frontiers | Frontiers in Political Science

TYPE Hypothesis and Theory
PUBLISHED 04 February 2026
DOI 10.3389/fpos.2026.1748562

OPEN ACCESS

EDITED BY
Mariana Grilli Belinotte,
Brazilian Army Command and General Staff College, Brazil

REVIEWED BY
Brett Van Niekerk,
Durban University of Technology, South Africa
Kostadin Bakov,
University of Plovdiv Paisii Hilendarski, Bulgaria

*CORRESPONDENCE
Roland Kelemen
kelemen.roland@ga.sze.hu

RECEIVED 18 November 2025
REVISED 22 December 2025
ACCEPTED 06 January 2026
PUBLISHED 04 February 2026

CITATION
Kelemen R (2026) The Cyberfare State: divergent models of digital governance and control.
Front. Polit. Sci. 8:1748562.
doi: 10.3389/fpos.2026.1748562

The Cyberfare State: divergent models of digital governance and control

Roland Kelemen*

Modern Technologies and Cybersecurity Law Department, Deak Ferenc Faculty of Law, Széchenyi István University, Győr, Hungary

The digital transformation of state functions has produced a profound paradox: technologies that enhance welfare provision simultaneously enable unprecedented surveillance and control. While optimistic accounts celebrate e-government and Digital-Era Governance for increasing efficiency and citizen engagement, critical scholarship warns of surveillance capitalism and digital authoritarianism. This article introduces the Cyberfare State as a new theoretical framework that transcends the utopia–dystopia binary, conceptualising digital governance as the dialectical unity of welfare and warfare functions in cyberspace. Drawing on historical welfare-state and warfare-state models, the analysis distinguishes two ideal-typical configurations: the smart total-control Cyberfare State, characteristic of authoritarian regimes, which fuses state and corporate power to maximise surveillance and offensive capability; and the cooperating Cyberfare State, viable only under rule-of-law constraints, which requires sustained, rights-compliant collaboration among state, private-sector, and individual actors. The cooperating model's viability hinges on systemic cybersecurity education and the integration of citizens as active co-producers of national resilience, yet persistent educational deficits and reliance on sporadic awareness campaigns leave individuals as the weakest link. Failure to implement comprehensive reform risks irreversible societal harm and strategic disadvantage against authoritarian rivals. The Cyberfare State framework thus offers a roadmap for transatlantic democracies to navigate hybrid threats while preserving democratic values.

KEYWORDS

cooperating Cyberfare State, Cyberfare State, cybersecurity education, digital governance, hybrid threats, smart total control, transatlantic resilience, welfare–warfare dialectic

1 Introduction

The idea that cyberspace and its associated systems can be utilized in the functioning of the state, thereby making its various subsystems more effective, is not a new concept. In his 1996 article, "Welfare vs. Cyberfare," published in the *Journal of Children and Poverty*, Gregory M. Kaladjian undertook to outline the necessity of reforming the welfare state. In the study, he argued for the use of electronic systems in social administration, which, in his view, would have made the existing social structure more transparent and equitable, thus rendering the system's operation more effective (Kaladjian, 1996).

Kaladjian recognized, in an early stage of cyberspace's development, its capacity to enhance the efficiency of state administration, state subsystems, and state functions, though he focused solely on one area: social administration and the renewal of its long-problematic system. However, his words at the time—likely due to the social sensitivity of the focused area and the early phase of cyberspace's development—did not result in significant change. Today, however, the entire system of public administration has, in one way or another, appeared in cyberspace; the activities of economic actors are unimaginable without the opportunities offered by the virtual space, and people spend a large portion of their daily lives in this environment. This, however, has not simply resulted in the reform of the welfare state but has effects that extend far beyond it. This process has created a completely transformed socio-economic environment that has also affected all state functions. It has fundamentally disrupted the entirety of the social totality, a transformation described in their own ways by the great social theories of the 20th century (Lukács, 1971; Habermas, 1984; Castells, 1996), including every one of its sub-complexes: the economy, law, public administration, and the armed defense sectors, where the digitalization of defense and the integration of cyber capabilities are fundamentally reshaping the nature and operation of armed forces (Egloff and Shires, 2021; Bhatia and Pallvi, 2025).

A characteristic of this "evolution" is that it has not only adopted, modified, and selected features of the welfare state according to the power ambitions of various actors but, due to the transformation of the geopolitical environment and the security problems posed by technological development, some states have also reverted to features of the warfare state. In the case of the warfare state, it must be emphasized that this is not a "bad state" opposing a "good state"—the welfare state—but rather a stage (or stages) of state development that has also appeared in the states of the transatlantic region. Its significance lies in the rationalization of state functions (operational, organizational, functional) and the centralization of defense and security actors that emerge as a response to impulses affecting the state, particularly social or external impacts on security (Sparrow, 2011). In his study, Porter (1994) explained in relation to the state development of the United States that this conception of the state was necessary for the creation of a strong federal state, as external—or civil war—threats always necessitated the rethinking, and in some cases, the rationalization of the state's operation. However, it cannot be ignored that this state conception, in the pre-1945 international legal environment, favored the escalation of international conflicts if the rule of law frameworks could not be strengthened or peaceful operation guaranteed.

