Ethics and Information Technology (2024) 26:24
https://doi.org/10.1007/s10676-024-09763-9

ORIGINAL PAPER

Cybernetic governance: implications of technology convergence on governance convergence

Andrej Zwitter[1]

Abstract
Governance theory in political science and international relations has to adapt to the onset of an increasingly digital society. However, until now, technological advancements and the increasing convergence of technologies outpace regulatory efforts and frustrate any efforts to apply ethical and legal frameworks to these domains. This is due to the convergence of multiple, sometimes incompatible governance frameworks that accompany the integration of technologies on different platforms. This theoretical claim will be illustrated by examples such as the integration of technologies on the "human platform" as it is referred to in the case of enhanced soldiers. Hence, successful governance might require new approaches borrowed from a distant relative, namely cybernetics. Insights gained from cybernetics for governance theories might be able to give guidance for a more efficient and adaptive governance approach that is able to deal with increasing complexity caused by technology and governance convergence. While cybernetics itself might be considered a governance approach, it has had surprisingly little reception in the wider field of governance within the area of social and political sciences. This article will develop cybernetic governance as a set of expandable governance principles that are applicable to an increasingly complex digital and smart society. It thereby tries to further galvanise what could be termed cybernetic governance theory as a subject of worthwhile insights from the combination of otherwise largely the disjoined fields of cybernetics and governance.

Keywords Cybernetics · Governance · Convergence · Enhanced soldiers · Regulation

Introduction

In 2014, the then-president of the United States, Barack Obama, announced the development of a new initiative that involved the creation of a protective suit called the "Tactical Assault Light Operator Suit (Talos)". He likened the suit to the one worn by the superhero Iron Man, which caused some laughter, but he was serious. The US military had already started working on the project, and a promotional video, resembling a video game, was released showing the suit wearer bursting into an enemy cell with bullets bouncing off the armour ("The Myth and Reality of the Super Soldier," 2021). According to the US Director of National Intelligence, John Ratcliffe, China is developing "super soldiers" through biotechnologies such as gene editing to enhance their military capabilities. He claimed that China is exploring ways to create soldiers with superior strength, speed, and resilience, which could pose a threat to the national security of the US and its allies. Ratcliffe called for greater transparency from China and international norms and regulations to govern the development and deployment of such technologies (Gabbatt, 2020).

In general, we are seeing an increasing interconnection and growing interdependency between cyber-digital and bio-physical systems and entities, also referred to as "technology convergence" (Helbing & Ienca, 2022). This convergence between the digital and the physical realm is in and of itself quite a novelty. The digital or cyber domain in these instances can be viewed as a control layer with governance function rather than a separate domain in and of itself (see below.) As such, it is underlining the increasing demand for regulation of digital and IT infrastructures as well as data governance. However, such a demand for more and new regulations sometimes overlooks that there are

Extended author information available on the last page of the article

Published online: 28 March 2024

already regulatory frameworks in place that govern some of the technologies as well as some of the conduct and actors involved. In other words, more governance tools might not make it easier to navigate the jungle of norms and competing jurisdictions of governing bodies that are interacting when cyber-physical systems and entities converge. This convergence of technologies and regulations prompts us to ask what governance approaches allow us to make sense of increasing technological complexity through a governance lense. To do this I will borrow from cybernetics (control theory).

The present article will elaborate on the concept and theory of cybernetic governance. The topic of cybernetic-governance[1] and the governance of complex systems has occasionally been discussed in different disciplines and under different titles, specifically in the context of digitalisation; but it has yet to receive more systematic treatment (Hazenberg & Zwitter, 2021; Keating et al., 2019; Kremer & Müller, 2013; Müller et al., 2017). The concept of cybernetic governance can be understood as a merger between the fields of cybernetics and governance. While both fields concern themselves with the control over systems, they have historically occupied different academic fields of inquiry, cybernetics being particularly relevant in engineering and the hard sciences and governance occupying predominantly the field of the social sciences.[2] The need for developing the concept of cybernetic governance as a merger between these disciplines stems from novel technological developments that mirror such a merger through the convergence of otherwise separate but adjacent fields also in our daily life. This convergence can be identified in discussions surrounding the increasing augmentation of daily practices through AI, increasing integration of digital technologies in daily practices, and issues emerging from so-called cyborgs (Barfield & Williams, 2017) and the human being as a technology platform (human augmentation and the "human platform", Development, Concepts and Doctrine Centre & German Bundeswehr Office for Defence Planning, 2021).

The first section will give an overview of traditional and modern forms of governance as discussed in the governance literature. It will further present structural changes that have accompanied the socio-economic and political landscape in the past decades with the gradual implementation of cyber-physical systems and digital technologies. These developments have effects on governance theories. It will in particular try to trace the origins of cybernetic governance. The illustrative example of human augmentation in the case of enhanced soldiers will illuminate the need for bringing together cybernetics and governance. This case will also highlight some norms and governance mechanisms that accompany such cases as a result of technology convergence leading to a governance convergence. The last part will introduce cybernetics as a form of governance and discuss basic cybernetic control systems and in particular Ashby's law of requisite variety as conceptual foundations for what could be termed "Cybernetic Governance". All in all, this article aims to build on extant but disparate work to further the investigation and research in the intersection between the fields of cybernetics and governance.

Governance and cybernetics

From traditional to network governance

The literature on governance has exponentially increased since the 1980s. The theoretical foundations of governance are as manyfold as the various forms of governance. And the implications, such as capture through political influence, information asymmetry, and cognitive biases have been discussed widely in the literature (Levi-Faur, 2012). While governance is often depicted as comprising old and new governance (Rhodes, 1996), it can be more usefully distinguished into three modes of governance: (1) hierarchical and vertical command and control structures, (2) increasingly horizontal co-regulation, and (3) network governance (Hazenberg & Zwitter, 2020).

Mode (1) governance refers to the traditional form of governance carried out by the state through hierarchical command-and-control structures. It relies on authoritative institutions to make policies through the enforcement of hard law, legitimized through justificatory strategies resting on public sovereignty and public input in political decision-making. It is inherently political and institutional and is identity-based, meaning that the state's identity is seen as authoritative and legitimate. Power relationships are static and governed via structured governance mechanisms, with the state as the dominant hierarchical authority in policymaking. Mode (2) governance is a newer approach to policymaking that moves away from traditional vertical command-and-control structures of the state to more horizontal modes of policymaking. It aims to create a level playing field between societal actors and changes the roles and power relationships of actors involved in policymaking. Mode (2) governance is role-based in the distribution of governance tasks, as opposed to identity-based. The distinction between modes (1) and (2) governance is not always clear in practice, and many hybrid forms exist.

The governance of the digital domain requires conceptualizing power relationships as fluid, distributed, and

[1] In contrast to cyber-governance which generally denotes the governance of cyberspace.

[2] There are notable exceptions; for example, the field of organizational cybernetics pioneered by Stafford Bier.

often residing in a network of distributed actors rather than in a single, centralized actor. Mode (3) governance was introduced to accommodate these findings. Described as "decentralized network governance", mode (3) governance involves distributing governing tasks according to capability and exerted power. In this form of governance, regulatory mechanisms must be flexible, and power must be perceived as residing in specific and changing relationships rather than identities or roles. Decentralized network governance understands power as fluid and dynamic, and different actors can possess power as a relational, variable and functional variable (Hazenberg & Zwitter, 2020).

