The Enemy Within: The Human Side of Governance, Innovation, and National Security in the Age of Data-Driven Big Tech

THE ENEMY WITHIN: THE HUMAN SIDE OF GOVERNANCE, INNOVATION AND NATIONAL SECURITY IN THE AGE OF DATA-DRIVEN BIG TECH

Authors: Rebekah Rousi, Leena Kunttu, and Juhani Merilehto

Abstract

The topic of artificial intelligence (AI) governance has rapidly become central to the debate on digital transformation and machine learning (ML) systems. While considerable efforts have been invested in developing frameworks and identifying sectors and governance strategy, responsibility and accountability models, and, perhaps more than anything else, data regulation (i.e., General Data Protection Regulation, GDPR), we still face a situation where systems and practices are beyond the jurisdiction of any one body. Moreover, the power imbalance is increasing between corporations, nations, and national sectors owing to a number of factors: knowledge and expertise of systems; ownership of computational resources, networks, and critical information communication technology infrastructure; the standards and regulations themselves; and those who support the law bending the law. Large technology business can derive huge benefits via the regulation of others who use its resources and then applying the safeguarding software and systems that the large companies themselves develop. In this chapter, the authors explain and illustrate the nature of the beast of AI governance and regulation and their impact on innovation and national security.

Keywords: Governance, General Data Protection Regulation (GDPR), innovation, economics, Big Tech, business, national security

Introduction

There is a war going on and this war entails information, public governance and corporate spheres in the context of national security and innovation. Amidst the actions of innovation and governance is a very human core of emotional control that is based on both reason and desire. In a statement made on X (formerly Twitter) on October 31, 2023, Google Brain co-founder Andrew Ng emphasized the role of open-source technology in driving AI development and the strategic incitement of irrational fear (fearmongering) powered by large technology corporations in order to tighten legislation, restricting the life-blood of innovation among smaller technology businesses, and the open-source community in general (Nolan 2023).

Accordingly, reason and a desire for techno-corporate dominance are competing against the background of governance. Here, *reason* has a two-fold significance. First, it pertains to a sense of rationality through the understanding that in order to progress in a technological landscape characterized by complex technology, some form of framework (ethical, security, and otherwise) is needed to maintain control by certain parties (e.g., governments and official administration (Borrás and Edler 2020). Second, reason or strategic reasoning operationalizes fearmongering rhetorically to influence the general public and key policymakers. Fear is a basic primal emotion (See, e.g. Ekman 1999) that impels humans to act prior to conscious thought, or in others words, impulsively.

Humans have a natural tendency to be prejudiced towards phenomena, scenarios, and narratives associated with negative emotions. That prejudice subsequently affects future decision-making practice (Cahir and Thomas 2010). There is a desire among corporate players and technologists alike towards

reaching the peak of technological science fiction fantasy and corporate dominance (Suarez-Villa 2016, 200) no matter what the cost. Governance is used as a weapon in anti-competition and national security (see, e.g., Brannen et al. 2020), suppressing the pace of democratic innovative advancement (Wu and Pang 2021). Ironically, there are current indications that large corporate technology players (here, Big Tech) are using fear and regulation to achieve their corporate domination goals. This battle is a complex one that is dividing industries and sectors alike (see e.g. Taylor 2021). What is at stake is not the pure aspect of healthy competition and, indeed, advancement of technological prowess but rather the security of nations internationally. The matter of national security itself is one of safety, autonomy, and ethics (Mowery, 2009; Weiss, 2014).

Research suggests that blind trust in technological advancement and implementation are inadequate options for the governance of the information society (Saariluoma, Karvonen, and Rousi 2019). Discussions and artificial-intelligence-related initiatives on the governance of emerging machine learning (ML), deep learning (DL), and related autonomous cognitive technologies are necessary not only from a societal order perspective (Sætra and Fosch-Villaronga 2021; T. Wu 2019) but also in relation to several aspects of ethical artificial intelligence (AI) – *human oversight*, *transparency*, *explainability*, and prevention of black-box scenarios (Jobin, Ienca, and Vayena 2019; Vakkuri et al. 2020). Nevertheless, due to the tensions brewing below the surface of the administrative level that pertain to economics and corporate competition, getting to the heart of who, how, and what should be regulated remains a silent part of the discussion. Individuals and small organizations dealing directly with personal data (researchers and research organizations included) are affected by policies such as the General Data Privacy Regulation (GDPR), according to which individuals and organizations must protect and promote advocacy of personal data through every stage of data handling from collection to storage. The GDPR is one of the most all-encompassing data protection laws ever enacted and has significantly contributed to increasing privacy awareness and directing data handling practices (Geradin, Karanikioti, and Katsifis 2021).

The *enemy within* is a manifestation of corporate versus national interests, seeing official governance posed with a conflict of interest between national and citizen safety, and the ownership networks that supply this 'safety'. The tension between private ownership of components of critical information communication technology (ICT) infrastructure, governance and regulation over the technology, and the worldwide information war that is rapidly unfolding (Siroli 2018; Smith 2006; Walker 2000) raises numerous considerations that must be addressed. On the basic level, companies, similar to nations from a techno-economic and cultural perspective (historical heroism, national rhetoric and propaganda), have to varying degrees frontier-style agendas for domination, and recognition. The technological landscape is characterized by a network of unruly information systems whose governance can be likened to providing a smoke screen for unethical corporate behaviour. This enemy within, or in other terms 'the Beast Inside' (Platform Revolution 2023), refers additionally to the socio-technical paradox of Big Tech's campaign for technology regulation while a) its systems often bypass this regulation through pervasive (multi-source) data collection and practices (Geradin, Karanikioti, and Katsifis 2021; Zarsky 2017), and the force of popularity coupled with economically-determined social-peer pressure mean that users are prepared to offer data no matter what the cost (i.e., the privacy paradox, (see e.g. Kokolakis 2017); and b) the fact that Big Tech's technology is used at the core of many critical infrastructures (Hendricks 2022). Currently, and increasingly in the current phases of AI deployment across societal sectors, information communication technology (ICT) infrastructure is critical for all the other critical infrastructure sectors (see Figure 1).

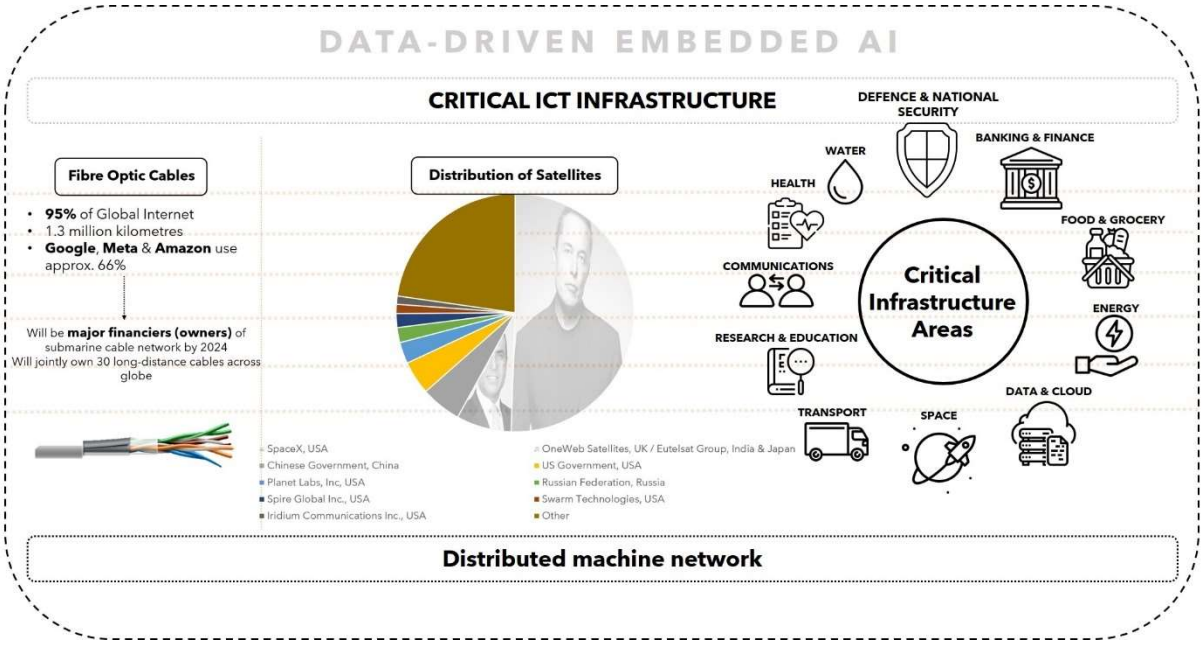

Figure 1 – Landscape of AI-embedded systems from a critical infrastructure & ownership perspective

The issues of governance (policy and regulation), AI-system development, and *Big Tech* are entangled in a complex assemblage of ethical considerations and security concerns that demand attention and strategic consideration. In this chapter, the authors explain and illustrate the nature of the beast of AI governance and regulation and their impact on innovation and national security. The chapter begins with a brief conceptual analysis of governance, AI governance, and ethics (Attard-Frost, Brandusescu, and Lyons 2023; Jobin, Ienca, and Vayena 2019). There follows an overview of national security and then considerations of the relationship between innovation and national security. The discussion highlights the tensions between governance, Big Tech (its connection to governance and presence within critical infrastructure), and the shortcomings of current European policy that is weakening innovation advancements among small to medium-sized enterprises. We approach this highly sensitive topic as a call to action towards delicate balancing act between competing economic and political interests in the context of a techno-economic superstructure that is no longer defined by nations per se – even in matters pertaining to national security.