Contemporary literature analyzing the impact of digitalization on the state largely proceeds along two often separate lines of inquiry. One optimistic stream, through concepts like the "digital state" and "e-government," celebrates the opportunities offered by technology. The central theoretical framework of this discourse is the "Digital-Era Governance" (DEG) model, which posits that data science and artificial intelligence enable a fundamental structural transformation in public services (Dunleavy and Margetts, 2023). Numerous empirical studies support this view, demonstrating that digital transformation—under appropriate conditions—increases governmental efficiency, improves service quality, and enhances transparency (Yang et al., 2024; Doran et al., 2023; Dhaoui, 2021). Accordingly, a significant portion of research focuses on the conditions and processes for successful implementation. Comprehensive literature reviews systematize the drivers and outcomes of digitally-induced change (Haug et al., 2023), while other quantitative analyses examine organizational and cultural barriers, as well as the key role of managerial activities in the process (Tangi et al., 2021). The literature identifies organizational "flexibility" (Gong et al., 2020) and the conscious management of human factors (Di Giulio and Vecchi, 2021) as fundamental prerequisites for a successful transformation. This optimistic narrative also extends to the promise of expanding citizen engagement, although critical voices point out that the expansion of formal participation opportunities does not necessarily translate into an increase in actual influence (Kovács-Szépvölgyi et al., 2025). However, even within this discourse, concerns have emerged that digitalization may paradoxically contribute to the retrenchment of public sector capacity (Collington, 2021).

Parallel to this optimistic discourse, a powerful critical literature focuses on the dark side of technology: the expansion of power and control functions. The cornerstone of this debate is Shoshana Zuboff's concept of "surveillance capitalism," which argues that the digital economy is built on a new logic of accumulation that transforms human experience into behavioral data for profit-oriented exploitation (Zuboff, 2015). This corporate logic is complemented by literature examining the role of the state, analyzing the spread of "digital authoritarianism." Authors like Larry Diamond warn that technology could become an instrument of "postmodern totalitarianism" (Diamond, 2019), while more recent analyses examine how digitalization is reshaping the nature and human rights consequences of authoritarian regimes, and how states are building "digital iron curtains" along the doctrine of "internet sovereignty" (Dragu and Lupu, 2021; Schlumberger et al., 2023; Gosztonyi, 2025). The latest research focuses on specific mechanisms such as "digital repression" against social movements (Earl et al., 2022), the governmental role of platforms (Törnberg, 2023), digital identity as a tool of surveillance (Masiero, 2023), and the inseparable fusion of corporate and state surveillance (Alshamy et al., 2024).

Although the two presented literary streams—the optimistic administrative and the critical political-economic—have largely developed in parallel, the most recent research increasingly recognizes the inseparability of the two domains. Concepts such as the "dialectics of surveillance and recognition" highlight that digital identity is simultaneously a tool for accessing welfare services (*welfare*) and an instrument of total surveillance (*warfare*) (Weitzberg et al., 2021). The "care-control dialectic" examines how care and discipline are intertwined in digital welfare systems (Pors and Schou, 2021; van Toorn et al., 2024). Other approaches, such as "digital biopolitics" or "platform governance," also analyze the blurring of boundaries between civilian and military functions (Zimmermann et al., 2022; Coveri et al., 2025). While these works take important steps toward synthesis, as literature analyses confirm, a comprehensive, widely accepted theoretical model that can systematically address the *welfare–warfare* dialectic is still emerging (Hjelholt, 2024).

This study aims to fill this gap in the literature by introducing the concept of the Cyberfare State. This model moves beyond the simplistic dichotomy of "digital utopia" versus "digital dystopia" and offers an analytical framework that examines the dialectical unity of the two faces of governance—*welfare* and *warfare* (Weitzberg et al., 2021). The added value of the concept lies not only in establishing the fact of this fusion but also in enabling an analysis of how, and in what institutional and political context, these processes occur. It examines how platforms become governmental actors (Törnberg, 2023) and how the blurring of civil-military boundaries (Acton, 2020) fundamentally defines the digital nature of a given state. Subsequently, based on this theoretical framework, the study analyzes in detail the impact of cyberspace on the state and then presents the potential developmental directions for 21st-century statehood that arise from it. Our aim is to create a comprehensive picture through which we can provide more nuanced answers to the complex challenges of state functioning in the digital age.

2 Methodology and analytical framework

2.1 Research approach and objectives

This study is a theory-building work, the primary objective of which is to introduce and develop a new, synthesizing analytical framework: the concept of the "Cyberfare State." The research is not based on empirical data collection but on a qualitative synthesis of the existing literature in political science, public administration, and security studies. The approach stems from the recognition that existing theoretical frameworks (e.g., models of the welfare state or the warfare state) are in themselves insufficient to understand statehood in the digital age. The study aims to identify the limitations of these models in the digital context and to propose a new, integrated conceptual framework that allows for a more nuanced understanding.

2.2 Analytical framework and methodological steps

The process of theory-building consists of three logical steps. First, the study deconstructs two dominant but often contrasted models of 20th-century statehood: the concepts of the welfare state and the warfare state, drawing on their classical and contemporary literature (e.g., Kaladjian, 1996; Porter, 1994). Second, it identifies the literary and theoretical gap that arises from the lack of analysis concerning the intertwining and dialectical relationship of these two models in the digital age. The contemporary literature review presented in the introduction confirms that although the recognition of this phenomenon has begun, a comprehensive, synthesizing model is still missing. Third, in the spirit of synthesis and model-building, the study introduces and constructs the concept of the "Cyberfare State," which is intended to describe the inseparable unity of these two seemingly opposing functions in the digital environment.

2.3 Key concepts

This study departs from the dialectic of two state models that have been central to 20th-century political thought. The welfare state is understood as the model in which the primary objective is to modify market forces along the ideal of social justice, provide services to citizens, manage social risks, and improve the quality of life. In contrast, the warfare state denotes a stage of state development that, in response to an external or internal security threat, subordinates all relevant state capabilities, functions, and powers to overcoming the security challenge, resulting in a powerful centralization of state operations and defense-security actors.

In the context of the digital age, these two models acquire new meaning. Welfare functions utilize technology to increase the efficiency and accessibility of services, while the logic of the warfare state applies digital tools to build total surveillance, social control, and centralized influence. The central thesis of this study is that these two functions have become inseparably intertwined in the digital space, creating a new quality that we term the Cyberfare State. This concept forms the basis for the subsequent analysis, which aims to explore the nature and models of this new logic of state operation.

