman, 23 March 2017)

The headline is interesting for at least two reasons: One, the framing of a technical problem (and possibly one for LEAs) as a military problem ("cyber-crime war"), and two, the lamentation of a lack of "clear command and control" in said war. This is underlined by the collocation of "accountability" with "command and control" in the above statement. The article starts with the following paragraph:

> With financial cyber-crime rising at alarming rates, Treasury committee chairman Andrew Tyrie believes greater focus is urgently needed. Members of the G20 often don't see eye-to-eye on global issues, but on the pressing concern of financial cyber-crime they appear keen to adopt the "all for one and one for all" approach. An agreement expected to be announced later this week by the finance chiefs of the world's top 20 economies would see them take a united front to tackling the problem in a bid to shore up financial stability. (The Scotsman, 23 March 2017)

The first line invokes rising crime rates as a justification for the claims of the headline. The next sentence talks of financial crime as a “pressing concern”. Citing the chairman of the treasury committee implicitly hints at the position from which the news outlet seems to be speaking, namely, the position of the elites in charge of the financial sector. It thereby offers an answer to the question “problem for whom?” by pointing towards a very specific group of people. This is reinforced in other parts of the statement, when the article mentions members of the G20 (i.e. the 20 largest economies in the world). Cybercrime is framed as a global issue, i.e. one that demands cooperation among otherwise often reluctant allies (“‘all for one and one for all’ approach”).

4.2.1 The West and the Rest

In some cases, issues of cybersecurity and cybercrime are framed in even more drastic terms than the familiar criminal activity frames. The *topos* of cyberwar is invoked frequently and suggests an even greater urgency of the issues than frames of crime and mitigation do. The *topos* of cyberwar seems to be practical from the point of view of (certain) news outlets because it is more comprehensive than (mere) cybercrime, as it suggests that the issue is not solely one of criminal motives (personal gain), but rather that the issue has a political dimension as well (which, it seems, is otherwise largely absent from British media representations). Cyberwar invokes the theme of cybersecurity, to be sure, and an important dimension concerns individual IT skills as well as business resilience. However, since war traditionally is the domain of the state, referring to incidents of cybercrime (whether politically motivated or not) as “war” suggests a greater responsibility on the part of the government to take action. It should be noted, however, that invocations of cyberwar are usually placed in the context of supposed geopolitical constellations. Consider the following headline from the Express (3 February 2017):

> Britain to pump BILLIONS of pounds into CYBER WARFARE against Russia, Michael Fallon says
>
> BRITAIN is set to pump billions of pounds into the cyber battle against Russia as Sir Michael Fallon unleashed a devastating warning to Vladimir Putin about the UK’s technological capabilities. (The Express, 3 February 2017)

The thrust of the above statement is quite contrary to many others found in the corpus which mention a lack of capabilities on the part of British citizens and professionals. When discussing the political dimension of cybersecurity, however, these considerations seem to recede into the background. The above headline is not without ambiguity, however, as concerns the capabilities. These are invoked simultaneously as already extant and as something yet to be achieved. The piece therefore simultaneously involves preparing the public for possible future expenditures in the name of national supremacy in cybersecurity matters, and as invoking the superior skills of Britons. The next paragraph reads:

> Fallon has issued a chilling warning to Putin about cyber warfare
>
> Fallon said during a speech at the University of St Andrews: “Today we see a country that in weaponising misinformation has created what we might now see as the post-truth age.”
>
> He added: “Russia is clearly testing NATO and the West. It is seeking to expand its sphere of influence, destabilise countries and weaken the alliance.” (The Express, 3 February 2017)

This paragraph qualifies what the expression “cyber battle” refers to. The theme of fake news and information warfare is usually absent from media articles about cybercrime, even though both are (or can be construed as) aspects of cybercrime. The paragraph also clarifies geopolitical constellations and the UK’s supposed position within them. The clarification further underlines the need for expenditures and skills development, even though now the thrust turns somewhat away from IT skills (spotting misinformation and fake news is probably not a matter of having IT skills). The culprit, in this scenario at least, is Russia, a country which supposedly is using misinformation to destabilise Europe and the NATO. In any case, Russia’s geopolitical interests are represented as illegitimate, as a threat to stability (“destabilise”). However, the extent of the threat is unclear:

> Sir Michael Fallon issued a warning to Russia at St Andrews University.
>
> The senior Tory claimed Russian hackers are targeting upcoming European elections in Germany, France, Holland, Montenegro and Bulgaria while manoeuvring itself as a “strategic competitor” to the West. (The Express, 3 February 2017)

The paragraph talks, not of (past) incidents, but rather of possible upcoming breaches with a decidedly political motive (since the supposed targets are upcoming elections in European countries). The extent of the threat is then rather ambiguously attributed to Russian hackers, a *topos* which arguably still invokes pictures of shady figures in black hoodies. In any case, it leaves the extent of the threat very much to the reader’s imagination. The next line is especially telling about the quality of evidence for the assertions:

> In a “persistent pattern of behaviour” Sir Michael highlighted recent cyber attacks that have been attributed to Russia. (The Express, 3 February 2017)

Where the attributions come from is not mentioned, however. As if to contradict the technical capabilities mentioned at the beginning of the article, the last paragraph reads:

> The speech comes after MPS, last Thursday, publicly savaged the Government’s ability to protect Britain from cyber attacks due to skills shortages and a severe lack of organisation.
>
> Britain has ramped up its cyber warfare budget
>
> The Public Accounts Committee said the Government had taken too long to co-ordinate its “alphabet soup” of agencies involved in protecting Britain in cyberspace.
>
> Meg Hillier MP, chair, said: “The threat of cyber crime is ever-growing yet evidence shows Britain ranks below Brazil, South Africa and China in keeping phones and laptops secure.”
>
> Yesterday’s speech by Fallon is in direct contrast to the Committee chairwoman's comments that Downing Street needed to “raise its game”. (The Express, 3 February 2017)

There are, it seems, conflicting opinions about the UK’s IT capabilities. This conflict might be attributed to the different agendas of the involved parties (parliament vs. government). However, it points to a deeper ambiguity between the rhetoric of power and one of lacking capabilities. One plausible explanation for the ambiguity might be that the Internet itself can only be partially represented, which makes it possible to attribute very different (even conflicting) qualities.

The International Business Times UK (23 May 2017) reports on Labour Party’s cyber defence strategy:

> Cyber crime is only mentioned briefly by Labour, alongside more general policing. "We will provide officers, police community support officers and civilian staff with the equipment and people they need to provide effective policing services, including from the growing threat of cybercrime."
>
> Regarding cyber warfare, Labour says if it wins the election it will "order a complete strategic defence and security review...to assess the emerging threats facing Britain, including hybrid and cyber warfare." The manifesto continues: "Cyber security will form an integral part of our defence and security strategy and we will introduce a cyber-security charter for companies working with the Ministry of Defence." (The International Business Times UK, 23 May 2017)

The two paragraphs mention both domestic and external security, thereby stressing the global dimension of cybercrime. The same phenomenon is thereby construed as being the domain of traditionally separated political fields. This suggests that the phenomenon of cybercrime undercuts traditional political divisions of labour. What is interesting, then, is not so much Labour’s position per se, but rather the way cybercrime and cyberwar are framed as being two sides to the same coin. In both cyberwar and cybercrime, threats are coming from outside and inside. The Liberal Democrats use a slightly different ontology:

> On cybercrime, the Liberal Democrats will "recognise the expansion of warfare into the cybersphere, by investing in our security and intelligence services and acting to counter cyberattacks."

In this paragraph (International Business Times UK, 23 May 2017), there is a more or less clear (but possibly blurring) distinction between the “cybersphere” and what can be presumed to be the “analogue” sphere. The responsibility invoked by the Liberal Democrats clearly lies with public authorities, however. On the other hand, cyber-attacks can be construed as pretence for expanding surveillance.

The daily Mirror (7 January 2017) also suggests an East-West-divide when it writes:

> President Obama vowed revenge on Russia for the cyber hacks
>
> The report assessed with "high confidence" that the GRU, Russia's military intelligence agency, had used those intermediaries to release "US victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks."
>
> WikiLeaks founder Julian Assange has said he did not receive emails stolen from the DNC and top Clinton aide John Podesta from "a state party." (The Daily Mirror, 7 January 2017)

The language used is quite strong and rather informal. “Revenge” in the first line arguably is not a category for (successful) geopolitics. Regardless of what Obama did or did not say, the choice of words suggests conflict between the US and Russia, alluding to a Cold War-type of mind-set.

4.2.2 An Army of Hackers

An article by the Express (20 May 2017) covers the WannaCry-cyberattack on the NHS to discuss mitigation strategies that individuals can take. The term “war” is here used to refer to an evolution in cybercrime:

> 'This is not cyber crime - it's WAR' Expert warns hackers exploiting THIS common mistake
>
> COMPUTER users are being warned to stop giving out their personal data on the internet after a massive evolution in cybercrime that is a tech "war".
>
> Experts are insisting anyone using the worldwide web, through any kind of device, must take immediate action to stop themselves becoming a victim. (Express, 20 May 2017)

At least two aspects of this statement are striking: The first is the use of martial (almost military) language in the headline, which is then somewhat attenuated by putting the term “war” in quotation marks. Spelling what are key terms from the news outlet’s point of view in capital letters is common in a certain brand of journalism. Here, the words “war” and “this” (followed by “common mistake”) are capitalized. The military metaphor has been commented on already. The second part of the headline invokes IT-illiterate users which make “mistakes” that can be “exploited” by hackers. The statement therefore constructs the problem as being of a global scale (“war”) and simultaneously constructs the public (i.e. those people who cannot be considered “expert” users) as ignorant about the consequences of their behaviour. Interestingly, the second paragraph issues a warning about the dangers of giving away personal data on the Internet that are due to a “massive evolution” in cybercrime, thereby underscoring the “war”-interpretation once again. However, it might be pointed out that giving away personal data on the Internet (or anywhere else) could have been a problem before cybercrime reached current levels. The connection between those two phenomena remains largely unexplored, however. The article also fails to mention another dimension of data protection resp. data breaches: It is not just criminals who might exploit individuals’ personal data. This is also done on an increasing scale by companies (sometimes legitimate, sometimes not). There are parallels between personalized ads and personalized attacks, however: both involve personal data of the target, and both are customized based on those data.

The Sun (29 June 2017) uses an even more direct war metaphor:

> GADGETS NOT GUNS Warfare to move ‘from battlefield to the web’ as risk of cyber conflict grows, National Crime Agency warns
>
> The National Crime Agency issued chilling warning today in an official report
>
> THE next global conflict could begin with the sending of an email booby-trapped with nasty software.
>
> Britain's top cops have said that conflict will no longer be played out on the battlefield but in a "cyber environment".
>
> The National Crime Agency imagines fights waged over computers, with states using technology to disrupt enemy's society.
>
> Its annual report stated: "It is also likely that future conflict will be less confined to the traditional battlefield and will increasingly encroach on a cyber-environment, with the aim of disrupting societies, leading to a decreasing divide between cyber conflict and cyber crime."
>
> It claimed that the "primary threat" to the UK stemmed from Russian-speaking nations but added that the threat is "increasingly global". (The Sun, 29 June 2017)

Irony is used in the headline by contrasting the entirely un-ironic nature of warfare with the somewhat belittling term “gadgets”. This might also be a distancing strategy, insofar as it is implied that real wars still take place on more traditional battlefields. The next line contradicts this interpretation, however (“warfare to move from the battlefield to the web”). Overall, the article uses evocative, emotional language (“chilling warning”), which underscores the importance of being ready for cyberwar. It stresses conflict over consensus and turns on a supposed convergence of cyber war and cybercrime. The last two paragraphs paint a picture of an East-West conflict, something that is also topical in other discussions of possible cyberwar, but with the added notion of a global threat. An article by the Telegraph (8 January 2017) invokes the same (East-West) dichotomy:

> France blocks 24,000 cyber attacks amid fears that Russia may try to influence French presidential election
>
> Both Marine Le Pen and her French presidential rival Francois Fillon want closer ties with Russia
>
> France is to beef up cyber-security amid growing fears that Russian hackers could try to influence its upcoming presidential election following claims that Moscow orchestrated US computer attacks to help Donald Trump.
>
> Jean-Yves Le Drian, the defence minister, said French intelligence agencies were trying “to learn lessons for the future” from the allegations by their US counterparts.
>
> Mr Trump has dismissed the accusations and renewed calls for close ties with Russia.

> Mr Le Drian said that if the Russians had meddled in the US election, it amounted to an attack on western democracy. France and its political parties are “no less vulnerable,” he stressed.
>
> He said the risk became apparent when hackers took the French television channel TV5 Monde off air in 2015. French investigators suggested that the Kremlin was behind the cyber-attack. (The Telegraph, 8 January 2017)

The article discusses the relationship between Russia and France in the context of upcoming elections. Russia is often suspected to be behind attempts at hacking “Western” elections (e.g. in the US). Interestingly, these allegations are reinforced several times during the article, although there is no evidence presented anywhere. Regardless, the article reinforces the idea of an East-West conflict that is boiling somewhat under the surface, and is only visible periodically in alleged cyberattacks attributed to Russia.

The Daily Mirror argues in a similar vein (7 January 2017):

> Vladimir Putin 'directed cyber hacking campaign to help Donald Trump win US presidential election'
>
> US intelligence agencies concluded Russia sought to help Trump by discrediting rival Hillary Clinton
>
> Vladimir Putin ordered a cyber hacking campaign to help Donald Trump win the US presidential election , intelligence agencies have concluded.
>
> The Russian president sought to help the Republican candidate's electoral chances by discrediting Democrat rival Hillary Clinton .
>
> Russia's objectives were to undermine public faith in the US democratic process, denigrate former secretary of state Clinton, make it harder for her to win and harm her presidency if she did, an unclassified report said.
>
> "We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election," the report said.
>
> "We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments." (The Daily Mirror, 7 January 2017)

It is clear from this and the above article that Russia is a source of considerable cyber threat, at least from the point of view of the United States. Interestingly, the European Union and the UK do not feature in the story at all.

4.2.3 A War for Privacy?

An article published in the Independent (9 January 2017) begins with the following paragraph:

> Why Artificial Intelligence is the answer to the greatest threat of 2017, cyber-hacking
>
> Protecting ourselves raises an interesting dilemma. What level of monitoring and activity reporting are you prepared to put up with to enable more accurate or earlier collaborative identification of malice?
>
> Our lives are now heavily mediated by digital technology (music streaming, social media, e-banking etc.). We are increasingly and often continuously online, open to engagement in a myriad of services and simultaneously open to cyberattack.
>
> 2016 saw further high profile and financially driven security incidents, such as Tesco and TalkTalk, together with one of the highest profile attacks ever – the apparent compromise of the Democratic

> party's information systems with potential influence on the US Presidential Election. We now need to defend against the lone wolf hacker, organised crime and terrorism, and nation states with well-funded advanced capabilities. (The Independent, 9 January 2017)

The author's point is that with the increasing amount of Internet traffic we will be forced (resp. are already forced) to resort to artificial intelligence to control it, which has implications for the way we handle privacy as well. What is interesting about the above section is the way the threat caused by hackers is framed throughout. Additionally, the author offers a technical reason for the increasing lack of sophistication an skills on the part of users, albeit a rather sympathetic one (it is simply impossible for human beings to handle the amounts of traffic). The view is founded in a dilemma described by the author in the second paragraph of the above section where he states that the increasing amount and sophistication of cyberthreats counteracts our wish for privacy protection. In any case, the statement includes the same rather condescending attitude towards non-expert users, albeit this time attenuated by a somewhat technical explanation for the latter's lack of skills:

> The 2016 cyber message is clear – we have a big problem, it's going to get worse, and we need help.
>
> Artificial Intelligence (AI) is a promising source of such help. It comprises theory and techniques that enable intelligent processing of information. It underpins many current robotics and other smart systems (e.g. driverless cars) but its current dominant application area is the analysis of large and complex data repositories (usually referred to as Big Data analytics).
>
> The intelligence of AI is often interpreted as mirroring human capabilities, but the scale of data potentially relevant for security purposes typically places analysis well beyond human capabilities. Internet traffic, for example, is predicted by networking giant Cisco to reach several zetabytes (billion trillion bytes) by 2019. AI is needed to make sense of data at (and well below) these scales and cyber defence has little option but to make significant use of it. (The Independent, 9 January 2017)

The dilemma mentioned above is then explicated in the following terms:

> Protecting ourselves raises an interesting dilemma. What level of monitoring and activity reporting are you prepared to put up with to enable more accurate or earlier collaborative identification of malice? The privacy versus security issue is not new (witness the furious Ed Snowden debate) but this doesn't just apply to state monitoring. We will see increasing efforts to square the circle here, providing more effective security whilst supporting privacy.
>
> We will see AI emerging as a major and a powerful tool in both the detection and investigation of malice and in the construction of systems resilient to attack. But what's sauce for the goose is sauce for the gander. Cyberhackers can use AI too and so the cyber-arms war will continue. We will also need to deal with that. (The Independent, 9 January 2017)

The dilemma is presented as follows: The increasing sophistication of cyberattacks necessitates increasingly sophisticated detection mechanisms. The state-of-the-Art way to do this is by using Big Data Analytics, which in turn involve the readiness on the part of end-users to give up parts of their privacy. The situation is thereby construed as an arms race (even though the author uses the somewhat vaguer term "cyber-arms war"). It should be noted that for end-users (citizens), it does not matter much whether their data are misused by criminals or by other actors. The entire argument is therefore premised upon a rather misleading us-vs.-them assumption ("bad" hackers versus "good" citizens). This dichotomizing framework grounds the argument for the emergence of an arms race that ultimately seems to leave the non-expert users at the mercy of "both" sides.

4.3 Strengthening Cybersecurity: Humans in the Loop?

4.3.1 Banks: Educating the Public?

The Daily Mail (08 May 2017) reports on a strategy to tackle online fraud launched by UK-based bank Barclays. The strategy targets credit cards and enables their holders to manually block them online. The anti-fraud measure enables the bank's customers to turn off the card's remote shopping function. According to the Daily Mail, this feature is targeted at customers who don't shop online (often) and want to reduce their fraud risk but might also be used by customers who want to restrain their online shopping habits. The blocking function works by logging on to Barclays' app. These changes can be made effective and reversed almost instantly, but customers would still have to have their cards blocked permanently if stolen. The same article mentions a survey of 6000 adults, also conducted by Barclays, which found that people aged between 25 and 34 are twice as likely to be victims of online fraud as are older generations. Barclays said that their measures were about giving customers greater control; this can be interpreted as a step towards empowering customers, but it is also a step towards greater individualization of responsibility. With the new options in place, it falls upon customers to select the security features that best suit them. The measures follow data which testify to a decline in online spending since 2013. The framing of the issues in these two articles points towards empowerment and responsibility. Both articles leave readers to believe that it falls upon them to protect themselves.

The Daily Record (11 June 2016) reports about efforts by the Royal Bank of Scotland to educate the wider public about security measures. According to the article,

> "the biggest threats to individuals are rudimentary scams, carried out by modern-day confidence tricksters". (The Daily Record, 11 June 2017)

The bank's position in this case is that of an ignorant public – sometimes implied in the notion of insufficient "awareness" for cybersecurity risks – that needs to be educated about the ways they might be scammed. The position, then, turns on a juxtaposition of experts and laypeople (who need to be educated). The framing of the issue, however, seems to divert focus from the fact that even IT security experts often seem to be at a loss when it comes to tackling cybercrime. The solution which involves better educating laypeople seems to be a mere diversion, then, as it remains unclear exactly how better cybersecurity skills on the part of the general public might actually help to fight cybercrime.