Governance, AI systems, and Ethics

Challenged by grand societal challenges, wicked problems, accelerating globalization, and increasing uncertainty, many countries are searching for a new form of governance that is better adapted to the times to gain an advantage in economic competitiveness and create substantial and sustainable social growth. The English word *governance* derives from Latin (*gubernare*) and ancient Greek (*kubernaein*), the original meaning being to steer, control, guide, and manipulate (Mohan, 2023). The word *governance* has long overlapped with the word *government*, mainly used to refer to administrative and political activities related to national public affairs (Keping 2018). Governance is a term that is used widely but not always precisely. The term governance is typically used in several contexts, such as corporate governance, international governance, national governance, and local governance. James Rosenau (1999) deems all types of governance as "mechanisms for steering social systems toward their goals" (cited in Weiss 2000, 801). Francis Fukuyama (2013) defines governance as the "government's ability to make and enforce rules, and to deliver services, regardless of whether that government is democratic or not" (p. 3).

Currently, the data policies of technology giants dominate the handling of private users' data. As consumers are increasingly adopting data-driven digital technologies, the data they generate, such as

location-tracking and other personally identifiable information, can create opportunities for companies to enhance consumer engagement. Once processed and classified, the data provide relevant information for companies on consumers' interests and activities, which is extremely useful for advertising (Esteve 2017). Users' personal data have certain commercial value to the companies, as they may use data to better understand unmet customer needs. Insights into consumer data help companies develop new products and services and personalize advertising and marketing (Anant et al. 2020).

As governance and regulation are mainly top-down processes, where the policymakers and governing bodies make and implement new rules and legislation, the role of private citizens, users, and particularly small organizations and enterprises is very much to obey and adapt to new regulations, such as GDPR (Watt 2021). In this context, the choices of private users are very limited - they are required to accept the new rules (terms and conditions) set by the service providers if they want to continue using the services. In the current debate around data protection and fair use of private users' data, bottom-up perspectives and the inclusion of different user groups as the voice of end users of digital services are widely neglected topics (Kalliomäki et al. 2022). It should also be noted that the relationship between technology providers (Big Tech companies) and governance is complex. Commercial providers must both follow regulations established to implement governance; however, technology providers are also setting their own rules for users to permit them to benefit financially from the data provided by the users (Breen, Ouazzane, and Patel 2020; Tosza 2021; West 2005).

Governance from user to policy

Private citizens and the users of digital services face dilemmas related to the sharing of personal data (see Figure 2). Internet-based services require users share their personal data and give the service providers permission to use that data. Users being forced to accept the rules set by companies encourages this form of corporate behaviour (Zuiderveen Borgesius et al. 2017; Margulies 2021). That tacit approval enables companies, particularly Big Tech, to use the data for commercial purposes, while users are often unclear about how their personal data is used (Anant et al. 2020). Users also voluntarily and carelessly share their personal data and other content, such as images and videos, on social media platforms. However, it may be quite unclear to the users how the data is actually used by the service providers, for which ML and AI provide new tools to make even more commercial value from the users' personal data than before.

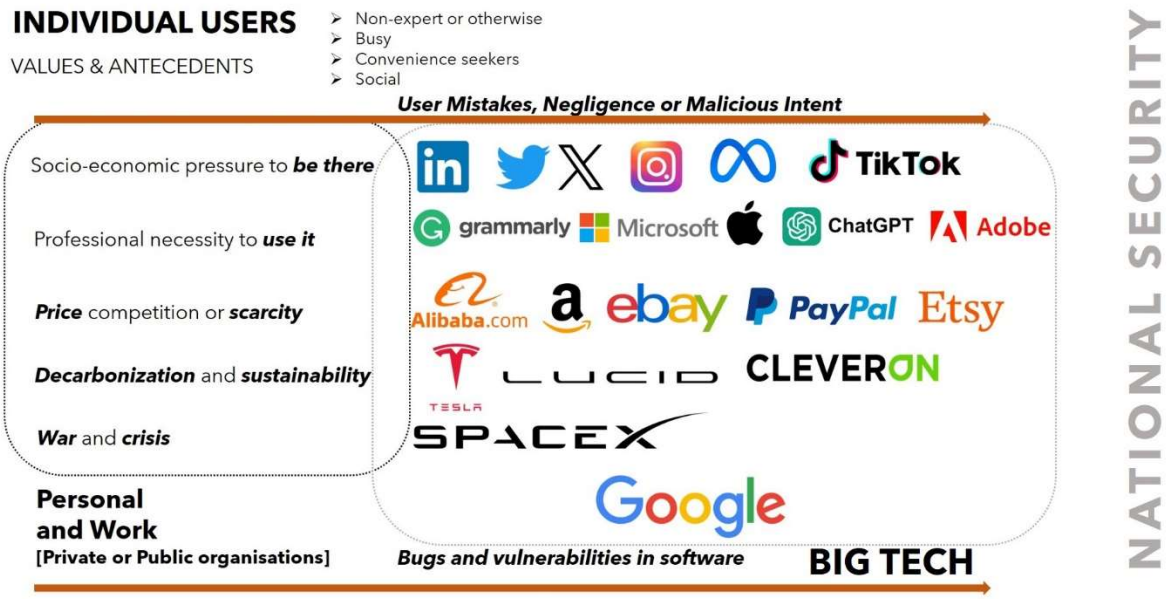

Figure 2: The relationship between individual users and national security via Big Tech

The positive implications of GDPR are overshadowed by several factors that both impinge on fair corporate competition (between company sizes and types) and harm innovation ecosystems. Furthermore, for all the control that GDPR places on screen-based and mobile applications, the pervasiveness of other data-gathering systems, including the Internet of Things, means that significant quantities of personal data are collected without the subject's knowledge (Costin 2016; Wood 2016). These issues are coupled with the internal user conflict of a desire for a seamless user experience without interruption via cookie privacy statements, the fear of missing out (FOMO), and regular self-disclosure on social media *to be seen and represented* (see e.g. Nabity-Grover et al. 2020). The fact that numerous points of human-technology interaction, data collection, and handling not only occur without individual agency over personal data but are forced upon individuals as conditions of service (voluntary and involuntary alike) by Big Tech and public sectors means that this is no equal playing field (Karaboga et al. 2017). These are not only intrusions into individual privacy but constitute national security concerns (Zajko 2018).

When discussing regulation, security, safety, and ethics, scholars and experts encounter three core problems: 1) the field of internet-connected and enabled technology is already too complex and complicated to govern in a genuine sense. The internet was not originally developed with security and governance in mind; quite the reverse, creative freedom, democracy of knowledge, and information sharing were its ideological bases (Oppliger 1997); 2) a corporate agenda not only conflicts with established and emerging policies, laws, and standards designed to regulate the field, but adherence to these places Big Tech in a position of advantage due to their size and social popularity (see e.g. Moore and Tambini 2021); and 3) the pull of the imagination – AI and other forms of autonomous technology have long been in the collective consciousness via popular culture (Cave and Dihal 2019), fear is easily incited among people, and is likely to drive support for *hasty* decisions, tight regulation, and immature policy strategies (Liwång 2022).

Traditionally, a bureaucratic and political governmental approach has been mainstream practice for governance in Europe (Pagallo, Ciani Sciolla, and Durante 2022). Governance has been applied via a means–end rationality, legal rules, and the exploitation of scale economies (Ansell, Sørensen, and Torfing 2021). However, during the past few decades, there has been growing criticism regarding the inability of public bureaucracy to solve complex or wicked societal problems that are often characterized by unclear problem definitions, complex causalities, conflicting goals, and a lack of standard solutions (Peters 2017). Consequently, a number of scholars have argued that the best approach to solving complex problems is through multi-actor collaboration in networks and partnerships that help mobilize valuable resources, spur innovation, and build common ownership over joint solutions (Ansell, Sørensen, and Torfing 2021; Kunttu and Neuvo 2019; Torfing 2019; Wegrich 2019).

