Kompetenzzentrum
Öffentliche IT

Working Paper

Digital infrastructure as a public good: A European perspective

Information Systems Research: Pure Theory paper

Autoren: Roland W. Scholz, Markus Kley, Peter Parycek

Gefördert durch:

Bundesministerium des Innern, für Bau und Heimat

Fraunhofer FOKUS

Impressum

Roland W. Scholz[123],
Markus Kley[4],
Peter Parycek[45]

Die Inhalte dieses Papiers sind in weiterer Bearbeitung und sind in einem wissenschaftlichen Journal zur Begutachtung eingereicht. Die Leser sind eingeladen Rückmeldungen zu diesem Arbeitspapier zu geben.

The content of this paper is in further processing and have been submitted for review in a scientific journal. Readers are invited to give feedback on this working paper.

Corresponding author: roland.scholz@emeritus.ethz.ch,
Department of Environmental System Sciences,
ETH Zurich Universitaetstrasse 22,
8092 Zurich,
Switzerland.
Tel: +41 79 422 4401

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

[1] ETH Zurich, Department of Environmental System Sciences, ETH Zurich Universitaetstrasse 22, 8092 Zurich, Switzerland
[2] Danube University Krems, Department of Knowledge and Information Management, Dr.-Karl-Dorrek-Strasse 30, 3500 Krems, Austria
[3] Institute for Advanced Sustainability Studies (IASS), Berliner Strasse, 130, 14467 Potsdam, Germany
[4] Danube University Krems, Department of E-Commerce and E-Governance, Dr.-Karl-Dorrek-Strasse 30, 3500 Krems, Austria
[5] Fraunhofer Fokus, Fraunhofer Institute for Open Communication Systems, Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany

Inhalt

Digital infrastructure as a public good

Information Systems Research: Pure Theory paper

Abstract

The digital infrastructure is conceived as a form of infrastructure (such as water) and, thereby, a public good. It includes the competing and network resources, the functionalities that it affords and the organizational and institutional settings that keep them running. Currently, a major share of hardware and software is privatized and controlled by a few oligopolistic companies. Rules for (global) interaction between private digital infrastructure and national governmental institutions are just under development. The present is guided by Tim Berners-Lee's question of what we, as users, must do in order for digital-infrastructure providers to provide what societies want. The present paper (1) discusses critical aspects of the current digital infrastructure (including transparency, user safety and security, the current pay model, commercial and political surveillance, trade-offs between the rights of the individual and society, the fuzziness and incompleteness of legal systems, and aspects of power); (2) provides a coupled human–digital environmental view for understanding the role of digital infrastructure; and (3) describes why and which parts of digital infrastructure may be reframed. We conclude that large digital-infrastructure providers are not stakeholders but rather have a role as supranational (techno-economic) actors, that digital global infrastructure may have to adapt to sociocultural constraints, and that new forms of collaboration between nation-states and digital-infrastructure providers should be developed on the way towards a resilient global web.

Key words: Digital transformation, digital infrastructure, critical infrastructures, data economy, data sovereignty

1. Digital infrastructure as a public good

Public infrastructures such as transportation, water, energy, and telecommunication are complex technical, legal, economic, and politically managed systems. Material and social infrastructure services satisfy a broad range of requirements. They become *critical infrastructures* if the essential public works of a country, state, or region depend on them (Kroeger, 2008; Zio, 2016). Often, *digital infrastructure* is conceived of as the *hardware*, *software*, and *organizational and institutional settings* for *transferring* (e.g., networks/transmission), *storing* (e.g., cloud data storages), *accessing* (retrieving as machine-readable), *processing* and/or *using* digital data (done by using algorithms and depending on computational power; Henfridsson & Bygstad, 2013; Scholz et al., 2018). Yet, the technical and organizational layer "allow multiple stakeholders to orchestrate their service and content needs" (Constantinides, Henfridsson, & Parker, 2018, p. 381). Thus, the "good is not the infrastructure system itself, but the functionalities that it affords" (Constantinides & Barrett, 2015, p. 42).

Digital infrastructure, as a form of infrastructure such as energy or water, could therefore be considered a *public* and not a *private good*. It is a foundational layer of *social*, *economic*, and *environmental* systems' viability. Digital infrastructure has *personal* (needs-related), *social* (functions), *economic* (business activities ranging from communication via transportation to financial security), and *cultural-political components*. Thus, it is classified as a genuine *common*. Various trade-offs and dilemmas exist at the public–private interface (Hodge & Greve, 2005). Whether water is considered common property or a commodity (market good), how (drinking) water is priced, who pays for it (governments or users), whether all water resources should be privately owned or controlled, and/or what share of the water supply should enter the market all depend strongly on differences between cultures, nations, and situational constraints (Barraqué, 2003; Langford, 2005). Finally, water such as internet access is a resource held in common and access to it is a key UN human right (Gleick, 1998; Hanna, Lawrence, Buller, & Brett, 2020).

Core domains of the digital universal infrastructure, particularly global data transfer, (cloud) data storage, and communication on the World Wide Web (WWW), are handled by a few, globally performing companies. We call these few global *digital*-infrastructure *providers* DIPs

(currently, Alphabet/Google, Amazon, Facebook, Apple, Microsoft, and *Alibaba*). The DIPs deliver foundations for a broad range of essential activities, including individual communication; social infrastructure; operations for small, medium, and large companies; political information; and communication with public works and utilities of a country, state, or region. Somewhat surprisingly, the current DIPs' services are widely offered at no cost, particularly for private users. This became possible by utilizing personal or company data as an economic commodity that could be traded for marketing and other purposes.

There is increasing concern about the *governance, authority, and control of digital infrastructure*. The inventor of the WWW, Tim Berners-Lee (2001) posed the question, "What must we do [to ensure] that the WWW is doing what 'we' want?" (Berners-Lee, 2019). In the following, "we" is conceived as (the user's) *sustainable development perspective.* We do not approach *sustainability* from a triple bottom line approach (social, economic, environmental) but instead take a *systemic perspective*. Sustainable development is seen as an (i) *ongoing inquiry* for (ii) maintaining the viability (i.e., avoiding collapses) of *critical subsystems or principles of society* that we (iii) want *to sustain from a normative perspective* (e.g., intra- or intergenerational justice as a regulating rule, see Laws et al., 2004; Scholz, 2017). We particularly consider fundamental social issues such as *dignity* (e.g., avoiding the spread of hate speech), the *right to privacy* (e.g., avoiding surveillance society; Warren & Brandeis, 1890), the *maintenance of democracy*, the *right to know* and, thus, to access reliable, *trustworthy sources of information* (see the US Freedom of Information Act; U.S.C., 1988), and other *human rights* as valuable social rule system we wish to sustain. The question how we can attain such goals is one aspect of reframing digital infrastructure.

Section 2 discusses critical aspects of the current digital infrastructure. Section 3 presents a coupled human–digital environment framework that better allows us to understand the transition of social systems and the role of DIPs. Section 4 provides a quantitative market analysis on what functions are covered by the major DIPs. The discussion (Section 5) and conclusion (Section 6) address the questions of which elements of the digital infrastructure call for reframing and why, how, and based on what goals. The paper takes a European Union perspective and widely refers to the European Union's socioeconomic, cultural, political, and constitutional constraints, objectives, and rules.

2 Critical aspects of the current digital infrastructure

2.1 Key critical aspects

From a societal perspective, we distinguish three critical challenges, trade-offs, or dilemmas of the current *digital infrastructure*. These are *transparency and comprehensibility*, *societal safety and trustworthiness*, and *serving public needs.*

2.1.1 Transparency and accountability related to the commercialization of digital data

Transparency, a key component of the right to know (Florini, 2007), refers to the question of whether the rules and practices for transferring and utilizing (e.g., trading or using for economic purposes) data by DIPs are transparent and accessible by users. D*igital data* (D) have become the fourth key economic variable complementing *capital* (C), *labor* (L), and *natural resources* (R) (Scholz et al., 2018). Yet, what kinds of data can be traded legally (in which countries or according to which regulations) or transferred under what constraints to intelligence services? Currently, there is a significant lack of *commercial transparency* about data collection and use and what accounts for added value. There are different policies for private and economic data protection in the EU influence (particularly the 2018 EU, General Data Protection Regulation, GDPR), the US, China, and other parts of the world that may constrain the commercialization of data.

A core challenge is the *commercialization* or *capitalization* of digital data. The *privatization* of large elements of the digital infrastructure takes place in a *non-transparent, private business model*; this can be seen as a business model for data capitalism (West, 2019). For noncommercial users, many domains of the digital infrastructure are widely offered free of charge and without government subsidies. This became possible as some DIPs based their business model on data economy, i.e., on commercializing data and/or information about their users' activities. How digital data are actually commercialized is not transparent on either a national or global level. The Cambridge Analytica case (Cadwalladr & Graham-Harrison, 2018) showed that there are different legal systems on ownership of data which allow for commercialization (of cloud data) in one country but not in another (Boerding et al., 2019) and that there is intended (criminal) economic misuse of digital data.

We know that Google applies sophisticated behavioral-economics knowledge to their users' search habits and markets this knowledge in profiled marketing. Zuboff talks about information- or surveillance-based (micro)targeting advertising programs. In 2016, advertising comprised 89 percent of the profit for Google's parent company, Alphabet (Zuboff, 2019, p. 93). The DIPs provide the substructure or master essential components of digital technologies, digital devices, digital platforms, and digital data (Chaffey & Ellis-Chadwick, 2019). The foundation is the monetization of users'/customers' data by DIPs, by Google's search data, by Facebook's social network data, by LinkedIn's professional network data, and so on. The user pays according to the value of the data and the behavioral patterns – also called *behavioral surplus* – on the web, which have monetary value for certain market actors. The DIPs and other proprietary platforms such as Google interact, rule (by partnership models), and implicitly control (by entry barriers) a vast ecosystem of APP store application developers who utilize this knowledge for marketing.

The commercialization of data also includes a *political dimension*. YouTube, Facebook, and others have access and provide access to data which include the potential of affecting or manipulating elections, the basic element of democracy. Together with AI driven political robots even the buying of percentages of votes seems feasible. Data-economic activities may result in political activities which may result in political power that has the potential to become economic power and value by indirect pathways. In China, where a political credit system for citizens is transferred to company obedience scores used for providing (governmental) contracts or not, may be taken as example (Ankenbrand, 2019; Helbing et al., 2017; Petring, 2019).

Not utilizing digital infrastructure is not a choice. The *want-nots* (Sugiyama et al., 2017) are excluded from certain domains of social life. But we are also facing a couple of dilemmas related to difficult trade-offs between maintaining *personal and human rights* within the digital environment, particularly with respect to *informational self-determination* and the *creation of proper market rules* for the use of digital data in cyberspace. Often, the terms and contracts of use, which rely on users' fast clicks to accept without actually having read them, include ambiguous formulations by which users agree to DIP companies' internal data use (without clarifying what types of enterprises belong to a specific DIP company), etc. (Couldry & Mejias, 2019) liken this to colonialism, as colonists – like users – did not like the terms they were given but

had no freedom of choice because, without their agreement, the infrastructure would not be available.

Network effects promote oligopoly or monopoly situations (with only one dominant platform; Kerber, 2016). Which types of digital transfers and authorized or legal and which have are unauthorized is, from a global perspective, fuzzy and ambiguous. Operations take place in different countries with different legal systems. Where core data are stored is unknown. This can be seen as a need for transparent cross-boundary data management. Further, we may question whether flexible (microtargeted), price-setting algorithms and information asymmetries between market actors and internet platform providers violate consumers' rights (potentially causing unwanted market dynamics due to market failures).

Some DIPs are involved in conventional businesses with the help of electronic order systems. Amazon is a leading mail-order company, and Amazon Web Services is becoming a market leader in selling cloud-based web services (Kenney & Zysman, 2016). This allows them to utilize the economics of business-transaction data in a privileged manner which led to an antitrust probe under EU competition laws (van Dijck, Nieborg, & Poell, 2019).