4.3.2 SMEs: The Prime Target for Cybercriminals?

Small and medium-sized enterprises are presented as an attractive target for cybercriminals precisely because they are small and usually do not have appropriate security measures in place. The International Business Times UK (18 April 2017) reports the views of the British Chambers of Commerce, an independent business network:

> Even though big businesses are major targets, we all need to improve security.
>
> Has your business been hacked? One in five UK firms hit by cybercrime
>
> One in five businesses in the UK has fallen victim to a cyberattack in the past 12 months, with larger firms considered a juicer quarry for hackers than their smaller counterparts, according to a new report released this week by the British Chambers of Commerce (BCC).
>
> The powerful business network, which surveyed over 1,200 firms in January of this year, found that 20% had been hit by a cyberattack in the past 12 months. The majority of the firms in the study were

> small-to-medium companies. A total of 22% operated in the manufacturing sector with the remainder in the services sector. (International Business Times UK, 18 April 2017)

The reports on SMEs’ vulnerabilities when it comes to IT security are somewhat ambiguous. On the one hand, it is frequently stressed (as in the above example) that large enterprises are the more frequent targets of cybercriminals. Regardless, this very fact is often constructed as a good reason for cybercriminals to attack SMEs as well, because the fact that they are seldom attacked makes them unaware and therefore an easy target. Tellingly, the headline is phrased as a question (“Has your business been hacked?”) followed by a vague assertion (“One in five UK firms hit by cybercrime”). The first part is supposed to raise awareness, while the second part is quite ambiguous as to who the most vulnerable targets of cybercriminals actually are. If it’s just large companies, why the need for SMEs to adapt? Cybercrime is constructed as a problem which is not scalable. It affects businesses of all sizes, even though there are effects besides size:

> Over the past two years there has been a spike in cyberattacks hitting big-name companies, from Tesco Bank to TalkTalk. However according to John Madelin, chief executive of Reliance ACSN, the findings from the BCC were unsurprising.
>
> "A cyberattack can mean anything from an entry-level phishing scam – which targets every business large or small – to sophisticated and targeted high-impact attacks, and everything in-between," he said. "There is a distinct lack of knowledge on how organisations can protect themselves."
>
> Madelin said there needs to be a "culture shift" in the relationship between industry and government. "The current security systems that many organisations use to hold people's data, like retailers and banks, just aren't being managed in the right way," he asserted. (International Business Times UK, 18 April 2017)

The paragraphs above invoke knowledge and culture as two pillars of counteracting cybercrime. Cybercrime is constructed as so endemic that any countermeasures require nothing less than profound cultural change. What remains unclear, at least in the above paragraph, is the extent to which such a culture shift would impact other aspects of life.

> Tips on how to stay secure from security firm Tripwire:
>
> •Start by understanding the risk you have. You have to conduct regular, preferably continuous, assessments of configuration and vulnerability risk across your IT systems. The attackers will be doing the same.
>
> •Don't ignore the simple, best practices. Keep software up to date, apply security patches, change passwords, and make sure terminated employees and contractors don't have access. This security hygiene goes a long way to making the attackers' job more difficult.
>
> •Train your employees on how to recognise a scam. Much of cybersecurity is about human nature and social engineering. Training must be ongoing because the attackers change their tactics. (International Business Times UK, 18 April 2017)

These security tips (apparently BBC-approved) are telling because they involve the same individualizing stance that construct end-users as potentially ignorant and dangerous for IT systems (see below). It is the individual’s responsibility to conduct regular assessments of vulnerabilities and risks and to keep themselves up to date on matters of IT security (even though, possibly, individuals have better things to do than worrying about something for which there are experts). The last paragraph is even more telling. It constructs human nature as something inherently opposed to cybersecurity. At the heart of this opposition lies a more fundamental valuation: If human nature (which remains undefined and presumably is hard to influence) is somehow opposed to IT security (if it is fundamental aspects of humans which make attaining IT security difficult), it follows that IT security is “upgraded” vis-à-vis more human aspects. The idiosyncrasies of machines are constructed as more important than human purposes and values. The last paragraph also includes a (albeit hidden) reference to a supposed evolution of the Internet that has to be counteracted by constant individual efforts (such as “life-long learning”).

4.3.3 Politics of Cybercrime: Education, Awareness, Control

The International Business Times UK (23 May 2017) reports the positions of UK’s political parties (Conservatives, Labour, Liberal Democrats) on cybersecurity and cybercrime. The three stances are reported and commented on separately without comparing the three positions to one another. The article was published prior to the 2017 elections as part of a series of the International Business Times UK on the parties’ programmes.

> The Tories have by far the most to say of the three main parties when it comes to online safety, devoting an entire section of their 2017 manifesto to the topic. But a couple of lines have already caused a stir in the technology sector. (International Business Times UK, 23 May 2017)

At the centre of the Conservative Party’s stance is regulation, and since the industry (or at least parts of the industry) would be regulated, criticism from this direction is understandable. In any case, it is noteworthy that the Conservative Party seems to construct cybersecurity and cybercrime as matters of more regulation, as can be seen in the following paragraph.

> Towards the end of the 88-page manifesto, the party says: "Some people say that it is not for government to regulate when it comes to technology and the internet. We disagree. While we cannot create this framework alone, it is for government, not private companies, to protect the security of people and ensure the gardens of the rules by which people and businesses abide." (International Business Times UK, 23 May 2017)

The Internet, but also technologies more generally, are imagined by the Tories as something to be tolerated and, if possible, regulated. The paragraph implicitly acknowledges that the Internet, while increasingly becoming a critical infrastructure, was not created by governments (or individual players from any industry, for that matter). Even so, the party manifesto argues, the right to use force should remain with the state, and therefore, it is the state’s responsibility to enforce regulations, even on the Internet. The paragraph therefore simultaneously acknowledges and rhetorically extends the national power monopoly. The next section is about empowerment and its converse, vulnerability:

> The government asks tech companies to give young users the right to delete all "personal data" held about them when they turn 18, if they so wish. The manifesto states: "We will give people new rights to ensure they are in control of their own data, including the ability to require major social media platforms to delete information held about them at the age of 18, the ability to access and export personal data, and an expectation that personal data held should be stored in a secure way." (International Business Times UK, 23 May 2017)

Here, young users (under the age of 18) are imagined to be the most vulnerable Internet users. The other theme running through this section, besides vulnerability (of certain groups, at least), is empowerment as a mitigation strategy. That this is directed at personal data (with the explicit demand for social media platforms to give young users control over their data) almost recedes into the background on this reading. Regardless of their efforts to empower people with respect to their personal data, the paragraph goes some way at establishing the idea that there are groups of people who are especially vulnerable when it comes to IT security and who therefore require special protection. On the other hand, it is social media platforms (or, more precisely, the companies behind those platforms) which are given the responsibility (or obligation) to empower young people.

In the next paragraph, the Conservative Party calls for an ethics of the Internet which should ideally reflect the ethics that govern people's offline lives:

> The Conservatives continue: "We must takes steps to protect the vulnerable and give people confidence to use the internet without fear of abuse, criminality or exposure to horrific content." The party's starting point is how "online rules should reflect those that govern our lives offline." (International Business Times UK, 23 May 2017)

Tellingly, the "rules that govern our lives offline" remain unexplained. It is not surprising that a Conservative Party would place an emphasis on morality, of course. But still, it remains unclear how exactly they imagine a code of conduct for the Internet.

Expanding on this point, the Conservatives say: "It should be as unacceptable to bully online as it is in the playground, as difficult to groom a young child on the internet as it is in a community, as hard for children to access violent and degrading pornography online as it is in the high street, and as difficult to commit a crime digitally as it is physically."

> The Tories will make it clear that "platforms" – understood to be social networks like Facebook – are responsible for enabling systems for reporting "inappropriate, bullying, harmful or illegal content, with take-down on a comply-or-explain basis." Similarly, internet companies will be pushed to "develop technical tools to identify and remove terrorist propaganda". (International Business Times UK, 23 May 2017)

The above paragraph is interesting in at least two respects: One, it assigns clear responsibilities and accordingly a pronounced interpretation of who are the most important actors in cyberspace. Responsibility to detect and control what is on the Internet is clearly assigned to Internet companies and online platforms, a stance which seems very different from representatives of the industry (experts); the latter frequently argue that end-users need to be educated in order to be able to manage their own cybersecurity. Here, we are offered a very different approach which argues that companies willing to operate on the infrastructure that is the Internet have to have at least some degree of accountability. On the other hand, when it comes to issues such as cybergrooming, the Tories' strategy targets individuals:

> Educating children on the dangers of being groomed online is as important as sex education in schools, the Conservatives say. "We will educate today's young people in the harms of the internet and how best to combat them, introducing comprehensive relationships and sex education in all primary and secondary schools to ensure that children learn about the risks of the internet including cyberbullying and online grooming." (International Business Times UK, 23 May 2017)

Here, the main strategy to counter cybercrime against vulnerable individuals such as children seems to be education. The Internet is here imagined as a space of risk and vulnerability especially for children. Responsibility to educate them falls upon the government and the communities.

> With regard to the growing threat of cybercrime, the Tories say they will "bolster the response to cyber threats on private businesses, public services, critical national infrastructure and individuals, working with the National Cyber Security Centre to prevent attack whenever possible and with the police...to ensure perpetrators are brought to justice." The government's £1.9bn investment in cyber security will be continued, to "further strengthen" the country's defences, while requiring "all public services to follow the most up to date cyber security techniques appropriate." (International Business Times UK, 23 May 2017)

The last paragraph speaks about responsibility. Clearly, the Conservative Party differentiates between different kinds of cybercrime along the lines of crimes against property and crimes against persons. The strategy mentioned in the last paragraph concerns public and private entities as well as individuals, but it seems to be restricted to crimes against property. Crimes against individuals, such as cybergrooming, are mentioned elsewhere.

In general, then, the Conservative Party has a rather pessimistic stance on the Internet. The latter is imagined as something to be regulated and controlled, even if to empower people.

The Labour Party's views and ideas converge in some of these matters:

> Labour shares with the Conservatives an insistence on tech companies allowing young users to delete content before they turn 18. The party says: "We all need to work harder to keep children safe online. Labour will ensure that tech companies are obliged to take measures that further protect children and tackle online abuse. We will ensure that young people understand and are able to easily remove content they shared on the internet before they turned 18." (International Business Times UK, 23 May 2017)

The *topoi* of protection and empowerment (and its opposite, vulnerability) are present here as well. Children are imagined as the most vulnerable group which therefore deserves special protection. As is familiar from the Conservatives' manifesto, the responsibility to protect children is sought with tech companies. In addition, Labour also wants to empower the general public with respect to control over their personal data. This should happen through educating the public about the way personal data are handled, and also via obligating companies to delete data on request. The section thereby reinforces the position that it is companies who are the main actors on the Internet, and that the public is generally oblivious to what happens to their data (especially if individuals in question are under 18) and therefore needs to be educated. Cybercrime is imagined by Labour to be continuous with "offline" crime:

> Cyber crime is only mentioned briefly by Labour, alongside more general policing. "We will provide officers, police community support officers and civilian staff with the equipment and people they need to provide effective policing services, including from the growing threat of cybercrime." (International Business Times UK, 23 May 2017)

Cyberwar is treated separately:

> Regarding cyber warfare, Labour says if it wins the election it will "order a complete strategic defence and security review...to assess the emerging threats facing Britain, including hybrid and cyber warfare." The manifesto continues: "Cyber security will form an integral part of our defence and security strategy and we will introduce a cyber-security charter for companies working with the Ministry of Defence." (International Business Times UK, 23 May 2017)

What is striking here is the fact that (similar to many other mentions), cyberwar is described as "emerging threats". This suggests a scenario of threats which have not yet emerged, calling for intensified future action. Cyberspace is not, therefore, imagined to be actually dangerous, but rather something that is potentially dangerous. Potentialities are notoriously more difficult to assess (let alone explicate) than actualities. Imaginations of threats and defences arguably always involve an element of potentiality, though. What is striking about the above paragraph is the assumption (nowhere questioned) that cybercrime and cyberwar will continue to be issues that need to be tackled.

The Liberal Democrats are the last party whose position is discussed in the article. The party seems to put special focus on issues of data protection and surveillance. The latter theme seems to be largely absent from the Conservative's and Labour's manifestos. For the Liberals, surveillance seems to be a central issue:

> "Snooping" by the government and net neutrality are a prime focus of the Lib Dem's 2017 manifesto. The party's introduction states: "[Our young people] want to live in a country where the state isn't snooping into their emails and tracking their internet use." (International Business Times UK, 23 May 2017)

The language used in the programme is instructive and might be regarded typical for Liberal’s stance towards state power. The usage of the term “snooping” (instead of the more neutral “surveillance” for example) suggests a government illegitimately intruding into citizens’ privacy. This attitude is not restricted to the government, however:

> The party adds that it wants to "introduce a digital bill of rights that protects people's powers over their own information, supports individuals over large corporations, and preserves the neutrality of the internet." (International Business Times UK, 23 May 2017)

Here, the already familiar *topos* of empowerment pops up again. This time, it is directed more generally at individuals (not just children). What is striking about the paragraph is the suggestion to craft a digital bill of rights which would make individual rights over personal data much more concrete than mere obligations for companies. The *topos* of empowerment is here connected to the *topos* of net neutrality. Empowerment, it is suggested, is also a matter of economic policies that control the emergence of (net) monopolies.

> With regard to mass surveillance, the Lib Dems state they will: "Roll back state surveillance powers by ending the indiscriminate bulk collection of communications data, bulk hacking, and the collection of internet information." (International Business Times UK, 23 May 2017)

Now the term surveillance does come up. The use of terminology (all rather informal) suggests that there is already a lot of state surveillance going on which needs to be curbed. The section also suggests that most of the surveillance activities are unnecessary, as indicated by the use of terms such as “bulk collection”.

> Additionally, the party pledges to "support free media and a free and open internet around the world, championing the free flow of information." (International Business Times UK, 23 May 2017)

Tellingly, the above passage does not specify what would make the flow of information “free”. However, it might be expected of a liberal party that freedom is somehow central to their world view. What the section does suggest is that at the moment, the Internet is not free (or: the flow of information is somehow inhibited). The Liberals offer a very different imagination of the Internet, compared to the Conservatives, when they champion a free and open Internet, i.e. an Internet which should not and cannot be regulated to realize its full potential.

The Liberal and the Conservative manifesto thereby testify to two very different imaginations of the Internet. The Conservative vision of the Internet is of a space which is potentially harmful and needs to be controlled, whereas the Liberal vision is that of an enabler which needs to be left to its course as much as possible.

> On cybercrime, the Liberal Democrats will "recognise the expansion of warfare into the cybersphere, by investing in our security and intelligence services and acting to counter cyberattacks." (International Business Times UK, 23 May 2017)

All three manifestos acknowledge that there is a national security dimension towards cybercrime. All three discussions thereby reinforce and actualize the idea that there is such a thing as cyberwar, and that there consequently must be a military dimension to the Internet.

4.4 Concerns of Citizens, Concerns of Professionals

4.4.1 Perceived Threats: Cyberspace as a “Crime Problem”

Cybersecurity and Cybercrime are prime concerns for citizens and businesses alike. Especially SMEs are worried about the threats posed by cybercrime (more so than about Brexit) (The Telegraph, 29 June 2017). As a result, SMEs are reported to want to spend more on cybersecurity. SMEs are particularly concerned about their abilities to manage multiple threats, the Telegraph concluded. Emerging technologies are increasingly becoming a must-have for small businesses to survive. Especially businesses believe cybercrime is becoming increasingly sophisticated (The Independent, 17 April 2017). One fifth of businesses believe that cyber threats are hampering growth, according dot the same newspaper (ibid.). Most seem to rely on (external) experts to resolve these issues for them, such as IT providers and LEAs (ibid.).

According to the Mirror, citizens’ trust in financial institutions is low due to cyber threats. Attacks against banks (and consequently, savings) are described as particularly worrisome. So much so in fact, that according to a survey reported by the Mirror, 20% of UK citizens wants to return to a cash-only society (The Mirror, 09 April 2017). Financial institutions are not perceived as having the relevant cybersecurity skills (ibid.). The Mirror reports a study among 500 adults of which 82% believe that cyber fraud is among the biggest threats. 76% see the responsibility for counter measures with banks and financial institutions. The article explicitly mentions trust (or rather, lack of trust) as a problem for the financial sector. (ibid.)

The Scotsman (30 May 2017) reports a survey among financial professionals which finds that cyber threats and political upheaval are the most feared threats. Cybercrime is here portrayed as the biggest threat to the industry (and, one might add, to society at large due to the central role played by the financial system). Additionally, the financial industry is believed to be doing too little about it (ibid.). However, concerns about cybercrime do lead to finance firms spending more on cybersecurity, reports the Telegraph (05 April 2017). As concerns SMEs, the consequences of cyberattacks may be severe, according to the Telegraph (11 January 2017). The threats are explicitly linked to reputational damage and loss of trustworthiness (aside possible legal consequences.

A Daily Mail article from 31 March 2017 juxtaposes increasing security efforts by financial institutions (colloquially referred to as “lenders”) with an increased victimization risk on the part of customers. The article argues from statistical increases in fraud incidents and losses incurred following such incidents. These numbers are presented as a direct result of financial institutions’ efforts to fight cybercrime through e.g. increased security measures, a framing which suggests that increasing security measures actually causes increased cybercrime activity of a different sort (displacement). Increasing cybersecurity, it is suggested, increases the risk for other attack strategies such as social engineering, directed more at customers and less at the banks themselves. These include contacting the customers via phone, email, or text message, but criminals are also increasingly resorting to cash machine attacks. The article cites voices who claim a responsibility on the part of financial institutions to inform the public about these “increasingly sophisticated techniques to dupe their victims”. Here, the reader once again encounters the narrative of a digitally illiterate public which makes an easy target for criminals. The message, it seems, can also be read as: Banks and businesses have done their job of providing IT security, now it falls upon individuals to do their part as well. Overall, this falls well in line with the initial juxtaposition of banks and businesses’ efforts and the adverse effects on cybercrime rates. This apparent dilemma is resolved, in the remainder of the article, by calling on more individual responsibility, but also responsibility of experts (from businesses) to provide education for the public.

A recurring theme is reputational damage to businesses incurred through cybercrime incidents. The Independent (17 April 2017) thus writes:

> “Cyber attacks risk companies’ finances, confidence and reputation, with victims reporting not only monetary losses but costs from disruption to their business and productivity,” he [Adam Marshall, Director General of the BBC] said. (The Independent, 17 April 2017)

And also:

> Last week, a study commissioned by cyber security firm CGI and conducted by Oxford Economics, found that companies’ share prices fall by an average of 1.8 per cent on a permanent basis following a severe cyber security incident – where large amounts of sensitive information is compromised. (The Independent, 17 April 2017)

Having appropriate (and effective) IT security becomes, not just a matter of stability and security, but also a moral obligation which, if not properly met, can incur reputational damage to a company. The motivation for companies given in the second paragraph above is monetary, to be sure. But the appeal to “reputation” and “confidence” suggests an ethical dimension to IT security as well. Having appropriate IT security thereby becomes a matter of being able to fulfil societal expectations.

The Telegraph (11 January 2017) is even more drastic in its formulation:

> But the consequences of an attack can be severe. An assault on a business's IT systems, infrastructure or devices could mean the difference between staying afloat or going under, especially if reputational damage results in losing trade, or it faces legal consequences.
>
> With 38pc of UK SMEs having experienced an attack in the past year, ignoring the issue is no longer an option. (The Telegraph, 11 January 2017)

The reputational damages that result from a cyberattack are connected to probable monetary losses in the above statement; the moral obligation of businesses appealed to above concerns the duty to – well – do business, lest “reputational damage result[s] in losing trade”.

4.4.2 (Lack of) Cybersecurity Skills: Constructing the User as Ignorant

A common theme that runs through the British press corpus we collected is the issue of cybersecurity skills on the part of the workforce and on the part of the public. The issue has multiple dimensions, as cybersecurity skills are a business factor (businesses have to have adequate cybersecurity measures which entails finding the experts) whereas the cybersecurity skills of the public are frequently imagined to be non-existent by corporate actors which entails the latter’s obligation to educate the general public in matters of IT security and social engineering. The Express (3 February 2017) calls into question the authorities’ ability to protect the public from cyberattacks due to a shortage of skills. The Guardian (16 January 2017) reports a story about a cybersecurity firm and their (successful) search for sponsors and investors. The two news outlets appear to incorporate very different journalistic values. Regardless, the general thrust is the same, namely, that there is a shortage of skills when it comes to cybersecurity. The Guardian employs the somewhat more positive framing of a business success story, while the Express is rather pessimistic about the UKs chances of prevailing in “cyber warfare”, but the underlying assumptions are remarkably similar. Disregarding the different framings, the narrative is roughly the same. The two differ markedly in their framings, though. The Guardian story then goes on to analyse the difficulties faced by cybersecurity firms in entering new markets, which qualifies the narrative of a lack of skills. Cybersecurity, by definition, involves a “hurdle” that companies willing to enter the market have to take, and unlike other domains, that is 100% security. In addition, a lack of understanding for security matters on the part of potential investors (again a lack of skills) makes it difficult for these companies to secure investments.