As the process of governance is related to decision-making and the implementation of the decisions, the analysis of governance should cover the formal and informal actors involved in these processes (Starke and Lünich 2020). Adaptive governance refers to the ability to deal with complex societal issues involving many stakeholders, diverging interests, and uncertainty about the actions to be taken, such as in climate-change-induced community relocations (Bronen and Chapin 2013). Evidence-informed governance ensures that decisions are made based on the best available information, analyses, and assessments through governance structures that absorb, adapt, and respond to new evidence (Janssen and van der Voort 2020). Anticipatory governance requires an evidence-informed approach and, at the same time, emphasizes a whole-society perspective with an inclusive approach. Inclusive governance aims to provide equal opportunities for different members of society to benefit from and participate in innovation (Kunttu et al. 2021). When governance is inclusive, it should effectively serve and engage everyone and consider gender and other facets of personal identity. Inclusiveness also requires that the institutions, policies, processes, and services be accessible, accountable, and responsive to all members of society (OECD 2014). An important principle in the anticipatory governance approach is to learn from past experiences and feedback, which makes it possible to use them in real-time decision-making. Being able to do so is particularly important in a societal context where the problems are complex and the speed of change rapid (Ansell, Sørensen, and Torfing 2021). Governance is implemented on micro, meso, and macro levels, from smaller projects and organizations via structured processes, rules, and

protocol (Hall, Link, and Scott 2001; Klijn et al. 2013) to regional scale governance comprising departments and offices. The scenario encompasses laws and regulations (Spanhove and Verhoest 2007) and national administration as a whole, as well as governing rules, regulations, and legislation.

Ethical principles and governance

Ethical principles play a central role in effective governance (e.g. Congleton 2020). From an ethical perspective, management rules, practices, and processes are driven by moral principles. Ethics promotes greater responsibility in transactions between citizens and administration. It helps to foster confidence in interactions in such a way that citizens can be convinced that the administration is working in favour of the public interest (Fejzullahu and Batalli 2019). For this reason, every action in *good governance* (Weiss 2000) must be taken in accordance with ethical rules and principles. As with governance, ethics play a central role in business. Since corporations and their leaders exercise great power in our society, ethical viewpoints consider corporate behaviour should be governed by a more demanding set of standards than those that apply to private individuals. Then business ethics refers to the standards for morally right and wrong conduct in business. Law partially defines this, but legal and ethical are not always the same. Business ethics may refer to contemporary organizational norms, values, or principles that govern individuals' behaviour in business organizations. Accordingly, business ethics extends the law by outlining acceptable behaviours beyond government control.

The notion of ICT governance refers to how ICT decision-making responsibilities and rights are distributed between various stakeholders and their accompanying procedures and rules (Peterson 2004). This form of technological governance mainly applies to the corporate sector, attempting to isolate the levels and components of responsibility and intervention needed to maintain an optimal direction in technological development, implementation, and performance (Ferguson et al. 2013). An increasingly popular form of governance, and one that is fast becoming one of the most valid in light of the technological landscape, is AI governance. Governance models for AI span the components of accountability and responsibility to concepts that are both challenging to define and highly complicated to decipher in emerging ML-based systems (Rousi 2022). Numerous efforts have been made to establish AI governance models and frameworks, one such being Jean-Francois Gagné's (2018) *Framework of AI Governance*. In that model, a scale of autonomy is represented across a spectrum ranging from IT that is directly human-controlled, coached, or driven to fully autonomous technology. The dimensions of governance comprise 1) performance – completeness, accuracy, and bias; 2) security – adversarial robustness and adaptability; 3) privacy – IP data capture and affected users; as well as 4) transparency – intent and explainability.

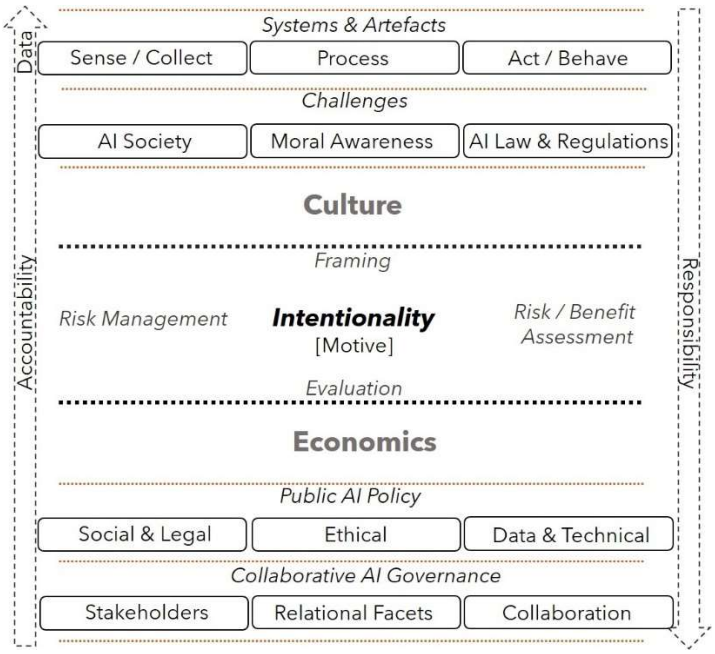

Figure 3: Layered AI governance model (adapted from Rousi, 2022)

Other noteworthy data-driven technology governance models include the *layered model for AI governance* (Gasser and Almeida 2017) that divides the technology across the fabric of technical (data governance, algorithm accountability, and standards) and societal layers (social and legislative – norms and regulation). In this model, consideration is given to the temporal-spatial dimension that impacts all layers. The *ethical responsibility model for robot governance* (Rousi 2022) builds on the layered model and incorporates *trust* as the cornerstone of ethical AI-driven systems (see Figure 3). The model draws on two frameworks: 1) an applied framework represented by Hubert Laferrière (n.d.), who operationalizes trust as the result of compliant, effective, and principled system design, and 2) an integrated AI governance framework for public administration that accounts for the dark sides of AI (Wirtz, Weyerer, and Sturm 2020). Laferrière stresses that policymakers seeking to develop and maintain effective governance in social-technological systems of systems must adopt an acute cybernetic (human and technology) approach to ensuring the compliance of privacy, security, transparency, explainability, fairness, human oversight (human-based control), and training model performance. This training model performance links to other elements in the framework and is especially enhanced by data literacy to ensure issues such as bias and discrimination are not inherent within the systems (Agbese et al. 2021; Vainio-Pekka et al. 2023).

The intersection between governance and security, however, can be seen to rest in the heart of intentionality (Rousi 2022) – the motives, goals, and intentions behind behaviour and decision-making. This conceptualization assumes a consciousness spanning both short- and long-term objectives. This intentionality can be exhibited through political decision-making and national or international level policies and regulations (Starke and Lünich 2020) that are designed with the interests of citizens in mind. It may also manifest on a deeper level of *personal interest* with strong economic implications and incentives. Here, it is important to dissect the concept of national security.

National security

The term national security conjures many ideas and thoughts about military, private state-run operations, and warfare (Wolfers 1952). Unfortunately, in a global society run by humans with varying interests, values, aims and objectives, national territory, patriotism, and politics can be likened to a team sport and, at their worst, a personality battle between dictators and superpowers (see, e.g. Mann 2023). Accordingly, state-run and national-level operations are as much about political ideals, rhetoric, and influence as they are about keeping citizens safe (Leffler 1990). In the context of the United States, national security has been described as “an ambiguous symbol” (Leffler 1990, 144). The term *security* encompasses numerous goals, rendering it difficult to offer a concise definition (Wolfers 1952). National security alludes to more than the mere survival of a nation. Analyses of the concept, such as those offered by Barry Buzan (2011), posit that scholarly realists concentrate on the factor of power within national security, while idealists emphasize peace.

There is also a tendency to raise ethical, moral, and legal aspects as priorities dwarfing the core aspects of security itself (Leffler 1990). David A. Baldwin described the cottage industry of redefining the concept of security in which emphasis has been placed on re-framing policy agendas of nation-states rather than scrutinizing and capturing the basic components of what security entails in and of itself (Baldwin 1997). Accordingly, redefinition has seen the proposals of agenda that, for instance, promote human rights, sustainability, health, social justice, economics, and crime (including cybercrime). There is also consideration given to military threats. Yet, what Baldwin critiques is the normative assumptions of which values should be protected and promoted on behalf of certain communities in populations. Security mingles with value-based and ideological levels, with highly practical consequences (Martill 2022). Other points of focus linger on the extension of geopolitical territories and mixing into corporate interests (Verstein 2017).

This current chapter focuses on corporate aspects that transcend national boundaries while simultaneously threatening them (Lutterbeck 2005; Reveron and Savage 2020). We seek to highlight

the conflict between concern for national security in a globally connected AI landscape with embedded core values (Leffler 1990) of corporate logic and technological development. This desire to highlight holds equally for the interwoven relationship between AI ethics and national security. While focusing on the obvious in terms of, e.g., algorithmic bias, the threats of job displacement, copyright, and data privacy (Agbese et al. 2021), matters of corporate ownership and its link to black box algorithms (lacking transparency and explainability) remain overlooked (Yu and Carroll 2021).