2.1.2 Needs for safety and trustworthiness

From a user's perspective, infrastructure services must be safe, affordable, and reliable with respect to availability and service quality. Trustworthiness is a factor not only for traditional critical public infrastructures but also for information. Incorrect, inaccurate, misleading, or inappropriate information can lead to problematic personal, economic, and other decisions (Xu, Sandhu, & Bertino, 2009). The question is whether the digital infrastructure itself and a DIP's data process and transfer protocols are trustworthy. This suggests two primary lines of thought.

First, digital infrastructure services must meet *users' safety needs*. For example, public roads and highways gained safety because of "crash barriers" and guardrails to help prevent accidents. For digital infrastructure, this means that the Internet should be designed in a way that prevents computer-based attacks by third parties on private, commercial, and governmental users' data, software, and hardware. This is linked to *security* steps taken by the user and services provided by the DIP as well as a myriad of applications. The latter are not and cannot be

under governmental control. One aspect is the *integrity of the economic actor*. We have learned from auto industry scandals (e.g., Dieselgate) that aggressive business strategies can include criminogenic kernels of behavior by company managers willing to "*take risks and bend rules*" (Spapens, 2018). In the case of digital infrastructure, this can become critical; one example is utilizing personalized, microtargeted data for aggressive, greedy marketing in violation of the European Union General Data Protection Regulation (EU, 2018). Another may be Facebook's managers' brazen growth strategy pioneering "techniques to lure in new users and keep them coming back for more" (Kuchler, 2019). Moreover, cybercrime and cyberterrorism launched by third parties represent a specific dimension since all national users are severely affected if attacks render e-government structures useless (Dawson, Omar, & Abramson, 2015).

National security, digital infrastructure, and individual safety are potentially endangered by (foreign) intelligence services. We may consider intelligence services as a hidden layer of the global geopolitical power game. Snowden's revelations about US intelligence services extensive use of personal and other data strained many non-US actors' trust in the global web. The (national) autonomous discretionary power of governments and of other agents for protecting data from (foreign) artificial intelligence systems' access (Antsaklis, 2017) is of key interest for a future architecture of the cloud. A critical question from a *national security* perspective is, that there is no institution which ensures that the digital infrastructure will not shut down by economic or (geo-)political (e.g. trade war) reasons and that it will continue to be available in the long term.

Second, the *reliability and trustworthiness of information* are critical. Transmitting fraudulent information to reap benefits is an important evolutionary adaptation, as demonstrated, for instance, by bee-mimicking flies. Yet the digitalization of information and acquiring large segments of it gained a new dimension that Degeuchi (Sugiyama et al., 2017) called *reality shift*. The problem is that different (groups of) individuals receive biased, disembedded, (artificially) constructed, virtual information without "evolutionary feedback loops." Whether a cooktop is hot or not can easily be verified by touching it, i.e., a direct, physiological feedback resulting in pain or the lack of it. By contrast, there is a broad scope for how fraud related to digital data can be generated on the web; this ranges from falsifying data (e.g., one digit) to machine-learning–based, real-time deep fake manipulation. Moreover, a range of critical issues exists with

respect to how individuals, decision-makers, and others have to adapt to deepfake, i.e., replacing a person in a video with another person without having a chance to recognize the deceit. One issue is that AI-based programs are insufficiently able to detect deepfake fraud; in fact, Korshunow and Marcel (2018) reported a 90% "miss" rate.

2.1.3 Infrastructure governance: Serving public needs in a democratic society

Most important *is whether the infrastructure is designed in a way that enables it to provide the basic services in a minimum satisfactory (i.e., satisficing) way necessary for forming resilient and sustainable social institutional structures.* In democratic societies, the governance of critical infrastructures such as water is a subject of *governmental institutions* that *define* the *rules*, e.g., what is common, what is private, and the *roles* of the operational and regulatory systems (Kessides, 2004). The rules outline what part is under public and what part is under private management, the standards (i.e., efficacy – what level of water quality must be provided), the organizational design (e.g., decentralized vs. centralized or what control structures exist), and the policies for public–private partnerships (where do we allow competitive market behavior) or forms of cooperation (Janssen & Ostrom, 2006). The digital infrastructure is exceptionally complex and includes multiple uncertainties. "Vulnerabilities in cyberspace are real, significant, and growing rapidly" (Schreier, Weekes, & Winkler, 2015, p. 12).

Regulatory rules follow the implementation of technology. "The rapid expansion of the internet *has far* exceeded regulatory capacity. And this absence of authority has opened space for more abuses" (Schreier et al., 2015, p. 11). The implementation of new laws for personal data protection (EU, 2016), intellectual property rights in digital markets (EU, 2019), and taxation of digitalized business are as delayed as traffic regulations were. The first road-traffic legislation was enacted in 1906 (Königliche Regierung zu Cassel, 1906). This was several decades after motor-operated traffic had taken its position on the roads because of critical road-traffic mortality rate. In relation to the number of cars it was 62 times higher than a century later (Statistisches Bundesamt, 2008).

Liability rules may play an important role in the history and future of governmental framing of internet governance. "Since the mid-nineties, legislators have provided online intermediaries, such as access or hosting providers, with exemptions from liability for wrongful activities committed by users through their services" (Frosio, 2017), a move meant to promote the

development of the internet. For instance, the liability of internet intermediaries for online platforms and hosts (e.g., if information was transferred by these users that harmed someone) was restricted in the US to facilitate market entrance in the late nineteen-nineties. Moreover, we have cross-national conflicts as freedom of speech which allows racist speech in the US but not in most EU countries (Frydman & Rorive, 2002). In 2013, German politicians (Merkel, Seehofer, & Gabriel, 2013) targeted internet providers as having to take more responsibility. Clearly, liability rights may become an important tool in the course of reframing digital infrastructure.

Regulations in regard to users' internet behaviors are lacking and difficult to formulate and implement. For instance, secret services of democratic countries collect, store, and analyze personal and other types of data for national security reasons. Operating in the World Wide Web, social media functions offered by DIP are essentially global. The cloud is a seemingly non-geographic space where boundaries take new forms. Thus, this global infrastructure requires new governance models. Entrusting our data processing and communications to a handful of giant DIP whose businesses depend on marketing revenues creates a new generation of *surveillance intermediaries* (Rozenshtein, 2018). However, China, Russia, and several other countries have opted out and participate selectively (in economic, scientific, and other platforms), instead offering their own national networks. A WWW serving as a global form of "communications intended to allow anyone, anywhere to share information" (W3C, 2019) is far from being a reality. Yet we must also understand that there are different political systems framing digital infrastructures. Thus, one could argue that societal resilience demands for globally accepted rules on fundamental issues of human rights regulating what information is allowed to be shared and what should be banned (e.g., whether one may show videos on the beheadings of two female Scandinavian students in Morocco; Redmond, Jones, Holman, & Silver, 2019).

Various strategies for *digital sovereignty* are developing. The question of who or what agency should have access to what data, for what purposes, and when emerged after 2013 when Edward Snowden revealed that the NSA and the US Secret Service were collecting and analyzing bulk data on a broad scale including personal, business, and other data *worldwide* (Verble, 2014). This prompted the Canadian Government, for example, to take national control in regard to how digital data were generated, transmitted, processed, and stored in Canada and to

introduce terms such as “data residency,” stressing that when *data enter the cloud, data security becomes a shared responsibility with hyperscale cloud provider services.* “This means that Canada cannot ensure full sovereignty over its data when it stores data in the cloud” (Treasury Board of Canada, 2018). Thus, various regulations such as the Cloud Act (see above), the Safe Harbour privacy ruling (EU, 2000a), and the *EU–US Privacy Shield* (Sotto & Hydak, 2016) emerged. At a closer look, these contractual solutions cannot completely satisfy all countries expectations, in particular if there exists no don’t spy agreement. Since, currently, the needs and governmental rules between nation-states differ, this induces trends towards regional structures (Lillington, 2019; Schrems, 2014) or even fragmentation of the WWW.

2.2 What might a reframing of the digital infrastructure mean?

The cultural setting matters. In the following, *framing* means “to fit or adjust especially to something or for an end” (Merriam Webster, 2019). Thus, reframing has a *cognitive, value-oriented kernel* since it is related to an *end* (i.e., a purpose) and includes an *action-oriented, political dimension*. The term *end* includes a strong normative component, as usually provided by sociocultural rules as European culture, which has become subjected to governmentalization (Barnett, 2001). *End* is conceived as the function of infrastructure to meet societal needs for services required for socioeconomic development and quality of life. Since World War II, the nation-state, as a self-governing authority (Parsons, 1961) “is responsible for ensuring that the basic requirements of community life are maintained for the human beings within its jurisdiction – namely, law and order, has become the major stratum for society causing severe conflicts if, for instance, countries included competing cultures or religions” (Brown, 1984, p. 510). From a European Union perspective, the French-enlightenment–shaped *ideal* including personal freedom, social responsibility (fraternity), and equal rights for all humans comprises basic principles. Freedom is seen as a prerequisite of autonomy and, thereby, of personal digital-data self-determination. This view differs from the Chinese collective, harmonious, disciplined, hierarchical (not stressing equality), sociocultural principles that see human rights from a pragmatic “food, shelter, clothing, and job and health care” perspective (Gold, 2011). We may consider the current Chinese trends toward (accepting) *social credit score* and a monetary-profit orientation as variants of these cultural patterns.

Users' national legislative framings are important. Some countries attempt to take firm control regarding the internet. Here, naturally, legislative (re-)framing is something we might think of first. One variant is the nationalizing of internet governance infrastructures, i.e., the efforts of nation-states such as China, Russia, or Venezuela to gain greater sovereignty over formerly widely (nationally) ungoverned digital infrastructures. Demchak and Dombrowski discussed this potential "beginning of a new cyber Westphalian world of virtual borders and national cyber commands as normal elements of modern cybered governments" (2013, p. 35). This idea has, for instance, been launched by the US Trump administration "to nationalize the United States' next-generation 5G wireless network in an effort to guard against competitive and cybersecurity threats from China" (Stewart, 2018). In the US, a nationalist polity is linked and in conflict with several global structures, yet the behavioral side of reframing also includes ICT users.

Creating an internet safety culture is a challenge. Internet behavior is a matter of lifestyle or cultural consumer patterns (King, Watson, & Fleiter, 2019). We suggest that internet behavior calls for the development of new (common) *safety culture*. Just as our earliest ancestors had to learn what foods were dangerous to consume and should be avoided, users should learn what security means and what standards are necessary under what constraints. This change in *internet culture*, which is a combination of self-responsibility and societal rules and regulations, is part of infrastructure reframing. A critical question in this context involves negative rebounds of customers' willingness to pay for internet services by providing personal or business data.

Reframing is a very comprehensive issue. We hypothesize that reframing is *not only* a matter of regulating DIPs *but* also a product of the future relationships between *DIPs* and *users* and between DIPs and governmental framing agents. If we do not want to revert to a segregated Westphalian infrastructure, the situation calls for new forms of collaboration between public and private entities on a global-international level or even a global-supranational level. The development of digital literacy includes, for instance, knowledge about how DIPs make money with data and services as well as changes in the internet, but in addition, change of behavior is a factor. However, reframing may also include changes to the payment scheme for certain internet services. The strong requirement of privacy is a priority from a European culture perspective whereas the violation of rules of fair competition are a global issue. In order to better

understand how these conflicts can be managed, some social and technological system analysis is needed.

3. Some theoretical background: the digital layer

3.1 The digital transition is changing human systems

To better understand the emergence and roles of digital infrastructure and DIPs, we refer to *social system theory* (Lenski, 2005; Parsons, 1951) and introduce the *coupled human and environmental systems* approach (HES; Miller, 1978; Scholz, 2011). One fundamental proposition is that human systems show a level hierarchy with completely different rationales and drivers. The number of levels of human systems (see Fig. 1) depends on the development, i.e., complexity of technologies (Chapple & Coon, 1953). *Society* is a major subdivision of the *human species*. Hunter and gatherer societies were characterized by small, tribal kin groups. With the development of technologies (e.g., sophisticated weapons), *institutions* (e.g., armed groups with professional warriors and commanders) developed (Bowles, 2009). We define institutions as special types of organizations founded by societies to secure their maintenance. After World War II, societies were built by *nation-states* (and its subunits, Parsons, 1971). This changed with the development of globalization by industrial societies' transportation technologies and global telecommunication**s**. *Supranational institutions* such as the European Union (EU) evolved as a new layer between the human species and the nation-states (Fig. 1). The future world may be organized by a small number of *supranational systems* rather than by nation-states organized in the United Nations, which is an international organization of 193 exceptionally heterogeneous nations. Rules of *suprasocietal/-national institutions* like the EU are binding and can sanction member nation-states for non-compliance. The EU is moving toward the principle of "kompetenz-kompetenz" by authorizing member states "to confer individual sovereign powers on the Union (power attribution)" (Blanke, 2013).