It is crucial to clarify that the term 'Cyberfare State' is not a synonym for cyber warfare; rather, it represents a state-theoretical construct describing the dialectical fusion of digitalized welfare and security functions, where the state's traditional roles are fundamentally redefined through their integration into the cyber domain.

3 Analysis: the dual nature of the digital state

This chapter analyzes the dual nature of the digital state by examining the two primary, yet seemingly contradictory, transformations driven by technology. The first part explores how digitalization has been employed to enhance and expand the traditional functions of the welfare state, focusing on efficiency, service delivery, and innovation. The second part investigates how the same technological advancements are utilized to strengthen the capabilities of the warfare state, centering on surveillance, social control, and the consolidation of power. Through this dual analysis, we lay the groundwork for understanding their ultimate synthesis.

3.1 The digital welfare state: technology as a tool for progress

The welfare state represents the conscious application of organized governmental power to modify market forces along the lines of a certain ideal of social justice and distribution. It specifically sought to achieve this in three areas: (1) guaranteeing a minimum income for individuals and families (independent of work or wages); (2) reducing economic insecurity, thereby managing certain social risks; and (3) ensuring the highest possible level of provision for specific services. While the first two goals could be partially realized by the social state, the third objective extended beyond this model, aiming to shift the system toward equal treatment. This occurred because the negative effects of the market economy came into focus, necessitating their mitigation and regulation. However, unlike the social state, the system no longer strove to guarantee the minimum but moved toward the optimum (Briggs, 2006).

The rise of the classic welfare state was the result of complex historical processes. Its emergence was enabled by a confluence of factors, such as the extension of universal suffrage, the competitive logic of political democracy, a more complex social stratification, the growing influence of interest groups, and the need to provide a viable alternative to the welfare promises of socialist state models (Esping-Andersen, 1990). As part of the expansion of democratic rights, this state model created complex welfare systems aimed at mitigating a wide range of social disadvantages, investing in future generations, and establishing the basic conditions for personal well-being (Titmuss, 2006). To achieve these goals, it employed instruments such as social insurance, cash and in-kind benefits, and partnership collaborations (Briggs, 2006). It is important to emphasize, however, that neither the scope of functions nor the set of instruments was static; specific solutions varied along national traditions and political cultures, creating different "welfare regimes" (Esping-Andersen, 2002), and the range of policies continuously adapted to the contemporary challenges of each era.

The social processes of the 21st century are once again testing the adaptability of welfare systems and the state. For instance, the emergence of a service-based economy is bringing significant changes to the world of work. According to the World Economic Forum's Future of Jobs 2020 report, 85 million jobs are expected to be displaced by 2025 due to the rise of machines, while 97 million new roles will emerge that require more effective adaptation to the interactions between humans and machines (World Economic Forum, 2020). Naturally, this includes the transformation of the workplace, as businesses necessarily strive for cost-effectiveness. This process is reinforced by the phenomenon of "demonetization": a growing level of digitalization reduces physical costs, which, while creating a competitive advantage, also accelerates the erosion of traditional professions and increases inequality, especially among more vulnerable groups of workers (Ghosh and Chaudhury, 2020; Unni and Dev, 2021). The literature agrees that to avoid the adverse social consequences of this knowledge- and skill-intensive economy, the state must play a key role and make significant investments in the continuous education, reskilling, and upskilling of the workforce (Lagna and Ravishankar, 2021; Addo and Senyo, 2021).

The changing and evolving technologies, increasing global integration, the ability to adapt to them, the excessive dominance of the service sector, and the knowledge-intensive economy it has spawned collectively create divides within societies, and these trends also increase polarization among states. It has become necessary to rethink our conception of the state as well (Esping-Andersen, 2006). In contrast to the non-interventionist "night-watchman state" of the free-competition era—which limited the state's role to maintaining public order and security and ensuring the operational conditions for the economy—the welfare state was an "interventionist state" (Nozick, 1974; Pierson, 2006). In this changed environment, which encourages the state to take active measures, it is self-evident that only a conception of the state that reinforces these welfare attributes can successfully address the challenges of the era.

One of the pioneers of this thinking was Kaladjian, already cited in the introduction, who saw the potential for reforming the welfare state in digitalization. Due to the incredible technological development in the first decades of the 21st century, Kaladjian's ideal of a digitally enhanced, more efficient, and fairer welfare system seems to be partially realized. This process is also based on the specific state conception of welfare states, as their creation generated a societal demand for the establishment and development of high-quality public administration. As a consequence, public administration evolved from being a mere executor of laws into a citizen-centric, service-providing administration (Dunleavy et al., 2006). Thus, the technological revolution necessarily results in the transformation of the welfare state, and therefore also necessarily brought about the reform of public administration and, ultimately, the entire functioning of the state.

State institutional systems had to compete with a transformed service industry that made nearly everything accessible from home through smart devices. The state entered this competition by gradually developing e-government, which made administrative systems more efficient, up-to-date, and citizen-friendly. Systematic literature reviews consistently confirm that e-government developments improve service accessibility, increase efficiency, and, in most cases, significantly accelerate procedures (Maclean and Titah, 2021). Estonia represents the paradigmatic case for the evolution of the Cyberfare State, where technological capacity has been integrated into the very core of statehood (Lember et al., 2018). This centralized digital ecosystem facilitates a 'power–knowledge regime' that produces what Björklund (2016) terms a 'moral citizen': a subject who is simultaneously a de-politicized consumer of digital welfare services and a participant in a strongly politicized, digitally-mediated national identity. The Estonian model demonstrates how the fusion of centralized data registries and administrative routines allows the state to redefine the social contract through technological mediation, balancing efficient service delivery with systemic oversight (Lember et al., 2018; Björklund, 2016).