In *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, Franklin D. Kramer (2009) stated that the cyber world is not secure. Kramer (2009) highlights that every level of cyber, or cyberspace (human, technical and informational elements of the internet-connected digital domain), is prone to security vulnerabilities. These vulnerabilities leave cyber susceptible to what was termed *breakdown* in various ways, both intentional and unintentional. The numerous layers of cyber comprise software, hardware, information, and human factors, and any are subject to breakdown, via accident, leak, infiltration, or organized attack (Humayun et al. 2020). The baseline of these systems involves the techno-corporate infrastructure and systems of systems involved in this (Clarke and Knake 2019). Observing the situation from a national societal level reveals that all areas of public administration are now reliant on cyber-based information systems. Critical infrastructures are at the mercy of vulnerabilities that threaten all types of information assets (White House 2003). In addition to the systematic organized attacks, there are always challenges that arise from weaknesses in the technology itself.

This observation carries over into 2023 and perhaps becomes more pronounced as we enter into the era of *data warfare*. Data warfare can be described as being more about *people* than territories (Berman, Felter, and Shapiro 2018). In particular, civilians are in focus as they are the main sources of critical information. Another juncture for this transformative form of warfare is market gravity and socio-technical behaviour. A recent example of the oscillation between the individual and collective can be seen in the case of the data-driven assistive writing (a form of AI) software Grammarly. Grammarly was introduced to the market in 2009 by Alex Shevchenko, Max Lytvyn, and Dmytro Lider (Venture Beat 2018). The software was created by the developers of My Dropbox and was intended to aid in improving English language skills. Due to its capabilities in polishing text, the software boomed in popularity (Tameem, 2020) and was quickly adopted by individuals and institutions alike. Over 1400 universities alone had purchased Grammarly licences as of June 2023 (Essential Grammarly Statistics 2023). However, as early as 2018, Grammarly's beta version browser extension was discovered to expose authentication tokens to websites (Tavis 2018). Consequently, websites had direct access to users' data, including documents (Ormandy, 2018). Grammarly adopted a hotfix approach to rectifying the problem with the help of white hat hackers (ethical security hackers) (Okpa et al. 2022; see e.g. Sinha and Arora 2020) to find vulnerabilities. Grammarly is again on the banned technology list of organizations and national states in 2023 (State of Nevada, 2023). The add-in and browser extensions of the software are not recommended for use with the Microsoft network because they open access to information rights management protected content in documents and emails – a problem already detected in 2018 (Warren 2019).

Seemingly, individual-focused security threats are one concern. Nevertheless, the repercussions of targeting individual users or groups of users are another. Direct implications of data breaches can be identity theft, financial loss, reputational damage, operational downtime, loss of sensitive data, and legal action (MacKay 2023). Specifically, each individual user and their numerous documents, user accounts, platforms, access to administrative and enterprise software, etcetera, can be seen as gateways to organizations – businesses, institutions, and even governmental departments themselves. It only takes one person to compromise an entire network, either due to accidentally utilizing vulnerable software such as Grammarly, via creating weak credentials (Kaspersky 2023), or through unethical and/or malicious intent as seen in the case of Alibaba in 2019 (tied with Aadhaar in 2018, see (Hill and Swinhoe 2022)) where 2.2 billion users' personal information including names, addresses and biometric data were scraped and sold. From the micro (individual) through to the macro (nation-state), the risk sequences of security and the compounded vulnerabilities posed by data-driven (AI) systems leave software like Grammarly on banned technology lists. Others include Alibaba, Tencent Holdings,

TikTok, and Huawei Technologies – all either linked to China by ownership or otherwise tied to the Chinese authoritarian government (see 2News 2023). Interestingly, Grammarly, founded in Ukraine, does not have direct public links to either China or Russia. A recent report of Grammarly's security ranks it at 888 out of 950 (an acceptable rating), with issues of HTTP Strict Transport Security (HSTS) not being enforced (vulnerabilities to man-in-the-middle attacks), HttpOnly cookies not used (client-side attack vulnerabilities), no use of secure cookies (possibilities for third-party interception of information), among others (Upguard, 2023).

Given the expansiveness of information systems and the integration of AI throughout all sectors of society, it is increasingly vital to engage in what Kramer (2009) terms *the cyberpower of support for national security* and, even more so, to apply a detailed theoretical (cyber power theory) approach to understanding critical elements in international security. All critical infrastructure is dependent on cyber information systems. Increasing complexity, as in the inevitable case of AI-driven technology, heightens the likelihood of vulnerabilities from countless perspectives.

Fearmongering and doomsday thinking of artificial general intelligence (AGI, the uncontrollable AI), from a technical and AI practitioner perspective, are based on very little tangible premise (Bieger, Thórisson, and Wang 2015; Goertzel 2014). Instead, from a security and governance perspective, the malicious implementation of AI solutions such as large language models (LLMs) by bad actors to be used in contexts such as amplifying disinformation is a more realistic concern (Baum et al. 2023). Further, the actual impacts of advanced AI such as LLMs are not to be found in the fictional doomsday scenarios of rampart AGI but in the widespread societal impacts of a general technology (Eloundou et al. 2023). The idea of creating regulations that would blanket-ban certain types of technologies or force the reporting of certain computational-based metrics (as in Executive Order, (White House 2023) might sound like a reasonable way to control the development of AI, there is a lack of empirical and impact-driven justification of the problems that these are supposed to answer.

The chicken and egg of innovation and national security

When the GDPR was officially implemented in 2018, shockwaves were felt by small to medium businesses, as well as other organizations. Big Tech companies such as Google and Facebook were among those who campaigned for GDPR. While in the short-term, it was predicted that Big Tech players such as Google and Facebook (Meta) would find it easier to gain consent to earn revenue from personal information than smaller businesses, it was seen that as time goes by, there would be a backlash by the European Union (Proud 2018). In 2023, the predicted scenario is still yet to prove itself. However, the reality that did emerge during GDPR's early days was that of the 'spooking effect' that the regulation and its sanctions would have on small to medium businesses. The sanctions are so stringent that detection by national regulators of GDPR breaches could mean either a fine higher than EUR 20 million or four per cent of the business's annual global turnover (ibid.).

From a practical perspective, GDPR means the obligatory appointment of a data protection officer – meaning resources spent on hiring an extra employee for the position or using the time resources of existing employees for data protection-related duties (ibid.). AdTech (advertising technology, e.g., ad trackers, targeted advertising) in particular dropped significantly in value, losing 18–31% of the market share as ad trackers decreased in usage post-GDPR introduction (Lomas 2018). In contrast, the market value of Google slightly increased by just under 1%. Google, Amazon, Facebook, and Apple were seen as too big to be affected by regulation (Yueh 2018). Google is a search engine. Its logic is to collect and match data, and in the era of AI, Google is in the best position to develop AI as its core business deals with the *mind game* – knowledge retrieval and sharing. Nevertheless, similarly to the mantra of Ng (2023) in his critique of the fear stirred by Big Tech towards the development of AI, Google is said to be taking a cautious route to AI development (see, e.g. Aten 2023).

Regarding contemporary discourse on the relationship between national security and governance in the forms of policymaking and regulation, there is much discussed in online media about the challenges in regulating fields of technology. While many highlight the risks taken when allowing Big Tech to occupy

central provider roles in infrastructure (see, e.g. Hendricks 2022), a lack of affordance towards smaller companies (start-ups through to medium-sized enterprises) to freely engage in development means: a) decreased agile innovation that can strengthen national security on the international front; and b) less technological democracy that would spread *control* of the cyber systems among many.

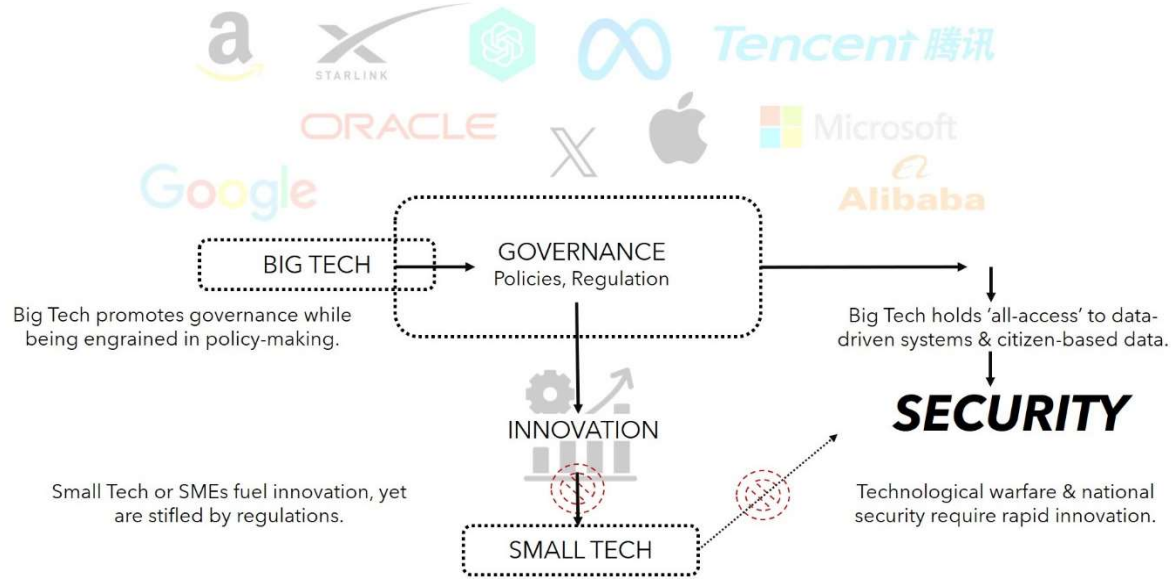

Figure 4: Maximized innovation potential equals increased likelihood for cutting-edge national security. Restricting small to medium-sized business innovation capacity via fear of penalty or increasing resources placed on data handling compliance weakens capability in national AI advancement overall.