We argue that global DIPs are going to become (economic) *suprasocietal systems*. This follows "the emergence of a supranational telecommunications regime" (Sandholtz, 1998) by abolishing national postal, telephone, and telegraph monopolies, in particular by EU mobile and postal

directives, that facilitated cross-border communication around the year 1996. At about that time, graphical browsers such as Mosaic (1993) and Internet Explorer (1995) for PC, Mac, or UNIX provided easily accessible Internet hardware. Berners-Lee's hypertext-based *World Wide Web* became accessible by mouse clicks, and multimedia via networks emerged as a fast-evolving technology and the internet as a research-oriented tool (Weber, 2018). Today, there are about 4.5 billion internet users, and the stocks of Microsoft, Facebook, Amazon, and Apple account for 28.4% of the top 500 companies in the Standard & Poor Index, the S&P 500 (Pisani, 2919).

One might argue that DIPs are in a situation similar to that of large automobile companies like Toyota or Daimler Benz. Yet, industrial production *differs fundamentally* from digital infrastructure. An automotive or truck factory operates under *national* factory *acceptance tests*, including site acceptance for machinery, national safety, occupational safety, environmental regulations, and other standards. This seems *not possible by design* for DIPS due to the globally distributed computing and the spread of globally cloud-hosted digital data and APPs. DIPs are currently, largely without control, where data are produced, processed, stored, transferred, and processed. In addition, the location of added value can be assessed less reliably than for vehicle production. DIPs in most countries are far from being severely restricted by regulatory controls. The EU General Data Protection Regulation (GDPR; EU, 2018) protecting privacy may be seen as an exception.

However, the most important and essential factor is that data and algorithmic power-based implicit (i.e., hidden) and explicit governance (i.e., targeted, action-based banning of certain users) can be conducted by DIPs on all levels of human systems ranging from the individual to the human species (see Fig. 1). What this means and the impacts that may result from a concerted action have not yet been evaluated. Yet, it is evident that, if the oligopoly of DIPs halts services, many functions of nation-states would essentially break down. We posit that this is an exceptional circumstance that calls for a reframing of digital infrastructure. Therefore, we argue that DIPs differ fundamentally from other global industrial players such as the automotive, food production, energy, etc. with respect to transparency, rules of security, taxation, etc. Their independence of business actions from national states *and* other stakeholders (Scholz, 2011)

that do not have a realistic choice of opting out creates a specific type of DIP sovereignty with global power that makes them (economic) supranational systems.

Fig. 1 also includes *large internet groups* as a new type of human system supplementing *small* (< 25 people) analogously communicating *groups*. DIPs provide formats, censorship, etc. for social media, chatrooms, etc. that host these groups that, potentially, have multiple impacts on social (Montag & Diefenbach, 2018) and political systems (Awan, 2017; Fuchs, 2012).

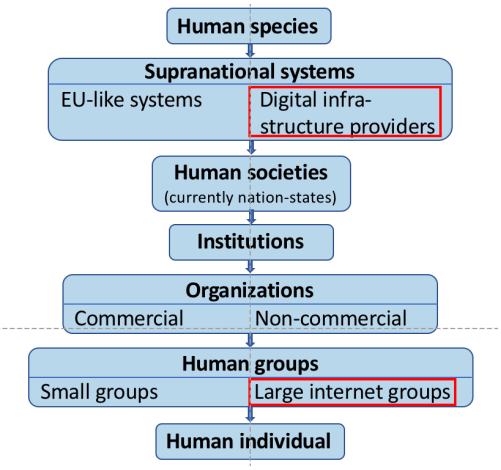

Fig. 1: Level hierarchy of human systems and new layers in the shift to the digital age; (angular) boxes designate new types and levels of human systems emerging from the rise of globalization and digital technology.

3.2 The digital curtain: A ubiquitous digital layer mediates human–environment interactions

The coupled human systems–environment system view provides insights in the functions of digital infrastructure and roles of DIPs (Scholz, 2011). We define a *human individual* as the sum activity of all living cells (and their interactions) that emerged from the zygote. A *company*, X, as a *human system* is defined as the sum of the *activities of* the company's owners' and employees' *living cells* which emerge from the zygote that are legally assigned to company X. This definition allows for a *consistent definition of environment* for all human systems of Fig. 1, if we define the *environment of a human system* as all atoms of the universe minus the atoms of the living cells of the persons' activities assigned to a human system.

In Fig. 2, we distinguish for all human systems the material-biophysical layer (H_m, the "body") and the social-epistemological-cultural layer (H_s, the "mind") of a human system. The "mind" of an organization, for instance, includes rules, assignments of tasks, competences, a company's mission, etc. A *digital system* comprises digital *data* (i.e., a place-value digital number system) and *algorithms*. The digital environment, E_{digi}, includes all physically-technologically stored data and algorithms that have been programmed to process the data to transmit (electronic, optical, or other) signals to devices, systems, machines, and their primary technical equipment (see red bar in Fig. 2). E_{digi} usually consisted of electronic computers, which are part of the abiotic environment, E_{abio}. Note, that E_{digi} also includes some biocomputers, whose basic units of storing data consist of genetically modified E. coli bacteria (Benenson, 2009).

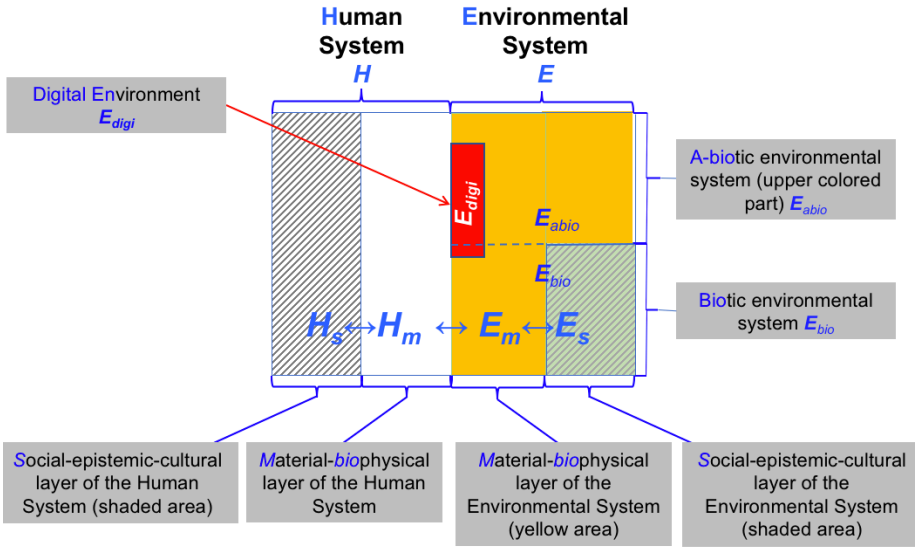

Fig. 2: Defining human and environmental systems, the digital environment, and the biotic layer and information layer related to human activities and the digital environment, which may be conceived as a constraint [due to the digital nature] and as augmentation.

The potential of the power of DIPs becomes visible when we reflect that DIPs may influence interaction on (i.e., horizontally) and between (i.e., vertically) all levels of human systems (see Fig. 3a). The algorithms of ranking companies or non-commercial websites on search engines or smart use (selling or not selling) have a huge impact. Actually, social or political bots are typically directed from the level of companies or non-governmental organizations (such as political parties). For instance, about 30% of the Trump/Clinton Twitter followers in the 2016 US presidential campaign were social bots that generated a heated and polarized atmosphere and spread misinformation (Hegelich, 2016).

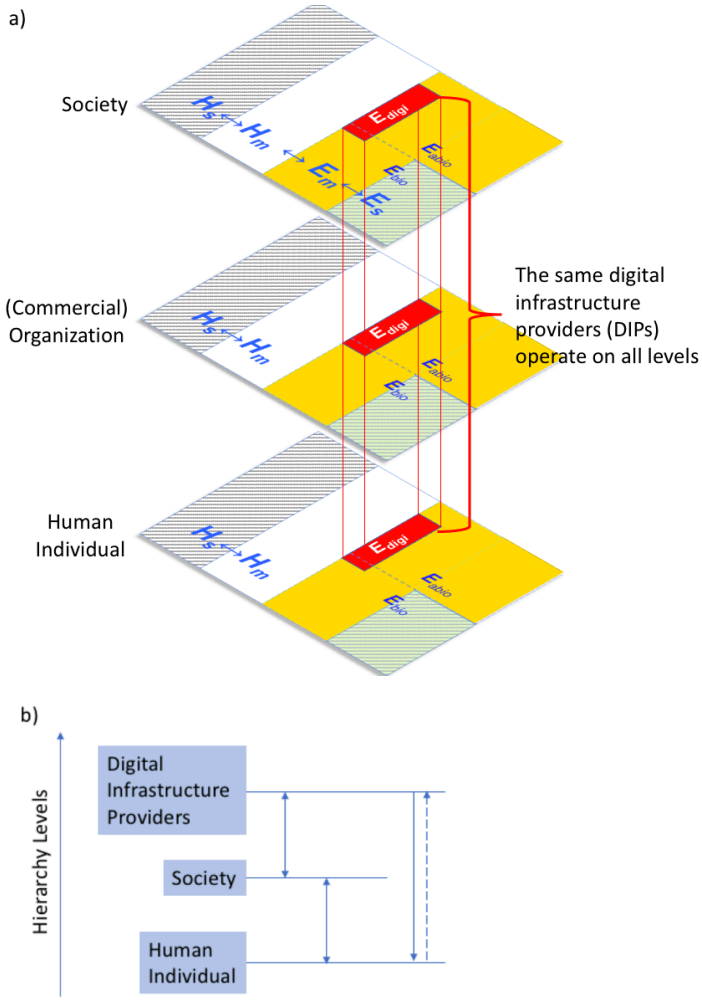

Fig. 3: (3a) DIPs serve all levels of human systems; the Figure. presents just three exemplary levels. The middle red bar also includes the intermediate levels (see Fig. 2) and the two layers, including (the collective mind of) the human systems (if all nations were to allow access). (3b) Illustration of level hierarchy with potential asymmetric relations in top down and bottom up causation (Variables are defined in Fig. 2)

Given that data collected by DIPs refer to *all* levels of human systems (Fig. 3a), knowledge about the rationales of users and their interactions has potentially vast scientific and practical impacts. Fig. 3b presents the idea of the level hierarchy, which is characterized by upward and downward causation. We can see that there is an asymmetric relationship between DIPs and users. The power of DIPs results from their status as being on a superior level that – in principal – directs and controls what lower levels receive. This situation can be reframed if, for instance, national rules are applied effectively for the governance of data. Supplementary Information 1 (SI1) describes a case where rules of protecting Swiss casino gamblers cannot be transferred to online gambling (as wanted by a public referendum) because of internet's encryption options.

3.3 A coupled user × digital infrastructure perspective on social dilemma

Digital technologies *augment* as well as *constrain* human action and interaction (see Fig. 2). The unintended side effects of the digital transition on human systems was a key of science-expert roundtables (Scholz et al., 2018; Sugiyama et al., 2017; Viale Pereira et al., 2020). There was much concern how *DIPs* and platforms/social media utilize microtargeted information as part of to induce filter bubbles, echo chambers promoting *large internet groups* or individual's over-use overuse/addiction which is a matter of *societal healthcare* (see Fig. 1, Montag & Diefenbach, 2018). From a coupled HES perspective (see Fig.1), we are facing the question what share digital (or analog) information are critical, e.g. for an individual or socio-cultural systems to avoid critical harms (e.g., internet addiction or loss of basic social concepts such as trust). The cultural perspective becomes evident if we compare Japanese affinity and Europeans reservation with respect to nursing robots. Anthropologist argue that real world-oriented Shinto and Buddhist cause that Japanese prefer humanoid robots whereas according to Christianity principles of resurrection and salvation more focus on the program/performance and allow for the appreciation of nonhumanoid (Geraci, 2006).