Despite their differences, all three governance forms share common assumptions when it comes to actors, resources, and regulatory tools. All three types of governance typically involve entities such as States, Companies, International Organizations (IOs), Non-Governmental Organizations (NGOs), and Civil Society. Governance theories and political theories focus on the management and allocation of resources, including raw materials, money, territory, and productivity. These resources are considered essential for the functioning and stability of societies, as they determine the distribution of power and wealth among different groups. Effective management and allocation of resources are key elements of governance, and different entities such as states, companies, IOs, and NGOs play a role in this process. Governance theories typically consider law, contracts, and enforcement as relevant mechanisms to regulate the behaviour of actors. Law provides a framework for behaviour and sets guidelines for actions, while contracts establish specific obligations between parties. Enforcement ensures that the rules and agreements are followed and provides consequences for non-compliance (Hazenberg & Zwitter, 2021).

Emergence of cybernetic governance

The word governance (lat. *gubernare*) shares with cybernetics the same Greek root of *kybernan* meaning to steer or direct (Schneider & Hyner, 2006). In military parlance, cyber in the sense of the digital domain (the internet, other networks, IoT etc.) is often referred to as the fifth domain of warfare besides land, water, air, and space. However, rather than seeing it as a separate domain, it is useful to consider cyber(-space) a control layer on top of all other domains with impact on each of them.

The concept of cybernetic governance can still be considered in a infancy stage without sharp delineations and with contributions covering a varieties of governance domains and technology critiques. This covers, for example, the application of cybernetic theories to governance in the corporate domain, (Schwaninger, 2018) as well as also the governance of IT and digital infrastructures (Skeivys, 2016). Birnbaum's idea of the cybernetic institution, which integrates existing governance models and emphasizes self-correcting processes, comes closest to what the etymological root of governance and cybernetics would suggest. Birnbaum argues that administrators can effectively coordinate and balance various subsystems within an institution by adopting leadership and management approaches consistent with cybernetic principles, including using multiple frames, increasing institutional monitoring systems' sensitivity, and emphasizing selected elements of organizational life (Birnbaum, 1989). Another stream of cybernetic governance, based on Karl Deutsch's *The Nerves of Government*, focuses on the role of information in its various forms and the management of information streams for decision-making (Peters, 2012). Yet another perspective is that of how to govern complexity through the application of complexity theories (Schneider, 2012).

Günter Anders' (Anders, 2002) work on the *Obsolesce of Man*, a philosophical critique of technology and society, can be considered next to many other critiques of the effects of an encroaching digitalisation of many aspects of governance (Helbing et al., 2017; Zwitter, 2014). specifically a critique of the *cybernetization* of society (Nosthoff & Maschewski, 2019). In this context, one also has to view the idea of cybernetic citizenship as a concept closely related to the management of citizens through accumulation of and management through personal data, such as in the example of China's social credit score (Reijers et al., 2023). In this context, it is worthwhile to mention the Chilean experiment with cybernetic governance as an application of Stafford Bier's organizational cybernetics and the Viable System Model (which he viewed as a *liberty machine*, Beer, 1975) and its ultimate failure - the Cybersyn Project 1971–1973 (Espejo, 2014). The government of Chile, deeply impressed by the application of cybernetic theories of the management of complex systems invited one of the most eminent scholars in organizational cybernetics, Stafford Beer, to Chile to help the struggling socialist state out of its difficult socio-economic situation through introducing cybernetic principles in the governance of the state and its centralized industry and production. Beer was tasked to develop a computational algorithmic modelling and management system as an alternative to socialist central planning. In the words of one of the project managers, Espejo (2014):

> The intention was measuring in real-time significant changes in the behavior of essential variables for workers and managers. Significant methodological and practical developments were made designing indices. Local people measured their daily actualities to compare them to their capabilities, or the best

> they could achieve with existing resources, and their potentialities, or the best they ought to achieve with investment to remove restrictions and bottlenecks. These indices were used to collect data in as near to real-time as practically possible and processed using a statistical formalism. The Cyberstride suite was the software for this processing. The data collection was underpinned by a significant modeling capacity. Operational researchers produced quantified flowcharts for plants, enterprises and sectors to work out their capabilities and bottlenecks, and discuss with managers potentialities to design performance indices.[3]

The project ended on September 11, 1973, with a military coup d'état of Salvador Allende's government. This does not take away from the alure of cybernetic governance, and similar ideas are currently being proposed in Peru (Rodriguez-Ulloa, 2022).

Conceptually cyber and cyberspace in the context of governance can be understood as an augmentation of control functions through adding a layer of digital means of information management, control and decision-making functions. The addition of this digital control and information layer adds a variety of variables to enhance regulation and thereby changes drastically what political science traditionally considers entities, resources, and regulatory mechanisms. From this perspective cybernetic governance refers to the ways in which entities manage and regulate cyberspace and the other domains through means available through cyberspace. It consequently consists of several additional key actors, including traditional actors such as states and corporations. Furthermore, it gives a special role to enterprises in the digital and technology domain (e.g. Nvidia, Google or Meta), online interest groups, hackers and hacktivists, cyber-criminals, and digital entities. The latter set of actors are typical for cyberspace and are much more attuned in using its tools (Hazenberg & Zwitter, 2021).

In terms of control mechanisms for the management of control systems, cybernetic governance shifts the attention away from classical raw materials and military prowess towards ways and means that facilitate the control of data and by data as well as the extraction of informational value from it. The governance literature provides insights which resources are particularly relevant for cyber-governance:

1. Data: The digital age has generated enormous amounts of data, which is a valuable resource for many stakeholders (Mayer-Schönberger & Cukier, 2013). However, the collection, use, and protection of data is a key issue in cybernetic governance.
2. Technology: With the increasing reliance on technology, the security of information systems and infrastructure is critical for cybernetic governance (Zwitter, 2014).
3. Human capital: Cybernetic governance also involves managing the human capital involved in the development, operation, and protection of digital systems (Lajili, 2015).
4. Intellectual property: Intellectual property rights are an important control mechanism in the digital economy, and the enforcement of these rights is crucial for the functioning and persistence cybernetic governance mechanisms (Xaydarov, 2022).
5. Infrastructure: The physical and digital infrastructure that supports the internet and digital communications is also central control mechanism that must be managed to ensure stable cybernetic governance (Wegrich et al., 2017).

The means of extracting value from data also changes from human and industrial productivity to artificial intelligence (AI) as an extraction method for informational value generation. A particular place might be given to generative AI as a tool for such value creation. Generative AI has the potential to generate value by using data to automate processes, improve decision-making, and create new opportunities for innovation and growth. More specifically, this can be done through various techniques such as generative design, content creation, and deep learning. Generative AI can also help to automate repetitive tasks and optimize processes, leading to increased efficiency.