World Bank data demonstrates that GDPR has damaged European economic growth, showing that China (2.25%) had outpaced Europe by far (Germany 0.4% and France 0.3%) by the year 2021 (Lewis 2022). It is imperative for both economic and military strength that entrepreneurship and innovation processes are reasonably free from tight regulation (see Figure 4). That is, innovators should be given opportunities in which experimentation, research (data-driven), and development occur without fear of being penalized. Furthermore, small tech players with more agile structures for innovation are often bought by Big Tech once significant breakthroughs are made (Affeldt and Kesler 2021; Manne, Bowman, and Auer 2021).

Breaking up the Big Ones?

There are arguments for disrupting current trends in the exponential growth of Big Tech to force major players into breaking the corporations up into small companies (Lewis 2022), as seen in the break up of the Bell System that led to mass innovation in 1982. This type of phenomenon was seen in Finland with the downfall of Nokia, whereby thousands of former Nokia employees either founded their own technological start-ups or went to work at other companies. There was a distribution of innovation, and perhaps in many senses, an enabling of innovation that would not have been possible in the former large company. The City of Oulu has reaped the benefits of start-ups originated by ex-Nokia employees (see e.g. Belton 2015). Supercell (revenue 2022, 1.6 billion euros – now owned by Tencent China), Gofore (revenue 2022, 78 million euros), drawElements (now owned by Google), Pryte (merged into Meta Platforms), Jolla and Sailfish are just some companies that sprouted from the demise of Nokia. Nevertheless, Nokia was already falling. Its bureaucracy was too rigid and pervasive, perhaps similar to the logic behind strict AI regulation. Moreover, Nokia was slow to recognize opportunities and the importance of culture around products, as Apple had done with its lifestyle branding. Finally, the internal competitive culture of Nokia was said to be toxic and self-destructive. Both of these former reasons could be attributed to overly constrictive and regulatory administration (Cannon 2022).

Transferring the Nokia experience to national security, David C. Mowery (2009) argues for the application of the national systems of innovation (NSI) framework to analyse policy and performance in light of defence-related research and development investment and its subsequent innovation. That NSI framework is particularly useful in terms of its isolation of the factors that encourage innovation and the relationship between organizations or institutions (including culture), learning, and evolutionary processes (Borrás and Edquist 2013; Edquist 2006). The chicken and the egg of the relationship between Big Tech and national security is that throughout history, once discoveries have been made in publicly funded science, entrepreneurs have taken the seed discoveries to the next level. For instance, the world wide web had its beginnings at the European nuclear physics research facility, CERN, yet was transformed into a network of networks by American entrepreneurs (Mowery, 2009). Without governmental (European) financial backing, combined with entrepreneurial freedom, the 'new electricity' of the twenty-first century, the web – and its subsequent enabling of AI – could not have developed in the way that it has (Jewell 2019).

There is a to recognise the limiting effects of regulation on innovation, and as a result, the vulnerabilities placed on national security when innovation does not advance at the rate of international rivals (Lewis 2022). Ironically, when observing nations such as China, this does not mean that there is an absence of regulation or, indeed, AI ethics. The Chinese government is taking strides in AI governance, leading to consequences for national security and the global development of AI alike (Sheehan 2022; Zhu 2022). Separate branches of the Chinese administration exhibit three approaches to AI governance that guide opinions on strengthening ethical governance of science and ethical norms for new generation AI: 1) rules for online algorithms – focus, public opinion (Cyberspace Administration of China (CAC)); 2) tools for testing and certification of trustworthy AI systems including trustworthy facial recognition applications and protections plan (China Academy of Information Communications Technology); and, 3) establishing AI ethics principles and creative tech ethics review board within companies and research institutions (Ministry of Science and Technology). The CAC is by far the strongest and most mature regulator in China and has published a three-year roadmap to govern all algorithms on the internet. Accordingly, if successful, Chinese initiatives on AI governance could affect AI governance in all nations. Given the market strength of Chinese Big Tech (Alibaba, Tencent, Huawei, ByteDance – the owner of TikTok, etc.) and the fluidity of multinational ownership, there is a possibility that the Chinese government will be involved in critical infrastructure globally[1].

Discussion and Conclusions - *From ethical considerations to wicked problems*

In this chapter, we have considered a complex technological landscape riddled with contradictory goals, needs, and targets of governance, technology companies, and citizens. Governance (incorporating both policymaking and regulation), technological development (implicated in the advancement of ML and AI systems), and Big Tech each have their own preferences regarding how data-driven digital transformation unfolds. Of particular interest here has been the nature of Big Tech's relationship with regulation and critical ICT infrastructure from an innovation-propelled national security perspective. A key concern is the rate at which AI-based methodologies advance and in which context. Where the corporate slogan is "move fast and break things" (Taplin 2017), an alternative slogan for national security might be "move faster, before others break *our* things." While cutting innovation capacity due to tight regulations that either a) require extra resources for already struggling smaller businesses or b) scare smaller organizations away from engaging in high-risk, high-gain research, one might say that nations or unions of nations are leaving themselves exposed to the elements.

There are clear conflicts of interest between what is planned and implemented on the policy level and what is happening in practice within the technological systems themselves are dominated by the financial interests of Big Tech. Rapid technological development enables new methodologies for using data collected everywhere, including from private citizens' everyday lives. Those data will continue to grow in importance until they resemble the *oil of the twenty-first century* until ML is so advanced that

[1] Incidentally, the official mobile devices of Danish and Canadian governmental workers cannot have TikTok installed (2News, 2023).

original input is no longer needed. The situation can be seen emerging in synthetic data generation (see, e.g. Kishore et al. 2021). The implementation of governance maintains certain interests towards data and system integrity from the viewpoint of national security. The 'enemy within' or 'the beast inside' (Platform Revolution 2023) refers to Big Tech's interest in taking over governance and competition. There is a motive and intention on the part of Big Tech to utilize data regulation to serve its own financial interests. That is most likely to happen through crippling smaller competition unable to afford either regulatory implementation or penalties while sneaking in the backdoor with socio-technical systems that many cannot refuse (social media, even public administration software, and platforms). Via data, this backdoor opens up critical infrastructure to more external (international) threats.

Accordingly, these dynamics lead to slower security development and regulation that is able to expand the grey areas in data private users' data security (Mowery 2009). This kind of development may also cause data security vulnerabilities due to the lack of transparency in data regulation (Heiman 2020). Whereas AI governance and regulation have an impact on innovation, private users' data protection, and national security, they also call for ethical considerations and security concerns that require attention and consideration in terms of which organizations, who, and for what reasons they have access to critical infrastructure. Consideration of these factors cannot only involve applying a top-down (policy and administration-led) approach to governance but must include a bottom-up approach starting with individual users. The latter aspect would help ascertain how stakeholders and societal groups enhance and impact national security via participation in AI-driven socio-technical systems. Moreover, once arriving back at the top again, there is a need to move inwards towards the economic superstructures that sustain critical (ICT) infrastructure, thus underlining the continuous interaction between micro and macro levels in the societal context.

If AI governance is to be taken seriously in Europe, policymakers must pay careful attention to the actions of external neighbours. The Chinese AI Ethics policies (Zhu 2022) are not only initiatives to ensure harmonious human-AI symbiosis but are mechanisms for establishing an ethic that sees citizens embrace the systems via a perceived "*fairness"*. Meanwhile, technological AI advancement is at the helm of often quite ruthless corporate competition and under-the-table development behaviour that leads to radical innovations (Hartmann and Henkel 2020; Lundvall and Rikap 2022). In China, this form of corporate competition feeds governmental efforts as tight relations are maintained between business and government, including recruitment of ex-industry professionals. In Europe, there is often a substantial distance between policymaking and expert technical knowledge (Lowes and Woodman 2020; Sharon 2021). Our advice for policymakers is to provide small to medium-sized businesses with a safe space to innovate and to encourage curiosity through educational efforts addressing *white hat hacking* and other ethically driven explorations of the technology being developed. Then, finally, build strong relationships with and employ fresh industrial experts and less institutionalized radicals to continuously test, stress, and exceed the system boundaries. This way, our nations' capacity to protect critical infrastructure will not be limited to the regulations in place.