We may ask whether global digital infrastructure hampers democracy, in particular the development of *citizens' democratic capability* (German: Demokratiefähigkeit) A democratic society sees the adult human as an active, responsible, sovereign (free), and informed political voter. Hate speech, digital violence, conspiration theories are well promoted via the internet. They destabilize democratic processes. The different definition of freedom of speech in the US and in most EU countries (Bleich, 2014; Frydman & Rorive, 2002) has been mentioned above. For preventing for instance hate speech, but also cybercrime, governments are facing the Dark Web Dilemma. Encryption or operations on the Tor browser promote hate speech, financial fraud, and cybercrime (see 2.1.2). Yet, anonymous speech is often the only form to express opinion for marginalized groups (see 2.1.3). Contrary, encrypted data transmission is a prerequisite for functioning economy (see 2.1.1) and personal data protection. Thus democratic countries need socio-technological solutions which provide balanced, satisficing tradeoffs between these and other perspectives (Tzanetakis, 2018, see 2.1.2).

3.4 The body and the mind of digital data

Digital data have meaning only in the minds of human systems. Thus, it makes sense to distinguish between *physical* (usually electronic) storage of *coded digital data* (which may be known) and the *information* related to a decoding of data allowing for meaning. Someone may steal a computer with all its (stored) data but not have access to the password or encryption tool required to access the data. However, if someone destroys the cloud-storage center (the material base), the meaning of the data (for a human actor) is also compromised. This is relevant for cloud-computing security. Louise Amoore reported on the activity of 17 US intelligence agencies in 2015 and stressed that data centers are "located in places with plentiful land, favorable tax rates, affordable energy, water for cooling, and proximity to the main trunks of the network" (Amoore, 2018). The territorial spatial formation of E_{digi}-centers (see Fig. 2) is of geopolitical as well as terroristic interest. A dematerialized conception that places the digital world only at the virtual levels E_s as an abstract, encrypted, non-local, virtual, non-physical Big Data space is insufficient. One may argue that, from a technical perspective, cloud-based distributed data storage with hyperscale computing has, in principle, lower risk (is more economic, etc.) than mono-local storage and computation. Yet, the physical side (and its exposure to geopolitical impacts) should not be neglected in reframing of digital infrastructure.

4. A technology market view on the digital infrastructure providers (DIP)

Reframing digital infrastructure has *technological* (see 2.1.1) and *economic* (see 2.1.2) dimensions. Understanding the technological structure or layer of the digital system is necessary to comprehend what technology design issues are involved in the management of security, business fraud, or economic data; informational self-determination; or other critical aspects of the current digital infrastructure (SI2 provides some access to latter). Subsequently we focus on data economy and market structure.

4.1 Search engines' and social media's data economy

The economic value of personality profiles is marketed (Conti, Cozza, Petrocchi, Spognardi, & Ieee, 2015). The search-engine user (actor) pays for "free use" with the indirect remarketing of his or her personal digital behavioral profile (e.g., click rates, backlinks). This often means that the user does *not* get the result(s) desired but instead gets result(s) preselected according to the provider's economic objectives (e.g., patterns of click behavior which is well-paid).
The technological side of search engines is based on assessing and indexing previously created information in the background in order to deliver a search result that is as accurate as possible in the shortest possible search time. These index values are continuously generated or kept up-to-date in the provider's data centers from web information collected by search robots (crawlers). Such an index consists of index terms (keywords) as well as the corresponding website information (e.g., URL, title, text passages, images). The ranking and sorting of the search results is essential from a user perspective. Behind the ranking, there is a multitude of mathematical algorithms that evaluate and weight the individual results. Google's PageRank algorithm (Benincasa et al., 2006) evaluated the results on the basis of over 200 parameters (Dean, 2019) and criteria. Additionally to the mutual number of links (backlinks) and the link weighting, the focus is on referring domains, click rates, domain information, mobile user experience, retention times, and content quality. This is one way to acquire data for behavioral surplus analysis. Yet the favorable page ranking on an infrastructure tool is also a key issue for companies (Kathuria, 2019). Google, which is both a host and (related to its own products) a competitor to other company's products, should not be allowed to do this as it violates the US treaty on preventing "dominant undertakings" that "impair effective competition" (EU, 2009).

Social media enable users to interact with each other and actively refer to an issue content through comments, evaluations, and recommendations. The border between producer and consumer becomes blurred (BVDW, 2019), particularly when social and political bots participate. Social media communication relies individually or in combination on text, images, audio, and/or video. They can take place independently on platforms which now have a granular selection of addressees via groups of different actors and criteria (friends, organizations, interests) or from random groups, e.g., for events or sudden regional events (flash mobs, weather warnings, etc.). Social media platform operators do not verify the identity of actual persons or

companies; this allows them to construct fake profiles, spread false information or reports, and/or insult or discredit other persons or companies (Woolley, 2016) without being identified (see Sections 3.2 and 3.3). Any reframing of the internet must certainly address strategies for identifying junk-mail senders, social bot news, and harmful (dis)information.

4.2 Market share and power

The Herfindahl–Hirschman Index (HHI; 0 ≤ HHI ≤ 1, Herfindahl, 1967) is a standard method of measuring market concentration. We look first at the global market. The HHI is simply the sum of the squares of the market shares of firms. Values above .25 indicate *high concentrations*, values above .15 *moderate concentrations,* and below .15 *unconcentrated industries*.

Network/ Transmission (HIH, 2019)		**SSL CA (W3Techs, 2019)**		**Cloud Storage/ Computing (Richter, 2019)[6]**		**Browser (Marketshare, 2019a)**		**Search Engine (Marketshare, 2019b),** for parentheses **(StatCounter, 2019)**		**Social Media (Buggisch, 2019)**	
T-Online	30	IdenTrust	49.4	Amazon	33	Chrome	65.9	Google	83.7 (92.9)	Communica-tion	Media
1&1/ Versatel	26	Sectigo	23.7	Microsoft	16	Safari	19.0	Baidu	6.2 (0.8)	Facebook Google Plus LinkedIn Threema (CH) Twitter (USA) WhatsApp XING (DE)	Amazon Prime Instagram Netflix (USA) Snapchat (USA) Spotify (Schwe-den) YouTube
Vodafone	22	DigiCert Group	15.5	Google	8	Firefox	4.0	Bing	6.0 (2.3)		
O2	11	GoDaddy Group	6,8	IBM	6	Internet Ex-plorer	2.6	Yahoo!	1.8 (1.6)		
Uni-tymedia	11	Others	13.4	Alibaba	5	Edge	2.5	Yandex	1.0 (1.1)		Collaboration
Other	8			4 next largest providers	12	Other	6.0	Other	1.3 (1.2)		Pinterest (Ire-land)
HHI-In-dex	0.24		.35		.16		0.48		.71 (0.87)		

Table 1: Percentages of market share of ICT service providers for key components of global digital infrastructure (all abbreviations without company names are defined in Section 3.1; Network/Transmission data from Germany

The analysis reveals the (economically highly profitable) monopolistic structure of search engine markets with an HHI of .71 (Google taking 83.7%; see Table 1). Other statistics – presumably deviating due to the unreliability of Chinese data – provide a market share of 93.0% (HHI = .87). The browser market (HHI = .48) and the encryption market look critically high. The Social Media/Communication market was highly concentrated as Facebook had a market share of 75.5% in 2018 (Angelowska, 2019). Yet the communication behavior of young people changed. Facebook dropped to 23% at the end of 2019 and WhatsApp popped up to 29%, yet got bought by Facebook which provides HHI = .21. In 2019 the (German) network transmission increased to .28 by a merger of Vodafone and Unitymedia. The global cloud computing showed moderate concentrations (HHI = .16). Just for comparison, in 2015, the largest 10 automotive car companies made 75% of all sales providing an HHI = .08 across all car companies (Focus2move, 2019, February).

The national concentration is a critical issue of global markets' security perspective. In Germany, almost 90% of security (SSL CA; Tab. 1) certificates and their security keys were issued by only four US companies. Less than 0.1% market share is claimed, e.g., by German providers D-Trust (Bundesdruckerei) and telesec (Telekom).

5. Discussion: What may be reframed, why, and how?

We discuss the findings of the critical analysis (Section 2), the in-depth analysis of the *digital layer* from the hierarchy analysis (Section 3), and the techno-economic inquiry (Section 4) from the following questions: *What parts* of the digital infrastructure can be reframed? (5.1) Reframing for *what* goals? (5.2) and *How might reframing take place*? (5.3)

5.1 What may become subjected to reframing: A status-quo view

5.1.1 The global perspective

Digital market *mechanisms instead of public needs as drivers:* Digital data of commercial and non-commercial users' behaviors, which on the web are linked to economic, political, and other informational preferences, interactions with other users; purchases or other financial activities, gaming, etc. Click behaviors have become a key economic variable. *Surveillance data* are used for marketing by advertisers, for directly addressing customers based on microtargeted information, for developing business strategies or products, and for other purposes such as political monitoring or campaigning (West, 2019; Zuboff, 2015). This may conflict with societal and individual interests (Section 2.1.1). In some domains such as health care, the individual and scientific interest is to provide the most optimal information for the individual, e.g. for public health, and not what results in the best economic return for a DIP (and thus is presented at the top of websites). We may question how the global digital data market can be framed and what role DIPs and other new forms of supranational systems might play.

Opaqueness of data economy: What is actually done in the data-driven economy is opaque and hidden by the DIPs. The DIPs reign huge digital ecosystems . We are facing new forms of commodification (of contacts, user profiles and user networks; Fuchs, 2017), new forms of markets on building connective (data) platforms, and new economic principles. Developing a viable platforms, APPs, etc. that function successfully on the *users' data pay principle* is linked to exceptionally high fixed entrance costs and low or no marginal costs as including additional customers has negligible costs. How economic transactions with digital data-based products or services actually work is widely unknown to the public. Governments can efficiently monitor the number of cars produced *but not* the trade of internet users' data profiles. Thus, how a fair globalized taxation system for the digital part of value generation could look like is not yet known.

Asymmetric relations between digital platform providers and other economic actors: There is an asymmetric, unilateral relationship and/or distribution of power among global DIP oligopolists and other economic actors. Amazon, for instance, serves as both a host for upstream and a competitor for downstream actors. It has the best information about what products are doing

well. This suggests that there is a need for new forms of *competition rules* and their *implementation*.

Surveillance power and internet governance: Internet surveillance is presumably the most effective and efficient way of wielding political and economic power as it affects all levels of social systems (see Fig. 3). The political "Big Brother" strategy, based on governance by algorithms, has been most effectively applied in China, an autocratic society. The economic side of surveillance is based on data capitalism. Both forms of surveillance are linked to non-transpa-rent access to data which fundamentally bypasses principles of global justice and human rights.

The network monopoly phenomenon: Historically, market economy is expected to function if there is a diversity of goods and suppliers for (price-based) competition and for customer choice. At the earliest beginning of the internet's history, it was recognized that these basic laws of economics were overridden by the advantages of interoperability (i.e., standardization and compatibility) and the costs of switching networks and other factors (Katz & Shapiro, 1994). The internet connects people to other people to provide information, and "the more people that are connected to the Internet, the more valuable the connection is to each of the members" (Lemley, 1995). As consumers (users) benefit from a higher number of people, "the optimal number of 'Internets' in a free market economy is one" (Lemley, 1995). This leads to the paradox that, at first glance, in nation state structured world, economic principles promote that a communication and information infrastructure of all consumers does best economically with a monopolistic "all-in-one" solution. One challenge of reframing is the identification of functions of the digital infrastructure that may become subject to market competition (Furstenau, Baiyere, & Kliewer, 2019) and, possibly, new business models for others (that do not allow for traditional market competition).