However, the transformation did not stop there. Technological innovations based on cyberspace are causing explosive changes and foreshadowing general transformations in scientific and social subsystems, enabling humanity to take giant leaps in addressing previously unsolvable problems (Harari, 2016). This is well illustrated by the rapid development of quantum computers. In 2019, Google announced it had achieved quantum supremacy when its 54-qubit processor performed a calculation in 200 s that would have taken the world's fastest supercomputer at the time 10,000 years (Arute et al., 2019). The development is exponential: just 3 years later, in 2022, IBM unveiled its 433-qubit Osprey processor, while intense competition in the field continues between the United States and China (Zhong et al., 2021). A development of similar magnitude is the world's largest 3.2-gigapixel digital camera, built by the SLAC National Accelerator Laboratory, which aims to uncover the nature of dark matter and dark energy by collecting 15 terabytes of data nightly (SLAC National Accelerator Laboratory, 2022).

Tangible results can be demonstrated in education, research, healthcare, and the social sphere, where technologies such as the Internet of Things (IoT), smart devices, Artificial Intelligence (AI), and Big Data are gaining increasing prominence. The vast amount of data (Big Data) generated by interconnected devices and the digitalization of prior knowledge, processes, and activities has brought about a revolutionary transformation in these areas of public service (Alvarenga et al., 2020).

This has brought revolutionary changes to healthcare, including reducing diagnostic errors, enabling the discovery of previously hidden correlations, and developing new, personalized treatment methods. Recent systematic reviews confirm that Artificial Intelligence (AI) and Big Data have led to breakthroughs, particularly in the early detection of cancerous diseases and in increasing diagnostic accuracy. Concurrently, E-Health systems are expanding access to healthcare services, reducing infrastructural and geographical inequalities (Alowais et al., 2023). The involvement of smartphones in monitoring, assessing, and recognizing mental illnesses is also revolutionary, as applications installed on these devices allow for real-time evaluation (Lakhtakia et al., 2022). Similarly, artificial intelligence is proving effective in gait analysis, where it efficiently identifies abnormal gait patterns, thus aiding in the diagnosis of certain diseases (Lim et al., 2022).

The application of modern technology is also creating new opportunities in the fields of education and research. Through Artificial Intelligence (AI) and smart devices, personalized, adaptive learning and the effective transfer of knowledge have become a reality, holding significant potential for democratizing education and improving learning outcomes (Kamalov et al., 2023). The literature extensively discusses AI-based intelligent tutoring systems (ITS) that provide real-time, individualized support to students, thereby assisting those who are falling behind and challenging the talented (Lin and Huang, 2023). In major educational markets like India and China, vast resources are being invested in the digitalization of education, recognizing its societal-level benefits. Furthermore, systems in the United States that focus on individual development demonstrate that AI can act as a digital assistant, supporting the work of teachers and the progress of students without replacing the role of human interaction (Ahmad et al., 2021).

The rise of Big Data and AI is also creating unprecedented, cross-border networks in research, dramatically accelerating innovation. This acceleration continuously opens new horizons for scientific progress. Moore's Law, which famously predicted that the complexity of integrated circuits would double approximately every 18 months, was the engine of the computing revolution for decades (Moore, 1965). Although this type of growth has slowed due to the physical limits of silicon technology, progress has not stopped. On the contrary, in the "post-Moore" era, new engines of performance growth, such as hardware specialized for artificial intelligence and quantum computing, are creating new paradigms that offer the potential for even greater leaps forward (Leiserson et al., 2020; Lundstrom, 2022).

The proliferation of disruptive technologies is dominant, seemingly making people's daily lives easier. The integration of Artificial Intelligence (AI) and the Internet of Things (IoT) enables the creation of complex smart cities, where intelligent transportation systems and autonomous vehicles improve mobility and safety (Alahi et al., 2023). In the field of smart healthcare, wearable sensors and remote monitoring systems allow for the management of chronic diseases and preventive care, potentially saving lives (Alshehri and Muhammad, 2021). This self-perpetuating process of technological advancement is described by the "law of accelerating returns," which posits that progress in one technological area (e.g., AI) accelerates progress in another (e.g., robotics, bioinformatics), generating exponential growth (Kurzweil, 2005).

However, the transformation of the state's functioning did not stop at the modernization of welfare systems; modern technology has fundamentally reshaped all state operational mechanisms, as well as the interactions between the state and economic actors, and between the state and its citizens. As a result, modern technology has penetrated every level of life, exerting significant influence on, among others, law enforcement and the judiciary (Talukder and Hossain, 2024), transportation and logistical systems (Zamani and Gheybari, 2022), and not least, the world of defense and security (Kelemen et al., 2024a,b).

In many respects, these solutions make people's daily lives more livable and rationalize the state's functioning. At the same time, however, service-centricity and access to data have shifted the classic welfare state's ideal of equality toward an elitist mode of operation, where effective control over data assets forms the basis of decision-making (Birch and dos Santos, 2021). Perfect examples of this are privately-owned smart cities, where large corporations have almost complete access to citizen data, extending their governance-like power into urban life (Mosco, 2019; Makanadar, 2024). In Western states, transnational tech companies are building a "virtual sovereignty," massively collecting individual data, while the state's own access to data is constrained by constitutional checks and balances (Kelton and van der Vleuten, 2022). In contrast, as we will see, Eastern authoritarian states use digital reforms to concentrate total control over data in the hands of the state.

3.2 The digitalization of the warfare state: the reality of total security challenges in cyberspace

Eastern states, particularly China and Russia, are significantly exploiting the security capabilities arising from technological innovations. An egregious example of this is the opportunity for total surveillance and data collection veiled in the welfare-like possibilities offered by the smart city. China began building such systems from the early 2010s. Astonishingly, nearly half of the approximately one thousand smart city projects currently underway worldwide are attributable to China. The central elements of this are the so-called "Citizen Cloud" platforms, which on one hand consolidate government services—from health records to parking space finders—and on the other hand, enable the central collection of citizen data (Mosco, 2019). The emerging system could be a perfect example of the state functioning desired in the previous chapter, that is, a service-providing state capable of transferring its welfare institutions into the digital environment and even enhancing them. However, there is a huge "but" at the end of the sentence, as these systems enable China not only to do this but also to track, classify, and effectively possess people's data (Yin and Lu, 2023).