References

2News. 2023. "TikTok, Other Apps Blacklisted From Nevada Government Devices." https://www.2news.com/news/tiktok-other-apps-blacklisted-from-nevada-government-devices/article_c107814c-cf28-11ed-903e-1fff34062371.html.

Affeldt, Pauline, and Reinhald Kesler. 2021. "Big Tech Acquisitions—towards Empirical Evidence." *Journal of European Competition Law & Practice* 12(6): 471–78.

Agbese, Mamia et al. 2021. "Governance of Ethical and Trustworthy Al Systems: Research Gaps in the ECCOLA Method." In *2021 IEEE 29th International Requirements Engineering Conference Workshops (REW)*,, 224–29.

Anant, Venky, Lisa Donchak, James Kaplan, and Henning Soller. 2020. *The Consumer-Data*

Opportunity and the Privacy Imperative. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative#/.

Ansell, Christopher, Eva Sørensen, and Jacob Torfing. 2021. "The COVID-19 Pandemic as a Game Changer for Public Administration and Leadership? The Need for Robust Governance Responses to Turbulent Problems." *Public Management Review* 23(7): 949–60. https://doi.org/10.1080/14719037.2020.1820272.

Aten, Jason. 2023. "The 2 Words Google's CEO Keeps Repeating About AI Are an Insightful Lesson for Every Leader." *Inc,*. https://www.inc.com/jason-aten/the-2-words-googles-ceo-keeps-repeating-about-ai-are-an-insightful-lesson-for-every-leader.html (November 28, 2023).

Attard-Frost, Blair, Ana Brandusescu, and Kelly Lyons. 2023. "The Governance of Artificial Intelligence in Canada: Findings and Opportunities from a Review of 84 AI Governance Initiatives." *SSRN Electronic Journal*.

Baldwin, David A. 1997. "The Concept of Security." *Review of International Studies* 23(1): 5–26. http://www.jstor.org/stable/20097464.

Baum, Kevin et al. 2023. "From Fear to Action: AI Governance and Opportunities for All." *Frontiers in Computer Science* 5. https://www.frontiersin.org/articles/10.3389/fcomp.2023.1210421.

Belton, Padraig. 2015. "Finnish Phoenix: The Start-Ups Rising from Nokia's Ashes." *BBC News*. https://www.bbc.com/news/business-31044810.

Berman, Eli, Joseph H. Felter, and Jacob Shapiro. 2018. *Small Wars, Big Data: The Information Revolution in Modern Conflict*. Princeton University Press.

Bieger, Jordi, Kristinn R Thórisson, and Pei Wang. 2015. "Safe Baby AGI BT - Artificial General Intelligence." In eds. Jordi Bieger, Ben Goertzel, and Alexey Potapov. Cham: Springer International Publishing, 46–49.

Borrás, Susana, and Jakob Edler. 2020. "The Roles of the State in the Governance of Socio-Technical Systems' Transformation." *Research Policy* 49(5): 103971. https://doi.org/10.1016/j.respol.2020.103971.

Borrás, Susana, and Charles Edquist. 2013. "The Choice of Innovation Policy Instruments." *Technological Forecasting and Social Change* 80(8): 1513–22. http://dx.doi.org/10.1016/j.techfore.2013.03.002.

Brannen, Samuel J., Christian S. Haig, Katherine Schmidt, and K.H. Hicks. 2020. *Twin Pillars: Upholding National Security and National Innovation in Emerging Technologies Governance - Policy File*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200123_Brannen_TwinPillars_WEB_FINAL.pdf.

Breen, Stephen, Karim Ouazzane, and Preeti Patel. 2020. "GDPR: Is Your Consent Valid?" *Business Information Review* 37(1): 19–24. https://doi.org/10.1177/0266382120903254.

Bronen, Robin, and F Stuart 3rd Chapin. 2013. "Adaptive Governance and Institutional

Strategies for Climate-Induced Community Relocations in Alaska." *Proceedings of the National Academy of Sciences of the United States of America* 110(23): 9320–25.

Buzan, Barry. 2011. "The National Security Problem in International Relations." In *Security Studies*, Routledge, 18–23.

Cahir, Caitriona, and Kevin Thomas. 2010. "Asymmetric Effects of Positive and Negative Affect on Decision Making." *Psychological reports* 106(1): 193–204.

Cannon, James. 2022. *Toxic Cultures at Work: The Eight Drivers of a Toxic Culture and a Process for Change*. Taylor & Francis.

Cave, Stephen, and Kanta Dihal. 2019. "Hopes and Fears for Intelligent Machines in Fiction and Reality." *Nature Machine Intelligence* 1(2): 74–78. https://doi.org/10.1038/s42256-019-0020-9.

Clarke, Richard Allen, and Robert K. Knake. 2019. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press.

Congleton, Roger D. 2020. "Ethics and Good Governance." *Public Choice* 184(3): 379–98. https://doi.org/10.1007/s11127-020-00824-3.

Costin, Andrei. 2016. "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations." In *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, TrustED '16, New York, NY, USA: Association for Computing Machinery, 45–54. https://doi.org/10.1145/2995289.2995290.

Edquist, Charles. 2006. "Systems of Innovation: Perspectives and Challenges" eds. Jan Fagerberg and David C Mowery. *The Oxford Handbook of Innovation*: 0. https://doi.org/10.1093/oxfordhb/9780199286805.003.0007.

Ekman, Paul. 1999. "Basic Emotions." In *Handbook of Cognition and Emotion*, eds. T. Dalgleish and M.J. Power. John Wiley & Sons Ltd, 45–60.

Eloundou, Tyna, Sam Manning, Pamela Mishkin, and Daniel Rock. 2023. "Gpts Are Gpts: An Early Look at the Labor Market Impact Potential of Large Language Models." *arXiv preprint arXiv:2303.10130.*

"Essential Grammarly Statistics." 2023. https://zipdo.co/statistics/grammarly/.

Esteve, Asunción. 2017. "The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA." *International Data Privacy Law* 7(1): 36–47. https://doi.org/10.1093/idpl/ipw026.

Fejzullahu, Artan, and Mirlinda Batalli. 2019. "The Role of Ethics in Public Administration." *SEER: Journal for Labour and Social Affairs in Eastern Europe* 22(2): 267–78. https://www.jstor.org/stable/27096120.

Ferguson, Colin, Peter Green, Ravi Vaswani, and Gang (Henry) Wu. 2013. "Determinants of Effective Information Technology Governance." *International Journal of Auditing* 17(1): 75–99. https://doi.org/10.1111/j.1099-1123.2012.00458.x.

Fukuyama, Francis. 2013. “What Is Governance?” In *CGD Working Paper 314*, http://www.cgdev.org/content/publications/detail/1426906.

Gagné, Jean-Francoise. 2018. “Framework for AI Governance.” https://jfgagne.com/blog/framework-for-ai-governance/ (November 21, 2023).

Gasser, Urs, and Virgilio A F Almeida. 2017. “A Layered Model for AI Governance.” *IEEE Internet Computing* 21(6): 58–62.

Geradin, Damien, Theano Karanikioti, and Dimitrios Katsifis. 2021. 17 European Competition Journal *GDPR Myopia: How a Well-Intended Regulation Ended up Favouring Large Online Platforms - the Case of Ad Tech*. Taylor & Francis. https://doi.org/10.1080/17441056.2020.1848059.

Goertzel, Ted. 2014. “The Path to More General Artificial Intelligence.” *Journal of Experimental & Theoretical Artificial Intelligence* 26(3): 343–54. https://doi.org/10.1080/0952813X.2014.895106.

Hall, Bronwyn H., Albert N. Link, and John T. Scott. 2001. “Barriers Inhibiting Industry from Partnering with Universities: Evidence from the Advanced Technology Program.” *Journal of Technology Transfer* 26(1–2): 87–98.

Hartmann, Philipp, and Joachim Henkel. 2020. “The Rise of Corporate Science in AI: Data as a Strategic Resource.” *Academy of Management Discoveries* 6(3): 359–81. https://doi.org/10.5465/amd.2019.0043.

Heiman, Matthew R. A. 2020. “GDPR and the Consequences of Big Regulation.” *Pepperdine Law Review* 47(4): 945–54.

Hendricks, Vincent F. 2022. “Critical (Democratic) Infrastructure and BigTech.” *OECD Forum Network*. https://www.oecd-forum.org/posts/critical-democractic-infrastructure-and-bigtech (November 27, 2023).

Hill, Michael, and Dan Swinhoe. 2022. “The 15 Biggest Data Breaches of the 21st Century.” *CSO*. https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html.