Some DIPs have gained the status of supranational systems: DIP's key services are cloud-based storage, (algorithm-based) processing, retrieval, transmission, etc. for IoT-based technology and industry and global information and communication. DIPs have tremendous and asymmetric power over users ranging from nation-states to individuals (see SI2). This is metaphorically conveyed by the cloud concept, which is above terrestrial boundaries, seemingly in a space without ownership. Pinpointed, only the governments of the countries of the DIPs'

headquarters, the US and China, have control on the technical facilities, employment structure, etc. Other countries are currently in a "take it or leave it" position. There is a *subsidiarity principle-like relationship* for certain key performances offered by DIPs which cannot be directed at the national level of these other countries.

The physical layer of digital infrastructure cannot be ignored: The physical protection of cloud data centers including multiple-security data storage is controlled by DIP (see 2.2.1). Countries that do not host DIPs and their data centers have only limited influence (e.g., by legal regulation such as the GDPR) on the standards of data security and liabilities applied to cloud storage. The same holds true for the management of environmental disasters, cyberterrorism, hacker-attack protection, and energy standards. Governance principles are needed for the physical and material sides of digital infrastructure.

The supply security of the digital infrastructure calls for special attention: Currently, due to the technology innovation–regulation gap (see 2.1.3), digital infrastructure supply security is, at least in Germany, not developed in a manner similar to that of other resources. The provision of oil, for instance, is managed by the German Petroleum Stockpiling Law (Bundesrepublik Deutschland, 2012), which urges states to build strategic oil reserves of at least 90 days. Given an interruption of the global network for political reasons, a country such as Germany would not be able to construct the technological facilities needed by various reasons (Krempl, 2019). Thus, supply security is a critical challenge of reframing digital infrastructure.

Seggregation of the web: Some countries such as China and Russia seek internet sovereignty (Budnitsky & Jia, 2018; Schulze, 2019). They are building an *online Iron Curtain* and/or routing web traffic through a state-controlled national digital infrastructure. This is done to control their societies, to protect their markets, and to break US companies' economic internet hegemony. Several other nations such as Canada and Germany are targeting *national data residency* (see 2.1.3). There are currently strong asymmetric downward impacts of global DIPs and for most countries (see Fig 3b). And there is no political supranational global system which may govern global public good of digital infrastructure (as UN is only an international organization). Thus, we are facing the core dilemma that opportunities provided by a global internet for national or foreign political and economic actors are widely controlled and censored by DIPs with

headquarters in the US and not by elected governments. This results in cyber-security concerns and raises cyber-sovereignty goals in different forms (Budnitsky & Jia, 2018)

Conflicting sociocultural conceptions of human rights: One may argue that a globally acting technological system should be framed by one and the same legal system. Yet, unfortunately, the UN's principles and its Universal Declaration of Human Rights (UN, 1948) do not provide a universal reference system. First, we may note that there also exists a Charter of Fundamental Rights of the European Union (EU, 2000b), which shows some breaches of the UN right (Deprez, 2019; IGF, 2014; Robertson, 1968). Human rights according to the UN are not accepted by several Islamic states, which refer to the Cairo Declaration on Human Rights in Islam (CDHRI, 1990), which, for instance, denies women "full equality with men" (Hilal, 1997). Contrary France's "right to commit blasphemy" including Prophet Muhammed (Macron, 2020) is not tolerated by states following Sharia law.

5.1.2 The societal perspective

The private-public dilemma of digital infrastructure: The *internet, its network and data centers* are the technological pillars of key *critical infrastructures* (Section 1). The digital infrastructure became a *private good.* It is owned widely by few companies (Table 1). It provides the ground layer for basic communication, the IoT and AI-based monitoring, industrial production, business and financial operations, medical services, and for supporting all the processes of life and contemporary societies' critical infrastructures. This makes the *digital infrastructure* a *common* or *public good* that should be genuinely characterized by the *collective ownership of the governance of the digital infrastructure.*

The privately-owned web emerged and provides exceptional high performance. The services the digital infrastructure provides and their level of quality and risk, the kinds of operations that are allowed and those that are not, and what safety and security standards are applied are all, to a great extent, under the control of the DIP. Only a low level of national governmental control exists in regard to the physical and informational operations of infrastructure. Practically speaking, this means that some properties of *web infrastructure serving the public good*, *particularly trustworthy information, and communication sovereignty* are on an insufficient level. In

general, any *reframing* of the digital infrastructure must clarify in what way(s) the traditional trust *doctrine of public control of infrastructure* has to be redefined and for which functions.

The individual rights vs. societal responsibility dilemma: *The individual first vs.* society/state first trade-off is a challenging and controversially discussed issues related to the internet infrastructure. In the US, the First Amendment guarantees the freedom of speech to all US citizens. In China, individual interests are subordinate to the Confucian responsibility for the collective good (from family to the state). Cultural history-based differences cause dilemmas for reaching globally accepted rules when reframing digital infrastructure. This question refers not only to political-state surveillance and control but also to questions about whether medical data, personal data, private-property data, etc. should be public (see 2.1.3). Western democracy and Asian as well as autocratic societies refer to different interpretations of weighing human rights.

Democracy capability vs. autocracy: The perils of mobilizing public revolts in autocratic countries through open internet discourse (Eltantawy & Wiest, 2011) has long been considered as a potential source of democratization. But the picture is changing. Social media have also become tools for stabilizing autocratic societies, e.g., by counter-mobilization or launching unfair elections through the spread of false information (Gunitsky, 2015). Syria borrowed Iran's online-surveillance expertise (Morozov, 2011). Thus, digital technology may be used to promote or damage democracy.

5.1.3 The individual's user perspective

***Dilemmas around protecting the individual*.** The privacy vs. society dilemma becomes one of liberty vs. security when protection against terrorism enters the picture. The Apple DIP became a third agent in the 2012 San Bernardino case, where the FBI asked Apple to hack into the phone of a possible terrorist (involved in killing 14 persons) to disclose potential associates of future attacks (Blakely, Elam, Langley, Morrison, & Robinson, 2016). Apple's CEO, Tim Cook, refused, and Apple faced the dilemma of protecting a customer's privacy or being seen as an irresponsible member of society. Though, in the San Bernadino case, the information sought was retrieved with the help of hackers, we are facing malignant tradeoffs of keeping anonymity.

The user's safety culture: Fig. 4 presents the digital data flow for a typical individual or commercial human actor in Germany. The steps are described in the legend. The *user's safety* and *encryption culture* (see SI1) develops slowly. The amount of the global user's encrypted internet traffic passed 50% in 2017 and is around 90% now (Infotech News, 2019), the VPN use is close to 30% (GeoSurf, 2020, Mach 21). This is represented by the squared Roman numerals in Fig. 4 and indicates that the commercial and non-commercial user takes responsibility for the security level. For instance, European users are concerned that Facebook, Twitter etc. that data which are sent to their next neighbor, first enter cloud centers in the US (see Fig. 4, arrow ❹). Thus, reframing should include the development of proper safety cultures for uses of all types.

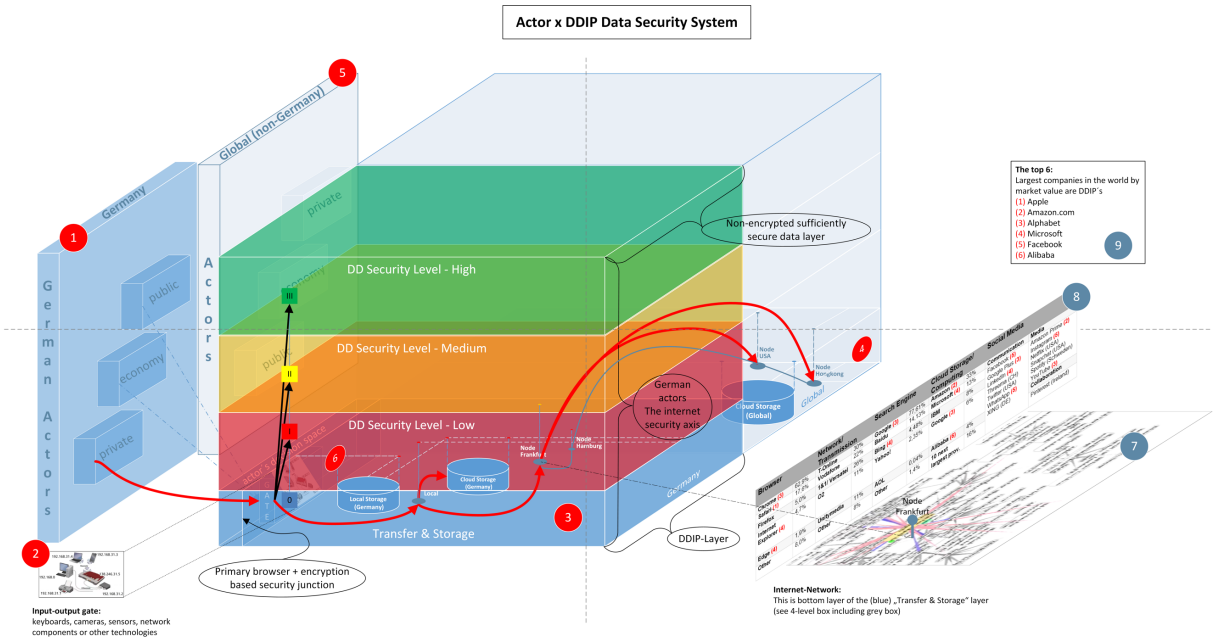

Fig. 4: German actors ❶ provide digital via an input-output gate ❷ to local nodes or to *internet* hubs such as the DE-CIX node Frankfurt that are located on "normal" data routing without security measures ❸. Data are transferred to global nodes. Cloud storage takes place predominately in the US ❹and is processed and (partly) used by non-German actors ❺. The actor's decision space represents the software and hardware means a user can take to choose security strata I , II , III. ❼ presents the global internet nodes, ❽ the actors and market share of Table 1, and ❾ the list of the top 6 DIPs according to stock market value.

Personal data protection: The GDPR is based on privacy as a fundamental human right (see Charter of EU Rights). The regulation refers to the personal data of all people (including cookies, IP addresses, location data, etc.) which are processed in EU countries. "Organizations without an EU presence that target or monitor EU individuals … must appoint an EU-based representative" (Goddard, 2017). The GDPR is the first internet law that applies ethical principles such as fairness and lawfulness, integrity and confidentiality, and data minimization. This seeks to address protection default and design. GDPR emphasizes transparency and openness (see 2.1.1)

in data processing for the user. Users have the right to receive extensive information that must be provided in regard to where the user's data are stored and to whom they are transmitted. We may learn from this that reframing has different regional and cultural ethical drivers.

5.2 Reframing for what goals

Reframing is goal-oriented (see 2.2), and goals are related to actors and their drivers related to their societal, political, economic etc. interests. The hierarchy of human systems/actors (Fig. 1) includes global DIPs as economic supranational players. A key conflict among levels of the human systems is that between the *DIPs' economic* and *national public good interests*. We discuss four major perspectives related to this issue.

The *first* is forming a societally beneficial *public–private* relationship. Digital technology and AI are used to represent most processes of reality in a virtual way. A digital twin exists for critical public infrastructures, geographic and environmental system (e.g., GPS-based data on extreme events, contamination, etc.). Economic activities are oriented toward market short- and mid-term profits. Governmental activities must guarantee public and ecosystem services (e.g. drinking water) for long. How this can be governed is largely unclear, at least from a European perspective. One public goal for reframing is a transparent model that considers what data may be used by whom, what data should be classified as open data, and what corporate digital responsibility and safety measures (public or private) digital infrastructure providers must guarantee.