From a regulatory perspective, cybernetic governance adds to the toolbox of control mechanisms in a variety of ways. Besides traditional governance tools such as policy, regulation and law, terms of use and similar asymmetric contracts (between large corporations and individual customers) pertaining to intellectual property law are used to regulate the behaviour of users whether in social media networks or in relation to blockchain and other distributed ledger technologies – both on-chain and off-chain regulation are to be considered (Atzori, 2017; Campbell-Verduyn, 2017; Hazenberg & Zwitter, 2020; Reijers et al., 2018). The code running digital networks as well as the user interfaces have regulatory function (Lessig, 1999). And the increasing use of bots, bot-nets, smart viruses and other smart digital (non-human) entities in cyberspace adds to the potential regulatory space (Blauth et al., 2022).

This widening of the governance space and mechanisms as well as the range of actors and the nature of resources has dramatic effect of how one conceptualizes governance as cybernetic governance. Coming back to the term *kybernan*,

[3] For a very insightful account of the history of the Cybersyn Project and its ambitious and futuristic albeit dystopian vision Espejo (2014), who was involved in the project himself, is very recommended.

the term "cyberspace" was coined by science fiction author William Gibson in his 1984 novel "Neuromancer". Whether intended by Gibson or not, from the perspective of cybernetic governance, cyberspace is not merely a digital space. It is at the same time a digital space as well as a digital control layer that governs and steers all other spaces – it is in and of itself the archetypical space of governance in the digital age.

From technology convergence to governance convergence

According to Helbing and Ienca, technological convergence describes the phenomenon that involves the increasing distribution of computing capabilities across physical objects and biological organisms, blurring the lines between physical, digital, and biological domains due to emerging technologies like AI, gene editing, nanotechnology, neurotechnology, and robotics. This convergence is characterized by the frequent co-occurrence of these technologies and their large-scale distribution, which may be difficult to detect, protect from, and manage. The authors argue that current regulations are insufficient and fragmented, and call for the establishment of a new governance system that is able to address the complex ethical and legal issues that arise from the convergence of different technologies (Helbing & Ienca, 2022).

From a legal and normative perspective, this technology convergence on the human platform leads also to a governance convergence. A governance convergence is commonly discussed in the field of corporate governance where it describes the process by which different governance systems, frameworks, or approaches move towards a common set of principles, norms, and standards. In other words, governance convergence involves the alignment of various governance systems towards a common set of goals and objectives (Yoshikawa & Rasheed, 2009). This convergence can happen at different levels, from local to global, and across different sectors and domains, such as environmental governance, corporate governance, or digital governance.

An illustrative case to illuminate how technology convergences leads to governance convergence can be found in the field of armed conflict, specifically the discussion on human augmentation to create enhanced soldiers with superior battle field awareness and other combat relevant skills that go beyond the average soldier's capacities.The enhancement of soldiers through technological means is as old as warfare itself. New weapons, armour, intelligence collection capabilities, communications, transport and logistics, all these aspects are constantly enhanced to increase operational, tactical and strategic advantages over adversaries. In the last decades, these techniques have increasingly started to become more invasive of the human body. The human body increasingly becomes a platform of technological, biological, chemical, and other enhancements affecting physical, psychological, and social performance. For example, considering human vision such an enhancement could range from mere glasses to increase vision to binoculars and night vision goggles, to smart heads-up displays and even to gene-editing for superior visual performance (Development, Concepts and Doctrine Centre & German Bundeswehr Office for Defence Planning, 2021, p. 12).

Considering the human body as a platform, different approaches to enhance human capabilities are being researched. For example: Soldiers are equipped with exoskeletons with embedded sensors and motors that can detect when the wearer is exerting effort and provide assistance (Geggel, 2016). Schumann and O'Regan describe a new non-invasive approach to sensory augmentation which integrates an auditory compass signal into human perception. This approach provides humans with a sixth sense which they normally don't have (Schumann & O'Regan, 2017). Defence Advanced Research Projects Agency (DARPA) is exploring the use of electrical stimulation to improve human learning by up to 30%. The technique called "Targeted Neuroplasticity Training (TNT)" involves delivering mild electrical currents to specific areas of the brain to enhance neural activity during learning tasks. The goal is to accelerate the learning process for military personnel, particularly for skills that require a rapid uptake of information, such as language learning and target identification (Dockrill, 2017). Another potential domain is "telexistence". This is more than mere telepresence and describes the human embodiment in robotic or virtual form: "Telexistence is a concept that denotes an extension of human existence, wherein a person exists wholly in a location, other than his or her actual current location, and can perform tasks freely there. The term also refers to the system of science and technology that enables realization of the concept." (Tachi, 2015).

No longer mere science fiction, brain interfaces, i.e. interfaces that enable brain-computer and computer-brain interaction, are also being researched. For example, Jiang et al. presented a first multi-person, non-invasive interface for brain-to-brain collaborative problem solving. The researchers used electroencephalography (EEG) to record brain signals. Transcranial magnetic stimulation (TMS) was then utilized to deliver information noninvasively to the brains of other participants (Jiang et al., 2019). The final frontier of enhancement of soldiers are genetic manipulation and enhancements of soldiers and the use of synthetic bio- and nano-weapons (Del Monte, 2017; Geraghty, 2023; Knutzen, 2021).

An important consideration in all this is that exoskeletons, brain-computer interfaces, gene-editing, and nanotechnology etc. heavily rely on digital infrastructure and increasingly involves AI for their development and implementation. This indicates the vulnerabilities that these digital infrastructures cause. At the same time, ethical dilemmas surrounding the limits of experimentation as well as moral agency of artificial intelligence must be raised. In short technological convergence, as shown with the example of human augmentation, leads to new governance issues. Some are entirely new; others emerge out of the interaction of regulatory spaces which hitherto never interacted. This becomes clearer when we have a look at a hypothetical enhanced soldier based on existent research. This cybernetic enhanced soldier would have an exoskeleton with embedded sensors and motors that provide physical advantages. Sensory augmentation that translates information directly to the human brain would provide additional senses beyond the common five. Genetic engineering would boost senses, physical abilities, healing, and resilience against adverse environmental effects. Nano-technology would further augment these features and provide additional abilities to digitally interface with the human platform. Finally, brain interfaces would enable brain-computer and computer-brain interaction, allowing for collaborative problem-solving on the battlefield. The big downside would be that this would expand the field of cyberwarfare to have immediate effect on the human body. With the integration of cyber-physical systems, a cyber-attack could directly sabotage the biophysical functioning of the body.

Overall, governance convergence can be seen as a positive development that can enhance the effectiveness, legitimacy, and accountability of governance systems and contribute to more sustainable and inclusive outcomes. However, in the present case of technology convergence in the field of warfare and enhanced soldiers the coordinated aspect of convergence is largely missing. Additionally, convergent technologies lead to an amassment of various norms and governance jurisdictions. For example, in the case of enhanced soldiers and in the context of warfare the general and specific rules of International Humanitarian Law apply, such as The Hague Conventions and the Geneva Conventions as well as additional protocols and separate treaties on chemical weapons or cluster munition. At the same time, human rights law continues to apply where not derogated from or replaced by more specific IHL (*lex specialis derogat lex generalis*) (Schabas, 2007). The utility of AI and large training sets might trigger the application of the European General Data Protection Regulation and the AI regulation (currently in the making). The experimentation on soldiers would further trigger the principles enshrined in the 1949 Nuremberg Code on human experimentation and the 1964 Declaration of Helsinki on clinical research by the World Medial Association besides numerous national laws and regulations such as the so-called Common Rule on human subject research.[4] In addition, increasingly well-established governance frameworks in the field of Bioethics come in to play (Have, 2016; Veatch & Guidry-Grimes, 2019). Add to that the variety of ethical and governance principles that emerge around data and AI governance. These norms, laws, and regulations taken together make for an intricate and most likely unsolvable legal and normative jungle - the dark side of governance convergence. In addition, these governance fields also bring with them a variety of jurisdictions and governance domains of different regulatory bodies adding to the complexity of governance mechanisms. In addition, the digital tools of control and management of data as well as steering mechanisms provided through digital technology and cyberspace discussed above are also added to the mix of governance mechanisms.