House, White. 2003. *The National Strategy to Secure Cyberspace.* Washington DC.

———. 2023. “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.” https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

Humayun, Mamoona et al. 2020. “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.” *Arabian Journal for Science and Engineering* 45(4): 3171–89. https://doi.org/10.1007/s13369-019-04319-2.

Janssen, Marijn, and Haiko van der Voort. 2020. “Agile and Adaptive Governance in Crisis Response: Lessons from the COVID-19 Pandemic.” *International Journal of Information Management* 55: 102180. https://www.sciencedirect.com/science/article/pii/S0268401220309944.

Jewell, Catherine. 2019. “Artificial Intelligence: The New Electricity.” *WIPO Magazine*.

Jobin, Anna, Marcello Ienca, and Effy Vayena. 2019. “Artificial Intelligence: The Global Landscape of Ethics Guidelines.” *Nature Machine Intelligence* 1(9): 389–99. https://arxiv.org/pdf/1906.11668.

Kalliomäki, Helka, Johanna Kalliokoski, Leena Kunttu, and Jari Kuusisto. 2022. “Inclusive Innovation Policy - Lessons from EU-US Comparison.” *Business Finland Policy Brief No. 2/2022*.

Karaboga, Murat, Tobias Matzner, Hannah Obersteller, and Carsten Ochs. 2017. “Is There a Right to Offline Alternatives in a Digital World?” In *Data Protection and Privacy: (In)Visibilities and Infrastructures*, eds. Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth, and Paul De Hert. Cham: Springer International Publishing, 31–57. https://doi.org/10.1007/978-3-319-50796-5_2.

Kaspersky. 2023. “How Data Breaches Happen.” https://www.kaspersky.com/resource-center/definitions/data-breach (November 28, 2023).

Keping, Yu. 2018. “Governance and Good Governance: A New Framework for Political Analysis.” *Fudan Journal of the Humanities and Social Sciences* 11(1): 1–8.

Kishore, Aman et al. 2021. “Synthetic Data Generation Using Imitation Training.” In *2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW)*,, 3071–79.

Klijn, Erik-Hans et al. 2013. “Context in Governance Networks: Complex Interactions between Macro, Meso and Micro. A Theoretical Exploration and Some Empirical Evidence on the Impact of Context Factors in Taiwan, Spain and the Netherlands.” In Cheltenham, UK: Edward Elgar Publishing. https://www.elgaronline.com/view/edcoll/9781781955130/9781781955130.00027.xml.

Kokolakis, Spyros. 2017. “Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon.” *Computers & Security* 64: 122–34.

Kramer, Franklin J. 2009. *Cyberpower and National Security*. eds. Franklin D Kramer, Stuart H Starr, and Larry K Wentz. University of Nebraska Press. http://www.jstor.org/stable/j.ctt1djmhj1.

Kunttu, Leena, Helka Kalliomäki, Sorin Dan, and Jari Kuusisto. 2021. “Developing Social Impact Evaluation Methods.” *Technology Innovation Management Review* 11(5).

Kunttu, Leena, and Yrjö Neuvo. 2019. “Balancing Learning and Knowledge Protection in University-Industry Collaborations.” *Learning Organization* 26(2).

Laferrière, Hubert. 2020. “Artificial Intelligence Governance: An Operational Challenge 2020.” http://governmentanalytics.institute/magazine/december-2020/artificial-intelligence-governance-an-operational-challenge/.

Leffler, Melvyn P. 1990. “National Security.” *Journal of American History* 77(1): 143–52. https://doi.org/10.2307/2078646.

Lewis, James. A. 2022. “Tech Regulation Can Harm National Security.” *Center for Strategic and International Studies*. https://www.csis.org/analysis/tech-regulation-can-harm-national-security.

Liwång, Hans. 2022. “Defense Development: The Role of Co-Creation in Filling the Gap between Policymakers and Technology Development.” *Technology in Society* 68: 101913. https://www.sciencedirect.com/science/article/pii/S0160791X22000549.

Lomas, Natasha. 2018. “GDPR Has Cut Ad Trackers in Europe but Helped Google, Study Suggests.” *TechCrunch*. https://techcrunch.com/2018/10/09/gdpr-has-cut-ad-trackers-in-europe-but-helped-google-study-suggests/?guccounter=1

Lowes, Richard, and Bridget Woodman. 2020. “Disruptive and Uncertain: Policy Makers’ Perceptions on UK Heat Decarbonisation.” *Energy Policy* 142: 111494. https://www.sciencedirect.com/science/article/pii/S0301421520302408

Lundvall, Bengt-Åke, and Cecilia Rikap. 2022. “China’s Catching-up in Artificial Intelligence Seen as a Co-Evolution of Corporate and National Innovation Systems.” *Research Policy* 51(1): 104395. https://www.sciencedirect.com/science/article/pii/S0048733321001918

Lutterbeck, Derek. 2005. “Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe.” *European Security* 14(2): 231–53. https://doi.org/10.1080/09662830500336193

MacKay, James. 2023. “5 Damaging Consequences Of A Data Breach.” *MetaBlog*. https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach

Mann, Michael. 2023. “Wars, Rulers, Rationality.” *European Journal of Sociology / Archives Européennes de Sociologie* 64(1): 123–52. https://www.cambridge.org/core/article/wars-rulers-rationality/3DF7D3104945F0D724873CA26998B95D

Manne, G. A., S. Bowman, and D. Auer. 2021. “Technology Mergers and the Market for Corporate Control, 86 Mo. L. Rev. (2021) Available At:” *Missouri Law Review* 86. https://scholarship.law.missouri.edu/mlr/vol86/iss4/5

Margulies, Natalie. 2021. “"Please Respect Our Terms and Conditions”: A Causal Analysis of GDPR Impact on Privacy Policies.” Harvard College.

Martill, Benjamin. 2022. “Ideology and National Security.” In *The Routledge Handbook of Ideology and International Relations*, Routledge. https://www.routledgehandbooks.com/doi/10.4324/9781003026754-6

Mohan, Rajat. 2023. "Good Governance is Good Development". In *From Here to Denmark: The Importance of Institutions for Good Governance*. Oxford Academic. https://doi.org/10.1093/oso/9780198893103.003.0003.

Moore, Martin, and Damian Tambini. 2021. *Regulating Big Tech: Policy Responses to Digital Dominance*. Oxford University Press. https://doi.org/10.1093/oso/9780197616093.001.0001

Mowery, David C. 2009. “National Security and National Innovation Systems.” *Journal of*

Technology Transfer 34(5): 455–73.

Nabity-Grover, Teagen, Christy M K Cheung, Jason Bennett, and United States. 2020. "Inside out and Outside in: How the COVID-19 Pandemic Affects Self-Disclosure on Social Media." *International Journal of Information Management* 55(January): 1–5.

Nevada, State of. 2023. "Banned Technology List." https://it.nv.gov/uploadedFiles/itnewnvgov/content/Governance/Security/FINAL_S_6_02_07_A_BannedTechnologyList.pdf (November 28, 2023).

Nolan, Beatrice. 2023. "Google Brain Co-founder Says Big Tech Companies Are Inflating Fears about the Risks of AI Wiping out Humanity Because They Want to Dominate the Market." *Yahoo*. https://finance-yahoo-com.cdn.ampproject.org/c/s/finance.yahoo.com/amphtml/news/google-brain-cofounder-says-big-113049941.html

OECD. 2014. *Accountability and Democratic Governance*. https://www.oecd-ilibrary.org/content/publication/9789264183636-en.

Okpa, John Thompson et al. 2022. "Cyberspace, Black-Hat Hacking and Economic Sustainability of Corporate Organizations in Cross-River State, Nigeria." *SAGE Open* 12(3): 21582440221122740. https://doi.org/10.1177/21582440221122739.

Oppliger, Rolf. 1997. "Internet Security: Firewalls and Beyond." *Commun. ACM* 40(5): 92–102. https://doi.org/10.1145/253769.253802.

Ormandy, T. (2018). "Issue 1527: Grammarly: auth tokens are accessible to all websites" project-zero. Google. Available at: https://project-zero.issues.chromium.org/issues/42450579

Pagallo, Ugo, Jacopo Ciani Sciolla, and Massimo Durante. 2022. "The Environmental Challenges of AI in EU Law: Lessons Learned from the Artificial Intelligence Act (AIA) with Its Drawbacks." *Transforming Government: People, Process and Policy* 16(3): 359–76.

Peters, B Guy. 2017. "What Is so Wicked about Wicked Problems? A Conceptual Analysis and a Research Program." *Policy and Society* 36(3): 385–96. https://doi.org/10.1080/14494035.2017.1361633

Peterson, Ryan. 2004. "Crafting Information Technology Governance." *Information Systems Management* 21(4): 7–22. https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2

Platform Revolution. (2023). BigTech's Role in Shaping Government Policy. Retrieved November 23, 2023, from: https://platformthinkinglabs.com/materials/power-of-bigtech-companies-in-the-platform-economy/ (November 23, 2023).