The second perspective is national governmental control in regard to the reliability and trustworthiness of digital data. This focuses the regulative and legislative perspectives of the first perspective, and it may result in a reliable information act designed to support the right to know, which may include, for instance, tracking or trace-back rules. A significant share of internet information and social media interaction is maliciously falsified. Here a clearinghouse for fake news may be an objective. But some countries face the potential cyberwar-like infiltration of critical infrastructures. Thus, certain actors may call for a digital-data monitoring act that provides national governments and their security forces with extended access to control of digital infrastructure. In fact, governments may want and, occasionally, may require something

like an encryption backdoor (i.e., a key that allows encrypted messages to be read), e.g. in order to combat organized crime or terrorism. The design of the global web, e.g., VPNs, the darknet, and similar tools, is not designed for this. Such a situation may thus call for legislative and executive plans for closing internet borders (see SI1). In principle, currently, countries are facing the darknet dilemma to participate in the privately managed, widely encrypted global, not accessible web with all its benefits or to close and nationalize the web which makes it more controllable but opens the gate for a surveillance state.

The third perspective refers to the supranational role of DIPs. The code of competition does not exist in actuality in some domains of privatized digital infrastructure (see Table 1). Many of the services of digital infrastructure are provided by an oligopoly. If some of the DIPS were to (suddenly) halt their services for any reason, this would have negative effects for many actors and countries. Thus, if we compare the digital infrastructure to other infrastructure services, it is clear that the power in the traditional principal–agent relationship between national governments and infrastructure providers is widely reversed in the case of digital infrastructure. In a pointed view one may face a syndrome with the (interactions of the) following components: (i) DIPs are headquartered in the US (and exposed to political pressure), (ii) with a limited liability for the (impact of) content of the web (as a non-financial subsidy of the US government, the EU and some other countries promote start-ups on the web in the nineteen-nineties) and (iii) almost-unlimited freedom of speech (e.g., hate speech and political extremism). and no common international standards (which may ask for innovative sociotechnological solutions). Further, (iv) DIPs practice a near-perfect practice of the encapsulation of their commercial exploitation of data and information. This is due to the architecture of the semantic data base. (v) There are digital services where nation-states are in a “take it or leave it” position. And there are missing regulations on data (stored by DIPs). (vi) The characteristics of non-transparency are supported by encrypted information, location-independent (and sometimes unknown) data storage, and the anonymization and encapsulated management of data and operations. If there would be illegal action, this could almost only be detected by whistle blowing.

The *fourth* perspective is societal responsibility on the level of the individual. Simplified, one may require or postulate that society should provide safe, reliable, and trustworthy commercial, professional, and institutional environments to the individual. If the environment becomes too complex, e.g., when riding a car or plane, you need a license. This meets (in some way) the

goals of the European Computer Driving License (ECDL) that emerged 25 years ago to convey "competencies required to perform basic tasks using a personal computer" (Barnes, 2020). We argue that the ideas behind it are correct and worthwhile but that what has to be learned goes far beyond the technological level and has to be refurbished.

The global *DIP economy vs. national public goals dilemma* is a malignant type of conflict. Fragmenting the internet according to the national boundaries is not a meaningful goal as it would imply a harmful segregation and regression of global economy and other systems. A key challenge for democratic societies is a proper mix of regulation or non-regulation which keeps the viability of democratic processes. Yet, combining the case of the Great Firewall and censorship in Mainland China with the ideas of the European Union's digital strategy may open the door to ways of resolving the *dilemma*. Europe's digital strategy is one that strives to control their own countries' data with a maximum of harmony of the EU cluster with the global net. Russia is taking a route similar to that of China, while the US government is following security-driven autonomy strategies in a manner that is similar to that of the EU (and is facing the advantage of hosting the big DIPs and most *data* centers). We may well imagine that other big players such as India or clusters of smaller nations may develop across the world. This would imply a shift from the 193 nation-states to a small *set of differently closed world clusters* that inherently represent somewhat harmonious sociocultural, political, and economic goals. The aims among such clusters might differ with respect to democracy as a political goal, the interpretation of personal rights including the protection of individual data, the degree of governmental surveillance, the level of data sovereignty, and participation in a globalized (localized) cloud. Economically, an antitrust oriented decentralization (Tilson, Lyytinen, & Sørensen, 2010) which allow for competition of economic actors (Cheng, Bandyopadhyay, & Guo, 2011; van Dijck et al., 2019) might also allow better to meet regional cluster's public goals.

We may also think whether the *economic scheme of financing* the costs of digital infrastructure for free of charge services by commercializing behavioral user data (e.g., from social media) is a proper economic model to serve the public good. Actually, this might be a *fifth* layer of goal formation for reframing the digital infrastructure.

5.3 How might a reframing take place?

Generally, countries are viewed as principals and governments as agents for public infrastructure as governing infrastructure operations ranks high in national security. For digital infrastructure the oligopoly of the US headquartered DIPs currently has currently an economic top-down power on most countries which is similar to the political power of EU. This DIPs are viewed as economic supranational systems. They operate globally and can decide which country/customer gets what services. Their cooperation with national governments is limited. They take increasingly control of data. Thus, they own a tremendous surveillance power. They have acquired vast private research potential on AI and organizing and retrieving data. And they operate in a nontransparent, perplexingly encapsulate manner.

Up to now, DIPs' business seems not to be driven by political or sociocultural motives. Yet reacting to political demands is restricted by the web architecture. For instance, a single small country such as Switzerland (see SI2) has no chance of succeeding in its request that – due to its national gambler-protection ethics – foreign online casinos shall not be accessible to Swiss gamblers. Banning end-to-end encryption for gambling operations is not compatible with the internet practice.

Country clusters such as the EU may build the grid of the future web, building a cyber Westphalization on a larger scale. Given the current scattered geopolitical global landscape, there are no strong global institutions that could develop strategies on what to be done so that the internet provides what citizens of various countries would like to have. The UN Internet Governance Forum is a global multistakeholder discussion forum that addresses certain aspects such as trust, data, or climate-impact management and did not discuss overarchingly on digital infrastructures (IGF, 2020). Global institutions such as the World Trade Organization are weakened in a world shaped by trade wars. They are looking for new modes of work practices (Hoekman, 2019). Therefore, no global organization may cope with the challenge of reframing infrastructure when touching the fundamental tradeoffs and dilemmas discussed. A development of a polycentric bottom up approach for shared governance rules (Constantinides & Barrett, 2015) may be a possible option.

Including secret services in a reframing is impossible as they may be seen as a hidden and inconsistent geopolitical power actors. The Snowden affair drew much attention on the issue that after 9/11 the US national securities agencies created doors to get multiple access to digital data. In European countries, much public concern developed with the idea that US secret services may have easy access to European users' data as any information sent via social media from a user to his/her neighbor first passes through US American data centers. This also has been one trigger of promoting European actors to establish a localized data infrastructure (German Federal Government, 2019). Yet, secret services may listen everywhere.

We may assume that a continuous, institutionalized interaction between DIPs and governmental institutions in regional clusters may facilitate the management of maintaining sociocultural norms, the possibility of being able to access data in cases of crime, hate speech, child abuse, conspiracy theories, etc. on social media and elsewhere. Yet, this is relative. As outlined in SI1, the internet has a highly decentralized *technical* architecture. The use of VPNs or the Tor browser allows anonymization, given some interoperability of the clusters. We may also postulate that questions of data security, long-term availability of data, and guaranteeing low pricing of services that are viewed as a public service for all, will be a difficult part of reframing.

The liability *law* regulating social responsibility plays an important role. If DIPs, APP providers, and other digital actors were to accept liability for negative impacts resulting from information transmitted that violates national laws, many problems might be solved. Yet, this would demand that persons, companies, etc. providing service and operating on the web become legal entities and anonymous activities would become abandoned. Thus, there is another dimension of transparency most difficult to establish.

6. Conclusions

Human development is facing a new stage. In principle, all members of the human species can interact in a networked real-time system. There is a vast, seemingly unlimited external digital memory. All human-made information can be stored and immediately retrieved by smart

algorithms. The virtual digital world, i.e., a digital layer or curtain functions as a *modulator* between the perceptual system of human systems and the real world. From a coupled-systems perspective, the digital world is a modulating intermediate entity of all human systems interacting with the real (analog) biophysical environment (Fig. 2 und 3). This digital curtain is augmenting human capacity and provides a tremendous extension and amplification of human activity. The virtual world of the digital layer allows us to monitor (survey) and simulate real-world processes, in turn, making the digital curtain the most powerful economic system and a form of *universal infrastructure*. Digital data have become a new commodity, good, human resource, and currency in the way that energy did in the industrial age and are now a key variable of the economic system (i.e., data economy). The digital world has become a basic tier of all domains of human life and thus a genuine public good.

This digital layer has developed rapidly in about a quarter of a century. A fundamental novelty of human development is that this digital layer (i.e., the fundamental facilities and systems of the digital infrastructure) is currently widely owned, developed, and maintained by a few oligopolistic economic actors (see Table 1) and their economic interests. Google, e.g., widely manages and controls what information is presented to whom though providing basic information to all is usually considered as a public good.

The political world order has been based on national law and politics. Thus, there are potential conflicts between the drivers and rationales of DIPs as economic actors and sociopolitical (i.e., nation-states) and other human actors' needs and wants (see Fig. 2). The new evolutionary entity of large (internet) groups (see Fig. 1) is included here.

Understanding the technological design of the global net (see SI1) is important in order to understand the *power of the DIPs* as a new type of supranational (economic) actor and the *relationship and interferences between DIPs and nation-states*. The net and, principally, the global cloud system are highly decentralized systems. Where storage and computation take place is widely arbitrary and difficult to trace. Particularly as most of the data is encrypted. Even if DIPs would provide national agencies with access to data, it would be difficult to perform executive operations for technological reasons. This leads to two mayor conclusions.

First: DIPs are a global *supranational system* above the level of the nation-state. They are *not* a (political or economic) stakeholder group. There is only limited European regulatory control on DIPs web and cloud management. Due to their (nearly) monopolistic situation, for instance, browser or search engine DIPs (see Table 1) are not really affected by other stakeholders. They are financially independent from nation-states. DIPs are poor of subsidies. The pay model of commercializing behavioral and other internet data, which is obviously appreciated by many users, allows DIPs to offer a major share of basic services to private users related to communication, information, and data without direct monetary payment (naturally, the cloud-based software stack of *platform service* and the *application laye*r of the web are not free). Which information is disseminated or not via their platforms and services, is under the control of DIPs. For any governmental actor (perhaps with the exception of the US), it is difficult to know where what data are hosted (see Fig. 4). Although there are no (incorporeal) data without physical (corporeal) storage, encryption places data in a kind of legal vacuum.

Second: A reframing of the digital infrastructure from the perspective of fulfilling society's wants and needs, calls for understanding the interferences and conflicting drivers of goal systems of *nation-states* and *DIPs*. Simplified, we may distinguish between (a) the traditional (democratic or autocratic) physical and institutional infrastructure system governance and (b) the current global, market-driven digital infrastructure services whose operation are primarily offered by a few private oligopolistic DIPs. They are, in the Western world, only moderately dependent (see Fig. 3) on nation-states and other users.

These provide new challenges for reframing the digital infrastructure of democratic countries (whose perspective is taken). We conclude that the identification of

- *Conflicts of goals* between DIPs and users' interests,
- *Trade-offs* within different interests of users (e.g., between individual freedom and societal control) and also of DIPs, and sometimes even
- *Dilemmas,* e.g., between DIPs and users, for instance, caused by the encryption architecture

is an indispensable prerequisite for reframing digital infrastructure.

The present paper (which takes in many parts a perspective of European nation states) has discussed a long list of conflicts, the management of which will be subjects of reframing.

On the *economic side,* DIPs, governmental, and other actors have to reflect on the *pay model* (e.g., how does the pay model affect information flows) and *antitrust rules.* For what domains is a monopoly structure critical, in which domains acceptable or indispensable? What rules of transparency or supply security and *competition rules* (for instance, for DIPs which work in many business domains) would be necessary?