To solve these complex phenomena and regulatory and normative gaps, overlaps, and interactions, different governance solutions come to mind. Most commonly, scholars would propose that a new regulation for the new phenomenon would be necessary. In the field of enhanced soldiers, scholars in fact argue that a new convention would be necessary (Shereshevsky, 2020), as has been the case with other weapons such as 1997 Ottawa Anti-Personnel Mine Ban Treaty and the 2008 Oslo Convention on Cluster Munitions. Convergent technologies, however, bring together legal and regulatory frameworks in complex and shifting constellations. Cybernetics as a field was developed to regulate complex systems, but it has hardly been systematically applied to or merged with the field of governance specifically. The next section will discuss cybernetics as a form of governance and the insights that can be gleaned from the merger of the two fields.

The example illustrates a profound transformation in the realms of technology and governance, driven by the phenomenon of technological convergence, as theorized by Helbing and Ienca. This convergence is characterized by the merging of physical, digital, and biological domains through advancements in AI, gene editing, nanotechnology, neurotechnology, and robotics. This blending not only redefines the boundaries between these domains but also challenges existing governance frameworks that are ill-equipped to manage the complex ethical, legal, and social implications arising from such integration.

Beyond that the concept of governance convergence, parallel to technological convergence, suggests a movement towards a field of interacting governance frameworks that

[4] Title 45 Code of US Federal Regulations, Part 46 (45 CFR 46). See: https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html.

can span multiple domains and levels, from local to global. This idea is rooted in the acknowledgment that the disparate governance systems, standards, and norms currently in place are inadequate to address the multifaceted challenges presented by convergent technologies. At the same time, they are overlapping, leave governance gaps and might in some instances cancel each other out. The potential for governance convergence in this context is both a necessity, due to the intertwined nature of these technologies and their impacts, and a formidable challenge, given the diversity of jurisdictions, regulatory domains, and ethical considerations involved.

Figure 1 presents a layered approach to understanding the interplay between technology and governance convergence. On the right, "Technology Convergence," is characterized by multiple technologies that merge on a unified "Technology integration platform," indicating the synergistic interaction of different technologies for example the "human platform". This is mirrored by "Governance Convergence," where various regulatory layers, from international to national and industry standards, integrate into a cohesive governance framework. The bidirectional arrows labeled "Complexity" suggest that as technology converges, it becomes more complex, necessitating a similarly complex, integrated governance structure. The central tiers labeled "Convergence Layer 1," "Convergence Layer 2," and "Convergence Layer 3" imply a stepwise integration process, where each layer represents a deeper level of integration between technologies and regulatory frameworks, reflecting the multifaceted challenges resulting from interacting norms and regulations concerning the managing of the implications of technological advancements across different levels and across domains.

The key argument for governance convergence lies in the necessity for a holistic and coordinated approach to regulating the factual convergence of technologies and their deeper integration into societal functions. In addition, meta-regulation that could stem from cybernetic governance might be better able to adapt to the rapid pace of technological innovation and its broad implications across all facets of society. This approach would necessitate the establishment of new governance systems or the transformation of existing ones to ensure they are capable of addressing issues that span across traditional regulatory boundaries. Such a governance system would aim to harmonize various legal, ethical, and normative principles, thereby facilitating a more effective, legitimate, and accountable governance landscape. The next section will illustrate how cybernetics as control theory provides insights into strategies for meta-governance of situations of governance convergence.

Cybernetic governance

Cybernetics as governance

The founding father of Cybernetics, Norbert Wiener, defined the term in the following way:

> We have decided to call the entire field of control and communication theory, whether in the machine or in the animal, by the name Cybernetics, which we form from the Greek κυβερνήτης or *steersman*. In choosing this term, we wish to recognize […] that governor is derived from a Latin corruption of κυβερνήτης. We also wish to refer to the fact that the steering engines of a ship are indeed one of the earliest and best-developed forms of feedback mechanisms. (Wiener, 1985)

This definition illustrates quite clearly that Wiener from the very inception of the field envisioned that the term cybernetics would be closely related to governor, government and governance. The term governance, however, has separated into its own field of study and like the term sustainability

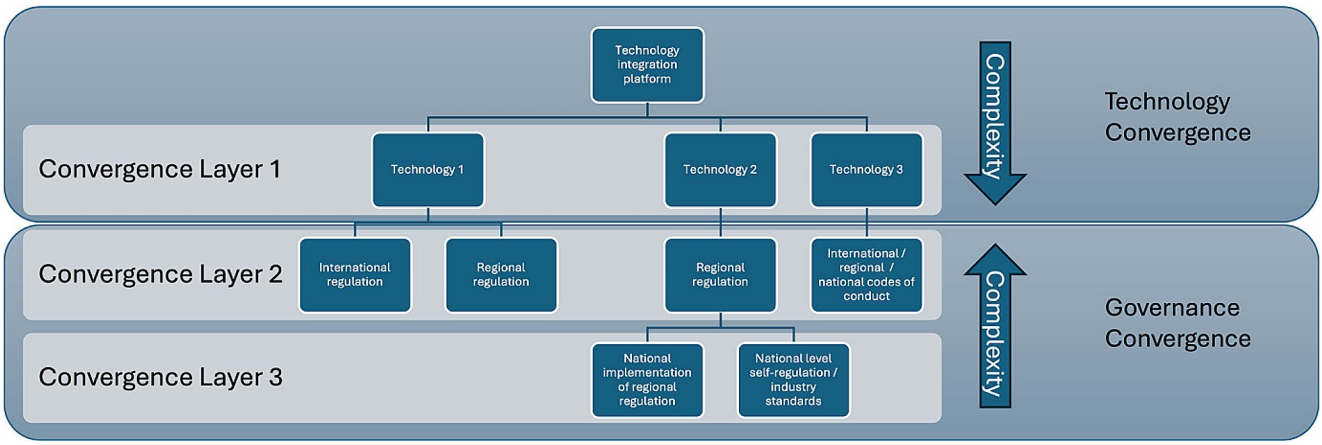

Fig. 1 From technology convergence to governance convergence

has taken on so many different meanings that it can sometimes lack clarity – going back to the origin of the terms and borrowing from the insights in the field of cybernetics can indeed yield some more clarity (Andrew, 2008). Using the term Cybernetic Governance then might at first sight seem like a tautology, but it is far more than that. By recognizing that the fields of cybernetics and governance have by and large catered to different disciplines and have historically had hardly any overlap, merging cybernetics and governance into the field of "Cybernetic Governance" should be understood to refer to the combination of these fields into an overarching theoretical framework. Cybernetic Governance then borrows insights and theoretical developments in the field of cybernetics for governance approaches and for solving issues that emerge from technology and governance convergence.