Proud, Liam. 2018. "Breakingviews - Breakdown: EU Gains New Powers for Big Tech Fight." *Reuters*. https://www.reuters.com/article/us-britain-data-breakingviews-idUSKCN1IM0V1/

Reveron, Derek S, and John E Savage. 2020. "Cybersecurity Convergence: Digital Human and National Security." *Orbis* 64(4): 555–70.

https://www.sciencedirect.com/science/article/pii/S0030438720300454.

Rosenau, James N. 1999. "Toward an Ontology for Global Governance. Approaches to Global Governance Theory." In Martin Hewson and Timothy J. Sinclair (Eds.) *Approaches to Global Governance Theory*: 287–301. Suny Press.

Rousi, Rebekah. 2022. "With Clear Intention—An Ethical Responsibility Model for Robot Governance." *Frontiers in Computer Science* 4(April): 1–13.

Saariluoma, Pertti, Hannu Karvonen, and Rebekah Rousi. 2019. "Techno-Trust and Rational Trust in Technology–A Conceptual Investigation." In *Human Work Interaction Design. Designing Engaging Automation: 5th IFIP WG 13.6 Working Conference, HWID 2018*, Espoo Finland: Springer International Publishing, 283–93.

Sætra, Henrik Skaug, and Eduard Fosch-Villaronga. 2021. "Research in AI Has Implications for Society: How Do We Respond?" *Morals & Machines* 1(1): 62–75.

Sharon, Tamar. 2021. "Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers." *Ethics and Inf. Technol.* 23(Suppl 1): 45–57. https://doi.org/10.1007/s10676-020-09547-x

Sheehan, Matt. 2022. "China's New AI Governance Initiatives Shouldn't Be Ignored." https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127 (November 28, 2023).

Sinha, Shivanshi, and Yojna Arora. 2020. "Ethical Hacking:The Story of a White Hat Hacker." *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)* 8(3). https://ssrn.com/abstract=3670801 or http://dx.doi.org/10.2139/ssrn.3670801

Siroli, Gian Piero. 2018. "Considerations on the Cyber Domain as the New Worldwide Battlefield" *The International Spectator* 53(2): 111–123. 10.1080/03932729.2018.1453583

Smith, Craig A. 2006. "The World Wide Web of War." In *US Army War College*,.

Spanhove, Jürgen, and Koen Verhoest. 2007. "Analyzing Government Governance at Different Levels: Developing a Normative and Analytical Framework Based on Principles, Processes, Instruments and Cycles." In *Paper for the EGPA SEMINAR FOR DOCTORAL STUDENTS AND JUNIOR RESEARCHERS*, Madrid (Spain).

Starke, Christopher, and Marco Lünich. 2020. "Artificial Intelligence for Political Decision-Making in the European Union: Effects on Citizens' Perceptions of Input, Throughput, and Output Legitimacy." *Data & Policy* 2(e16). doi:10.1017/dap.2020.19.

Suarez-Villa, Luis. 2016. *Globalization and Technocapitalism: The Political Economy of Corporate Power and Technological Domination*. Routledge.

Tameem, R. (2020). How Grammarly Grew to 7 Million Daily Users. Medium. Available at: https://bettermarketing.pub/how-grammarly-grew-to-7-million-daily-users-4fcd5aef6765

Taplin, Jonathan. 2017. *Move Fast and Break Things: How Facebook, Google, and Amazon Have Cornered Culture and What It Means for All of Us*. Pan Macmillan.

Tavis, O. 2018. "Project Zero." https://bugs.chromium.org/p/project-zero/issues/detail?id=1527 (November 28, 2023).

Taylor, Linnet. 2021. "Public Actors without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector." *Philosophy & Technology,*. 34(4): 897–922.

Torfing, Jacob. 2019. "Collaborative Innovation in the Public Sector: The Argument." *Public Management Review* 21(1): 1–11. https://doi.org/10.1080/14719037.2018.1430248.

Tosza, Stanisław. 2021. "Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors." *Computer Law & Security Review* 43: 105614. https://www.sciencedirect.com/science/article/pii/S026736492100087X.

UNODC. "What Is Good Governance?" In *Knowledge Tools for Academics and Professionals UNODC Module Series on Anti-Corruption*, https://www.unodc.org/e4j/zh/anti-corruption/module-2/key-issues/what-is-good-governance.html.

Upguard. (2024). Grammarly. Available at: https://www.upguard.com/security-report/grammarly

Vainio-Pekka, Heidi et al. 2023. "The Role of Explainable AI in the Research Field of AI Ethics." *ACM Trans. Interact. Intell. Syst.* https://doi.org/10.1145/3599974.

Vakkuri, Ville, Kai-Kristian Kemell, Joni Kultanen, and Pekka Abrahamsson. 2020. "The Current State of Industrial Practice in Artificial Intelligence Ethics." *IEEE Software* 37(4): 50–57.

Venture Beat. 2018. "Grammarly Brings Its AI-Powered Proofreading Tools to Google Docs." *VentureBeat*. https://venturebeat.com/ai/grammarly-brings-its-ai-powered-proofreading-tools-to-google-docs/. (November 23, 2023).

Verstein, Andrew. 2017. "The Corporate Governance of National Security." *University Law Review*. https://ssrn.com/abstract=3001658.

Walker, George K. 2000. "Information Warfare and Neutrality." *Wanderbilt Journal of Transnational Law* 33(5): 1079–2000.

Warren, Tom. 2019. "Microsoft Bans Slack and Discourages AWS and Google Docs Use Internally." *The Verge*. https://www.theverge.com/2019/6/22/18713270/microsoft-slack-ban-aws-google-docs-prohibited-list-details

Watt, Eliza. 2021. *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. Edward Elgar Publishing, 2021.

Wegrich, Kai. 2019. "The Blind Spots of Collaborative Innovation." *Public Management Review* 21(1): 12–20. https://doi.org/10.1080/14719037.2018.1433311.

Weiss, Linda. 2014. *America Inc.?: Innovation and Enterprise in the National Security State*. Cornell University Press.

Weiss, Thomas G. 2000. "Governance, Good Governance, and Global Governance: Conceptual and Actual Challenges." *Governance, good governance and global governance: conceptual and actual challenges* 21(5): 795–814.

West, Joel. 2005. "The Economic Realities of Open Standards: Black, White and Many Shades of Gray." *Standards and Public Policy*.

Wirtz, Bernd W, Jan C Weyerer, and Benjamin J Sturm. 2020. "The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration." *International Journal of Public Administration* 43(9): 818–29. https://doi.org/10.1080/01900692.2020.1749851.

Wolfers, Arnold. 1952. "'National Security' as an Ambiguous Symbol." *Political Science Quarterly* 67(4): 481–502. https://doi.org/10.2307/2145138.

Wood, David Murakami. 2016. "Towards Spatial Protocol: The Topologies of the Pervasive Surveillance Society." In *Augmented Urban Spaces*, Routledge, 93–105.

Wu, Tim. 2019. "Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems." *Columbia Law Review* 119(7): 2001–28.

Wu, Xi, and Min-Seok Pang. 2021. "How Data Privacy Regulations Affect Competition: Empirical Evidence from Mobile Application Market." In *ICIS 2021 Proceedings*, https://aisel.aisnet.org/icis2021/cyber_security/cyber_security/4.

Yu, Shasha, and Fiona Carroll. 2021. "Implications of AI in National Security: Understanding the Security Issues and Ethical Challenges BT - Artificial Intelligence in Cyber Security: Impact and Implications: Security Challenges, Technical and Ethical Issues, Forensic Investigative Challenges." In eds. Reza Montasari and Hamid Jahankhani. Cham: Springer International Publishing, 157–75. https://doi.org/10.1007/978-3-030-88040-8_6.

Yueh, Jedidiah. 2018. "GDPR Will Make Big Tech Even Bigger." *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2018/06/26/gdpr-will-make-big-tech-even-bigger/?sh=353d8e6c2592.

Zajko, Mike. 2018. "Security against Surveillance: IT Security as Resistance to Pervasive Surveillance." *Surveillance&Society16(1): 39-52* 16: 39–52.

Zarsky, Tal. 2017. "Incompatible: The GDPR in the Age of Big Data." *Seton Hall Law Review* 47(4): 2. https://heinonline.org/HOL/LandingPage?handle=hein.journals/shlr47&div=37&id=&page=.

Zhu, Junhua. 2022. "AI Ethics with Chinese Characteristics? Concerns and Preferred Solutions in Chinese Academia." *AI & SOCIETY*. https://doi.org/10.1007/s00146-022-01578-w.

Zuiderveen Borgesius, Frederik S. Kruikemeier, Sanne C Boerman, and Natali Helberger. 2017. "Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the EPrivacy Regulation." *European Data Protection Law Review* 3(3): 353–68.