Security and *safety* are important for economic, political, and other perspectives. We may distinguish between a *physical side of data* (e.g., for how long can we guarantee reliable access to data for what costs) and an *informational* side. The latter refers not only to the *availability* and protection of data but also to the *trustworthiness* of information. For this, there are roots, e.g., in the US Freedom of Information Act (U.S.C., 1988): Any lack of trustworthiness may endanger economic and social systems. The genuine involvement and potential interaction of essentially different actors such as citizens, economic actors, public agencies, political leaders, infrastructure providers, as well as hackers or secret service agents (Lai & Syed, 2012) may become subjects of sophisticated and criminal activities. The European Council (Council of Europe, 2001) launched the Convention of Cybercrime (also called the Budapest Convention) as a treaty to protect society against cybercrime. This is the only binding international instrument in this domain. It has been ratified by 64 states (Council of Europe, 2019; not including, e.g., China and Russia). From a reframing perspective, we may argue that a safety and trustworthiness approach may call for technological means for building a resilient web, with blockchain-like technologies or quantum-security for providing secure communication, trustworthy identities and interoperability. We conclude that security and safety reasons are important issues of reframing.

We have presented numerous reasons and examples of reframing in the light of maintaining resilient *sociocultural* structures. In principle, the vision of a worldwide open web, widely data economy-driven web (as it currently exists) practice is often in sharp conflict with regions' legally, morally, or culturally legitimate codes of conduct or terms of service. This meets the dilemma that there are no unambiguously accepted global human rights as regional sociocultural systems are conflicting. We also face a trade-off between *individual rights* and *societal*

responsibility, which is managed differently in Europe, the US, Russia, China, and Iran, to mention a few regional actors. The *individual*, personal side is embedded in the sociocultural one. The American and German–European goals of the individual's right to have his or her data protected by GDPR (which has to be followed by all data collectors) and the discussion about the individual's property rights related to data show conceptual and historic differences that are relevant for the economic use of data and the applied pay model. The right to privacy in many states of the US is pragmatically reasoned (Warren & Brandeis, 1890) "resulting in minimal online protection," whereas the European conception is normative related to dignity and personal honor (Kant, 1797). We may conclude that different societies have different conceptions of privacy at different points in time. These have impacts on data economy, but the internet transcends these legal and cultural rules and guidelines, and thus finding a transatlantic solution may be difficult.

When we look at the *process of reframing* global infrastructure, governmental actors and DIPs are the main actors. But in addition, the individual and other users must think about the safety culture and the issues discussed in this paper. Developing digital literacy on the level of users below the level of society is certainly part of reframing (see Fig. 4). From a societal perspective, there is no homogeneity among national players. Cyber-Westphalia is a threat. Presumably, clustered action, such as practiced by EU countries, may be a meaningful intermediate step, for instance for building a smart data hub. This hub would connect centralized and decentralized (European) infrastructures that interact with other parts of the global web in an open manner but still allow – to some degree – for societal transparency. For DIPs, as global economic actors and supranational entities, this opens new and different markets and novel – and perhaps disruptive – forms of competition. Whether and perhaps how this will be compatible with the DIPs current position is open to discussion.

Acknowledgements: We want to thank Nassrin Hajinejad, Dirk Helbing, Karoline Krenn, Sören W. Scholz, and Gerald Steiner for their input and Elaine Ambrose for the English editing.

References

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography, 42*(1), 4-24.
Angelowska, N. (2019). Facebook losing Uuers to Pinterest, Youtube and Twitter (market share by region), January 7, 2019. *Forbes*.
Ankenbrand, H. (2019). Komplett überwacht in China. *Frankfurter Allgemeine Zeitung, August 29. 2019,* p. 20.
Antsaklis, P. (2017). Editorial control systems and the quest for autonomy. *IEEE Transactions on Automatic Control, 62*(3), 1013-1016.
Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society, 54*(2), 138-149.
Barnes, J. E. (2020). White House Official Says Huawei Has Secret Back Door to Extract Data, February 11, 2020. *New York Times*. Retrieved from https://www.nytimes.com/2020/02/11/us/politics/white-house-huawei-back-door.html
Barnett, C. (2001). Culture, policy, and subsidiarity in the European Union: from symbolic identity to the governmentalisation of culture. *Political geography, 20*(4), 405-426.
Barraqué, B. (2003). *Past and future sustainability of water policies in Europe.* Paper presented at the Natural Resources Forum.
Benenson, Y. (2009). Biocomputers: from test tubes to live cells. *Molecular Biosystems, 5*(7), 675-685. doi:10.1039/b902484k
Benincasa, C., Calden, A., Hanlon, E., Kindzerske, M., Law, K., Lam, E., . . . Valentine, E. (2006). Page Rank Algorithm. *Department of Mathematics and Statics, University of Massachusetts, Amherst, Research*.
Berners-Lee, T. (2019). Wie wir das Netz bekommen, das wir wollen. *Frankfurter Allgemeine Zeitung, 11.03.2019*. Retrieved from https://www.faz.net/aktuell/wirtschaft/diginomics/tim-berners-lees-vision-fuer-die-zukunft-des-world-wide-web-16083091.html
Berners-Lee, T., & Fischetti, M. (2001). *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*: DIANE Publishing Company.
Blakely, T., Elam, K., Langley, D., Morrison, W., & Robinson, D. (2016). Apple's conundrum: Liberty vs. security and modern terrorism. *Intellectual Archive, 5*(3), 32.37.
Blanke, H.-J. (2013). Artcle 1. Establishment and Functioning of the Union. In H.-J. Blanke & S. Mangiameli (Eds.), *The Treaty on European Union (TEU). A Commentary* (pp. 45-109). Heiderlberg: Spinger.
Bleich, E. (2014). Freedom of expression versus racist hate speech: Explaining differences between high court regulations in the USA and Europe. *Journal of Ethnic and Migration Studies, 40*(2), 283-300.
Boerding, A., Culik, N., Doepke, C., Hoeren, T., Juelicher, T., Roettgen, C., & Schoenfeld, M. V. (2019). Data Ownership—A Property Rights Approach from a European Perspective. *Journal of Civil Law Studies, 11*(2), 5.
Bowles, S. (2009). Did warfare among ancestral hunter-gatherers affect the evolution of human social behaviors? *Science, 324*(5932), 1293-1298.
Brown, S. (1984). The world polity and the nation-state system: an updated analysis. *International Journal, 39*(3), 509-528.
Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594-613.
Buggisch, C. (2019). Social Media, Messenger und Streaming – Nutzerzahlen in Deutschland 2019. Retrieved from https://buggisch.wordpress.com
Gesetz über die Bevorratung mit Erdöl und Erdölerzeugnissen (Erdölbevorratungsgesetz - ErdölBevG), (2012).
BVDW. (2019). Glossar: Social Media. Retrieved from https://www.bvdw.org/themen/publikationen/detail/artikel/glossar-social-media/.
Cadwalladr, C., & Graham-Harrison, E. (2018). The Cambridge analytica files. *The Guardian, 21*, 6-7.
CDHRI. (1990). Cairo Declaration on Human Rights in Islam. Retrieved from http://www.religlaw.org/interdocs/docs/cairohrislam1990.htm
Chaffey, D., & Ellis-Chadwick, F. (2019). *Digital marketing*: Pearson UK.
Chapple, E. D., & Coon, C. S. (1953). *Principles of anthropology*. New York, NY: Henry Holt.
Cheng, H. K., Bandyopadhyay, S., & Guo, H. (2011). The debate on net neutrality: A policy perspective. *Information systems research, 22*(1), 60-82. doi:10.1287/isre.1090.0257
Constantinides, P., & Barrett, M. (2015). Information infrastructure development and governance as collective action. *Information Systems Research, 26*(1), 40-56.
Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Platforms and infrastructures in the digital age. *Information systems research, 29*(2), 381-400. doi:10.1287/isre.2018.0794
Conti, M., Cozza, V., Petrocchi, M., Spognardi, A., & Ieee. (2015). TRAP: using TaRgeted Ads to unveil Google personal Profiles. In *2015 Ieee International Workshop on Information Forensics and Security*.

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 20*(4), 336-349.
Conventionon Cybercrime , ETS No185 (November, 23, 2001), also referred to as the Budapest' Convention, (2001).
Council of Europe. (2019). T-CY News: Peru joined the Budapest Convention on Cybercrime, August 26, 2019.
Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In M. Khosrow-Pour (Ed.), *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549): IGI Global.
Dean, B. (2019). Google's 200 Ranking Factors: The Complete List (2019). Retrieved from https://backlinko.com/google-ranking-factors
Demchak, C., & Dombrowski, P. (2013). Cyber Westphalia: Asserting state prerogatives in cyberspace. *Georgetown Journal of International Affairs*, 29-38.
Deprez, C. (2019). The admissibility of multiple human rights complaints: Strasbourg and Geneva Compared. *Human Rights Law Review, 19*(3), 517-536. doi:10.1093/hrlr/ngz022
Eltantawy, N., & Wiest, J. B. (2011). The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory. *International Journal of Communication, 5*, 18.
2000/520/EC. The safe harbour privacy principles (Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce)2000/520/EC, 25/08/2000, (2000a).
Charter of Fundamental Rights of the European Union (2000/C 364/01), (2000b).
Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings ((2009/C 45/02)), (2009).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1., (2016).
The EU General Data Protection Regulation (GDPR), (2018).
EU. (2019). Fact Sheets on the European Union, authored by Mariouz Maciejewski, Christina Ratcliff / Andreea Dobrita.
Florini, A. (2007). *The right to know: transparency for an open world*. New York, N.Y.: Columbia University Press.
Focus2move. (2019, February). Global Data & Ranking, Manufacturers Ranking. Retrieved from https://focus2move.com/world-car-group-ranking-2018/
Frosio, G. F. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Northwestern University Law Review Online, 112*, 18.
Frydman, B., & Rorive, I. (2002). Regulating Internet content through intermediaries in Europe and the USA. *Zeitschrift für Rechtssoziologie, 23*(1), 41-60.
Fuchs, C. (2012). Social media, riots, and revolutions. *Capital & Class, 36*(3), 383-391.
Fuchs, C. (2017). *Social media: A critical introduction (2nd edition)*. London: Sage.
Furstenau, D., Baiyere, A., & Kliewer, N. (2019). A Dynamic Model of Embeddedness in Digital Infrastructures. *Information systems research, 30*(4), 1319-1342. doi:10.1287/isre.2019.0864
GeoSurf. (2020, Mach 21). VPN usage statistics.
Geraci, R. M. (2006). Spiritual robots: Religion and our scientific view of the natural world. *Theology and Science, 4*(3), 229-246.
German Federal Government. (2019). Digital summit in Dortmund. Data sovereignty is paramount. Retrieved from https://www.bundesregierung.de/breg-de/themen/digitalisierung/kanzlerin-bei-digitalgipfel-1686406
Gleick, P. H. (1998). The human right to water. *Water Policy, 1*(5), 487-503.
Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research, 59*(6), 703-705.
Gold, T. B. (2011). Understanding Chinese Society. *Foreign Policy Reserach Institute Footnotes, 16*(1), http://www.fpri.org/docs/media/1601.201104.gold_.chinesesociety.pdf.
Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics, 13*(1), 42-54.
Hanna, T. M., Lawrence, M., Buller, A., & Brett, M. (2020). Democratic Digital Infrastructure. *DPO - Democratic Public Owenership*.
Hegelich, S. (2016). *Invasion of the social bots*. Facts & Findings. Konrad Adenauer Stiftung. Berlin. Retrieved from https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_46486_2.pdf/04db80c6-543e-40ff-23e7-03cc44fe6766?version=1.0&t=1539650238695
Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., . . . Zwitter, A. (2017). Will Democracy Survive Big Data and Artificial Intelligence. *Scientific American. Feb, 25*.