It is worth dwelling on these solutions. The Chinese Golden Shield Project, as highlighted in Freedom House's (2020) internet freedom report, is the globe's most modern and complex surveillance system. Emphasis must be placed on its complexity, as it no longer merely monitors cyber activities but integrates numerous systems operating in both physical and digital spaces: public cameras, health applications introduced during COVID-19, big data-based analytical systems, and facial recognition technologies (Freedom House, 2020). We cannot forget the Great Firewall of China, which ensures that external content is inaccessible. This comprehensive data collection and censorship infrastructure creates the foundation for the social credit system, which results in the consolidation of the political and social status quo by tying citizen behavior and social mobility to scores achieved within the system (Cheung and Shen, 2021).

As Gosztonyi (2023) points out, this phenomenon is not unprecedented and is finding more and more followers. While it is not possible to place all Asian countries under a single regulatory model, a general trend is nonetheless visible: in matters of internet and content regulation, they have chosen a much stricter path than Europe or the United States. The main purpose of this stricter regulation is political: to prevent the spread of ideas in the online world that could potentially incite political resistance in real life (Gosztonyi, 2023). Although this group of states is not homogeneous, it is becoming increasingly evident that more and more states are choosing to control their citizens in cyberspace and through related devices, and to supervise the internet as fully as possible.

Singapore's "Smart Nation" project shows a similar example, where the goal is to create a centralized operations center to manage data collected from citizens and visitors, enabling comprehensive surveillance and strict regulation of behavior. Although official objectives include the faster mapping of disease spread or more effective counter-terrorism responses, the model is built on a close fusion of state institutions and private sector companies. The government stimulates economic development by sharing data, making both the state and tech companies mutually invested in maintaining the status quo. In this model, the user receives improved public services in exchange for their freedom and data, without any real possibility of choice. Similar smart city projects that combine central surveillance with the digitalization of services can be observed in Dubai, Rio de Janeiro, and several major cities in Southeast Asia (Mosco, 2019).

The system was completed by the creation of a sovereign internet and its total surveillance, as seen in China's Golden Shield project or the Russian internet (Gosztonyi, 2021). This allows these state formations to maintain almost total control over their own citizens, as they can block any content deemed undesirable by the state authorities. This solution, much like the smart city projects, has also found followers. Iran intends to build a "halal" internet using direct Chinese know-how (Reporters Without Borders, 2016), a path also followed by Zambia in blocking critical content. Furthermore, blocking anti-government or government-critical voices on social media platforms has become common practice, employed by Cuba, Nigeria, Colombia, Bangladesh, and Senegal, while the Republic of the Congo, Chad, Armenia, and Myanmar block internet access entirely (Gosztonyi, 2021). The basis for these states' actions is the principle previously articulated by China or Russia: the principle of the sovereign internet, according to which every state has free disposal over its associated cyberspace, into which no other state may interfere, and where it can freely determine the accessible content and access to it. The aforementioned Freedom House report points out that China and Iran are the most closed in terms of their own internet, but Russia, Turkey, and Vietnam are also approaching this camp, and the camp is continuously expanding (Freedom House, 2020).

In recent years, it has also become clear that states are using technological innovations in an equally active manner against other states. Cyber operations incorporated into the toolkit of hybrid conflicts provide a wide range of options for attacking the systems of an opposing state. Disinformation campaigns pose a continuous threat and have become a primary tool of modern warfare (Kelemen et al., 2024a,b). Russia's persistent disinformation activities have been observable over the past decade. During this time, they interfered in the 2016 US presidential election by spreading fake news, leaking compromising information about opposing candidates, or delivering timed news packages to users through social media platforms (Rosenstedt, 2021). During the yellow vest protests in France, fake news was spread in several European languages, and efforts were made to discredit traditional media professionals (Makela, 2019). According to one analysis, the identified fake news stories were viewed by more than 105 million people (Avaaz, 2019), which clearly demonstrates the close relationship between social media platforms and hybrid warfare (Kelemen and Farkas, 2025). Furthermore, both China and Russia conducted intense disinformation campaigns regarding the COVID-19 pandemic and the effectiveness of Western vaccines, thereby complicating the region's pandemic response (Dubow et al., 2020).

The Russia-Ukraine war that erupted in 2022 has become a paradigmatic case of digital information warfare. The conflict starkly highlights how social media platforms have transformed into a central battlefield for the struggle over narratives. Russia employs sophisticated, bot-driven campaigns to spread pro-Kremlin narratives and undermine Western support (Marigliano et al., 2024). In response, Ukraine builds effective counter-narratives, using social media to foster national unity and global solidarity (Ghasiya and Shah, 2023). This information struggle, where both sides use tools of disinformation and emotional manipulation, makes objective information gathering almost impossible. The constant flow of often unverifiable content erodes trust in media and institutions, challenging the maintenance of a fact-based discourse (del Sánchez Vas and Arcila Calderón, 2024).

At least as significant is the commission of cyberattacks of varying intensity, whether against civilian and economic targets or against state institutions (Devanny and Stevens, 2022). Among the best-known of these are the 2007 attack on Estonia and the 2008 attack on Georgia, which the literature regards as early, paradigmatic cases of cyber warfare (Devanny and Stevens, 2022). The WannaCry ransomware attack, linked to North Korea, can also be considered in this category, having caused significant damage to several states and economic actors (Department of Justice, 2018). The financial damage caused by cybercrime is continuously increasing; according to the latest FBI report summarizing 2024 data, reported losses have already exceeded $16.6 billion (FBI Internet Crime Complaint Center, 2025). The use of this tool is also observable in the Russia-Ukraine war, where cyber operations form an integral part of hybrid warfare (Willett, 2022).