An article by the Independent (17 January 2017) reports extensively on this “cyber-security skills gap [that is] threatening UK companies”. It cites a survey conducted by job portal Indeed which tried to quantify the gap between supply of and demand for cybersecurity skills in the UK. The Indeed study puts the figure at 31% (of positions on offer could be filled). Indeed even spoke of a crisis and the need for British businesses to attract more professionals into cybersecurity roles. This implies the possibility of a translation of cyber threats into a demand for more cyber security experts and, therefore, into labour market policies.

The same newspaper reported on 17 April 2017 that businesses seldom rely on in-house IT expertise but rather resort to IT providers to resolve issues. The article employs a rather drastic wording. Citing the BBC, it warns of “consequences UK companies face if they fail to tackle digital skills deficiencies within their workforce”. Again, an (abstract) threat is translated into demands for a more skilled workforce.

In a different vain, the Scotsman (22 May 2017) reports of a Horizon 2020 project by the name TITANIUM which

> “aim[s] to develop and implement tools to reveal common characteristics of criminal transactions, detect anomalies in their usage, and identify money-laundering techniques”. (The Scotsman, 22 May 2017)

Additionally, the project will also

> “carry out training to develop skills and knowledge among European law enforcement agencies”. (The Scotsman, 22 May 2017)

The underlying narrative is again very similar, suggesting a quickly evolving universe of cyber-threats which, at the moment, is not met by an equally quick evolution of skills to tackle said threats. In general, this is also true about framings of cybercrime. The Internet is portrayed as a vast and complex realm which necessitates the continuous adaptation and development of skills and mitigation strategies on the part of individuals, businesses, and policy makers.

The Scotsman (23 March 2017) was more straightforward. Citing Andrew Tyrie, a member of the Treasury committee, the article claimed that “banks need greater IT expertise at main board and senior management level”, and they also need greater resources for modernising banks’ IT infrastructures. The first part of this statement refers back to the claim made above, namely that a common narrative in cybersecurity discourse concerns a supposed lack of understanding for these matters among the general public, but also among professionals who have to deal with these issues on a daily basis. Both have a potentially devastating effect on businesses and consequently the economy. Interestingly though, individual harm is almost never mentioned in discussions of cyber security skills, as if these were a purely professional matter. The public is (though not in this example) more often imagined as ignorant and unable to manage even their own financial transactions, as testified by frequent campaigns launched by financial institutions.

The Telegraph (11 January 2017) offers yet a different angle on the issue of cyber security skills when it says the especially SMEs often find cyber security issues so outside of their comfort zone that they often ignore the issue hoping that as a small business they would not make an attractive target:

> From encouraging a culture of caution, to backing up files, here's how SMEs can defend themselves against hacking threats.

> Unlike larger companies, small businesses often operate without dedicated IT professionals, and rarely regard themselves as attractive targets for cyber attacks. But this very attitude, and the knock-on effect of being left undefended, is precisely what may make them tempting to hackers. (The Telegraph, 11 January 2017)

In the article, the Telegraph describes a culture of security that needs to be maintained among employees in the health sector, as these are required to handle extremely sensitive data. The article goes on to describe aspects of such a culture of security in a vivid and transparent way. The article stresses how a culture of security is maintained and is at the heart of a cybersecurity strategy. At the centre of such a security culture is, one again, the individual’s responsibility when handling sensitive data. The article is based on the (albeit tacit) assumption that IT infrastructures are not “fixed”, but rather in constant flux which necessitates not only specific measures, but also a very peculiar mind-set (a “culture of security”). These are presented as measures to counter a problem frequently faced by SMEs (but not by larger firms): SMEs usually do not have (or even cannot afford) the necessary IT expertise. What’s more, in many cases this leads to them just ignoring the issues of cybercrime. Framing the issue this way opens up the possibility of a special kind of counter-measures. If it is true that cyber security is a huge problem for SMEs, and if it is also true that these do not have the financial and human resources to tackle the problem, then the solution might be to establish a culture of security, i.e. to profoundly change their employees’ behaviour. Of course, these interpretive claims are open to debate, so long as it remains unclear whether such a relegation to culture of security matters is specific to IT security. It might be suspected, however, that security was never as big a part of corporate culture (and culture more generally) as it is now. This is referred to as “securitization” in the academic literature (cf. e.g. Lobato/Kenkel 2015).

A later article by the same news outlet (The Telegraph, 15 May 2017) talks about “carelessness” and “incompetence” as far as IT security is concerned. The article discusses the events surrounding the WannaCry attacks on the NHS. As before, security and crime are both framed as matters of individual capabilities (and possibly collective capabilities, in the case of SMEs). This framing suggests (in the form of a rudimentary argument) that, were employees and citizens more careful and/or more skilful, there would be no problem with IT security. On the other hand, cybercriminals with their backstories, motivations etc. are largely absent from these stories (which, arguably, might have something to do with the fact that they are difficult to grasp). The article then goes on to relativize a bit by saying that institutions other than the NHS were equally hit, so that a lack of cyber security is not just a problem for UK-based organisations.

Two concepts frequently employed when referring to the need for an increased security culture are education and awareness. Both are targeted at individuals resp. end-users and can therefore be regarded as continuous with the construction of end-users as ignorant described above. Thus, International Business Times UK (7 May 2017) writes:

> UK bank launches 'Great British Fraud Fightback' to help tackle online crime
>
> The drive kick-started by Barclays comes on the heels of a survey that revealed millennials are most vulnerable to cybercrime.
>
> Leading UK bank Barclays is launching a £10m nationwide initiative, dubbed the 'Great British Fraud Fightback', aimed at spreading awareness about financial fraud risks. The bank hopes to boost the protection of digital identities of Britons through the dissemination of information, tools and tips. (International Business Times UK, 7 May 2017)

The money deployed by Barclays is devoted to raising “awareness about financial fraud risks”. It might be added that awareness alone will change nothing about cybercriminal activity. The campaign and the way it is described here do not, therefore, tell a lot about how to tackle cybercrime. However, they do reveal a lot about the way the issues and the relevant actors are imagined. Here, end-users (or, the general public) is constructed as largely unaware, otherwise there would be no need for an awareness campaign. The next paragraph offers a familiar theme of empowerment:

> The digital safety drive launched on Monday (8 May) marks the first attempt by a high street bank to enable their customers to assume full control over how their debit cards would operate. Customers would be able to use the Barclays mobile banking app to instantly enable or disable remote purchases and set their daily ATM withdrawal limits. Branch employees will also have access to a new police hotline to be used in instances when customers are scammed. (International Business Times UK, 7 May 2017)

The aim of the campaigns, the reader learns, is to ultimately empower customers and the general public and thereby to turn them into competent arbiters in the fight against cybercrime.

> The bank will also extend its awareness campaign beyond its customer network. UK residents will be able to assess their own digital safety level online through the Barclays website. (International Business Times UK, 7 May 2017)

The above paragraph alludes to empowerment, but it also entails individualization. When citizens are asked to “assess their own digital safety”, this inevitably constructs them as responsible entities.

> Additionally, the bank will launch a £10m multimedia nationwide campaign to spread awareness about fraud related risks. (International Business Times UK, 7 May 2017)

“Risk” serves a rhetorical function that is very similar to “emerging threats” above. Technically, a risk is just a probability. It does not strictly speaking refer to any part of reality. Regardless, the mere existence of risks calls for action; citizens need to be made aware of risks related to online fraud. The underlying *topos* is one of activation. The Internet is here once again constructed as a realm of dangers (and risks) that needs to be regulated. What is more, it is not just the Internet that needs to be regulated, but rather, citizens need to adjust their behaviour as well.

> "Fraud is often wrongly described as an invisible crime, but the effects are no less damaging to people's lives" said Ashok Vaswani, chief executive of Barclays UK. (International Business Times UK, 7 May 2017)

The following paragraph is very explicit as to what the main functions of the Internet are, according to Barclays at least:

> "As a society our confidence in using digital technology to shop, pay our bills and connect with others has grown faster than our knowledge of how to do so safely. This has created a 'digital safety gap' which is being exploited by criminals." (International Business Times UK, 7 May 2017)

Digital technologies, the readers are told, are for shopping (which is named first!), paying bills (second), and only third for connecting with others (which, incidentally is what social network CEOs keep publicly insisting). The order in which these functions appear need not qualify them as more or less important, to be sure. But as a reader, one cannot help to interpret this as an implicit valuation. Additionally, the paragraph offers an explanation for the need to create awareness by postulating a “digital safety gap” between public confidence in and public understanding of digital technologies. This juxtaposition can be interpreted as another example of the construction of users as ignorant. It can also be interpreted as co-construction because it refers simultaneously to end-users and to the technologies in question. The former are constructed as ignorant and in need of education, whereas the latter are constructed as somehow essential for the accomplishment of mundane tasks (paying bills, communication over a distance) yet still

ill-understood by the general public. The last paragraph connects these themes to a more general narrative of national security:

> "I believe the need to fight fraud has now become a national resilience issue, and we all need to boost our digital safety levels in order to close the gap." (International Business Times UK, 7 May 2017)

National security is invoked in the above paragraph twice, once explicitly and then implicitly by reference to a national "we", suggesting an in-group dynamic with a moral imperative ("we need to boost our digital safety levels"). It thereby constructs the individual-as-citizen and as responsible for playing their part in securing cyberspace.

The Daily Record (22 March 2018) extends this perspective to LEAs as well:

> Officers face an ongoing challenge to keep ahead of the game when it comes to cyber crime.
>
> Insp Mullen added: "The types of crimes we face are changing.
>
> "We know about house breaking or vehicle crime, for example, but we now have advances in technology meaning that crime can be committed without people leaving their house.
>
> "Because of social media and cloud computing and smart phones, more and more people are using it to communicate and socialise but because that is becoming more prevalent it is giving criminals more avenues to explore.
>
> "We are constantly trying to keep up with the pace of change and trying to keep up with technology.
>
> "Because of that, criminal activity is going to be just as fast. (The Daily Record, 22 March 2018)

A recurring theme in the above paragraph is the pace at which technological change now takes place. Such is this pace that "[o]fficers face an ongoing challenge to keep ahead of the game when it comes to cybercrime". This short section invokes the by now familiar notion of an arms race between law enforcers and criminals, where it is now imperative (and increasingly difficult) for the former to stay ahead of the latter. This suggests the need to invest, to educate and train officers (which might justify increased spending in the law enforcement sector). LEAs therefore might have a stake in constructing their situation as an arms race. Interestingly, this is never so much directed at the present than at the future:

> Over the next 10 years, Police Scotland intend to make policing cyber crime a priority by training officers how to respond to cyber related crimes. (The Daily Record, 22 March 2018)

Even though cybercrime is said to be a pressing problem at the moment, the above statement talks of future investments or just intentions ("Police Scotland intend to make policing cyber crime a priority"). An important aspect of these endeavours is again the education of young people to empower them online:

> Work is also currently ongoing with schools across West Dunbartonshire.
>
> Police Scotland Youth Engagement officers give help and advice to pupils about online safety.
>
> Insp Mullen added: "Through our youth engagement officers we deliver packages to schools to teach children how to keep themselves safe online.
>
> "We want people to think if they would be happy with a stranger seeing something online before they post it.
>
> "If the answer is no then don't put it on." (The Daily Record, 22 March 2018)

This is interesting when read in the context of the "arms race" alluded to at the beginning of the article, because framing cybercrime as an arms race puts enormous pressure to "stay ahead of the game" not only on LEAs, but also (and by no means incidentally, one might add) on individuals. This is especially so when put into a slightly different context, namely the labour market and its apparent shortage in cyber security professionals. The constant reminders that end-users are somehow digitally unfit also tends to reinforce the stereotype that it is the individual’s responsibility to stay “ahead of the game”, especially when it comes to employment.

5 Case Study III: Cyberspace as Contested Territory (Germany)

5.1 Cybersecurity and Surveillance after Snowden

Media discussions of ICT in left-leaning German media (but not just) in the first half of 2017 seemed to centre on one theme: The Snowden Revelations of 2013 of mass surveillance activities by the US domestic intelligence agency NSA had incidentally revealed the involvement of many other intelligence agencies, including the British GCHQ and the German BND. As a consequence, Germany installed an investigation committee in 2014 to determine the extent to which high ranking officials and politicians up to and including Chancellor Angela Merkel were involved in resp. informed of these activities. The investigation ended in 2017 and was therefore widely discussed in the newspapers analysed here. The German media landscape around that time was therefore dominated by themes of espionage, surveillance and political responsibility. Disregarding the content of the accusations, the German parliament (the Bundestag) around the same time passed comprehensive legislation enabling forms of surveillance heretofore impossible such as wide-spread data retention (which incidentally was also introduced in Austria) as well as source surveillance of telecommunication (which was the legal term used) and wide-spread use of state Trojans (malware deployed by the police to spy on suspects). The following case study will therefore be centred on those two events and their media representations. Contrary to the Spain and UK case studies, the Germany/Austria case is therefore much more dependent on two specific events. However, this national idiosyncrasy can be justified by reference to the sheer extent of the discussions surrounding these two events. The aim of the chapter is not, however, to arrive at the “correct” depiction of the events in question, even though the course of events will be reconstructed as well as possible. Rather, the present chapter wants to sketch the basic assumptions and evaluations of the phenomena in question (which are: surveillance, espionage, and whistleblowing). In this respect, it especially instructive to juxtapose articles related to the Snowden revelations and the investigation set up by the German parliament, as well as the legislation connected to increasing surveillance measures.

5.2 Government Surveillance and the Discourse of Securitization

5.2.1 Vulnerabilities and Security: The Dilemma of Zero Day Exploits

One dominant theme in German surveillance discourse is the problem of so-called zero day vulnerabilities or zero day exploits. Under certain circumstances (e.g. when fighting terrorism) it can be opportune for intelligence agencies if the industry does not close known security gaps. These gaps (e.g. on mobile devices) can then be exploited by LEAs to collect data from suspects. However, security gaps are a gatekeeper not only for state-employed hackers, but also for everyone else. Therefore, their mere existence produces a dilemma: Is it legitimate to deliberately weaken cybersecurity in the name of domestic security?

> According to Europol, ransomware "WannaCry" hit at least 150 countries and 200,000 organizations and individuals on Friday. "WannaCry encrypted all data on the infected computers to demand payment of a ransom.
>
> During the attack the software exploited a security gap in Microsoft's Windows operating system that allowed it to automatically plug in new computers. The security gap was once kept open by the US secret service NSA for the purpose of surveillance, but was then made public by unknown hackers. (Süddeutsche Zeitung, 16 May 2017)

The notorious WannaCry attack which crippled the NHS in January 2017 (and hit many other organisations worldwide) exploited a security gap in Microsoft Windows which had been known to the

NSA but was deliberately kept open as a backdoor for surveillance. The exploitation of such “zero day vulnerabilities” seems to be common among intelligence agencies and is a topic widely discussed in German media. Such vulnerabilities can be exploited by everyone with the right IT skills; therefore, one argument goes, keeping such security gaps open inadvertently puts the cybersecurity of law-abiding citizens at risk. The growing federal interest in such security gaps has brought about a profitable market for zero day vulnerabilities:

> Meanwhile, a profitable market for security vulnerabilities has emerged
>
> In the meantime, a real market has emerged in which security gaps and malware are offered; many millions can be implemented worldwide. Where in the past machine guns and rocket launchers were traded, now states and their secret services deal with cyber weapons. Hackers or computer experts who come across a security gap in the network quickly earn seven-digit sums. You can contact the large IT companies that have developed this faulty, i.e. vulnerable software. Or they sell their knowledge of vulnerabilities to other hackers or governments. For example, the Israeli company NSO Group used a vulnerability that enabled the defence of various smartphone operating systems, including Apple and Android. The cost of the installation was $500,000. Another $600,000 was needed to monitor ten people, the New York Times once quoted from internal emails. (Süddeutsche Zeitung, 16 April 2017)

The above paragraph gives an impression how hacking for the state and hacking for criminal reasons can be indistinguishable on the face of it. Black markets for cyber weapons (such as vulnerabilities) are no longer just the domain of cybercriminals, it seems; governments buy them just as eagerly for their intelligence agencies. This suggests that the methods used by intelligence agencies to fight crime and terrorism are in many cases not very far removed from the methods of criminals and terrorists, at least when it comes to cyberspace. The next section describes some of these methods in more detail:

> The federal government to buy security gaps on the black market
>
> To understand the problems this poses, you need to know how authorities will act from now on if they want to access data. In order to install the malware on the suspects' devices, they need a security hole. IT security expert Linus Neumann of the Chaos Computer Club described the procedure in an expert report at the end of May.
>
> Investigators must either gain unnoticed access to the device, for example during a traffic control, or take over the iPhone remotely. Such a security hole would be extremely powerful. Anyone who knows them would not only be able to crack the suspect's smartphone. He could take over all the iPhones. "The possibly justified and legitimate interest to use a weakness for the purpose of criminal prosecution is thus inevitably confronted by the risk for the general public," Neumann sums up. What does the state want, the security of its citizens or its data? (Süddeutsche Zeitung, 16 May 2017)

The headline suggests the ambivalence associated with surveillance when it talks about governments shopping on the black market (which is illegal by definition). There is a further tension that arises when including the cybersecurity of law-abiding citizens in the equation. In order that LEAs be able to exploit security gaps, these need to be kept open for everyone. When put this way, the strategy seems to amount to decrease overall cybersecurity to (supposedly) increase security. We will see below in what ways this strategy is justified by government representatives. For the time being, we would like to point out that given the inherent strategic dilemma here, security might not be the ultimate goal behind zero day exploits. Rather, it may be just about access, or about increasing the possibilities of governments to spy on their citizens. This is by no means restricted to Germany, however. The following excerpt refers to a dispute between Apple and the FBI:

> The CIA listens in on everyone

> At the beginning of 2016, for example, there was a very public dispute between the FBI and the Apple Group. Investigators tried to solve the terrorist attack in San Bernardino, California, and wanted to read out the iPhone of the alleged assassin. Apple rejected this on the grounds that police would thereby learn to crack any iPhone. For Apple, commercial interests were also at stake because it wanted to prove to its customers that their data is secure on the iPhone. The US government, on the other hand, wanted to obtain a court ruling according to which there must be no apparatus that is completely removed from the state. In the end, the legal dispute was unnecessary because the FBI managed to read the telephone with its own means.
>
> Unlike a house search, there are no legal hurdles
>
> Such public disputes contradict the workings and self-image of the secret services. They prefer to read quietly and secretly without the public noticing. This also prevents the necessary political debate, the balancing of two interests: almost every citizen probably wants the authorities to be able to monitor terrorists, but he also does not want the Internet to become a completely insecure space. The CIA likes to complain that the Internet is becoming "darker" because so much data is encrypted, but in fact it benefits from the darkness as well by exploring and spying without society being able to debate their surveillance activities under full disclosure of all the circumstances. When the CIA operates abroad, it can do as it pleases anyway. While US security authorities usually require a court order to monitor the communication of American citizens, there are practically no hurdles for spying on foreigners. (Süddeutsche Zeitung, 11 March 2017)

The interests of the industry often appear to be closer to citizens' privacy concerns than the position of intelligence agencies:

> The old days when telecom companies cooperated closely with the secret services of their own countries are over. Today, US products such as WhatsApp (which belongs to Facebook) or the iPhone manufacturer Apple promise a well-protected exchange of messages, while secret services like the CIA try with enormous effort to participate in the confidential exchange anyway. As soon as the vulnerabilities that the CIA had exploited became known this week, Apple declared its intention to "quickly" close these gaps. Meanwhile, the CIA may be looking for the next gaps. (Süddeutsche Zeitung, 11 March 2017)

In fact, the situation might be characterised as an arms race, but not between governments but between governments and businesses:

> Arms race between companies and intelligence services
>
> Applications for mobile phones such as Signal or Whatsapp encrypt messages so that they cannot be read by strangers on the way from transmitter to receiver. The CIA, however, seems to be able to read these messages under certain circumstances while the text is still being typed in, i.e. before it is even encrypted. (Süddeutsche Zeitung, 11 March 2017)
>
> The new CIA papers show that an arms race has taken place - on the one hand, the companies that want to offer secure communication, and on the other, some governments that want to monitor this communication at all costs and acquire an arsenal of cyber weapons. In the USA, the special feature is that the technology companies from Silicon Valley are in an arms race with their own government. (Süddeutsche Zeitung, 11 March 2017)