In the 1950s and 1960s, the young field of cybernetics that started off as a form of applied mathematics would further split into different fields such as computer science and artificial intelligence (Denning, 2000). Cybernetics found entrance into other fields over time such as: "Self-organizing systems in the 1960s, the biology of cognition, management cybernetics and autopoiesis in the 1970s, reflexivity and its connection to ethics and macro-economics in the 1980s, design in the 1990s, and a fruitful critique of science in the 2000s" (Müller et al., 2017).

Cybernetics over the past decades has usefully helped the inception of new research domains and has otherwise enriched extant disciplines with new ideas and applications as illustrated with the Chilean experiment Cybersyn by Stafford Beer. In this section, we will explore whether these mostly disparate fields can be usefully merged to develop new governance mechanisms and strategies for an increasingly complex normative landscape.

Cybernetic control systems

Central to cybernetics is control theory, a sub-field of applied mathematics. "If physics is the science of understanding the physical environment, then control theory may be viewed as the science of modifying that environment, in the physical, biological, or even social sense."(Control Theory | Mathematics | Britannica, 2023) In the social sciences, the emergent field of computational social science has made use of control theory to describe complex decision making and coordination problems (Lazer et al., 2009). An adjacent field could be considered agent-based modelling for simulating social interaction and behaviour, which has been increasing in popularity in the past decades in computational social science (Conte et al., 2012).

The aim of control theory is to regulate a system's output to match a desired reference signal by using a feedback controller. This involves determining which output to monitor, how to compare it with the reference signal, and which system behaviours to adjust and how to adjust them. The difference between the expected and the actual output is called signal error. This error is used to adjust the input to lead to the desired output (Jin, 2018, p. 11). This process happens in feedback loops. In general, control theory distinguishes between three basic control systems (Heylighen & Joslyn, 2003):

(1) Open loop (or buffer) control system: In an open loop control system, the output of the system is not measured or compared to the desired output. Instead, the system is designed to follow a predetermined set of instructions or commands to produce the output. This type of control system is typically used in applications where the output does not need to be precisely controlled or where there are no significant external disturbances. Open loop control systems are used in applications such as household appliances.
(2) Feedforward control system: A feedforward control system tries to anticipate the output of a system based on the input and external disturbances and adjusts the control signals accordingly. It does not rely on measuring the output of the system, but rather uses a model to predict the behaviour of the system. This type of control system is often used in applications where the dynamics of the system are well-understood, and the external disturbances are predictable, such as aircraft and spacecraft control systems.
(3) Feedback control system: In a feedback control system, the output of the system is measured and compared to the desired output, and the difference is used to adjust the control signals to bring the output closer to the desired value. This type of control system is used in applications where the output needs to be precisely controlled, or where there are significant external disturbances that need to be compensated for. Feedback control systems are widely used in industrial and manufacturing processes, robotics, and automation, where precision and accuracy are essential. The use of feedback loops enables the system to automatically adjust to changing conditions, ensuring that the output remains stable and within the desired range.

In this context, regulation is an attempt to achieve a certain goal against a variety of disturbances (Ashby, 1991). As a fundamental principle underlying control theory, the law of requisite variety describes the relationship between a set of disturbances and a set of regulations. Control or regulation involves reducing variety to keep a system's internal state close to a goal state and prevent high variety perturbations

from affecting the system. In active regulation, the regulator must produce counteractions for each disturbance from the environment to maintain the essential variables in the system. The law of requisite variety states that the regulator must have a variety of actions at least as great as the variety of disturbances in the environment, to ensure a small variety of outcomes in the essential variables. Therefore, maximizing the internal variety of a system is important to be optimally prepared for any potential contingency (Heylighen & Joslyn, 2003).

One approach to improve control is to increase the variety in the regulator. This means that the regulator should have a diverse set of actions to respond to different disturbances and uncertainties in the environment. The law of requisite variety, introduced by W. Ross Ashby, states that "only variety can destroy variety"(Ashby, 1956, p. 207). This means that to effectively regulate a system, the regulator must have at least as much variety as the disturbances and uncertainties in the environment. Increasing the variety in the regulator can improve the system's ability to respond to unexpected disturbances and maintain stability. Another approach to improve control is to decrease the variety in the system to be controlled. This can be achieved through simplification, modelling, and abstraction. By reducing the complexity of the system, it becomes easier to understand and control. This strategy is often used in engineering and design, where complex systems are broken down into simpler components that can be more easily manipulated and controlled (Glanville, 2002; Heylighen & Joslyn, 2003; Wiener, 1985).

A third route, besides increasing variety in the regulator or reducing variety in the system, is meta-regulation. Meta-regulation refers to the process of regulating the regulators or the control systems themselves. Meta-regulation is a higher-order control strategy that can improve the robustness, adaptability, and performance of complex systems. Meta-regulation can improve control by providing a higher level of coordination, integration, and optimization among multiple control systems or subsystems. This can lead to better resource allocation, risk management, and resilience to disturbances and uncertainties in the environment. Meta-regulation can also help identify potential sources of instability, conflict, or inefficiency among the control systems and suggest ways to resolve them. One example of meta-regulation is the control of the immune system. The immune system is a complex regulatory network that defends the body against pathogens and maintains homeostasis. The immune system has multiple levels of regulation, including cell-to-cell interactions, signalling pathways, and feedback loops. The immune system can also be modulated by higher-order control systems such as the nervous system and the endocrine system. The meta-regulation of the immune system involves monitoring and adjusting the parameters of the immune system to optimize its response to different types of infections and other challenges (for the immune system acting as meta-regulatory mechanism see for example: Rahman et al., 2018).

Cybernetics' implications on governance

The implications of cybernetics in general and control theory and the law of requisite variety in particular are quite insightful for the further design of cybernetic governance principles. Ashby's Law of requisite variety states that the variety of the regulator must be at least as great as the variety of the system being regulated. In cybernetic governance, regulatory variety refers to the number of different regulatory rules or mechanisms used to control a system. For example, one can infer from Ashby's insights into requisite variety that in order to deal with the effects of technology convergence and the increasing convergence of governance frameworks that there are in principle three strategies to deal with increased complexity (see Fig. 2): (1) increase in regulatory variety; (2) decrease in allowed technological complexity through regulation; (3) application of meta-regulation.