In this context, it is worth noting that cyberspace has not in itself created new categories of conflict, but rather has represented an evolution of the previous toolkit of warfare: an increase in efficiency, a multiplication of force, and an enhancement of operational capabilities (Bachmann and Gunneriusson, 2015). Earlier scenarios of the Russia-Ukraine conflict also reflect this. According to military experts from West Point, the Russians employ the tools of cyber warfare, electronic warfare, and information operations in an unprecedentedly integrated and combined manner (Brantly et al., 2017). Indeed, Russian doctrine does not differentiate between various information operations but views the information space as a single battlefield targeting the entire "cognitive domain" (Splidsboel Hansen, 2021).

It is clear that the cyber toolkit has been integrated into the activities of armed forces, whether for influence, intelligence, or offensive purposes. Cyberspace has become an immanent part of peacetime combined arms preparation and the operational toolkit for active missions. Modern military doctrines no longer treat cyber capabilities as a separate domain but as an integral element of hybrid warfare scenarios, making it possible for conventional wars—as seen in the Russia-Ukraine conflict—to have hybrid scenarios (Harknett and Smeets, 2020).

Furthermore, cyberspace provides opportunities for separatist and terrorist groups to finance, recruit for, and plan their operations. Digital tools enable them to gather information, support and prepare for actions in cyberspace, and even to execute attacks against critical infrastructure (Lee and Sobol, 2021). In parallel, prior experience and networks play a key role in state-level hybrid warfare. The Russians have been highly successful in their hybrid conflict against the Ukrainians, as they were able to combine their modern digital toolkit with intelligence and influence methods inherited from the Soviet era (Bachmann and Gunneriusson, 2023).

The cyberspace and its attendant technological innovations are eroding the post-1945 international legal regime on numerous points. Hybrid threats and cyber operations often take place in a strategic "gray zone," exploiting the legal uncertainty between peace and war (Sari, 2020). The application of technological innovations has initiated the erosion of the general prohibition on the use of force laid down in the UN Charter, as most cyber actions do not reach the threshold of an "armed attack," thus complicating legal responses. The difficulties of attribution and the blurring of civilian-military boundaries during cyber conflicts make the application of traditional laws of armed conflict almost impossible (Dossi, 2020; Kello, 2021). The war in Ukraine has also highlighted that the principles of self-determination of peoples and their existence free from external state interference are dissolving in the face of great power ambitions. The line between war and peace has become blurred in recent years; in most conflicts, we do not know whether we are in a state of "just before" or "just after." This was also highlighted by the Russia–Ukraine crisis, as actual combat operations between the parties had begun long before the 2022 invasion.

The sum of these factors results in the redefinition of security and defense, a shift towards "total security" where security practices extend beyond traditional military and intelligence domains to permeate everyday life and the civil sphere (Klimburg-Witjes and Wentland, 2021). One pole of the international community's states has already taken this step, and these state formations—primarily through cyberspace—are moving much closer to the classic ideal of the warfare state, which sees the guarantee of its own security only through power, by means of force (Cook, 1964; Edgerton, 2006). In these states, the continuous strengthening of the armed forces has become a vital interest, with the trinity of political power, armed forces, and the economy serving a single purpose: to at least maintain the status quo, or, even more, to expand their sphere of power.

4 Discussion: the models of the Cyberfare State

The state has fundamental, indispensable functions that it must perform. There is no other institution capable of providing the essential conditions for organized communal life in place of the state. These core functions include maintaining the rule of law, ensuring the protection of private property (internal security), and national defense (external security) (Fukuyama, 2014).

The preceding chapters illustrate that cyberspace has transformed the security environment to such an extent that states, in many cases, are only able to meet these requirements temporarily and in a more limited scope than before (Sun et al., 2023). However, if "…social fears escalate… This results in a negative spiral. The more they do this, the greater the chaos and violence, and the greater the chaos and violence, the less capable states are of managing the situation; consequently, the more people withdraw their trust from the state…" (Szigeti, 2001). That is, the loss of trust in public order and the military-style bodies that guarantee it would nullify security, thereby dismantling the normal state of affairs.

States today are perfectly aware of the opportunities and challenges posed by cyberspace (it is no coincidence, for example, that NATO has designated cyberspace a domain of warfare (Păunescu, 2021)), and they are trying to respond to its security implications. However, this response is strongly influenced by the historical and social traditions of individual states, as well as their political, state, and legal traditions, and great power ambitions. From a cybersecurity perspective, one of the main agents is the individual, whether we observe them as a passive or active participant, who, as seen in the previous chapters, can have an unprecedented impact on national security. It is no coincidence that the reaction to the role of the individual, along the lines of traditions and political systems, is one of the most important dividing lines among the states under examination. As a result, two model-like systems have emerged. One model is the set of states operating within a rule-of-law framework, while the other comprises states that see and exploit opportunities in cyberspace and related tools, striving for the fullest possible control over their society. Of course, neither of these two sets is homogeneous; within them, the degree to which technology-based total control is realized on one side, and the extent to which the pillars of the rule-of-law paradigm are taken into account on the other, varies. Nevertheless, it is worthwhile to separate these models and analyze them fundamentally.

Nevertheless, it should be noted that while these categories represent ideal-typical endpoints for analytical clarity, the empirical reality often reveals more complex, hybrid paths. Emerging powers such as India or Brazil illustrate this duality; while pursuing ambitious digital welfare initiatives—such as digitized healthcare access (Al Dahdah and Mishra, 2023) or urban knowledge management systems (Baud et al., 2014)—they simultaneously construct data infrastructures that enable intensified population monitoring and centralized executive control. In these hybrid configurations, welfare-oriented digital systems often sit atop architectures that normalize granular tracking and coercive potential (Debnath and Bardhan, 2020), or engage citizens as active 'co-producers' in a surveillance apparatus that extends the state's technological gaze (Leal Neto et al., 2020), thereby blurring the boundaries between the cooperating and smart total-control models.