Many vendors of communication services such as WhatsApp have a stake in offering their users privacy. The above examples show, among other things, that there are business interests to be taken into account besides security and privacy considerations. The position of US IT firm Apple was that exposing security gaps would mean giving up the data security it had promised its customers. This is unusual because in most cases, intelligence agencies do not ask manufacturers for support. Instead, they just hack devices. In the case of Apple, however, FBI hackers were unable to gain access which is why they turned to Apple for help. What is striking about the first of the two above paragraphs is the position of the US government which wants there to be no part of cyberspace that cannot be accessed. This means that US intelligence agencies will strive for keeping at least some security gaps open. Accordingly, if these endeavours are successful, this means that there are vulnerabilities for end-users at any given moment. On the face of it, the industry seems to support user privacy, if only out of commercial considerations. However, given the fact that these companies do collect a lot of other information about their customers this should be taken with a grain of salt. The position of governments and LEAs is also the object of the next excerpt:

> Some intelligence officials and policemen reject encryption technologies, arguing that the state should never completely lose access to information. This argument is correct in certain respects, because there is also no home that security authorities are not allowed to search. However, the difference to the apartment is that the police usually need a court search warrant to get into the apartment. However, there is usually no judicial order when secret services read out mobile phones abroad or convert a smart TV into a bug. The person under surveillance does not notice that his mobile phone has been tapped. (Süddeutsche Zeitung, 11 March 2017)

The argument provided here is slightly different. It argues from a (supposed) analogy between homes (which are never completely off limits to LEAs) and mobile devices (which should never be completely off limits). The excerpt criticises this view on the grounds that home searches usually need a search warrant which is not usually the case with mobile devices. It might be argued, however, that the analogy is flawed on the grounds that breaking into suspects homes can be achieved without compromising the security of other homes. This seems to be impossible when it comes to cybersecurity. Additionally, it is not just legal procedures per se which make surveillance increasingly ubiquitous:

> Due to the introduction of several devices with microphones and cameras into the home which are increasingly connected to the Internet, surveillance - at least theoretically - will soon have no limits at all. This world of mobile phones, computers, networked refrigerators and Internet TVs is the reason for US secret services to speak of a "golden age of surveillance". When hardly anyone was discussing the risks of connected life, one NSA leader already cheered: "Who would have thought this would be Big Brother here? The agent showed a photo of Apple boss Steve Jobs proudly holding a mobile phone in the air. (Süddeutsche Zeitung, 11 March 2017)

The above paragraph suggests that it is up to end-users (to a degree, at least) to open their behaviour up to surveillance activities. The more devices are connected to the Internet, the more possibilities there are for intelligence agencies to exploit vulnerabilities. The statement by a leading NSA member in the above excerpt suggests that this is in fact the position of the intelligence service. The next excerpt suggests that with governments increasingly buying into the black market for vulnerabilities, their intelligence agencies also have a financial stake in vulnerabilities remaining open:

> CIA and NSA are exploiting the vulnerability of the network itself. Just as they used to have the ambition to have a lock pick for every lock in the world, today they search for a weakness in every device, in every messenger service, in every software. One of the most risky developments is business with zero-day exploits. These are discovered vulnerabilities in the software, security holes. There are companies that develop tailored scouting programs and several secret services, among them the BND, buy them from these companies. Governments are now paying millions for vulnerabilities discovered. This government action reveals the whole problem: According to its own statements, the US government reports several weaknesses to the industry so that it can fill the gaps, but also takes advantage of many gaps itself in order to be able to spy. Intelligence logic comes first. (Süddeutsche Zeitung, 11 March 2017)

Vulnerabilities are here discussed as investments for governments and their LEAs. Governments buy scouting software developed to discover weaknesses. Some of them are then allegedly reported back to the industry. However, since the aim of scouting for vulnerabilities is, ultimately, to increase possibilities for surveillance, governments would not report all exposed weaknesses. On the face of it, this does not sound problematic, provided governments abide the rule of law and exploit these vulnerabilities in service of their citizens' security. However, when it comes to cyberspace, that logic simply does not hold:

> What are the risks? In order to access the devices, the authorities must be able to identify and exploit security gaps in their software. IT security experts never tire of warning that such vulnerabilities that are deliberately left in place are dangerous because they can also be discovered and abused by criminals. Are there any examples? Just recently, a vulnerability in the Windows operating system originally discovered by the US wiretapping service NSA was exploited for a worldwide attack with the blackmail Trojan "WannaCry". It had become public after a data leak in the Secret Service. How do you make sure that the investigators can only read the ongoing communication as planned? The fact that once the Trojan has been installed on a device, one of the objections of critics of the plan is that it is difficult to restrict access. "The judge's reservation is completely insufficient to control the range of the software and to ensure that it is switched off again. A judge lacks the technical expertise and independent expertise," Hans-Christian Ströbele, member of the Green Bundestag, told the "Frankfurter Allgemeine Zeitung". Another point of criticism is that the plans were put into a long law "to make criminal proceedings more effective and practical" without much public debate. How easy is it to place such a Trojan anyway? Every day, online criminals demonstrate how to get into PCs. Modern smartphones have been given a much stronger architecture. Devices with the most used mobile system Android are considered by experts to be somewhat easier to hack because there are still many older versions of the software in circulation and the phones are built by many different manufacturers, while Apple has hardware and software itself under control with its iPhone. However, security holes have appeared in both operating systems in the past. There is a market for such vulnerabilities, which is also accessed by public authorities. (Chip, 22 June 2017)

> According to Schaar, the "WhatsApp law" also poses risks to IT security. "Authorities use exactly the same IT vulnerabilities as fraudsters and blackmailers," the expert complained. The state would no longer have any interest in eliminating such gaps. The chairman of the European Academy for Freedom of Information and Data Protection accused the grand coalition of passing new laws almost every week "which impair privacy and restrict civil rights". In doing so, neither consideration nor moderation is given. This is "a rather arrogant way of dealing with power at the expense of democracy and the rule of law". (Heise, 23 June 2017)

The WannaCry attack early in 2017 is a good example for why that strategy might be problematic. Vulnerabilities which are left in place are also open to cybercriminals. The security gap in the Windows operating system which was then exploited by the WannaCry virus was discovered by the NSA, but left open. Opponents of the practice therefore routinely point to the fact that once malware is installed on a suspect's device, it can be exploited by anyone (not just the police). Additionally, once a device is compromised, the police will have access not just to ongoing communications. These vulnerabilities and how intelligence agencies exploit them were also the object of revelations published by WikiLeaks:

> As with all hackeries, zero days and other vulnerabilities play an important role in the work of EDG. It is also clearly visible how all kinds of tips are stored in the wiki so that the work of programmers cannot be traced back to the CIA or the USA, for example through the recommendation to remove all time stamps that allow conclusions to be drawn about the work at CIA headquarters in Langley. After all, the "attribution" of a possible attack is one of the central themes of the "Cyberwar", as the search

> for "Russian hackers" shows. Vault 7 is only the first part of a larger document delivery. In his statement on the new project, WikiLeaks CEO Julian Assange stressed that WikiLeaks has already published more documents with Vault 7 than Edward Snowden in three years. At the same time, he denied that the publication of WikiLeaks had something to do with the enactment of US President Trump, who ordered a review of all Cyberwar programs within 30 days. (Heise, 7 March 2017)

The risks of zero day exploits for user privacy are discussed in the following excerpt:

> The surveillance law could "lead to a harmful weakening of IT security on the Internet, if not to a threat to digitisation processes in society and business", fears Norbert Pohlmann, board member at eco-Verband der Internetwirtschaft [Internet Economy Association]. This applies in particular if investigators used "zero-day exploits to place the state Trojans". Exploiting such security gaps poses a major risk both for companies and for the privacy of individuals. Such a procedure should not become common practice in criminal prosecution. The courts will have to decide whether the initiative is constitutional. (Heise, 23 June 2017)

The position of the activities of the German “Chaos Computer Club” is unambiguous:

> I do not mean to say that these questions are easy. One always finds oneself in dilemmas. But you have to look at the big picture. If the federal government decides to buy up the knowledge about an IT security gap on the black market in order to spy on Islamists, the result is that this security gap will continue - for all 80 million citizens. That is a high price paid by society. With this security gap, criminals and foreign intelligence services can spy on all citizens. (Süddeutsche Zeitung, 2 April 2017)

The argument is familiar – leaving security gaps open to spy on criminals or terrorists means risking everybody else’s cybersecurity as well. Recall that the industry has a stake at protecting consumers’ privacy, at least in some respects. Depending on the position one takes (government, business, consumer, or citizen) the apparent trade-off between privacy and security can appear very different:

> Close all gaps - or use some? It's a difficult trade-off
>
> So, when should secret services share their knowledge about security vulnerabilities and when should they keep it to themselves? It's a difficult balance: If you pass on the knowledge and close the gap, you may help companies, but you may take the opportunity to prevent an attack. Through the so-called Vulnerability Equities Process, NSA is supposed to pass on 91 percent of all discovered vulnerabilities to affected companies. Careful consideration is given to whether it is justified not to report a gap, but to exploit it. In the case of Wanna Cry, Microsoft was even notified - but only very late: after hackers had already bragged about the vulnerability. (Süddeutsche Zeitung, 16 May 2017)

The above paragraph suggests that there is a trade-off after all between closing and exploiting vulnerabilities. However, it is also evident that the precise kind of trade-off depends on the position one takes. In any case, the above excerpts turn on and thereby reinforce the notion that there is a trade-off (which is never quite fully explained, though) between privacy (of individuals) and security (of nation states). It appears as if both opponents and advocates of government surveillance accept this dichotomy, although statements such as the one by the “Chaos Computer Club” might be interpreted to the effect that in a digitized society, expanding surveillance might not simultaneously increase global levels of security. That is an argument that seems to work for analogue worlds, but it breaks down for digitized societies.

5.2.2 Security, Privacy, Democracy: A Post-Democratic Trade-Off?

In the same vein, the next excerpt argues that in order to understand the role of companies, geopolitical and ideological constellations need to be taken into account. The increasing culture of surveillance, the argument goes, has effectively weakened democratic culture to a degree that has enabled cybercrime as we know it (e.g. global ransomware attacks) in the first place. The argument turns on a notion of trust which has arguably been eroded by surveillance and been replaced by a form of corruption. Taking the WannaCry ransomware attacks as a starting point, the article argues that the supposed trade-offs between security and privacy might in fact be a false dichotomy based on the assumption that cybercrime is – much like "ordinary" crime – just a natural consequence of digitization that we have to live with. But what if, the article argues, the cybercrime pandemic is in fact caused by a shift in the role of governments and (large) companies one might call post-democratic? And, to take the argument further, is it correct to assume that crime is simply "out there"?

> WannaCry and Network Security
>
> Why the neofeudal cybersecurity structure is dangerous
>
> Governments should actually curb the destructive work of companies in a democracy. But cyberattacks like "WannaCry" reverse the situation.
>
> The wave of cyber attacks with the malware "WannaCry" has paralyzed the computer systems of hospitals, railway companies and companies worldwide. If you don't pay a ransom, your data remains encrypted. This should not be dismissed as a one-off prank by simple criminals who have taught themselves to hack. The attackers used tools and vulnerabilities originally developed by US intelligence services for their own attacks and espionage. Therefore, we can no longer ignore the uncomfortable fact that the increasingly neofeudal cyber-security structure "pay or go under" has arisen from the weakening of democratic-capitalist ideals, as they collapse under the burden of constant surveillance. The political legitimacy of democratic capitalism, this unlikely political development that brought us to the end of history and is now the only bulwark against right-wing extremism, is based on a clear separation of powers between governments and companies. Governments monitor companies to protect customers from rarely occurring damage from otherwise positive business activity. This system is considered democratic because populations can elect governments and vote them out at any time; it is capitalist because businesses depend on the rules of competition that reward efficiency, innovation and infinite growth. This logic prevents stagnation, but can also have devastating consequences. This is precisely why various government measures are needed. That, in any case, is the Social Democratic consensus with which both centre-left and centre-right parties are d'accord. The questions of war and security have always posed problems for this system. This can be seen in the fact that political insiders regularly warn of the military-industrial complex shortly before retirement. Democratic standards are regularly ignored because governments want more control over the flow of information, classify more and more of their internal information and expand their monitoring activities without taking into account the separation of powers. (Süddeutsche Zeitung, 15 May 2017)

Surveillance is bad, this argument goes, precisely because it undercuts the separation of powers characteristic for democracies. The practices of intelligence agencies of increasing surveillance and acting increasingly secretive have effectively undermined public trust. Additionally, nowadays the boundaries between governments and companies are becoming increasingly blurred:

> Governments should actually curb the destructive activities of companies
>
> The standard criticism of this approach starts with the activities of the so-called "deep state" in the state, which are considered undemocratic because they are incomprehensible. The aim of the

> opponents is to make the "deep state" a "shallow state", i.e. more transparent. This should be done through campaigns to strengthen privacy, ideally in the form of legal intervention, transparency and accountability. The real problem, according to the advocates, is the failure of democracy, and it is easy to ignore the capitalist component of "democratic capitalism": All we needed was more and better legal instruments to better control the secret services. Unfortunately, in 2017 the world cannot be divided so neatly into categories of this system. Just think of the example of cyber security. Many rogue states are busy hacking their opponents' servers in Western Europe and North America. Similarly, it cannot be denied that non-state hacker groups take action for economic or patriotic reasons. (Süddeutsche Zeitung, 15 May 2017)

Arguments to the effect that government surveillance needs to be answered by more transparency and respect for privacy tend to ignore that democracies are usually also capitalist market economies. This democratic-capitalist consensus is threatened, the author argues, by the new state of surveillance because it gave rise to an entire industry of cyber insurers who do nothing more than exploit vulnerabilities caused by the state. This is true even in industries which are nothing to do with IT. Even in such domains, the argument goes, lots of resources go into cybersecurity measures because governments find vulnerabilities convenient for their own surveillance activities. The fact that governments create markets for security through their own irresponsible actions, the author argues, is one of the reasons for the state of affairs he terms “neo-feudalism”.

> None of this shakes the founding myth of democratic capitalism that governments are there to curb the destructive work of companies. New dangers give the state a more important role. But what is shaking this myth is the growing recognition that it is the democratic governments themselves, with their intelligence services, who are responsible for security holes in our communications networks, tampering with our smart TVs and shamelessly exploiting loopholes in our operating systems. WikiLeaks recently released CIA hacking tools. Governments do this for what many would call noble motives: to detect early signs of terrorist activity, to track down criminals, to block equipment used for conspiracies that could cause devastating damage to our cities. Whatever the motives, we should never lose sight of the far-reaching political impact. The extension of the surveillance measures of a democratic government requires a permanent structural uncertainty of our communication networks. This insecurity is not only exploited by democratic governments, but also by everyone else, including rogue states and non-state hackers. But once the uncertainty becomes structural, the right response is not an upgrade of security measures, but insurance. This also explains why cyberinsurance has become one of the most promising lines of business in the insurance market. Even in economic sectors such as manufacturing, which is becoming more and more digitized and networked, more and more money must be spent on insurance against damage from cyber attacks. Basically, cyberinsurance, like any other form of insurance, is the profession of rentiers who are looking to get regular premiums from those who use their services. What is new is that the risk posed by this new class of rentiers is partly, if not mainly, caused by government activity. Therefore, the logic of democratic capitalism no longer applies. Governments do not curb harmful business practices. On the contrary, they themselves cause damage through their actions, which in turn are mitigated by the companies. (Süddeutsche Zeitung, 15 May 2017)

Cyberspace is (at least for the time being) organized in such a way that predominantly benefits large corporations such as Google and Facebook to the detriment of SMEs and possibly users who have to turn to these corporations for protection of their privacy. Incidentally, then, it is precisely the surveillance activities of governments which have exacerbated the monopoly power of these corporations (even if they did not create it).

> More autonomy at own risk

> The second political effect of the ever-expanding surveillance apparatus is the disadvantage it brings to small businesses and NGOs, not to mention private individuals. Do you remember the early utopian visions of a digital world in which we all have our own mail servers and networked homes? Nowadays we want more autonomy at our own risk. Given the maturity of the cyber attacks, which target data theft and fake traffic on the attacked sites, it is obvious that the only companies that can protect ordinary users, whether they are individuals or companies, are large technology companies such as Google, Apple and Microsoft. This also violates the basic assumption of democratic capitalism. Citizens are urged to seek protection from companies, not governments, which are at best the reason why protection is needed at all. When spam and vulnerabilities are judged using the most advanced level of artificial intelligence, it is easy to forget that a small player can keep up with the companies that use the structural uncertainty generated by governments to further consolidate their quasi-monopoly. (Süddeutsche Zeitung, 15 May 2017)

If the analysis provided above is correct, then the real threat to democratic capitalism under conditions of a digitized economy does not originate with companies. In fact, the conditions of post-democracy are such that cybersecurity is often imagined as a natural problem which arises simply from the fact that more and more aspects of life are being digitized. The author of the present article takes an opposing view when he argues that many (possibly all) instances of cybercrime could be prevented if governments refrained from spying on their citizens. Not because this would somehow cause cybercriminals to turn their activities elsewhere, to be sure, but because then governments would not exploit security gaps but would instead help to close them:

> The world of cyber security works according to different rules. Imagine the government regularly sending a horde of well-paid and educated saboteurs to weaken the flood barriers and earthquake warning systems in our homes. Our only way of guaranteeing security would be the private sector, either in the form of better closures or better insurance. In this situation we find ourselves, however, cyber security disasters are almost entirely home-made and thus avoidable. In theory, governments might even agree with the statement that we need to strengthen personal rights in the face of all these threats. In reality, however, we all know that this would only result in governments sending more saboteurs with even more effective instruments to weaken our shields. Under these circumstances, who would stick to their trust in law and politics instead of choosing the protection that the market promises to offer? Unfortunately, cyber security is just one of many examples in which the legitimacy of democratic capitalism and also of the social democratic parties has expired, even if the approaches to discussion are still open. No wonder social democratic parties are collapsing. The elections in the Netherlands and France have shown that they claim to defend a system that does not follow words with action. (Süddeutsche Zeitung, 15 May 2017)

The upshot of the article’s discussion seems to be that the trade-off between security and privacy on which large parts of the surveillance discourse turn is in fact a false trade-off. The notion that there is such a trade-off only appears plausible when considered for non-digitized societies where it might be possible to achieve some level of surveillance without simultaneously putting all stakeholders at risk.

5.2.3 A Culture of (Cyber)Insecurity

In the same vein, many civil rights organizations in Germany argue that allowing LEAs to use ransomware is likely to create a culture of insecurity:

> Experts: "Trojan Blind Flights Act" would promote "culture of IT insecurity"

> Experts warned at a hearing against the CDU-SPD plan to provide prosecutors with Trojans. Prosecutors and the BKA [the German Federal Criminal Office] welcomed the project without compromise. With the legislative initiative to grant investigators a comprehensive licence to use state trojans in the fight against serious crimes, the German government has unpacked "the big guns". Ulf Buermeyer, judge at the Berlin Regional Court, made the statement at a hearing in the Bundestag on Wednesday. Those affected would thus be completely transparent to investigators, a situation criminal law has never known before: "From the POV of the rule of law, this is a really big picture". Buermeyer reminded the government that the Federal Constitutional Court set "the strictest guidelines" for this. Digital bugs should only be installed on IT devices when there is a "concrete danger for a crucial legal asset". The price for the use of such surveillance software for a constitutional state has proven to be very high: security gaps are necessary in order to be able to infect a target system. These could be exploited by any hacker, which would "contribute massively to the culture of IT insecurity". […] (Heise, 1 June 2017)

Taking into account the arguments discussed above exposes the weaknesses in the court’s position. The problem with installing procedural (legal) measures to control the use of zero day vulnerabilities by LEAs misses the problem, namely that the mere existence of these security gaps is responsible for a culture of (IT) insecurity. Without these vulnerabilities, however, increased surveillance is impossible. Setting up legal guidelines to control this kind of surveillance therefore misses the point of the critics since the problem seems to lie in the mere existence of security gaps, not in the fact that they might be exploited by the police.