Ad (1), to deal with increasing technological complexity one can increase the regulatory variety. On the positive side, the convergence of regulatory frameworks can provide a more holistic approach to governance, leading to

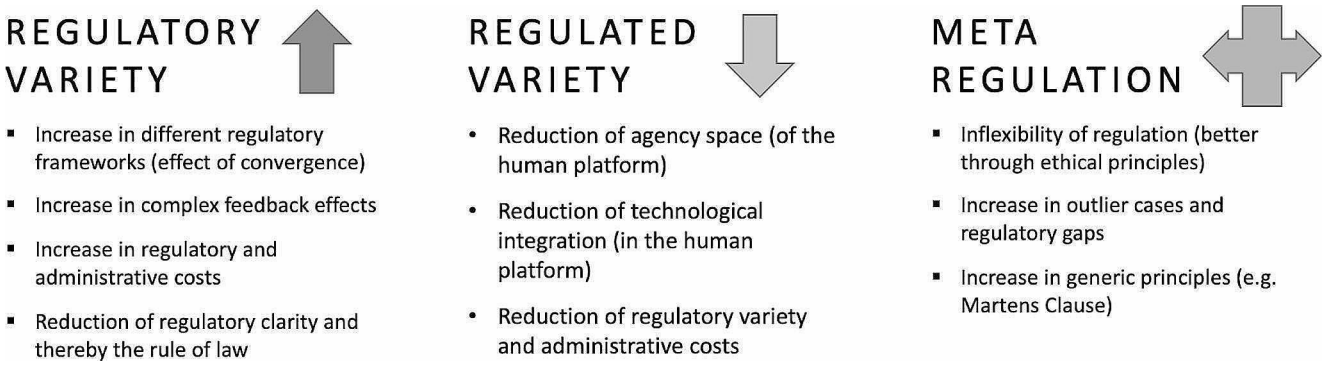

Fig. 2 Application of Ashby's law of requisite variety to governance principles

better coordination, more comprehensive policies, and more effective regulation. However, when regulatory variety increases, i.e. when governance frameworks converge for example through technology convergence, this can result in complex feedback effects between individual norms across governance domains and conflicting regulatory principles and mechanisms. Convergence can furthermore lead to increased regulatory complexity and administrative costs. With multiple regulatory bodies responsible for overseeing a specific governance domain, compliance costs can be substantial, especially for the regulator and for small and medium-sized businesses. This can create a barrier to entry for new entrants. Another negative effect of governance convergence is the reduction of regulatory clarity and the rule of law. When multiple regulatory bodies oversee a subject domain like the human platform, there can be confusion about which rules apply, which have precedence, and how they should be interpreted. This can lead to legal uncertainty, reducing the effectiveness of regulations and weakening the rule of law overall. Finally, the increase in complex feedback effects is another effect of governance convergence. The interconnected nature of digital technologies and cyberspace means that changes in one area can have unintended consequences in other areas. As a result, it can be challenging to anticipate and manage the feedback effects leading to unintended outcomes.

Ad (2), in order to manage converging governance fields and disruptions, a regulator can also resort to limit the complexity of a system – i.e. reduction of regulatory variety refers to the simplification or streamlining of regulatory frameworks in order to make them more manageable and effective. Reduction of agency space would be one approach in this governance approach. That means the space for human discretion or agency in decision-making is reduced. In other words, there may be fewer opportunities for humans to make decisions that are not fully determined by the regulatory framework, potentially limiting creativity and innovation. In the case of the human platform this strategy could be implemented by limiting the agency space of the human platform. In other words, the actors that work in relation to enhanced soldiers would be governed themselves tightly to abide by rules and regulations in their respective domain. To simplify the regulatory framework further, some technological integrations may need to be removed or reduced. For example, if a complex system of automated decision-making algorithms is difficult to regulate, it may need to be replaced with a simpler system that is easier to regulate. One could also limit the number of allowed technologies applied at the same time. This has the added value that a convergent field of governance benefits from clarity in the regulated space through the limitation of regulatory variety. A simpler regulatory framework can reduce the administrative costs associated with maintaining and enforcing regulations. By reducing the number of regulatory rules or mechanisms, it may be easier to monitor compliance and enforce regulations, leading to a reduction in administrative costs and of competing governance interests.

Ad (3), in the context of cybernetic governance, meta-regulation refers to a regulatory approach that focuses on establishing normative principles and regulations on a meta-level rather than specific rules and regulations for each specific governance matter that converges on one platform. This approach is designed to address the limitations of traditional regulation, which can be inflexible and struggle to keep up with rapidly evolving technologies and practices. Besides, this governance approach allows regulators to focus on broader principles and values that are relevant across a wide range of contexts, rather than attempting to prescribe specific rules and regulations. While meta-regulation can be more flexible than traditional regulation, it may also lead to an increase in outlier cases or situations that fall outside of the established ethical principles and norms. This can create regulatory gaps that need to be addressed to ensure that the system is functioning effectively. Meta-regulation often involves the establishment of generic principles and norms that can be applied across a wide range of contexts. For example, the Martens Clause is a generic principle in international humanitarian law to ensure that the protection of non-combatants is ensured in situations where specific rules of international humanitarian law do not exist (Ticehurst, 1997).[5]

Conclusion

The growing use of human augmentation and AI agency is leading to a convergence of regulatory frameworks, including ethical codes, regulations on AI, regulations on the digital domain, and technological regulations under the umbrella of cybernetic governance. This convergence reflects the need to address the complex and multifaceted nature of technology governance and the increasing complexity that follows from technological convergence, which touch on a wide range of issues from privacy and security to the ethics of using AI in decision-making. As these technologies continue to evolve and become more integrated into our daily lives, it is becoming increasingly important

[5] "Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience." Preamble To The 1899 Hague Convention (II) With Respect to the Laws and Customs of War on Land.

to establish clear and consistent regulatory frameworks that can guide their development and use.

By converging different regulatory frameworks, policymakers and regulators can ensure that technologies are subject to a coherent and comprehensive set of rules and standards. This can help to mitigate the risks associated with these technologies, while also promoting their potential benefits in areas such as healthcare, education, and public safety. However, as with any regulatory convergence, there are also risks and challenges associated with this trend. It will be important for policymakers and regulators to carefully consider the potential unintended consequences of regulatory convergence, such as the reduction of agency space, competing governance domains or the weakening of the rule of law.

The convergence of regulatory frameworks related to human augmentation as discussed in the case of enhanced soldiers represents a critical trend in global governance. Addressing the complex and multifaceted governance challenges posed by converging technologies is not a simple and straight forward task, and policymakers and regulators are often limited in their capacity to ensure that innovations resulting from technology convergence are developed and used in a responsible and ethical manner. While governance convergence can bring benefits such as increased cooperation and coordination among different regulatory systems, it also poses challenges to effective decision-making. One of the major challenges is the increased complexity of decision-making. As different regulatory systems converge, the number of actors involved in and norms affected by decision-making may increase, leading to greater complexity and difficulty in achieving consensus.

Moreover, convergence can also reduce regulatory clarity and the rule of law. When regulatory systems with different legal frameworks converge, it can be difficult to establish clear and consistent regulatory standards. This can create confusion for regulated entities, as they may be subject to different or conflicting regulations in different jurisdictions. Additionally, governance convergence may lead to a weakening of the rule of law, as regulatory standards may become more ambiguous or subject to interpretation by cross-reference of different governance frameworks.

In order to mitigate the risks of increased complexity and reduced regulatory clarity, policymakers can instead focus on establishing clear and consistent regulatory standards based on three initial findings from merging governance and cybernetics with a specific view of Ashby's law of requisite variety. Based on initial findings, cybernetic governance offers three possible governance responses that can be deployed in parallel to promote ethical and societal acceptability of emerging technologies: (1) increasing regulatory variety, (2) decreasing regulatory and agency space, and (3) applying meta-regulatory frameworks.