4.1 The authoritarian model: the smart total control Cyberfare State

The previous chapter has shown that a group of states is using technological developments not only to strengthen welfare functions but also to strive for the fullest possible control over their citizens. The foundation of this thinking is the extension of the classic principle of state sovereignty (Krasner, 1999) to the digital realm, creating the doctrine of "cyber sovereignty" (Pohle and Thiel, 2020). According to this concept, every state has the right to regulate, supervise, and defend its own national cyberspace according to its own laws and security interests, often in direct opposition to the model of a global, open internet. States such as Russia and China use this principle to justify total regulatory, law enforcement, and defense control over their national internets (Litvinenko, 2021).

The renowned American cybersecurity expert Adam Segal highlights that China formulates and seeks to fully establish the idea of cyber sovereignty largely because it is striving for a global power position in this domain as well; thus, it is not surprising that this concept has both internal and external aspects. However, this is not necessarily the reason for the thesis becoming more accepted. Rather, an increasing number of states are facing significant problems with disinformation, threats to privacy and private property, the economic consequences of cybercrime, and, not least, many states view the power concentration of large technology companies, which stems from the unregulated or under-regulated nature of cyberspace, as problematic. However, operating such a system requires adequate economic and technological capacity, as the mere proclamation of the principle will not in itself create and operate the technological background, which requires significant economic resources (Segal, 2020).

This underscores that the smart total-control model is not merely a product of technological acquisition but rests on profound institutional and structural foundations. As Smeets (2022) argues, effective state cyber power cannot be achieved through rapid technological leaps alone; empirical evidence suggests that a nation's science and technical knowledge base remains the most robust predictor of its cyber capacity (Calderaro and Craig, 2020). Turning this technical potential into usable state power requires significant organizational maturity and a coherent strategy to manage 'cyber uncertainty' (Devanny and Stevens, 2022). Ultimately, as Rasmussen and Erickson (2025) suggest, the evolution of national cyber power necessitates a holistic 'digital ecosystem' approach, where state control extends beyond mere security tools to the critical substructures of data and energy resources.

China has successfully executed all of this, making cyber sovereignty a clear and functional principle of its cyber diplomacy (Gosztonyi, 2021). The model has clearly found followers among states that are already inclined to restrict cyberspace access, share the aforementioned concerns, and are willing to adopt China's know-how as it pursues its global ambitions. It is no coincidence that we see the adoption of, or attempts to adopt, Chinese know-how in Ethiopia, Egypt, Jordan, Lebanon, Libya, Morocco, Saudi Arabia, and the United Arab Emirates. But this is not only embodied in technology and institutional systems but also in the copying of legal regulations. Tanzania has adopted a cybersecurity law similar to China's. Egypt, Laos, Pakistan, Uganda, Vietnam, and Zimbabwe have passed laws that, following the Chinese model, allow for website blocking, real-name registration, data sharing, and content removal (Segal, 2020). Thus, China offers a real and functioning alternative in terms of both regulation and technological achievements. North Korea, Russia, and Iran are also on this path, partly independently of China. Turkey and Singapore have also taken steps in this direction, albeit on a smaller scale. Therefore, it must be said that the Chinese conception of cyber sovereignty is clearly a model, not only from a technological perspective but also in terms of its legal and organizational regime.

Such a highly successful exploitation, utilization, and application of cyberspace and its related systems has created the power-based sub-model of the Cyberfare State. Within this framework, the state, through its possessed power, effectively creates its own sovereign cyberspace, owning and controlling it in its entirety. By exploiting the technical, regulatory, and defensive shortcomings of states in the separate external cyberspace, it is able to influence the fault lines of other societies, paralyze some of their subsystems, and export its own model of digital governance, challenging liberal norms (Moore, 2022). All this is achieved without, in most cases, engaging in actual armed confrontation with the attacked state.

Such a highly successful—albeit, from a European perspective, extremely controversial—exploitation, utilization, and application of cyberspace and its related systems, observed primarily in China and Russia, with partial adoption in states such as Iran, Vietnam, and Singapore—has created the power-based sub-model of the Cyberfare State. Within this framework, the state, through its possessed power, effectively or in a significant part of its territory, creates its own sovereign cyberspace, owning and controlling it in its entirety. By exploiting the technical, regulatory, and defensive shortcomings of states in the separate external cyberspace, it is able to influence and escalate the fault lines of other societies with unprecedented effectiveness, and to paralyze some of their subsystems (Moore, 2022). All this is achieved without, in most cases, engaging in actual armed confrontation with the attacked state.

This system is operated and its activities are realized because, in the new security environment, they view total surveillance and a total monopoly on violence as the ultimate guarantee of peace and predictable order. In its creation, as we have seen, the state and its economic actors operate, function, and develop in fusion. In these states, the individual lives under the fullest possible control, essentially reduced to being merely an operator of partial objects (through their work) and a consumer of the services permitted and offered by the system, with no real decision-making power over their own data assets. In this context, the effective functioning and security of the state are created by the fusion and common interest of the state and economic actors. For this common goal, they attempt to remove the individual as the most fragile link in (cyber)security, minimizing their role, the means to which is total control over their person and the totality of state and economic command over their data (Huang and Chen, 2022).

The development, continuous tracking, and necessary correction of the best practices that guarantee the (cyber)security of these states are the fruit of the common interest and cooperation between the state and the involved economic actors, in which the individual appears not as a stakeholder but exclusively as a directed, controlled resource. In this best practice, social and welfare institutions based on cyberspace-reliant technological innovations—ultimately the improvement and modernization of the service-providing administration—are combined with the possibility of total control and total command over data, to which, in many cases, the development of offensive potential is also linked. For the reasons above, we can call these states, which exhibit the power-based attributes of the Cyberfare State, the smart total control Cyberfare State (Figure 1).