If anything, the problem is exacerbated by the fact that the CIA seems to be utterly unable to protect their vulnerabilities from cybercriminals:

> Everyone can now read about CIA technology at WikiLeaks - and rebuild it. The federal government has even established a new authority called the Central Office for Information Technology in the Security Sector (Zitis). According to the Ministry of the Interior, it is to develop "technical tools in the fight against terrorism, cybercrime and cyber espionage". When Zitis starts work soon, the office will face a difficult decision: Should it buy such zero-day exploits and use them to fuel the business so that the authorities can continue to listen in or read along? In the end, this decision will lie with the Federal Minister of the Interior, who is actually a representative of a consistent encryption policy without any back doors used by the state. According to many experts, the cyber world is the battlefield of the future. In the history of the military, the bullet has always won against the armour. That is why there is arms control and disarmament negotiations. But in the area of the Internet, the discussion on the necessary rules of international law has yet to begin. The latest leak shows that the CIA is not even able to protect its cyber weapon blueprints: Everyone can now study their technique at WikiLeaks. And to recreate many a weapon. (Süddeutsche Zeitung, 11 March 2017)

The above excerpt suggests that given even mediocre technical skills, anybody can now go on WikiLeaks and build their own cyber weapons. This is hardly a cause for increased trust in the Internet infrastructure. What is striking above is the claim that the official position of the German interior ministry actually opposes zero day exploits precisely because of the dangers explained above. The problem, the second half of the excerpt suggests, might lie somewhere else entirely: With cyberspace, there do not seem to exist binding (international) rules at the moment to regulate the issues at hand. In any case, the article reinforces the suspicion that cyberspace is, as of yet, full of ambiguities which translate directly into ambiguous government positions. And as if this weren’t enough, the NSA has been exploiting security gaps on a global scale all along.

5.2.4 Intelligence Hacks: Secret Services as Cybercriminals?

In 2017, WikiLeaks published extensive documents about cyber weapons developed by the CIA:

> The documents and data, some of which have been edited because freely accessible cyberweapons are very dangerous, reveal the hacking programs and projects of the American secret services and make it clear once again after the NSA leaks that the US secret services have their fingers in the game worldwide and exploit security gaps to penetrate Samsung smartphones (iPhones, Android), computers or Internet-connected televisions, steal or manipulate data and transform them into eavesdroppers. For example, the CIA's Engineering Development Group, in cooperation with the British MI5, is to be able to convert televisions in hotels, even if they are switched off, into eavesdroppers. So far it is assumed that the material is authentic. (Heise, 8 March 2017)

The above paragraph suggests that the methods employed by secret services such as the NSA are not that different in principle from those employed by cybercriminals. The next paragraph lays out in detail these methods. The descriptions do not sound any different from descriptions of cybercriminal activities:

> The CIA has developed numerous Zero Days for IOS, acquired from the FBI, NSA or GCHQ or private cyber weapons manufacturers. For Android, the secret service had 24 "zero days" in 2016 alone, which can be used as weapons and bypass the encryption of applications such as WhatsAPP, Signal or Telegram. "This incorrectly implies CIA hacked these apps / encryption. But the docs show iOS/Android are what got hacked - a much bigger problem." - Edward Snowden Not only does this leave the devices vulnerable to the secret services, the vulnerabilities can also be exploited by others. The situation is similar for computers and routers with Windows, OSx and Linux operating systems. Since the CIA kept the security holes to itself and did not pass them on to the IT companies, as the Obama administration had actually ordered, the documents make a violation of these orders clear. WikiLeaks points out that the victims are not only individuals whose devices can be hacked, but also the government and Congress as well as large corporations and system administrators. And if the CIA hackers have also successfully hacked anti-virus programs, the secret services, which are supposed to protect national security, are undermining them. (Heise, 8 March 2017)

The above paragraph strikes a familiar chord: Despite being designed to protect national security, the activities of secret services in cyberspace go a long way at undermining the cybersecurity of citizens, as the secret services employ security gaps which are then very much open to be exploited by cybercriminals as well. The reader also learns that the CIA had actually been obliged by the US administration to report those gaps, which it did not. This reinforces the suspicion, on the part of the readers, that secret services are behaving just like cybercriminals, to the detriment not just of citizens, but also governments and businesses.

The next excerpts hints at the possible scale at which secret services worldwide (not just the CIA) were in fact exploiting security gaps. The examples given suggest to readers that many of the uses these security gaps were put to might not be in the general public’s best interests:

> A department called the Automated Implant Branch (AIB) has developed programs for automated infection of computers by various means and the control of malware such as Medusa or Assasin. It is very important that the cyberweapons or malware cannot be traced back to the CIA or the government in a forensic investigation. This will be no different with other intelligence services such as those of Russia or China, from which it can be deduced that the recently claimed attributions of hacks to Russian groups with links to Russian intelligence services on behalf of the Kremlin are great theatre. But the CIA wasn't just about eavesdropping and access to data. In October 2014, they were looking for ways to access the control systems of new cars and trucks. Reasons are not given, but it would be

> possible to stop vehicles from a distance or, as WikiLeaks notes, to make attacks that cannot be traced by accelerating the vehicles and allowing them to drive against an obstacle. (Heise, 8 March 2017)

The above paragraph is striking because it fleshes out some of the (immediate) (geo)political implications of zero day exploits. The attack strategies developed and employed by secret services are such that the attacks be untraceable. Since many countries have secret services, it can be assumed that they do not work in principally different ways. Therefore, the untraceability is a mutual fact about them, which, the above excerpt argues, makes recent allegations of cyberattacks (e.g. by Russian hackers on the US elections) mere “great theatre”.

> WikiLeaks aims to highlight the problems associated with previously uncontrollable cyberweapon programs. Once developed, cyber weapons are difficult to control. They could be stolen or copied by anyone, especially since the people who develop them also know how to make copies without leaving a trace. This is also a dangerous problem because there is a black market where criminals, the military or secret services pay a lot of money for cyber weapons. The secret services and contractors such as Booz Allan Hamilton have already had some data theft by insiders (which is also proven by their own leak). In February, Harold Martin was accused of collecting 50,000 gigabytes of secret CIA and NSA programs. (Heise, 8 March 2017)

The last paragraph discusses some of the rather dangerous implications of governments and secret services getting in on black market transactions of cyber weapons. The problem here is that cyber weapons get out of hand easily (much more easily than, say, missiles). Additionally, since these are digital devices, it is hard to detect who is in possession of copies. In this way, governments are indirectly fuelling black market transactions with cyber weapons.

To sum up briefly: The excerpts discussed in this section depict the Internet as a contested territory where governments attempt to seize control, in many cases through the same means employed by those labelled “cybercriminals”. All these allegations create what is repeatedly termed a “culture of insecurity” because in the scenarios described, it is governments who are responsible for not closing vulnerabilities, thereby putting citizens’ cybersecurity at risk.

5.2.5 Insecurity and Responsibility: The Ignorant User Reloaded

Interestingly, the same news outlet (Heise) offers a by now familiar argument to the effect that cybersecurity is to a large degree the users’ responsibility:

> "From the consumer's point of view, the threat has intensified significantly," Thomas Kremer, DsiN CEO and data protection expert at Deutsche Telekom, summarized the results. The knowledge of consumers about safety hazards has increased significantly, "but it is applied practically less". This is a "rather worrying result", as it creates a safety gap. (Heise, 24 May 2017)

Given the frequency of reporting about security gaps it should be hardly surprising that the knowledge about them has increased. As to that knowledge being applied less, this is hardly surprising if it is true that security gaps are largely the result of government action. The remedy proposed then strikes a very familiar chord:

> Appeal for data protection
>
> For the expert, the most important thing to do is "to motivate" the user. Again and again it is important to explain that security updates really have to be installed, that "123456" is not a secure password and should not be clicked on every mail attachment. In dealing with critical security gaps, he pleaded for a reporting obligation, as otherwise the risk for all would increase. Politics and

> business would have to ask themselves whether it was okay to set up "digital armouries". "State agencies should not collect any important security gaps that are in danger of being exploited by third parties," said Parliamentary State Secretary for Justice Ulrich Kelber. At the same time, however, he supported the initiative of the grand coalition to significantly expand the use of state trojans. The SPD politician assumes that "consumers expect safe devices". In view of the increasing complexity of the technology, it is impossible to protect oneself alone. Therefore, the service providers bear a high responsibility "that the systems have a basic security" and that this is maintained over the life of the product. (Heise, 24 May 2017)

Users, readers learn, need to be motivated. Interestingly, the expert cited in the above excerpt calls for a duty to report security gaps on the part of the users. Since users are (by definition) not security experts, the statement appears to be another example of the construction of the user as ignorant. At least it is acknowledged that security gaps which are unfixed increase the risk for all Internet users. The excerpt thereby reinforces the notion that what is needed is a culture of security. The *topos* of complexity which comes up in the last third of the excerpt is telling because it appears to be a mere cover-up for the dynamics of zero day exploits discussed at length above. The position of the Social Democratic politician cited above is a perfect example of this ambiguity, as he simultaneously argues for the use of government-controlled ransomware [state Trojans] and the closing of security gaps. Cyberspace then is not inherently ambiguous. Rather, it appears to be convenient for some stakeholders to uphold this idea and to leave the end-user to come to terms with that. Naturally, secret services have a different position when it comes to dangers to (national) security.

5.2.6 National Security and the Damage from Leaks: No Mercy for Whistleblowers

> CIA: WikiLeaks revelations put US citizens at risk
>
> […]
>
> Following WikiLeaks' revelations of CIA hacker attacks on smartphones, TVs and other devices, the CIA has accused the disclosure platform of endangering the lives of US citizens.
>
> Such revelations "not only put US personnel and operations at risk, but also provide our opponents with tools and information to harm us," said CIA spokeswoman Heather Horniak in Washington. The spokesperson did not wish to comment on the authenticity of the documents.
>
> US President Donald Trump is "extremely concerned" about the data leakage from the CIA that made the WikiLeaks revelations possible, according to a spokesman. Speaker for the presidential office Sean Spicer announced on Wednesday that he would take tough action against informants: "Anyone who passes on confidential information will be subject to the full force of the law," he said. (Süddeutsche Zeitung, 9 March 2017)

The simple fact that the CIA chose to comment on the revelations accords them some credibility ("The spokesperson did not wish to comment on the authenticity of the documents"). According to the CIA, it is the leaks, and not the practice surrounding vulnerabilities, that threaten security. Tellingly, however, the security in question is expressly not that of citizens, but rather of "US personnel and operations".

> Thousands of documents published - interception centre probably in Frankfurt
>
> The discovery platform WikiLeaks published more than 8,700 documents on Tuesday from the CIA Centre for Cyber-Enquiry in Langley near Washington. Have them give details of U.S. intelligence wiretapping techniques.

> According to the documents, the hacker force operates from the US consulate in Frankfurt am Main. The consulate was said to serve as a secret base for hackers in Europe, the Middle East and Africa. According to WikiLeaks, US government hackers are attacking Apple iPhones, Google Android devices, Microsoft software and even Samsung TVs to spy on users.
>
> Former US intelligence officer Edward Snowden, who unveiled the massive spy programs of the US secret service NSA in 2013, explained in the short message service Twitter that the documents published were "authentic". (Süddeutsche Zeitung, 9 March 2017)

The revelations discussed in the last two paragraphs concern the case of Germany, as the reader learns that many CIA cyberattacks were launched from Frankfurt, Germany. In any case, the excerpt reminds the reader that secret services appear to have comprehensive surveillance programs in place which target the mobile devices of everyone, not just (cyber)criminals and terrorists.

5.2.7 The Snowden Revelations and the BND Affair: Double Standards for Surveillance

The last theme running through the German surveillance discourse concerns the (domestic) political repercussions of the Snowden revelations and the ensuing discussions about (the extent of) mutual government surveillance:

> NSA scandal
>
> The NSA, the British GCHQ and other Western intelligence services extensively intercept international communication, spy on companies and government agencies and secretly oblige service providers to cooperate. Details were revealed by Edward Snowden. (Heise, 19 January 2017)
>
> The above excerpt gives an impression of the extent of government surveillance even among allies and in democratic states. However, despite the revelations of NSA programs by whistleblower Edward Snowden in 2013, Germany was one of the few countries to launch a full-blown parliamentary investigation.
>
> Secret File NSA Committee
>
> Since 2014, the NSA committee of the Bundestag has been examining the surveillance practices of the German secret services in particular, making the government's attempts at concealment clear. heise online looks back in a detailed series. (Heise, 5 March 2017)

Despite launching an investigation, the German government tried to cover up the scandal for a long term, the above excerpt suggests. As the investigation developed, it gradually touched upon the extent of the scandal.

> A timid attempt at clarification elsewhere
>
> The Bundestag is thus one of the few parliaments in the world to examine the secret service scandal more closely. In Britain, the House of Commons also set up a committee to shed light on the affair. Among others, they invited the heads of the three main national secret services MI5, MI6 and GCHQ. However, they only assured that they complied with all applicable laws.
>
> The British committee listened much more intensively to the then editor-in-chief of the Guardian, Alan Rusbridger. He had started the avalanche with Greenwald's first reports about Prism, but then had to defend the newspaper against accusations that the texts about the Snowden documents had supported terrorists. (Heise, 5 March 2017)

As the above excerpt makes abundantly clear, many governments involved in the espionage scandal preferred to prosecute the whistleblowers instead of starting a discussion about surveillance. This is especially true for Edward Snowden himself, who has been living in Russian exile since the revelations:

> In 2013, Edward Snowden unveiled the extensive surveillance practices of the NSA and its partners in the western world. Since June 2013 he has been living in a secret place in Moscow, but he interferes in current debates via Twitter and video switching not only for surveillance purposes. Russia has so far always rejected the US demand for his extradition and has instead extended asylum in the meantime. The current decision is probably intended to make it clear that even the change of US president will not change that. (Heise, 18 January 2017)

The next excerpt discusses the difficulties faced by investigation committees due the somewhat limited powers of parliaments:

> No help from businesses
>
> Since April 2014, the first committee of inquiry of the current legislative period has been dealing with the mass surveillance by the NSA and the role of the German Federal Intelligence Service in it, which was unveiled thanks to Edward Snowden. Since then, witnesses have been regularly questioned, which has provided at least some new insights into the work of the secret services. The representatives were to give an insight into the involvement of large US companies in the monitoring programmes. The agreed refusal was now unanimously condemned by the leaders of the government factions and the opposition. (Heise, 19 January 2017)

What is more, the investigation committee tried to illuminate matters that had already been revealed in principle by Edward Snowden, a task which was not always supported by the government:

> NSA Committee confirms allegations
>
> The "NSA Committee of Inquiry" of the German Bundestag is a prime example that supports this thesis and brings it out of the realm of conspiracy theories. It is true that in particular the scant handful of the opposition politicians of the Left and the Greens represented therein tried honestly to bring light into the darkness of the state affair and its German entanglements, which Snowden had revealed in principle.

What is striking about the revelations in the course of the investigation committee is the role played by the German secret service and office for the protection of the constitution:

> This has also revealed aspects that make upright democrats and civil rights activists' hair stand on end: Bundesnachrichtendienst (BND) [the German secret service] and "Verfassungsschutz" [office for the protection of the constitution] supply mobile phone data to the NSA, which carry the secret and in part human rights and international law violating U.S. drone war; the BND even spied on "friends" such as European authorities and companies for the U.S. partner and sucked large amounts of data from a Frankfurt network node and sent them across the pond in some cases. (Heise, 19 February 2017)

Apparently, readers learn, the role of the German secret service was less than glorious:

> But the matter is even worse: the "counter intelligence" of the local domestic intelligence service feels neither responsible for the Chancellor's intercepted mobile phone nor for the communication protection of German citizens in general. There are control instances for the mighty secret service apparatus, but these can be seen as symbolic in their range. (Heise, 19 February 2017)

Incidentally, the investigation committee was only installed after it became public that the NSA had spied on Chancellor Angela Merkel’s mobile phone.

> Secret file BND & NSA: The Merkel mobile phone as a catalyst
>
> Dozens of revelations about the massive surveillance of all people by Western secret services were not enough: It was only when it became known that the Chancellor was also spied on that was enough to set up a committee of inquiry.

The blatant criticism above suggests that for a long time, the governments involved in the surveillance scandal refused to take action. For many, the situation looked as if there was a double standard being applied:

> Katrin Göring-Eckardt of the Greens, however, criticized that the wire to the USA was only now glowing. The government is probably applying double standards and distinguishing between data protection for the citizens and for the Chancellor. Initial calls for a parliamentary committee of inquiry have now also been heard from the opposition. (Heise, 5 March 2017)

To be sure, Germany was one of the few governments to launch a full-blown investigation, but only after the government could not deny any more that even Chancellor Angela Merkel had become an NSA target.

> The affair really got going in this country, not because German citizens were being investigated overall, but with further indications of the targeted surveillance of the Chancellor. At the end of October 2013, Der Spiegel saw the evidence so strong that it reported on Angela Merkel's bugged cell phone and listening stations on the roofs of several foreign embassies in Berlin's government district. The agents apparently benefited from the fact that the Chancellor and CDU leader used different mobile phones in their different positions, all of which could not encrypt calls in principle. (Heise, 5 March 2017)

The reports about the investigation reveal a web of mutual ignorance and irresponsibility (or rather: non-responsibility) among officials:

> No recollections of praise or criticism
>
> He himself could also remember neither criticism nor praise "from above", Heiß said soberly. Several members of the committee did not understand what he said. SPD chairman Christian Flisek spoke of an "oath of revelation for the functioning of supervision" and a certificate of poverty. "They closed their eyes," he accused the witness. The Green Constantine von Notz appeared "deeply frustrated" that obviously nobody should be to blame. His colleague from the left, Martina Renner, asked if the chancellor's office could be fooled by the BND. At the latest from the hint that the Chancellor's cell phone had been tapped, it would have been necessary to investigate whether the BND was also investigating ministers, presidents, government agencies or representatives of the people.
>
> Members of parliament are not sacrosanct per se, the defendant replied. "It is quite possible to monitor parliaments." But it depends on "in which country". He could not discuss details in public. In general "we had to prepare many other things in the context of the Snowden publications. We didn't look for any special topics." (Heise, 26 January 2017)

Many of those in charge refused to give answers, apparently. The reader is left to wonder whether the extent of the affair could be even bigger. This is especially pressing when considering the extent to which political decision makers were (not) involved in the operations:

> BND espionage: Pofalla never informed Chancellor about spied friends
>
> Former head of the Chancellor's Office Ronald Pofalla wanted to wait for a report from the secret service before talking to Merkel, after being told that the BND had spied on "friendly embassies" in crisis countries. But he never came.