The case of the enhanced soldier and innovation approaches that view the human body as a technology platform illustrate the need for more effective and clear regulation. At the same time, they show that more regulation is not better. This article aimed to illustrate that insights from cybernetics can indeed help generate new governance principles that are adapted to deal with emergent problems caused by an increased reliance on digital control systems and the convergence of cyber-physical and cyber-biological technologies. It, therefore, indicates a need to further develop the yet emergent but still disjoint field of cybernetic governance. Insights from cybernetic governance would also yield applicability to other forms of technology-enabled governance mechanisms such as distributed ledger technology (e.g. blockchain enabled technologies), AI enabled technologies and the growing field of digital identity. Dangers of the misuse of such governance concepts for the further reduction of citizens' agency and increased centralization of power amongst governmental and corporate agents must also not be overlooked. This might require further research for example on the combination with networked and more horizontal governance approaches and maybe also with the growing field digital democracy.

Cybernetic governance is emerging as a field of study that connects digital, normative, technology and bio-physical mechanisms of controlling systems and agents. It opens the space for traditional governance research just as much as for the computational social sciences and many other disciplines in a disciplinary agnostic approach. In a time of accelerating technology convergence, governance needs new, smarter, and more adaptive tools than traditional laws and regulations provide. Cybernetic governance might provide just these tools that modern, digital technology-driven societies need.

Acknowledgements This paper benefitted from a research visit related to the project "CoCi: Co-Evolving City Life", supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant agreement No. 833168). I would like to thank Prof. Helbing and his Computational Social Science team at ETH Zurich for the inspiring exchange of ideas. Furthermore, revisions and improvements where made possible by a fellowship at The New Institute, Hamburg.

Declarations

Competing interests The author declares no competing interests.

References

Anders, G. (2002). *Die Antiquiertheit Des Menschen: Über die Zerstörung Des Lebens Im Zeitalter Der Dritten Industriellen Revolution*. C.H.Beck.

Andrew, A. M. (2008). Cybernetics and e-democracy. *Kybernetes*, *37*(7), 1066–1068. https://doi.org/10.1108/03684920810884414.

Ashby, W. R. (1956). An Introduction to Cybernetics. New York, J. Wiley. http://archive.org/details/introductiontocy00ashb.

Ashby, W. R. (1991). Requisite Variety and Its Implications for the Control of Complex Systems. In G. J. Klir (Ed.), Facets of Systems Science (pp. 405–417). Springer US. https://doi.org/10.1007/978-1-4899-0718-9_28.

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5.

B Keating, C., F Katina, P., Jaradat, R., M Bradley, J., & Hodge, R. (2019). Framework for improving Complex System performance. *INCOSE International Symposium*, *29*(1), 1218–1232. https://doi.org/10.1002/j.2334-5837.2019.00664.x.

Barfield, W., & Williams, A. (2017). Cyborgs and Enhancement Technology. *Philosophies*, *2*(1). https://doi.org/10.3390/philosophies2010004.

Beer, S. (1975). *Platform for change*. London. http://archive.org/details/platformforchang0000beer.

Birnbaum, R. (1989). The Cybernetic Institution: Toward an integration of Governance theories. *Higher Education*, *18*(2), 239–253.

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial Intelligence Crime: An overview of malicious use and abuse of AI. *Ieee Access : Practical Innovations, Open Solutions*, *10*, 77110–77122. https://doi.org/10.1109/ACCESS.2022.3191790.

Campbell-Verduyn, M. (Ed.). (2017). Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance (1st ed.). Routledge. https://doi.org/10.4324/9781315211909.

Conte, R., Gilbert, N., Bonelli, G., Cioffi-Revilla, C., Deffuant, G., Kertesz, J., Loreto, V., Moat, S., Nadal, J. P., Sanchez, A., Nowak, A., Flache, A., San Miguel, M., & Helbing, D. (2012). Manifesto of computational social science. *The European Physical Journal Special Topics*, *214*(1), 325–346. https://doi.org/10.1140/epjst/e2012-01697-8.

Control theory | mathematics | Britannica (2023). March 25). https://www.britannica.com/science/cybernetics.

Del Monte, L. A. (2017). Nanoweapons: A Growing Threat to Humanity. University of Nebraska Press. https://doi.org/10.2307/j.ctt1m3p0v7.

Denning, P. J. (2000). Computer science: The discipline. *Encyclopedia of Computer Science*, *32*(1), 9–23.

Development, & Concepts and Doctrine Centre & German Bundeswehr Office for Defence Planning. (2021). Human Augmentation – The Dawn of a New Paradigm. UK Ministry of Defense & German Bundeswehr. https://www.gov.uk/government/publications/human-augmentation-the-dawn-of-a-new-paradigm.

Dockrill, P. (2017). The US Military Wants to Hack The Human Brain to Help Us Learn a Second Language Faster. ScienceAlert. https://www.sciencealert.com/the-us-military-thinks-electrical-stimulation-could-boost-human-learning-by-30.

Espejo, R. (2014). Cybernetics of Governance: The Cybersyn Project 1971–1973. *Social Systems and Design*, 71–90. https://doi.org/10.1007/978-4-431-54478-4_3.

Gabbatt, A. (2020). December 4). China conducting Biological tests to create Super soldiers, us Spy Chief says. The Guardian. https://www.theguardian.com/world/2020/dec/04/china-super-soldiers-biologically-enhanced-john-ratcliffe.

Geggel, L. (2016). May 13). Power Up! Soft Exosuit helps you lift heavy loads. Scientific American. https://www.scientificamerican.com/article/power-up-soft-exosuit-helps-you-lift-heavy-loads/.

Geraghty, J. (2023). The coming threat of a genetically Engineered ethnic bioweapon's. *National Review*. https://www.nationalreview.com/corner/the-coming-threat-of-a-genetically-engineered-ethnic-bioweapon/.

Glanville, R. (2002). Second Order Cybernetics. In F. Parra-Luna (Ed.), *Systems Science and Cybernetics* (Vol. 3, pp. 59–85). EOLSS.

Have, H. (2016). ten. Global Bioethics: An introduction. Routledge.

Hazenberg, J., & Zwitter, A. (2020). Decentralized network governance: Blockchain Technology and the future of Regulation. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2020.00012. 3.

Hazenberg, J., & Zwitter, A. (2021). Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation. In B. Cappiello & G. Carullo (Eds.), Blockchain, Law and Governance. Springer International Publishing. https://doi.org/10.1007/978-3-030-52722-8.

Helbing, D., & Ienca, M. (2022). Why Converging Technologies Need International Regulation. ResearchGate. https://www.researchgate.net/publication/362570398.

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., van den Hoven, J., Zicari, R. V., & Zwitter, A. (2017). Will Democracy Survive Big Data and Artificial Intelligence? Scientific American - Online. https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

Heylighen, F., & Joslyn, C. (2003). Cybernetics and Second-Order Cybernetics. In R. A. Meyers (Ed.), Encyclopedia of Physical Science and Technology (Third Edition) (pp. 155–169). Academic Press. https://doi.org/10.1016/B0-12-227410-5/00161-7.