Henfridsson, O., & Bygstad, B. (2013). The generative mechanisms of digital infrastructure evolution. *Mis Quarterly, 37*(3), 907-+. doi:10.25300/misq/2013/37.3.11
Herfindahl, O. C. (1967). Depletion and economic theory. In M. Gaffney (Ed.), *Extractive Resources and Taxation*. Madison, WI: University Wisconsin Press.
HIH. (2019). Statista. Retrieved from https://de.statista.com/prognosen/953783/umfrage-in-deutschland-zu-hauptversorgenden-internetdienstanbietern-im-haushalt
Hilal, L. (1997). The Cairo Declaration on Human Rights in Islam and International Women's Rights. *Circles: Buffalo Women's Journal of Law and Social Policy, 5*, 85-89.
Hodge, G. A., & Greve, C. (2005). The challenge of public-private partnerships: Learning from international experience. In G. A. Hodge & C. Greve (Eds.), *The challenge of public-private partnerships: Learning from international experience* (pp. 1-37). Cheltenham: Edward Elgar Publishing.
Hoekman, B. (2019). Trade wars and the World Trade Organization: Causes, consequences, and change. *Asian Economic Policy Review, 15*, 98-114.
IGF, U. (2014). *The charter of human rights and principles for the internet. 4th ed.* New Yor NY: Internet Rights and Principles Dynamic Coalition UN Internet Governance Forum.
IGF, U. (2020). IGF 2020. Call for Validation of Thematic Tracks Inputs Analysis. February 12, 2020. Retrieved from https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/9615/1976
Infotech News. (2019). HTTPS encryption traffic on the Internet has exceeded 90%. Retrieved from https://meterpreter.org/https-encryption-traffic/
Janssen, M. A., & Ostrom, E. (2006). Governing social-ecological systems. *Handbook of computational economics, 2*, 1465-1509.
Kant, I. (1797). *Metaphysische Anfangsgründe der Tugendlehre: Metaphysik der Sitten. Zweiter Teil*. Königsberg: Nicolovius.
Kathuria, V. (2019). Greed for data and exclusionary conduct in data-driven markets. *Computer law & security review, 35*(1), 89-102. doi:10.1016/j.clsr.2018.12.001
Katz, M. L., & Shapiro, C. (1994). Systems competition and network effects. *Journal of Economic Perspectives, 8*(2), 93-115. doi:10.1257/jep.8.2.93
Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology, 32*(3), 61.
Kerber, W. (2016). Digital markets, data, and privacy: competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice, 11*(11), 856-866.
Kessides, I. (2004). *Reforming infrastructure: Privatization, regulation, and competition*. Washington, DC: The World Bank.
King, M. J., Watson, B., & Fleiter, J. J. (2019). Applying the Traffic Safety Culture Approach in Low-and Middle-income Countries. In *Traffic Safety Culture: Definition, Foundation, and Application* (pp. 251-274): Emerald Publishing Limited.
Königliche Regierung zu Cassel. (1906). Polizei-Verordnung über den Verkehr mit Kraftfahrzeugen. *Amtsblatt der Königlichen Regierung zu Cassel, A38, Mittwoch, den 19. September 1906*, 313-326.
Korshunov, P., & Marcel, S. (2018). Deepfakes: a new threat to face recognition? Assessment and detection. *arXiv preprint arXiv:1812.08685*.
Krempl, S. (2019). Digitale Souveränität: "Wir dulden eine flächendeckende IT-Unsicherheit“, .
Kroeger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering & System Safety, 93*(12), 1781-1787. doi:10.1016/j.ress.2008.03.005
Kuchler, H. (2019). How Facebook grew too big to handle. The tech giant’s ‘growth team’ brought it over a billion users – but did it also sow the seeds for current troubles? March 28, 2019. *Financial Times*.
Lai, R., & Syed, R. (2012). Analytic of China cyberattack. *The International Journal of Multimedia & Its Applications, 4*(3), 37.
Langford, M. (2005). The United Nations concept of water as a human right: a new paradigm for old problems? *International Journal of Water Resources Development, 21*(2), 273-282.
Laws, D., Scholz, R. W., Shiroyama, H., Susskind, L. E., Suzuki, T., & Weber, O. (2004). Expert views on sustainability and technology implementation. *International Journal of Sustainable Development and World Ecology, 11*(3), 247-261.
Lemley, M. A. (1995). Antitrust and the Internet standardization problem. *Conn. L. Rev., 28*, 1041.
Lenski, G. (2005). *Ecological-evolutionary theory: Principles and application*. Boulder, CO: Paradigm Publisher.
Lillington, K. (2019). Schrems II will seriously stress test EU’s data privacy rules, July 11, 2019. *The Irish Times*.
Macron, E. (2020). Macron decries 'Islamic Separatism,' defends blasphemy; September 4, 2020, by The Associated Press. *The New York Times*. Retrieved from https://www.nytimes.com/aponline/2020/09/04/world/europe/ap-eu-france-islamic-extremism.html

Marketshare, N. (2019a). Market Share for Mobile, Browsers, Operating Systems and Search Engines. Retrieved from https://www.netmarketshare.com/?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24nin%22%3A%5B%22Other%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Custom%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22browser%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22browsersDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222019-09%22%2C%22dateEnd%22%3A%222019-09%22%2C%22segments%22%3A%22-1000%22%7D.
Marketshare, N. (2019b). Search Engine Market Share. Retrieved from https://www.netmarketshare.com/search-engine-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%2C%22Mobile%22%2C%22Console%22%2C%22Handheld%22%2C%22Tablet%22%2C%22TV%22%2C%22Set%20top%20box%22%2C%22Bot%20or%20spider%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Custom%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22searchEngine%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22searchEnginesDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222019-09%22%2C%22dateEnd%22%3A%222019-09%22%2C%22hiddenSeries%22%3A%7B%7D%2C%22segments%22%3A%22-1000%22%7D.
Merkel, A., Seehofer, H., & Gabriel, D. (2013). *Deutschlands Zukunft gestalten. Koalitionsvertragzwischen CDU, CSU und SPD, 18. Legislaturperiode*. Germany: CDU, CSU and SPD.
Merriam Webster. (Ed.) (2019) Webster's Third New International Dictionary, Unabridged, accessed July 11, 2019, http://unabridged.merriam-webster.com. Springfield, MA: Merriam Webster.
Miller, J. G. (1978). *Living systems*. New York, NY: McGraw-Hill.
Montag, C., & Diefenbach, S. (2018). Towards Homo Digitalis: Important research issues for psychology and the neurosciences at the dawn of the internet of things and the digital society. *Sustainability, 10*(2). doi:10.3390/su10020415
Morozov, E. (2011). *The net delusion: How not to liberate the world*. New York, N.Y.: Penguin.
Parsons, T. (1951). *The social system*. New York, NY: The Free Press.
Parsons, T. (1961). General theory of sociology. In R. K. Merton, L. Broom, & L. S. Cottrell (Eds.), *Sociology today: Problems and prospects* (pp. 3-38). New York, NY: Basic Books.
Parsons, T. (1971). *The system of modern societies*. Englewood Cliffs, NJ: Prentice Hall.
Petring, J. (Producer). (2019, September 3, 2019). Handelskammern schlagen wegen Chinas Sozialkreditsystem Alarm. Retrieved from https://www.heise.de/newsticker/meldung/Handelskammern-schlagen-wegen-Chinas-Sozialkreditsystem-Alarm-4508616.html
Pisani, B. (2919). These five stocks have gotten so big, they are essentially becoming the market, June 26, 2019. Retrieved from https://www.cnbc.com/2019/06/26/a-group-of-five-stocks-have-gotten-so-big-they-are-essentially-becoming-the-stock-market.html
Redmond, S., Jones, N. M., Holman, E. A., & Silver, R. C. (2019). Who watches an ISIS beheading—and why. *American Psychologist*.
Richter, F. (2019). Amazon Leads the Race to the Cloud. *Statista Infographics*. Retrieved from https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.
Robertson, A. H. (1968). The United Nations covenant on civil and political rights and the European convention on human rights. *British Year Book of International Law, 21*, 21-48.
Rozenshtein, A. Z. (2018). Surveillance intermediaries. *Stanford Law Review, 70*, 99.
Sandholtz, W. (1998). The emergence of a supranational telecommunications regime. In W. Sandholtz & A. S. Sweet (Eds.), *European integration and supranational governance* (Vol. 1, pp. 134-164).
Scholz, R. W. (2011). *Environmental literacy in science and society: From knowledge to decisions*. Cambridge: Cambridge University Press.
Scholz, R. W. (2017). The normative dimension in transdisciplinarity, transition management, and transformation sciences: New roles of science and universities in sustainable transitioning. *Sustainability, 9*(991). doi:doi:10.3390/su9060991
Scholz, R. W., Bartelsman, E. J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., . . . Viale Pereira, G. (2018). Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. *Sustainability, 10(6), 2001; https://doi.org/10.3390/su10062001*.
Schreier, F., Weekes, B., & Winkler, T. H. (2015). *Cyber Security: The Road Ahead*. Geneva: DCAF.
Schrems, M. (2014). *Kämpf um deine Daten*. Wien: Editions A Verlag.

Schulze, E. (2019). Russia just brought in a law to try to disconnect its internet from the rest of the world. Retrieved from https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html
Sotto, L. J., & Hydak, C. D. (2016). The EU-US Privacy Shield: A how-to guide. *Law360*, 1-4.
Spapens, T. (2018). The 'Dieselgate'scandal: A criminological perspective. In T. Spapens, R. White, v. U. D., & W. Huisman (Eds.), *Green Crimes and Dirty Money* (pp. 109-130). London: Routledge.
StatCounter. (2019). Search Engine Market Share Worldwide - November 2019. Retrieved from https://gs.statcounter.com/search-engine-market-share
Statistisches Bundesamt. (2008). *Verkehrsunfälle 2007, Fachserie 8, Reihe 7*. Statistisches Bundesamt. Wiesbaden.
Stewart, E. (2018). The Trump administration's surprising idea to nationalize America's 5G network, explained. Nobody thinks it's a good idea, including the FCC. *Vox Media*. Retrieved from https://www.vox.com/policy-and-politics/2018/1/29/16946582/trump-5g-proposal-wireless-ajit-pai-fcc-china
Sugiyama, M., Deguchi, H., Ema, A., Kishimoto, A., Mori, J., Shiroyama, H., & Scholz, R. W. (2017). Unintended side effects of digital transition: Perspectives of Japanese Experts. *Sustainability, 9*(12). doi:ARTN 219310.3390/su9122193
Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research commentary—Digital infrastructures: The missing IS research agenda. *Information systems research, 21*(4), 748-759.
Treasury Board of Canada. (2018). ***Government of Canada White Paper: Data Sovereignty and Public Cloud, 2018-06-25***. Ontario: Treasury Board of Canada, Secretariat.
Tzanetakis, M. (2018). The darknet's anonymity dilemma. *Encore 2017. The Annual Magazine on Internet and Society Research*, 118-125.
Freedom of Information Act. § 552(a)(3), (1988).
Universal declaration of human rights, (1948).
van Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing platform power. *Internet Policy Review, 8*(2). doi:10.14763/2019.2.1414
Verble, J. (2014). The NSA and Edward Snowden: surveillance in the 21st century. *ACM SIGCAS Computers and Society, 44*(3), 14-20.
Viale Pereira, G., Estevez, E., Cardona, D., Chesñevar, C., Collazzo-Yelpo, P., Cunha, M. A., . . . Scholz, R. W. (2020). South American expert roundtable: Increasing adaptive governance capacity for coping with unintended side effects of digital transformation. *Sustainability, 12*, 718. doi:doi.org/10.3390/su12020718
W3C. (2019). World Wide Web Consortium (W3C). Retrieved from https://www.iotone.com/organization/world-wide-web-consortium-w3c/o205
W3Techs. (2019). Usage Statistics and Market Share of SSL Certificate Authorities for Websites. Retrieved from https://w3techs.com/technologies/overview/ssl_certificate/all
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review., IV*(5), 193-220.
Weber, M. (2018). Browser an browser wars. In N. Brügger & I. Milligan (Eds.), *The SAGE Handbook of Web History* (pp. 270-297). London: Sage.
West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & society, 58*(1), 20-41.
Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday, 21*(4).
Xu, S., Sandhu, R., & Bertino, E. (2009, June 15-19, 2009). *Tiupam: A framework for trustworthiness-centric information sharing.* Paper presented at the IFIP International Conference on Trust Management, June 15-19, 2009, West Lafayette, IN, USA.
Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety, 152*, 137-150. doi:10.1016/j.ress.2016.02.009
Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75-89.
Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. London: Profile Books.