> A kind of "waiting for Godot" was the reason why Chancellor Angela Merkel (CDU) repeatedly issued her famous slogan in the summer and autumn of 2013 that spying among friends was not an option at all, and the Federal Intelligence Service (BND) practiced this in parallel. At least former Chancellery Minister Ronald Pofalla described the tricky situation in the year of the first Snowden revelations on Thursday in the NSA committee of inquiry of the Bundestag. (Heise, 27 January 2017)

The entire affair also throws into light the relationship between the US and Germany more generally:

> Meaningful omission
>
> Merkel is said to have called US President Barack Obama on the same day. A spokeswoman for the US government told Der Spiegel that the person called assured the Chancellor that "the United States will not monitor and will not monitor its communications". Obama explicitly left open whether this also applied to the past. This could be interpreted as an admission that Merkel had been on the NSA target list or had at least got into interceptions around third parties. Shortly afterwards, the Frankfurter Allgemeine Sonntagszeitung confirmed that Merkel's mobile numbers had been on a list of NSA intelligence targets since 2002. According to Bild am Sonntag, Obama is said to have known about this since 2010. Keith Alexander, then head of the NSA, wants to inform him personally about the secret operation this year. The US president did not stop the action at first, but let it continue, the newspaper quoted a high-ranking NSA employee. The secret service was even able to investigate the allegedly bug-proof female chancellor's cell phone of a recent date, the paper continued. The eavesdropping attack against Merkel has therefore continued into the recent past. Former Chancellor Gerhard Schröder and other German government representatives are also said to have been in the sights of the US secret services, which documents later substantiated on WikiLeaks. However, since the telephone numbers contained therein were shortened by the final digits, the judiciary in this country did not want to regard them as proof of the interceptions carried out and to investigate them further. Crypto phones can encrypt calls and make them difficult to intercept, but this only applies to connections with comparable devices. It is not technically possible to keep conversations with unencrypted recipients confidential. However, the data stored on a crypto mobile phone such as the address book, documents or appointments should be protected against unwanted access by third parties as long as there are no backdoors or weakness in the operating system used. (Heise, 5 March 2017)

Apparently, the US had spied on German officials for over a decade. Despite her involvement in the affair, Chancellor Angela Merkel was unable during the investigation committee hearing to provide clarification:

> In the "grand finale" of the committee hearings in mid-February 2017, Merkel herself, as the last witness, was hardly able to contribute anything to the clarification. When she received hints on a paper "from which it could emerge that a mobile phone could possibly be monitored by me by US services", the Chancellor's main concern was to learn more about the facts of the case. In a telephone conversation with the then US President Barack Obama, she made it clear shortly afterwards that she disapproved of such activities. However, the investigation of the case by the Federal Public Prosecutor General ultimately "did not produce anything provable". The fact that her mobile phone had suddenly become the focus of attention "was not the central question for me, especially since I have cryptic communication options at my disposal," reported Merkel. The "interests of all citizens" had been the focus of her work, even if the suspicion of "mass spying" on large sections of the population that arose with the Snowden publications had, in her opinion, not been substantiated. The NSA affair finally ended the Chancellor and thus continued Ronald Pofalla's legacy. (Heise, 5 March 2017)

Her role was therefore discussed less-than-favourably by many German newspapers:

> Merkel in the web of ignorance
>
> The Chancellor presents herself innocent and ignorant in the NSA committee. Her government has fervently promised clarification - but has by no means kept to it.
>
> "It's an innocent thing that just went to confession for nothing." This is what Mephisto says about Gretchen in "Faust". And so Gretchen-like innocent Angela Merkel presented herself in the NSA committee of inquiry. She had not known anything about anything - nothing about the great wiretapping, nothing about the involvement of the Federal Intelligence Service in it, nothing about selector lists with which the BND was at the service of the USA. What Merkel did not say: Nor did her government do anything to clarify these actions that violate fundamental rights. The Merkel government has fervently promised clarification, but has by no means kept to it. (Süddeutsche Zeitung, 16 February 2017)

Merkel is portrayed here as confessing only to those aspects of the affair which could not be denied any longer. The tone of the excerpt suggests political irresponsibility with respect to fundamental (privacy) rights. Overall, the investigation committee is not portrayed as having been very successful at pinpointing political responsibility:

> The members of the Bundestag's committee of inquiry want to know a lot about the Chancellor. But Angela Merkel is not really willing to tell them much.
>
> Witness Dr. Angela Merkel has been questioned for about two and a half hours as the NSA committee of inquiry is concerned with the truth. By name, so to speak. Hans-Christian Ströbele of the Greens, a former master of parliamentary enlightenment, wants to know why the German government is not making it possible to question Edward Snowden, the man who unveiled the NSA affair worldwide. Ströbele suspects that the conflict with the Americans is shy, Merkel withdraws that the matter will be properly examined by the responsible ministries. (Süddeutsche Zeitung, 16 February 2017)

The above excerpt hints at the dynamics of the investigation committee. As the government is the target of the investigation, it falls very much on the political opposition (in the present case represented by the Green Party and the Left) to provide clarification. As the excerpt further suggests, it was precisely the government which thwarted attempts to question Edward Snowden (the original whistleblower) as a witness. Furthermore, Merkel’s initial reaction to the allegations had been to wholeheartedly condemn the alleged activities:

> Did she apologize to spied colleagues? No, the Chancellor answers
>
> Merkel first reads out an explanation from several sides. It takes her 25 minutes. "This is my memory I brought you," she would later say about the text. In it, she herself raises the issues that also interest the Members of Parliament most in the survey. The first is her well-known sentence from 24 October 2013, after it became known that her mobile phone had been tapped: "Spying among friends, that is not possible at all". It is important to Merkel that she has repeatedly advocated this principle since the beginning of the NSA affair. Apparently she wants to prevent the impression that she got really angry when the affair affected her personally. (Süddeutsche Zeitung, 16 February 2017)

Incidentally, that is precisely the impression that the public got, according to the media. So long as it had not been revealed that Merkel had been personally affected, the argument goes, government tried (successfully) to downplay the affair.

> The sentence, says Merkel, appeared to her at the time "from a German point of view as triviality", as a matter of course. But then he became a boomerang for the federal government. In the months that

> followed, it became known that the NSA's Federal Intelligence Service, with the help of so-called selectors, had not only provided technical assistance in spying on friendly states, but had even controlled such activities itself. "It was clear to me that this was incompatible with my political supremacy," admits Merkel. The activities had been discontinued. But, she admits, it is also thanks to the committee of inquiry that we have an overview of this today. (Süddeutsche Zeitung, 16 February 2017)

What is more, the extent of the affair was such that the German secret service was very much a part of the NSA activities. Therefore, pretending to be a victim was not an option for long:

> The Chancellor's Office acted as a victim, at the same time the BND listened to politicians all over the world
>
> Next Thursday, Dr. Merkel, Angela, has been invited to appear as a witness before the NSA Investigation Committee. This is probably the last meeting, the finale of a committee set up after the whistleblower Edward Snowden was revealed to find out what and whom foreign secret services intercept in Germany. After 130 meetings, you are no smarter than you were at the beginning of the summer 2013 affair. Snowden never testified. And yet this committee has a chance to go down in parliamentary history as one of the most successful. He revealed how the government deceived the public and parliament after the start of the NSA affair, sometimes concealed the BND's own role in the global wiretapping business, misrepresented it in a targeted manner or even did not want to know exactly about it. The list of misleaders is as long as the small and large questions which members of the Bundestag have addressed to the government since the beginning of the affair, which can still be viewed in the parliamentary archives today, and which have been answered incorrectly or incompletely. (Süddeutsche Zeitung, 13 February 2017)

The above paragraph is very explicit as to how the affair was one of deliberate deception of the public by government officials. The only thing the investigation committee could only incompletely work through was the extent to which the involvement of the German secret service was actually known to the executives. The next paragraph suggests that the government representatives chose to only admit to those aspects of the affair which could not be denied any longer:

> The government also missed subsequent opportunities to correct the initial picture of the affair. For example, when it came out in 2014 that the BND had listened in on a conversation between Hillary Clinton, then US Secretary of State, and Kofi Annan, then UN Secretary-General. The matter could not be concealed. The CIA had hired an agent from the BND to deliver a copy of the wiretapped call to the Americans. Justice Minister Heiko Maas was informed by the Federal Prosecutor's Office about the bizarre case, and the Chancellor's Office also found out about it. "I used to have to pay for this kind of entrance fee," Maas amused himself in front of confidants. Merkel's word that listening among friends was inappropriate was shaken. But the government declared that it was only a regrettable individual case, a "by-catch". Such communication was "not specifically collected", the Chancellor's Office explained to parliament and was therefore not at all comparable to NSA practices. (Süddeutsche Zeitung, 13 February 2017)

6 Outlook: Dominant meta-topics in cybersecurity discourse

As Niklas Luhmann observed[7], trust is inherently tied to risks. Where there is risk, there is, as he expressed it, contingency. Contingency in this sense is the domain of the social sciences. Since human beings cannot look into the future, human (inter)action always contains an element of contingency. Trust, Luhmann argues, is the solution moderns have found for this problem. Where action is required but outcomes are essentially unforeseeable, (inter)action is potentially risky and humans need to trust. The degree to which humans normally trust is determined by what Alfred Schütz[8] and others have referred to as everyday knowledge (which, insofar as it pertains to risk, includes knowledge such as “do not go into the park after midnight”, “do not get into cars with strangers” etc.). The Internet, it seems, has exacerbated problems of trust formation because it constitutes an infrastructure so vast that it is essentially impossible to overview. Criminologists have long (at least since the 1970ies) conceded the role played by the media in shaping perceptions of crime[9]. Levels of (public) concern are, many classic studies argue, determined more by media representations of crime (e.g. of certain areas as dangerous) than by actual victimization (which is usually much lower than levels of concern). Therefore, special attention needs to be paid to media representations of cybersecurity/cybercrime in order to develop a comprehensive understanding of public trust in the ICT infrastructure.

This last section identifies four meta-topics, which can be identified across the different case studies and play a significant role in shaping the often conflicting positions in public discourse. Especially regarding the creation of a “trustworthy internet” there is a high degree of disunity and uncertainty about cybersecurity measures, which shapes an ambivalent “discursive arena” including state, economic/business and civil actors.

6.1 Enforcing Cybersecurity: Co-Construction of Users and Technologies

One of the most striking topics on the discourse on cybersecurity, data protection, and surveillance concerns the conflicting and often contradictory roles accorded to the end-user. By definition, end-users (alternatively: consumers) are imagined as non-experts who are therefore the legitimate target of intervention such as education and awareness campaigns to prepare them for cybercriminal attacks. In particular, the construction of users is dependent on constructions of cyberspace and associated technologies. When these technologies are imagined as increasingly complex and abstract, users are imagined as increasingly ignorant and in need of education. The underlying narrative is that of a quickly evolving universe of cyber threats which are not met by an equally quickly evolving set of cybersecurity skills. The issue has at least two dimensions:

On the one hand, individuals are constructed as responsible customers. Here, the prevailing argument claims that with increasingly powerful cybersecurity architectures in place, cybercriminals turn to targeting the end users, who therefore need to be constantly reminded/educated about potential threats and mitigation strategies. On the other hand, cybersecurity skills are constructed as a business factor. In media discourse, the responsibility for acquiring these skills is accorded squarely to the individual, though this time in the context of a quickly evolving labour market.

[7] Luhmann, Niklas. (1979). Trust and Power. Two Works by Niklas Luhmann. With Introduction by Gianfranco Poggi. Chichester: Wiley.

[8] See for example Gardiner, Michael E. (2006). Everyday Knowledge, in: Theory, Cutlure & Society, Vol. 23(2-3).

[9] Furstenberg, Frank F. (1971). Public reaction to crime in the streets. In: *The American Scholar* 40, 601-610. Reprinted in: Jason Ditton; Stephen Farrall (Eds.). (2000). *The Fear of Crime*. Dartmouth u.a.: Ashgate, 3-12.

Developing cybersecurity skills is not to be confused with the general task of handling cybersecurity risks which are the responsibility of the service provider, which still is a base line for all cybersecurity measures. But the allocation of responsibility to the consumers of ICT products and services has to be seen in relation to the growing issue of "social engineering". Responsibility on the part of individual users is here constructed as necessitated by growing complexities. In fact, readers learn, it is the very measures businesses have put into place to protect their customers' data which have led cybercriminals to pursue other strategies geared more towards individual users as opposed to IT infrastructures. This shift highlights the point that trust and privacy are dispersed across a user's experience of the Internet. It takes us back to the concept of the Internet as a trusted infrastructure rather than as individual services.

6.2 Data Subjects: Risks for Privacy and Control

The notion of data subject is fundamental to all discussions of data collection, privacy, and control over personal data. It is therefore hardly surprising that a variant of this notion is present in (almost) all the articles sampled here. Personal data and data subjects are, it seems, two sides of the same construct. In so much as data are imagined to be the object of legitimate control, data subjects are imagined to be the subjects who exercise (or should have the right to exercise) said control. The implicit theory of privacy contained in this construction can be summarized as follows: Privacy concerns some aspects of an individual's life that, when somehow assessed or measured, turn into "(personal) data" that can be separated from the individual to be processed and shared, and that there are legitimate and illegitimate ways to do so.

Personal data therefore are imagined as distinct (or distinguishable) from individuals and capable of developing a life of its own. The discourse operates on the assumption that there are legitimate and illegitimate ways to handle personal data, which justifies qualifying some instances of data processing as legitimate and others as illegitimate. Personal data are constructed as private and as belonging to individuals, which simultaneously reinforces the notion that individuals should have at least some control over their data.

The notions of privacy, of control over personal data and data subject can therefore be interpreted as co-constitutive, i.e. one would not exist without the others. In other words, data subjects are simply assumed to have certain qualities (a right to their data, for example) to argue for rights and obligations. What is striking about these constructions is the approximation of data and property; the notion that something is "private" is very closely aligned with the notion of property. Even though nothing is explicitly said about property by labelling data (something very abstract) as "private", this conceptualization nevertheless resonates with conceptions of property. Privacy norms and privacy regulations are introduced as a means to protect the consumer. The latter is thereby interpreted as an entity worthy of (legal) protection.

A *topos* which pops up frequently in the all three case studies (UK, Austria/Germany, and Spain) is that of individual responsibility. Consumers or end-users of digital products and services are imagined in some sense or other to be in control of what happens to their data and who are therefore responsible (at least to a degree). The role accorded to individual responsibility becomes evident only when considered from the following viewpoint: One, information is an asset and two, assets need to be protected. This protection is supposed to be in the consumers' best interest.

Responsible "agency" is therefore nothing more than a driver of innovating business models: constructing consumers first as responsible for their data and then as worthy of protection opens up the space to commodify said protection. This commodification is cast in overtly positive terms, but the reader is left to wonder: If consumers are indeed responsible, active agents of their own data, why would they need businesses to take care of that for them?

6.3 Cyberspace as Contested Territory

The dominant theme in German surveillance discourse is the dilemma associated with so-called zero day vulnerabilities or zero day exploits. Under certain circumstances (e.g. when fighting terrorism) it can be opportune for intelligence agencies not to fix known security gaps (by informing the responsible actors such as service providers) in order to exploit them. However, security gaps are a loop hole not only for state-employed hackers, but potentially also for everyone else with the right set of skills and tools. Therefore, their mere existence produces a dilemma: Is it legitimate to deliberately weaken cybersecurity in the name of domestic security? The exploitation of such “zero day vulnerabilities” or if not yet implemented the lobbying for such tools seems to be common among intelligence and law enforcement agencies and is a topic widely discussed in German media. Such vulnerabilities can be exploited by everyone with the right IT skills; therefore, one argument goes, keeping such security gaps open inadvertently puts the cybersecurity of law-abiding citizens at risk. The growing federal interest in such security gaps has brought about a profitable market for zero day vulnerabilities. Black markets for cyber weapons (which target these vulnerabilities) are therefore no longer just the domain of cybercriminals.

Vulnerabilities are here discussed as investments for governments and their LEAs. Governments buy scouting software developed to discover weaknesses. Some of them are then allegedly reported back to the industry. However, since the aim of scouting for vulnerabilities is, ultimately, to increase possibilities for surveillance or to get access to incriminating data (acquiring digital evidence for criminal incidents), governments/governmental security agencies have also an interest not to report every exposed weakness. On the face of it, this does not sound problematic, provided governments abide the rule of law and exploit these vulnerabilities in service of their citizens’ security – as is argued by state security actors. The WannaCry attack early in 2017 was used by critics as a good example for why that strategy is problematic. The security gap in the Windows operating system which was then exploited by the WannaCry virus had reportedly already been discovered by the NSA, but had remained open. Opponents of the practice therefore routinely point to the fact that once opened on a suspect’s device, backdoors can be exploited by anyone (not just the police). Additionally, once a device is compromised, the police can access not just ongoing communications (for which there should be a legitimizing judicial decree) but any other personal data not related to a specific ongoing investigation.

The underlying issue is whether there is a trade-off after all between closing and exploiting vulnerabilities. However, it is also evident that the precise kind of trade-off between privacy (of individuals) and security (of nation states) depends on the position one takes. It appears as if both opponents and advocates of government surveillance accept this dichotomy, although some stakeholders make claims to the effect that in a digitized society, expanding surveillance might not simultaneously increase global levels of security.

The increasing culture of surveillance, the argument goes on, has effectively weakened democratic culture to a degree that has enabled cybercrime as we know it (e.g. global ransomware attacks) in the first place. Trust has arguably been eroded by surveillance and been replaced by a form of corruption. The supposed trade-offs between security and privacy might in fact be a false dichotomy based on the assumption that cybercrime is – much like “ordinary” crime – just a natural consequence of digitization that we have to live with. The problem with installing procedural (legal) measures to control the use of zero day vulnerabilities by LEAs misses the problem: The mere existence of these security gaps is responsible for a culture of (IT) insecurity. Without these vulnerabilities, however, law enforcement would be very limited in gathering digital evidence and detecting criminal behaviour. But even setting up legal guidelines to control this kind of surveillance activities cannot calm the voices of critics since the problem seems to lie in the mere existence of security gaps, not in the fact that they might be exploited by the police.

7 Attachment A: List of media articles

Daily Mail (8.5.2017): Cure for shopaholics: Now we can block our cards from online shopping to tackle fraud - or curb sprees. URL: http://www.dailymail.co.uk/news/article-4483138/Now-block-cards-online-shopping.html

Daily Mail (4.1.2017): Electronic voting risks cyber attacks, says former MI6 chief as he slaps down John Bercow's wish to introduce the system. URL: http://www.dailymail.co.uk/news/article-4086076/Electronic-voting-risks-cyber-attacks-says-former-MI6-chief-slaps-John-Bercow-s-wish-introduce-system.html

Daily Mail (28.4.2017): Knife crime has soared to a five-year high since Theresa May curbed police use of stop and search tactics, new figures reveal. URL: http://www.dailymail.co.uk/news/article-4452278/Police-record-5-5million-fraud-computer-offences.html

Daily Mail (31.3.2017): Bank fraud up as criminals hit individuals: Efforts by lenders to bolster IT security leads fraudsters to bombard customers with scams. URL: http://www.dailymail.co.uk/news/article-4366670/Bank-fraud-criminals-hit-individuals.html

Daily Mail (20.3.2017): Two Russian hackers are charged with money laundering after 'stealing more than £2million from UK banks in a sophisticated cyber fraud'. URL: http://www.dailymail.co.uk/news/article-4332126/Russian-hackers-charged-2m-cyber-fraud.html

Daily Mail (12.4.2017): Santander fobs off fraud victims in just 24 hours: We expose loopholes that may explain why so many of the bank's customers are being hit. URL: http://www.dailymail.co.uk/money/beatthescammers/article-4402732/Santander-fobs-fraud-victims-just-24-hours.html

Daily Mirror (30.1.2017): George Michael's former boyfriend Fadi Fawaz is victim of identity fraud. URL: https://www.mirror.co.uk/3am/celebrity-news/george-michaels-former-boyfriend-fadi-9721459#ICID=nsm

Daily Mirror (1.4.2017): Go fraud me: Scammers use charity sites to trick kindhearted donors flooding £2 billion industry. URL: https://www.mirror.co.uk/news/uk-news/go-fraud-me-scammers-use-10141963#ICID=nsm

Daily Mirror (4.4.2017): 'Stop trolling Travellers' says police chief who vows to track down anyone posting 'hate crime material' online. URL: https://www.mirror.co.uk/news/uk-news/stop-trolling-travellers-says-police-10153558#ICID=nsm

Daily Mirror (16.3.2017): 5,000 victims a day - the shocking scale of fraud in the UK and 5 ways to keep yourself safe. URL: https://www.mirror.co.uk/money/5000-victims-day-shocking-scale-10034489#ICID=nsm

Daily Mirror (23.5.2017): Former Premier League striker Nile Ranger jailed for eight months for online banking fraud. URL: https://www.mirror.co.uk/sport/football/news/former-premier-league-striker-nile-10485227#ICID=nsm

Daily Mirror (11.1.2017): Brit tourists hit by £1.5million Canary Islands bank card fraud. URL: https://www.mirror.co.uk/news/world-news/brit-tourists-hit-15million-canary-9605634#ICID=nsm

Daily Mirror (24.1.2017): Incredible 1,266% jump in cyber fraud as criminals switch to new tactics to steal your cash - how to stay safe. URL: https://www.mirror.co.uk/money/incredible-1266-jump-cyber-fraud-9679362#ICID=nsm

Daily Mirror (30.3.2017): Fraud soars as £24 stolen every SECOND from honest Brits - how you can stay safe from the criminals. URL: https://www.mirror.co.uk/money/fraud-soars-24-stolen-every-10127533#ICID=nsm

Daily Mirror (16.3.2017): Abta cyber attack leaves 43,000 holidaymakers at risk of identity fraud after email addresses and passwords stolen. URL: https://www.mirror.co.uk/news/uk-news/abta-cyber-attack-leaves-thousands-10037492#ICID=nsm

Daily Mirror (7.1.2017): Vladimir Putin 'directed cyber hacking campaign to help Donald Trump win US presidential election'. URL: https://www.mirror.co.uk/news/world-news/vladimir-putin-directed-cyber-hacking-9577475#ICID=nsm

Daily Mirror (11.1.2017): Ex-Premier League striker Nile Ranger could be jailed after admitting online banking fraud. URL: https://www.mirror.co.uk/sport/football/news/ex-premier-league-striker-nile-9603220#ICID=nsm