Jiang, L., Stocco, A., Losey, D. M., Abernethy, J. A., Prat, C. S., & Rao, R. P. N. (2019). BrainNet: A Multi-person Brain-to-brain interface for direct collaboration between brains. *Scientific Reports*, *9*(1). https://doi.org/10.1038/s41598-019-41895-7.

Jin, Z. (2018). Chapter 11—The System Dependability Problem. In Z. Jin (Ed.), Environment Modeling-Based Requirements Engineering for Software Intensive Systems (pp. 191–216). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-801954-2.00011-X.

Knutzen, M. (2021). Synthetic Bioweapons Are Coming. Proceedings, U.S. Naval Institute, Vol. 147/6/1,420. https://www.usni.org/magazines/proceedings/2021/june/synthetic-bioweapons-are-coming.

Kremer, J. F., & Müller, B. (Eds.). (2013). Cyberspace and International Relations: Theory, Prospects and Challenges (2014 edition). Springer.

Lajili, K. (2015). Embedding human capital into governance design: A conceptual framework. *Journal of Management & Governance*, *19*(4), 741–762. https://doi.org/10.1007/s10997-014-9295-8.

Lazer, D., Pentland, A., Adamic, L., Aral, S., Barabási, A. L., Brewer, D., Christakis, N., Contractor, N., Fowler, J., Gutmann, M., Jebara, T., King, G., Macy, M., Roy, D., & Van Alstyne, M. (2009). *Computational Social Science Science*, *323*(5915), 721–723. https://doi.org/10.1126/science.1167742.

Lessig, L. (1999). *Code and other laws of Cyberspace*. Basic books.

Levi-Faur, D. (2012). From Big Government to Big Governance? In D. Levi-Faur (Ed.), *The Oxford Handbook of Governance* (pp.

3–18). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199560530.013.0001.
Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
Müller, K. H., Umpleby, S. A., & Riegler, A. (2017). Possible Futures for Cybernetics. In New Horizons for Second-Order Cybernetics: Vol. Volume 60 (pp. 375–379). WORLD SCIENTIFIC. https://doi.org/10.1142/9789813226265_0058.
Nosthoff, A. V., & Maschewski, F. (2019). The obsolescence of politics: Rereading Günther Anders's critique of cybernetic governance and integral power in the digital age. *Thesis Eleven*, *153*(1), 75–93. https://doi.org/10.1177/0725513619863853.
Peters, B. G. (2012). Information and governing: Cybernetic models of Governance. In D. Levi-Faur (Ed.), *The Oxford Handbook of Governance* (pp. 113–128). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199560530.013.0008.
Rahman, A., Tiwari, A., Narula, J., & Hickling, T. (2018). Importance of feedback and Feedforward loops to adaptive Immune Response modeling. *CPT: Pharmacometrics & Systems Pharmacology*, *7*(10), 621–628. https://doi.org/10.1002/psp4.12352.
Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Cubillos Vélez, A., & Orgad, L. (2018). Now the code runs itself: On-Chain and off-Chain Governance of Blockchain Technologies. *Topoi*. https://doi.org/10.1007/s11245-018-9626-5.
Reijers, W., Orgad, L., & de Filippi, P. (2023). The rise of cybernetic citizenship. *Citizenship Studies*, *27*(2), 210–229. https://doi.org/10.1080/13621025.2022.2077567.
Rhodes, R. A. W. (1996). The New Governance: Governing without government. *Political Studies*, *44*(4), 652–667. https://doi.org/10.1111/j.1467-9248.1996.tb01747.x.
Rodriguez-Ulloa, R. (2022). Cybernetic governance of the Peruvian state: A proposal. *AI & SOCIETY*, *37*(3), 1207–1229. https://doi.org/10.1007/s00146-021-01329-3.
Schabas, W. A. (2007). Lex Specialis? Belt and suspenders? The parallel operation of Human rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum. *Israel Law Review*, *40*(2), 592–613. https://doi.org/10.1017/S0021223700013443.
Schneider, V. (2012). Governance and complexity. In D. Levi-Faur (Ed.), *The Oxford Handbook of Governance* (pp. 129–142). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199560530.013.0009.
Schneider, V., & Hyner, D. (2006). Security in Cyberspace: Governance by transnational policy networks. In M. Koenig-Archibugi, & M. Zürn (Eds.), *New modes of Governance in the Global System: Exploring publicness, delegation and inclusiveness* (pp. 154–176). Palgrave MacMillan.
Schumann, F., & O'Regan, J. K. (2017). Sensory augmentation: Integration of an Auditory Compass Signal into Human Perception of Space. *Scientific Reports*, *7*(1). https://doi.org/10.1038/srep42197.
Schwaninger, M. (2018). Governance for intelligent organizations: A cybernetic contribution. *Kybernetes*, *48*(1), 35–57. https://doi.org/10.1108/K-01-2018-0019.
Shereshevsky, Y. (2020). Are all soldiers created equal? - on the equal application of the law to enhanced soldiers. *Virginia Journal of International Law*, *61*, 271.
Skeivys, R. (2016). Governance of IT and cybernetics. 2016 IEEE Conference on Norbert Wiener in the 21st Century (21CW), 1–4. https://doi.org/10.1109/NORBERT.2016.7547458.
Tachi, S. (2015). Telexistence: Past, Present, and Future. In G. Brunnett, S. Coquillart, R. van Liere, G. Welch, & L. Váša (Eds.), Virtual Realities (Vol. 8844, pp. 229–259). Springer International Publishing. https://doi.org/10.1007/978-3-319-17043-5_13.
The myth and reality of the super soldier (2021, February 8). BBC News. https://www.bbc.com/news/world-55905354.
Ticehurst, R. (1997). The Martens clause and the laws of Armed Conflict—ICRC. *International Review of the Red Cross*, 317. https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm.
Veatch, R. M., & Guidry-Grimes, L. K. (2019). The Basics of Bioethics (4th ed.). Routledge. https://doi.org/10.4324/9780429507519.
Wegrich, K., Kostka, G., & Hammerschmid, G. (2017). *The governance of infrastructure*. Oxford University Press.
Wiener, N. (1985). Cybernetics or Communication and Control. *The animal and the machine* (2nd ed.). MIT Press. http://archive.org/details/cybernetics-or-communication-and-control-in-the-animal-and-the-machine-norbert-wiene-ocr.
Xaydarov, B. (2022). Impact of Intellectual Property Protection on the Digital Economy. *Journal of Academic Research and Trends in Educational Sciences*, *1*(11), Article11.
Yoshikawa, T., & Rasheed, A. A. (2009). Convergence of corporate governance: Critical review and future directions. *Corporate Governance: An International Review*, *17*(3), 388–404. https://doi.org/10.1111/j.1467-8683.2009.00745.x.
Zwitter, A. (2014). Big Data ethics. *Big Data & Society*, 1(2), 205395171455925. https://doi.org/10.1177/2053951714559253.

Authors and Affiliations

Andrej Zwitter[1]

✉ Andrej Zwitter
A.zwitter@rug.nl

[1] Department of Governance and Innovation, Faculty Campus Fryslân, University of Groningen, Groningen, The Netherlands