Daily Mirror (7.1.2017): British spies alerted America to Russia's cyber attack on US election. URL: https://www.mirror.co.uk/news/world-news/british-spies-alerted-america-russias-9577651#ICID=nsm

Daily Record (11.6.2017): Banks warn customers not to be taken in by scammers as cyber crime continues to rise. URL: https://www.dailyrecord.co.uk/lifestyle/money/cyber-crime-fraud-advice-safe-10546409#ICID=nsm

Daily Record (22.3.2017): Cyber crime on the rise as one person is targeted a week in West Dunbartonshire. URL: https://www.dailyrecord.co.uk/news/local-news/cyber-crime-rise-one-person-10077231#ICID=nsm

Daily Record (2.3.2017): Three men charged in £400k money laundering and online fraud probe. URL: https://www.dailyrecord.co.uk/news/scottish-news/three-men-charged-400k-money-9948167#ICID=nsm

Daily Record (20.6.2017): Frontline on cyber crime: How police are battling the crooks targeting our personal information. URL: https://www.dailyrecord.co.uk/lifestyle/money/frontline-cyber-crime-how-police-10583846#ICID=nsm

El Mundo (3.2.2017): Libertad con cargos para los dos detenidos en Barcelona por hackear la web del SME. URL: http://www.elmundo.es/cataluna/2017/02/03/5894927546163f7d338b4577.html

El Mundo (5.5.2017): Los 'osos elegantes rusos' que atacan a Macron, Nadal y Belmonte. URL: http://www.elmundo.es/cronica/2017/05/05/5905c9e4e2704ea8198b45ef.html

El Mundo (11.1.2017): Una nueva 'app' tramita el divorcio por Internet "en cinco sencillos pasos". URL: http://www.elmundo.es/f5/descubre/2017/01/11/587616f1e2704e20748b45cd.html

El Mundo (6.6.2017): Protección de Datos sanciona al Pacte del Ayuntamiento de Palma por el 'espionaje' a la oposición. URL: http://www.elmundo.es/baleares/2017/06/06/59364f8cca47413a698b45d4.html

El Mundo (7.2.2017): La Diputación de Bizkaia suspende al funcionario acusado de revelar datos. URL: http://www.elmundo.es/pais-vasco/2017/02/07/589a0d3346163ffe188b45f0.html

El Mundo (8.5.2017): La Policía alerta de una nueva estafa en WhatsApp que promete un año de Netflix gratis. URL: http://www.elmundo.es/f5/comparte/2017/05/08/59109ae1268e3eb7678b463d.html

El Mundo (9.2.2017): Un juez investiga a Santi Vidal por revelación de secretos y delitos informáticos. URL: http://www.elmundo.es/cataluna/2017/02/09/589c7104ca4741e9198b46bf.html

El Mundo (13.3.2017): Tim Berners-Lee, el padre de Internet, cree que la red está en peligro. URL: http://www.elmundo.es/tecnologia/2017/03/13/58c66ed846163f64668b45c8.html

El Mundo (31.1.2017): Hacker' arrestado que hackeó datos de más de 5.600 mossos. URL: http://www.elmundo.es/cataluna/2017/01/31/58907743268e3e736f8b465c.html

El Mundo (31.1.2017): Bailando con lobos. URL: http://www.elmundo.es/economia/2017/01/31/58908755268e3e3d0d8b4586.html

El Mundo (26.1.2017): Y tú... ¿Utilizas en todas tus cuentas la misma contraseña? URL: http://www.elmundo.es/blogs/elmundo/abogadored/2017/01/26/y-tu-utilizas-en-todas-tus-cuentas-la.html

El Mundo (29.3.2017): Los proveedores de Internet en EEUU podrán vender los datos de sus usuarios. URL: http://www.elmundo.es/tecnologia/2017/03/29/58db48a7468aeb19188b4659.html

El Mundo (30.1.2017): Del individuo al contexto en la banca moderna. URL: http://www.elmundo.es/economia/innovadores/2017/05/22/5922a121e5fdeaa5408b4576.html

El Mundo (26.4.2017): ¿Qué me pongo? ¡Lo que diga Amazon! URL: http://www.elmundo.es/blogs/elmundo/el-gadgetoblog/2017/04/26/que-me-pongo-lo-que-diga-amazon.html

El Mundo (23.1.2017): El Defensor reprende a la Junta por airear nombres de parados. URL: http://www.elmundo.es/andalucia/2017/01/23/58850a8c46163f5c768b4651.html

El Mundo (22.5.2017): El peligro de no cumplir con el RGPD a tiempo. URL: http://www.elmundo.es/economia/2017/05/15/59196edb22601ddd6e8b4596.html

El Mundo (23.1.2017): China hará aún más dura su censura de Internet. URL: http://www.elmundo.es/tecnologia/2017/01/23/58860f8c22601dfb548b45e0.html

El Mundo (25.4.2017): La campaña electoral de Emmanuel Macron fue víctima de hackers rusos. URL: http://www.elmundo.es/internacional/2017/04/25/58ff7182ca4741831f8b4657.html

El Mundo (20.1.2017): La inteligencia artificial y realidad aumentada aplicada a los negocios. URL: http://www.elmundo.es/economia/2017/01/20/5882588646163f1b488b4627.html

El Mundo (21.4.2017): El 'boom' del cibercrimen deja 3.000 denuncias al año en Baleares. URL: http://www.elmundo.es/baleares/2017/04/21/58f9b7e322601dba3b8b45e1.html

El Mundo (19.1.2017): La privacidad y la protección de datos en Internet están en manos de los consumidores. URL: http://www.elmundo.es/economia/2017/01/19/5881025a468aeb474b8b456f.html

El Mundo (17.3.2017): Bancos, las tecnologías del presente y del futuro. URL: http://www.elmundo.es/economia/2017/03/17/58cb9f8d468aebc2328b45ee.html

El Mundo (16.5.2017): La Autoritat de Protecció de Dades concluye que la ATC usa los datos fiscales legalmente. URL: http://www.elmundo.es/cataluna/2017/05/16/591b292222601d54688b4655.html

El Mundo (13.1.2017): El nuevo 'big data' sanitario, en marcha este año. URL: http://www.elmundo.es/cataluna/2017/01/13/587899c4268e3e22268b45a0.html

El Mundo (9.2.2017): La ANC pide donaciones para pagar la multa de 250.000 euros por usar datos de manera ilegal. URL: http://www.elmundo.es/cataluna/2017/02/09/589cb789ca4741f1318b465d.html

El Mundo (1.6.2017): Incertidumbre entre las empresas extranjeras por la nueva ley de ciberseguridad china. URL: http://www.elmundo.es/tecnologia/2017/06/01/592faee2e2704e9d738b4685.html

El Pais (5.6.2017): Siete de cada 10 aplicaciones para móviles comparten sus datos con otros proveedores. URL: https://elpais.com/tecnologia/2017/06/01/actualidad/1496311868_473587.html

Express (9.1.2017): EU MELTDOWN: Number of cyber attacks on Brussels servers SURGE amid Russian hacking fears. URL: https://www.express.co.uk/news/world/751773/EU-Brussels-Russia-cyber-hacking-increase-Russia-Julian-King-France-Germany-elections-nato

Express (14.1.2017): Cyber-attackers target security company used by British police to download personal data. URL: https://www.express.co.uk/news/uk/754217/Hackers-target-Cellebrite-Israeli-security-firm-British-police-download-personal-data

Express (3.2.2017): Britain to pump BILLIONS of pounds into CYBER WARFARE against Russia, Michael Fallon says. URL: https://www.express.co.uk/news/uk/762532/Britain-billions-pounds-cyber-warfare-Vladimir-Putin-Russia-Moscow-hackers-St-Andrews

Express (20.5.2017): 'This is not cyber crime - it's WAR' Expert warns hackers exploiting THIS common mistake. URL: https://www.express.co.uk/news/uk/806981/WannaCry-ransomware-virus-NHS-Microsoft-Windows-Operating-Systems

Express (24.5.2017): Ex-Newcastle United striker Nile Ranger jailed for online bank fraud. URL: https://www.express.co.uk/news/uk/808893/Nile-Ranger-Southend-online-bank-fraud-jailed-Newcastle-United-Premier-League

Evening Press (2.3.2017): Aberdeen men charged in connection with £400,000 online fraud and money laundering. URL: https://www.eveningexpress.co.uk/fp/news/local/aberdeen-men-charged-connection-400000-online-fraud-money-laundering/

Guardian (24.1.2017): UK fraud hits record £1.1bn as cybercrime soars. URL: https://www.theguardian.com/uk-news/2017/jan/24/uk-fraud-record-cybercrime-kpmg

Guardian (13.1.2017): London NHS hospital trust hit by cyber-attack. URL: https://www.theguardian.com/technology/2017/jan/13/london-nhs-hospital-trust-hit-by-email-cyber-attackers

Guardian (23.1.2017): Lloyds bank accounts targeted in huge cybercrime attack. URL: https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Guardian (18.4.2017): Met chief prioritises giving officers Tasers and fighting cybercrime. URL: https://www.theguardian.com/uk-news/2017/apr/18/met-chief-prioritises-giving-officers-tasers-and-fighting-cybercrime

Guardian (16.1.2017): Cyber security takes centre stage in the age of Trump. URL: https://www.theguardian.com/small-business-network/2017/jan/16/cyber-security-centre-stage-age-trump-investment-hackers

Guardian (5.5.2017): Cybercrime on the high seas: the new threat facing billionaire superyacht owners. URL: https://www.theguardian.com/world/2017/may/05/cybercrime-billionaires-superyacht-owners-hacking

Guardian (10.1.2017): Germany's spy chief calls for counterattacks against cyber-enemies. URL: https://www.theguardian.com/world/2017/jan/10/germany-spy-chief-hans-georg-maassen-calls-for-counterattacks-against-cyber-enemies

International Business Times UK (28.4.2017): 'TrickBot' malware now targeting 20 new UK banks in fresh cybercrime spree, IBM warns. URL: https://www.ibtimes.co.uk/trickbot-malware-now-targeting-20-new-uk-banks-fresh-cybercrime-spree-ibm-warns-1619186

International Business Times UK (10.3.2017): Europol claims high-tech cybercrime fuelling organised crime. URL: https://www.ibtimes.co.uk/europol-claims-high-tech-cybercrime-fuelling-organised-crime-1610803

International Business Times UK (7.5.2017): UK bank launches 'Great British Fraud Fightback' to help tackle online crime. URL: https://www.ibtimes.co.uk/barclays-launches-great-british-fraud-fightback-initiative-help-tackle-online-crime-1620292

International Business Times UK (5.6.2017): How is cybercrime evolving? Jaff ransomware tied to Russian Dark Web market trading stolen card data. URL: https://www.ibtimes.co.uk/how-cybercrime-evolving-jaff-ransomware-tied-russian-dark-web-market-trading-stolen-card-data-1624744

International Business Times UK (21.2.2017): Kim Jong-un's hacker army may step up cybercrime to offset losses incurred from China's coal ban. URL: https://www.ibtimes.co.uk/kim-jong-uns-hacker-army-may-step-cybercrime-offset-losses-incurred-chinas-coal-ban-1607711

International Business Times UK (23.5.2017): Election 2017: Where do the main parties stand on cybercrime and internet policy? URL: https://www.ibtimes.co.uk/election-2017-where-do-main-parties-stand-cybercrime-internet-policy-1622620

International Business Times UK (18.4.2017): Has your business been hacked? One in five UK firms hit by cybercrime. URL: https://www.ibtimes.co.uk/has-your-business-been-hacked-one-five-uk-firms-hit-cybercrime-1617468

International Business Times UK (26.2.2017): Microsoft launches cybersecurity facility to protect Mexicans against cybercrime. URL: https://www.ibtimes.co.uk/microsoft-launches-cybersecurity-facility-protect-mexicans-against-cybercrime-1608631

International Business Times UK (19.5.2017): 25 Koreans arrested in Philippines for alleged online gambling and fraud. https://www.ibtimes.co.uk/25-koreans-arrested-philippines-alleged-online-gambling-fraud-1622416

Insider (2.3.2017): IT Matters: Cyber security. URL: https://www.insider.co.uk/special-reports/it-matters-cyber-security-9878786#ICID=nsm

Metro (23.1.2017): Millions of Lloyds, Halifax and Bank of Scotland customers targeted in major cyber attack. URL: https://metro.co.uk/2017/01/23/millions-of-lloyds-halifax-and-bank-of-scotland-customers-targeted-in-major-cyber-attack-6400671/

The Herald Scotland (10.1.2017): Robertson calls for more help from UK security agencies to help parties counter cyber-threat. URL: http://www.heraldscotland.com/news/15013216.Robertson_calls_for_more_help_from_UK_security_agencies_to_help_parties_counter_cyber_threat/

The Herald Scotland (2.3.2017): Three charged in £400,000 online fraud probe. URL: http://www.heraldscotland.com/news/15129269.Three_charged_in___400_000_online_fraud_probe

The Independent (17.1.2017): A widening cyber-security skills gap is threatening UK companies. URL: https://www.independent.co.uk/news/business/news/cyber-security-skills-gap-widen-supply-demand-expertise-uk-companies-it-a7529986.html

The Independent (6.2.2017): Online dating fraud: How to identify the most likely scammer profiles. URL: https://www.independent.co.uk/life-style/love-sex/online-dating-fraud-how-to-identify-most-likely-scammer-profiles-scams-a7553616.html

The Independent (3.4.2017): Scientists to study a potential link between autism-like personality traits and cyber crime. URL: https://www.independent.co.uk/news/science/autism-link-cyber-crime-personality-trait-scientist-research-university-bath-dark-web-a7663086.html

The Independent (23.1.2017): Lloyds Bank reported to be trying to identify who was behind a cyber attack against its banking website. URL: https://www.independent.co.uk/news/business/news/lloyds-banking-group-cyber-attack-hacker-police-investigate-online-personal-banking-website-outages-a7541646.html

The Independent (17.3.2017): Brexit risks 'new dark phase' of cyber crime, warns Britain's most senior EU official. URL: https://www.independent.co.uk/news/uk/politics/brexit-cyber-crime-julian-king-eu-commissioner-theresa-may-terrorism-a7634296.html

The Independent (17.4.2017): Cyber crime: British Chambers of Commerce urges firms to ramp up defences after spate of hacks. URL: https://www.independent.co.uk/news/business/news/cyber-crime-security-british-chambers-of-commerce-companies-ramp-up-technology-a7687076.html

The Independent (9.1.2017): Why Artificial Intelligence is the answer to the greatest threat of 2017, cyber-hacking. URL: https://www.independent.co.uk/voices/artificial-intelligence-cyber-hacking-russia-malware-2017-biggest-threat-a7516916.html

The Independent (17.1.2017): .Gmail phishing: Latest cyber attack infects users by mimicking past emails. URL: https://www.independent.co.uk/life-style/gadgets-and-tech/news/gmail-phishing-latest-cyber-security-attack-hacking-infect-users-mimicking-past-emails-a7531981.html

The Independent (6.1.2017): Donald Trump still refuses to admit Russia's alleged cyber hack influenced the election. URL: https://www.independent.co.uk/news/world/americas/donald-trump-russia-cyber-hack-vladimir-putin-president-barack-obama-fbi-cia-intelligence-briefing-a7513966.html

The Mirror (13.1.2017): Massive cyber attack at UK's biggest hospital trust leaves THOUSANDS of patients at risk. URL: https://www.mirror.co.uk/news/uk-news/massive-cyber-attack-uks-biggest-9617475#ICID=nsm

The Mirror (5.1.2017): Russia used cyber propaganda to influence public opinion in Europe, US Senate told. URL: https://www.mirror.co.uk/news/uk-news/russia-used-cyber-propaganda-influence-9569457#ICID=nsm

The Mirror (9.4.2017): Increased threat of cybercrime has fearful Brits longing for return to cash-only society. URL: https://www.mirror.co.uk/news/uk-news/increased-threat-cybercrime-fearful-brits-10192962#ICID=nsm

The Press and Journal (2.3.2017): Two-north east men charged with online fraud worth £400,000. URL: https://www.pressandjournal.co.uk/fp/news/aberdeen/1184393/two-north-east-men-charged-online-fraud-worth-400000/

The Scotsman (21.6.2017): Cyber-crime hub planned for Kilmarnock's Halo project. URL: https://www.scotsman.com/business/companies/tech/cyber-crime-hub-planned-for-kilmarnock-s-halo-project-1-4481994

The Scotsman (21.4.2017): Fraser Nicol: Take control in the cyber-crime fight. URL: https://www.scotsman.com/business/management/fraser-nicol-take-control-in-the-cyber-crime-fight-1-4425103

The Scotsman (2.3.2017): Three charged over £400k online fraud and money laundering. URL: https://www.scotsman.com/regions/aberdeen-north-east/three-charged-over-400k-online-fraud-and-money-laundering-1-4381228

The Scotsman (13.6.2017): Police Scotland to create ‚cadre of experts‘ to beat cyber-crime. URL: https://www.scotsman.com/news/politics/police-scotland-to-create-cadre-of-experts-to-beat-cyber-crime-1-4474003

The Scotsman (23.3.2017): Clear command and control needed in cyber-crime war. URL: https://www.scotsman.com/business/companies/financial/clear-command-and-control-needed-in-cyber-crime-war-1-4401303

The Scotsman (30.5.2017): Cyber crime tops list of finance bosses’ key threats. URL: https://www.scotsman.com/business/companies/financial/cyber-crime-tops-list-of-finance-bosses-key-threats-1-4460668

The Scotsman (22.5.2017): Blockchain consortium seeks to tackle cyber crime. URL: https://www.scotsman.com/business/companies/tech/blockchain-consortium-seeks-to-tackle-cyber-crime-1-4453230

The Scotsman (26.6.2017): ZoneFox ramping up team in fight against cyber-crime. URL: https://www.scotsman.com/business/companies/tech/zonefox-ramping-up-team-in-fight-against-cyber-crime-1-4477748

The Scotsman (13.6.2017): Police Scotland to create ‚cadre of experts‘ to beat cyber-crime. URL: https://www.scotsman.com/news/politics/police-scotland-to-create-cadre-of-experts-to-beat-cyber-crime-1-4474003

The Scotsman (30.5.2017): Cyber crime tops list of finance bosses’ key threats. URL: https://www.scotsman.com/business/companies/financial/cyber-crime-tops-list-of-finance-bosses-key-threats-1-4460668

The Sun (5.1.2017): ACTING UP US spy chiefs accuse Russia of being a ‘full-scope cyber actor’ that threatens to cripple key infrastructure from power plants to elections. URL: https://www.thesun.co.uk/news/2544412/us-spy-chiefs-accuse-russia-of-being-a-full-scope-cyber-actor-that-threatens-to-cripple-key-infrastructure-from-power-plants-to-elections/

The Sun (16.3.2017): Google summoned to Cabinet Office to explain why Government ads are appearing alongside hate speech. URL: https://www.thesun.co.uk/news/3103098/google-facebook-advertising-boycott-fake-news/

The Sun (29.6.2017): GADGETS NOT GUNS Warfare to move ‘from battlefield to the web’ as risk of cyber conflict grows, National Crime Agency warns. URL: https://www.thesun.co.uk/tech/3912228/warfare-to-move-from-battlefield-to-the-web-as-cyber-conflict-threatens-society-national-crime-agency-warns/

The Sun (3.1.2017): HACK THE VOTE Electronic voting could leave British elections open to cyber attacks from hostile states, warns former boss of MI6. URL: https://www.thesun.co.uk/news/2527419/electronic-voting-could-leave-british-elections-open-to-cyber-attacks-from-hostile-states-warns-former-boss-of-mi6/

The Sun (23.1.2017): WEB ATTACK Lloyds Bank suffered cyber attack that left thousands of customers locked out of online services. URL: https://www.thesun.co.uk/news/2683705/lloyds-bank-suffered-cyber-attack-that-left-thousands-of-customers-locked-out-of-online-services/

The Sun (24.1.2017): WEB OF DECEIT Surge in cyber crime causes cost of fraud in UK to rise to more than £1BILLION… the highest in five years. URL: https://www.thesun.co.uk/living/2689494/surge-in-cyber-crime-causes-cost-of-fraud-in-uk-to-rise-to-more-than-1billion-the-highest-in-five-years/

The Sun (23.5.2017): Former Premier League striker Nile Ranger sentenced to eight months in jail after admitted to online banking fraud. URL: https://www.thesun.co.uk/sport/football/3633118/former-premier-league-striker-nile-ranger-sentenced-to-eight-months-in-jail-after-admitted-to-online-banking-fraud/

The Sun (21.4.2017): IS YOUR KID A CRIMINAL? Online gaming forums could expose your children to hacking and fraud masterclasses, cops warn. URL: https://www.thesun.co.uk/tech/3382817/online-gaming-forums-could-expose-your-children-to-hacking-and-fraud-masterclasses-cops-warn/

The Sun (5.1.2017): SCHOOL HACK HORROR Brit pupils' sensitive info at risk after headteachers are held to ransom for THOUSANDS by cyber thieves targeting school computer systems. URL: https://www.thesun.co.uk/news/2544567/brit-pupils-sensitive-info-at-risk-after-headteachers-are-held-to-ransom-for-thousands-by-hackers-targeting-school-computer-systems/

The Sun (31.1.2017): BANK HACK ALERT Cyber crooks find way to mimic legitimate banking apps and empty accounts without customers ever knowing. URL: https://www.thesun.co.uk/news/2468947/cyber-crooks-will-empty-your-bank-account-if-you-fall-for-this-fiendish-trick/

The Sun (18.2.2017): Inspector gadgets Security forces building a volunteer army of geeks to help in the fight against cyber crime. URL: https://www.thesun.co.uk/news/2899045/security-forces-building-a-volunteer-army-of-geeks-to-help-in-the-fight-against-cyber-crime/

The Sun (20.1.2017): Full level of UK corruption revealed as cops count cyber scams as offences for first time. URL: https://www.thesun.co.uk/news/2659042/full-level-of-uk-corruption-revealed-as-cops-count-cyber-scams-as-offences-for-first-time/

The Sun (11.1.2017): FOOTIE FRAUDSTER Former Newcastle United footballer Nile Ranger admits swindling vulnerable woman out of £2,000 in online banking fraud. URL: https://www.thesun.co.uk/news/2588001/nile-ranger-footballer-newcastle-united-southend-fraud-court/

The Sun (16.3.2017): TECH GIANTS BOYCOTT WARNING Google summoned to Cabinet Office to explain why Government ads are appearing alongside hate speech. URL: https://www.thesun.co.uk/news/3103098/google-facebook-advertising-boycott-fake-news/

The Sun (18.1.2017): HACKING BACK Cyber-crook shamed after trying to scam one of Britain's top online security experts. URL: https://www.thesun.co.uk/news/2645457/cyber-crook-shamed-after-trying-to-scam-one-of-britains-top-online-security-experts/

The Telegraph (29.6.2017): More small companies worried about cybercrime than Brexit, survey finds. URL: https://www.telegraph.co.uk/business/2017/06/29/small-companies-worried-cybercrime-brexit-survey-finds/

The Telegraph (5.4.2017): Finance firms to spend more on security as concern over cyber crime soars. URL: https://www.telegraph.co.uk/business/2017/04/04/finance-firms-spend-security-concern-cyber-crime-soars/

The Telegraph (19.1.2017): Fraud and cyber crime are now the country's most common offences. URL: https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/

The Telegraph (15.5.2017): It's time to smarten up our act in the fight against cybercrime. URL: https://www.telegraph.co.uk/technology/2017/05/15/time-smarten-act-fight-against-cybercrime/

The Telegraph (13.5.2017): Fighting cybercrime must be a top political priority. URL: https://www.telegraph.co.uk/opinion/2017/05/13/fighting-cybercrime-must-top-political-priority/

The Telegraph (8.1.2017): France blocks 24,000 cyber attacks amid fears that Russia may try to influence French presidential election. URL: https://www.telegraph.co.uk/news/2017/01/08/france-blocks-24000-cyber-attacks-amid-fears-russia-may-try/

The Telegraph (12.5.2017): NHS has to get on top of cyber crime. URL: https://www.telegraph.co.uk/news/2017/05/12/cyber-attack-nhs-stark-warning-society-still-vulnerable-cyber/

The Telegraph (10.1.2017): Italian brother and sister arrested over cyber espionage operation which tapped emails of ex-prime ministers and Vatican cardinals. URL: https://www.telegraph.co.uk/news/2017/01/10/italian-brother-sister-arrested-cyber-espionage-operation-tapped/

The Telegraph (13.1.2017): Largest NHS trust hit by cyber attack. URL: https://www.telegraph.co.uk/news/2017/01/13/largest-nhs-trust-hit-cyber-attack/

The Telegraph (11.1.2017): Easy ways to protect your business from cyber attacks. URL: https://www.telegraph.co.uk/connect/small-business/tech/easy-ways-to-protect-your-business-from-cyber-attacks/

The Telegraph (9.1.2017): Germany accuses Russia of cyber attack on Ukraine peace monitors, as Kremlin dismisses US intelligence claims as a 'witch hunt'. URL: https://www.telegraph.co.uk/news/2017/01/09/germany-accuses-russia-cyber-attack-ukraine-peace-monitors-kremlin/

The Telegraph (6.1.2017): Schools warned about cyber scammers who demand thousands in ransom from headteachers. URL: https://www.telegraph.co.uk/education/2017/01/06/schools-warned-cyber-scammers-demand-thousands-ransom-headteachers/

8 Attachment B: Codebook

- **1. People/Stakeholders**
  - **1.1 Tech Companies**
  - **1.1.1 Internet Service and Mobile Providers**
  - **1.1.2 Cellebrite**
  - **1.1.3 Online Platforms**
    - 1.1.3.1 Amazon
    - 1.1.3.1.1 Jeff Bezos
    - 1.1.3.2 Facebook
    - 1.1.3.3 Google
    - 1.1.3.4 Instagram
    - 1.1.3.5 Twitter
    - 1.1.3.6 Netflix
    - 1.1.3.7 YouTube
  - **1.1.4 Tencent**
  - **1.1.5 Alibaba**
  - **1.1.6 Kaspersky**
  - **1.1.7 Sony**
  - **1.1.8 Apple**
  - **1.1.9 Microsoft**
  - **1.1.10 WhatsApp**
  - **1.2 Political Actors and Institutions**
    - 1.2.1 Ronald Pofalla
    - 1.2.2 Günter Heiß (BND-Monitor)
    - 1.2.3 Federal Communications Commission (USA)
    - 1.2.4 House of Commons (UK)
    - 1.2.5 Data Protection Agency
    - 1.2.6 Zentrale Stelle für Sicherheit im Informationsbereich
    - 1.2.7 Bundesamt für Sicherheit in der Informationstechnik
    - 1.2.8 Donald Trump
    - 1.2.9 Hillary Clinton
    - 1.2.10 Vladimir Putin
    - 1.2.11 Barack Obama
    - 1.2.12 Joe Biden
    - 1.2.13 Teresa May
    - 1.2.14 Emmanuel Macron
    - 1.2.15 Mike Pompeo
    - 1.2.16 NSA Investigation Committee (Germany)
    - 1.2.17 Angela Merkel
    - 1.2.18 Bundestag
    - 1.2.19 European Parliament
    - 1.2.20 SPD
    - 1.2.20.1 Heiko Maas (German Minister for Justice)
    - 1.2.21 CDU/CSU
    - 1.2.21.1 Thomas DeMaizière (German Minister of the Interior)
    - 1.2.22 SPÖ
    - 1.2.23 ÖVP
    - 1.2.23.1 Wolfgang Brandstetter (Austrian Minister for Justice)
    - 1.2.24 Green Party (Germany)
    - 1.2.25 Die Linke (Germany)
    - 1.2.26 Peter Altmaier (CDU)
    - 1.2.27 Governments
    - 1.2.28 EU Chamber of Commerce
    - 1.2.29 China Cyberspace Administration
    - 1.2.30 Democratic Party (USA)
    - 1.2.31 Michael Fallon
    - 1.2.32 NATO
    - 1.2.33 Sir Julian King (EU Security Commissioner)
    - 1.2.34 European Commission
    - 1.2.35 Conservative Party (UK)
    - 1.2.36 Labour Party (UK)
    - 1.2.37 Liberal Democrats (UK)
    - 1.2.38 Kremlin
    - 1.2.39 Republican Party
    - 1.2.40 US Senate
    - 1.2.41 Chinese Communist Party
    - 1.2.41.1 Xi Jinping
    - 1.2.42 OSCE
    - 1.2.43 Matteo Renzi
    - 1.2.44 Mario Draghi
    - 1.2.45 Mario Monti
    - 1.2.46 Philip Hammond
    - 1.2.47 Parliament
    - 1.2.48 Federal Data Protection Officer (Ger)
    - 1.2.49 Bundeskanzleramt
    - 1.2.50 Scottish National Party
    - 1.2.51 Gerhard Schröder
    - 1.2.52 Benjamin Netanjahu
    - 1.2.53 Kim Jong-un
    - 1.2.54 George W. Bush
    - 1.2.55 John Kerry
  - **1.3 NGOs**
    - 1.3.1 Privacy International
    - 1.3.2 Republica Internet Conference Berlin
    - 1.3.3 British Chambers of Commerce
    - 1.3.4 American Civil Liberties Union
    - 1.3.5 WikiLeaks
    - 1.3.5.1 Julian Assange
    - 1.3.5.2 Information of the Public
    - 1.3.6 Chaos Computer Club
  - **1.4 TITANIUM Project**
  - **1.5 Security Agencies**
    - 1.5.1 Bundesamt für Verfassungsschutz (Germany)
    - 1.5.2 BKA
    - 1.5.3 Europol
    - 1.5.4 FBI
    - 1.5.5 ENISA
    - 1.5.6 Europol
    - 1.5.7 National Crime Agency (UK)
    - 1.5.8 Police
    - 1.5.9 Department of Homeland Security (USA)

1.6 Android

1.7 Intelligence Agencies

1.7.1 Five Eyes

1.7.2 GCHQ

1.7.3 BND

1.7.3.1 Hans-Georg Maassen (BND Chief)

1.7.4 GRU (Russian Military Intelligence)

1.7.5 FSB (Russian Secret Service)

1.7.6 CIA

1.7.7 NSA

1.8 Criminals

1.9 Tim Berners-Lee

1.10 Courts

1.10.1 European Court of Justice

1.10.2 German High Court

1.11 Safe Harbor (EC Agreement)

1.12 Deutsche Post

1.13 Terrorists

1.14 Real (Supermarket)

1.15 Hackers

1.15.1 Shadowbrokers (Hacker Collective)

1.15.2 Fancy Bears (Hacker Group)

1.15.3 Lazarus (Hacker Group)

1.15.4 Schaltaj Boljaj (Hacker Collective)

1.16 Consumers

1.17 Chelsea Manning

1.18 NHS Hospital Trust

1.19 Nile Ranger (Former Premier-League Football Player)

1.20 Edward Snowden

2. Geography

2.1 Near and Middle East

2.1.1 Saudi Arabia

2.1.2 Iraq

2.1.3 Israel

2.2 South America

2.2.1 Ecuador

2.2.2 Brazil

2.3 Africa

2.3.1 Lebanon

2.3.2 West Africa

2.3.3 Tanzania

2.3.4 Canary Islands

2.3.5 South Africa

2.4 North America

2.4.1 USA

2.4.2 Canada

2.5 Europe

2.5.1 EU-28

2.5.2 Sweden

2.5.3 Ireland

2.5.4 Eastern Europe

2.5.5 Austria

2.5.6 Germany

2.5.7 Spain

2.5.8 France

2.5.9 Holland

2.5.10 Bulgaria

2.5.11 Montenegro

2.5.12 Italy

2.5.13 UK

2.5.14 Ukraine

2.5.15 Switzerland

2.6 Asia

2.6.1 Japan

2.6.2 Philippines

2.6.3 China

2.6.4 North Korea

2.6.5 Singapore

2.6.6 South Korea

2.7 Australia

2.8 New Zealand

2.9 Russia

3. Business

3.1 Cybercrime Laws

3.2 Trustworthiness

3.3 Banking

3.4 Outsourcing

3.5 Labels

3.6 Growth

3.7 Consumer Protection

3.8 Virtual Payment

3.9 Data Protection Officer

3.10 Large Enterprises

3.11 Reputation

3.12 Concerns about Cybersecurity / Data Protection Laws

3.13 Costs

3.14 Obstacles to Commerce

3.15 Advertising

3.16 Insurance

3.17 Capitalism

3.17.1 Net Neutrality

3.17.2 Digital Monopolies

3.18 SMEs

3.19 Concerns about Cybercrime

3.20 Cyber Security Skills

3.21 Capitalizing IT Security

3.21.1 Market Access

3.22 Survey Data

3.23 Cyber Security Management

3.24 Transparency

3.24.1 Targeting

3.24.2 Transparency of Users

3.24.3 Transparency of Institutions

3.25 Trust

4. Critical Infrastructure
- **4.1 Elections/Online Voting**
- **4.2 Finance**

5 Data Protection
- **5.1 Fundamental Rights**
  - 5.1.1 Civil Rights
  - 5.1.2 Autonomy
  - 5.1.3 Right to be Forgotten
  - 5.1.4 Consent
  - 5.1.5 Democracy
  - 5.1.6 Fairness
  - 5.1.7 Respect
- **5.2 Security Measures**
- **5.3 Security Gaps**
- **5.4 Personal Data**
  - 5.4.1 Health Data
  - 5.4.2 Proportionality of Data Processing
  - 5.4.3 Data Processing
  - 5.4.4 Data Collection
  - 5.4.4.1 Big Data
  - 5.4.4.2 Selling Personal Data
  - 5.4.4.3 Benefits
  - 5.4.4.4 Data Storage
  - 5.4.4.5 Transparency of Data Collection
  - 5.4.5 User Profiles
  - 5.4.6 Data Transfer
  - 5.4.7 Commercialization of Personal Data
  - 5.4.8 Data Misuse
  - 5.4.9 Control over Personal Data
  - 5.4.9.1 Passwords
  - 5.4.9.2 Two-Factor-Authentication
  - 5.4.9.3 Anonymization of Personal Data
  - 5.4.9.4 Encryption
  - 5.4.9.4.1 Usability
  - 5.4.9.5 Virtual Private Networks
  - 5.4.9.6 Tails (Anti-Surveillance Operating System)
  - 5.4.9.7 Obfuscation through VPNs
  - 5.4.10 Trade-Offs
- **5.5 Auditing**
- **5.6 Responsibility**
  - 5.6.1 Political Responsibility
- **5.7 Privacy**
  - 5.7.1 Privacy Laws
  - 5.7.1.1 Fines/Penalties
  - 5.7.1.2 GDPR
  - 5.7.2 Privacy Settings
  - 5.7.3 Privacy vs Security
  - 5.7.4 Privacy Policy

6. Disclosure of Secrets (Whistleblowing)
- **6.1 Treason**
- **6.2 Whistleblowing as a Threat to National Security**
- **6.3 Protection of Sources (Journalism)**
- **6.4 Pardon**
- **6.5 Protection for Whistleblowers**
- **6.6 Extradition**
- **6.7 Asylum**

7. Cybersecurity and Cybercrime
- **7.1 Cyber Weapons**
  - 7.1.1 Regin (Cyber-Weapon)
- **7.2 Reluctance to report breaches**
- **7.3 Competence**
- **7.4 Technological Lag**
- **7.5 Motivation of Offenders**
- **7.6 Psychological Impact**
- **7.7 Vulnerabilities (incl. Risk, Threat)**
  - 7.7.1 Zero Day Vulnerabilities
- **7.8 Professionalization**
  - 7.8.1 Arms Race
  - 7.8.2 Internationalization and Organized Crime
- **7.9 Content Crimes**
  - 7.9.1 Extremist Online Material
  - 7.9.2 Hate Crime Material
  - 7.9.3 Child Pornography
  - 7.9.4 Offensive Material
- **7.10 Cyber-dependent Crime**
  - 7.10.1 Data Theft
- **7.11 Cyber-enabled Crime**
  - 7.11.1 Coercion
  - 7.11.2 Cyber Extortion
  - 7.11.3 Social Media
  - 7.11.4 Cyberbullying
  - 7.11.5 Cybergrooming
- **7.12 CaaS (Crime as a Service)**
- **7.13 MaaS**
- **7.14 RaaS**
- **7.15 Bitcoin**
- **7.16 Botnets**
- **7.17 Data Leaks**
- **7.18 Financial Crimes**
  - 7.18.1 Payment Fraud
  - 7.18.2 Credit Card Data
  - 7.18.3 Online Gambling
  - 7.18.4 Scam/Cyberfraud
  - 7.18.5 Banking Fraud
  - 7.18.6 Money Laundering
- **7.19 Dark Web**
  - 7.19.1 Grey Markets for Aggressive Software
- **7.20 Compromising a Personal Computer**
- **7.21 Protection against Attacks**
  - 7.21.1 TOR Network
- **7.22 Subjective Threat**
- **7.23 WhatsApp Scam**
- **7.24 Blockchain**
- **7.25 Cybersecurity Accelerator**

- **7.25.1 Fundraising**
- **7.26 Malware**
  - 7.26.1 Ransomware
  - 7.26.1.1 Trojans
  - 7.26.1.1.1 Pegasus (for Android)
  - 7.26.1.1.2 Petya
  - 7.26.1.1.3 Jaff
  - 7.26.1.1.4 WannaCry
- **7.27 Artificial Intelligence**
- **7.28 Criminal's Personality**
  - 7.28.1 Socialization of Hackers
- **7.29 Counter-attacks**
  - 7.29.1 Policing Cybercrime
- **7.30 Statistics or Survey Data**
- **7.31 Party Lines on Cybercrime**
- **7.32 Entry Barriers**
- **7.33 Online Sexual Exploitation**
- **7.34 Attack Strategies**
- **7.34.1 DDoS**
- **7.34.2 Social Engineering**
  - 7.34.2.1 Identity Theft
  - 7.34.2.2 Ad Fraud
  - 7.34.2.3 Online Dating Fraud
  - 7.34.2.4 Phishing
  - 7.34.2.5 Vishing
  - 7.34.2.6 Smishing
  - 7.34.2.7 Twishing
- **7.35 Mitigation Strategies**
  - 7.35.1 Code of Conduct
  - 7.35.2 Cyber Defence
  - 7.35.3 Voluntary Deletion of Material by Internet Companies
  - 7.35.4 Webblocking (Netzsperre)
  - 7.35.5 Control Procedures
  - 7.35.6 Return to Cash-Only
  - 7.35.7 Security by Design
  - 7.35.8 Security Cooperation
  - 7.35.9 Internet Traffic Analysis
  - 7.35.10 Geoblocking
  - 7.35.11 Double-Check Identities
  - 7.35.12 Fact Checking (Fake News)
  - 7.35.13 Leadership
  - 7.35.14 Recovery Plans
  - 7.35.15 Anti-Surveillance Software
  - 7.35.16 Backups
  - 7.35.17 Personalized Blocking of Debit Cards
  - 7.35.18 Offline Provision
  - 7.35.19 Reporting
  - 7.35.20 Digital Bill of Rights
  - 7.35.21 Prevention
  - 7.35.22 Regulation
  - 7.35.23 Assessment of Digital Safety
  - 7.35.24 Awareness
  - 7.35.25 Open Digital Access
  - 7.35.26 Education
  - 7.35.27 Software Updates
- **7.36 Cyberwar**
- **7.37 Safe Harbour (for Hackers)**
- **7.38 Fake News/Chatbots/Information War**
- **7.38.1 Censorship**
- **7.39 Hacking**
  - 7.39.1 Political Hacking and Cyber Propaganda
  - 7.39.1.1 Terrorism
  - 7.39.1.2 State-sponsored Hacking
  - 7.39.2 Taking Control of Devices

8. Espionage/Surveillance

- **8.1 CCTV**
- **8.2 Stop and Frisk ("Schleierfahndung")**
- **8.3 Targets**
- **8.4 IMSI-Catcher**
- **8.5 Sicherheitspaket (Austria)**
- **8.6 Predictive Policing**
- **8.7 Surveillance of Telecommunication**
- **8.8 Concerns about Surveillance**
- **8.9 Surveillance of Instant Messaging**
- **8.10 Industrial Espionage**
- **8.11 Curbing of Internet Speed**
- **8.12 Deep State**
- **8.13 Data Retention ("Vorratsdatenspeicherung")**
- **8.14 Smart Surveillance**
- **8.15 Smart Data**
- **8.16 Advertising**
- **8.17 Anti-Terrorism**
- **8.18 Profiles of Movement**
- **8.19 Disciplinary Society**
- **8.20 Electronic Monitoring**
- **8.21 Smart Homes**
- **8.22 Face Scans**