4.2 The democratic model: the cooperating Cyberfare State

In contrast, Western states had to start from a completely different foundation in shaping their own Cyberfare State model. They began the welfare reform of digitalization in the early 2000s and have achieved spectacular successes, albeit not in all areas. As seen in the previous chapter, they successfully transformed the service-providing public administration, and large-scale innovation has emerged in areas such as education, research, and healthcare. Additionally, highly successful smart city programs are underway (Berigüete and Rivas, 2024), and projects related to autonomous vehicles or AI programs also promise numerous benefits (Erman and Möller, 2022).

However, significant differences can also be identified here compared to the states of the other pole. In the Western model, the pioneers of technological development were the tech giants, but—unlike in China, for example—this did not mean a functional fusion of the state and economic actors. On the contrary, the relationship

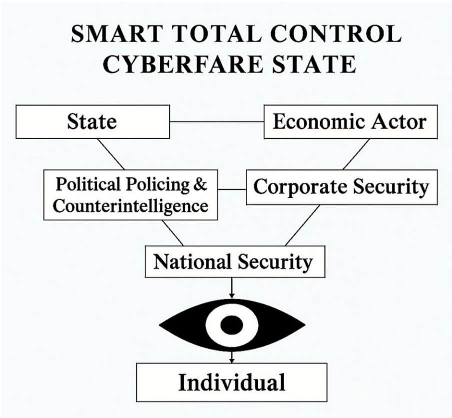

FIGURE 1
The smart total-control Cyberfare State schematic representation of the authoritarian cyberfare state model. State and corporate actors are fused at the top, jointly exercising political policing, counter-intelligence, and corporate security functions. National security is achieved through total surveillance (symbolized by the eye), reducing the individual to an object of control. Source: Own elaboration.

between democratic states and Big Tech is characterized much more by significant conflicts of interest, regulatory struggles, and the traditional distrust stemming from a capitalist conception of the state (Aho and Duffield, 2020).

The handling of individual data in these states also presents a completely different picture. In many cases, transnational corporations have misused the data they manage to advance their economic interests, which, although resulting in significant fines, has not changed their economic position or role in society. Here, the state or a community of states—such as the EU with its General Data Protection Regulation (GDPR)—is attempting to create increasingly strict rules (Hoofnagle et al., 2019). On the other hand, due to the changing security environment, the state is trying to reduce national security vulnerabilities and satisfy its related hunger for information. This, however, conflicts with the interests of economic and individual actors and faces significant obstacles due to constitutionally limited state operations, often followed by vocal opposition and proceedings before international judicial forums (Celeste and Pollicino, 2024).

In this environment, it would be inconceivable to establish a level of surveillance over individuals or even economic actors even remotely similar to what we have seen in China. Beyond control mechanisms, restricting access to cyberspace is also not conceivable to such an extent, as some states regard internet access as a fundamental right, and in other states, a host of guarantees protect it (Gosztonyi, 2020). Not to mention that this would significantly conflict with the profit-oriented interests of economic actors. These findings are true for peacetime, normal operations; they would be significantly transformed by a classic interstate conflict or extremist events attacking the internal order, which the state would have to resolve in a completely different authorization context. Avoiding such a situation, however, is becoming a primary interest for all stakeholders.

The conflicts and social tensions of recent years have made it clear that a shift is necessary in enhancing security in the digital terrain, as ransomware, denial-of-service attacks, and the activities of trolls (Aro, 2021) have slowly become part of everyday life, linked to other states (Whyte, 2020) or, in many cases, to organized crime (Martin and Holt, 2023). The "infodemic" that appeared alongside the COVID-19 pandemic [WHO (World Health Organization), 2020], or the filter bubble practice of social media platforms (Pariser, 2011), fake news, and deepfake content have already pushed freedom of expression in a direction where the individual often cannot distinguish between real and false content. The average user is significantly influenced in forming their opinions and decisions. The importance of a rule-of-law-based response to these threats is shown by the fact that the European Union is also seeking to place social media platforms under a stricter regulatory framework and to make the filtering mechanisms more transparent.

These tensions go hand in hand with the corrosion of security in the traditional sphere, as external actors negatively influence public trust. The impact of these campaigns is amplified by "lawfare," or the malicious abuse of law, as well as the legal vulnerabilities of states (Sari, 2020), which allow malicious actors to sow doubt and distrust within society (Hofstetter, 2020). The national security regulatory system of the transatlantic region, which must consider rule-of-law guarantees, has therefore come into focus because if the regulation of defence and security functions is not sufficiently modern and predictable, it can result in an erosion of trust in the state (Whitford and Prunckun, 2025). This also calls into question the legal order itself. As Szigeti (2001) previously argued, this can lead to a negative spiral where state bodies lose their social support, and individual actors take the provision of their security into their own hands. Such a process could lead to anarchy or a significant social fracture, which could ultimately transform the very foundations of the states in the transatlantic region at a systemic level.

And this brings us to the reason why the three core actors in transatlantic democracies—the state, economic actors, and the individual—must move from competition to sustained cooperation (Figure 2). As Figure 2 illustrates, the cooperating model is fundamentally characterized by a bidirectional relationship. This shift reflects a broader trend in public governance toward the 'co-production' of public value, where citizens participate not merely as service users but as active partners in ensuring systemic resilience (Voorberg et al., 2014; Khan and Krishnan, 2021). In the digital age, this manifests as 'digital citizen empowerment,' where proactive individual behavior and vigilance serve as critical bottom-up inputs that sustain national security and collective stability (Sharma et al., 2022; Chari et al., 2019). Consequently, the individual's role is transformed from a passive endpoint of security provision into a foundational and indispensable component of a circular resilience architecture. Only the cooperating Cyberfare State can reconcile the fundamental requirements of rule-of-law governance with the imperatives of security in the digital age. Unlike the smart total-control model, the pursuit of resilience here cannot come at the price of individual freedom. The economic sector has a direct stake in functioning state and societal subsystems—without which neither capitalist markets nor investment security are conceivable—as repeatedly demonstrated by the economic fallout from the Russo-Ukrainian war, the COVID-19 pandemic, and major terrorist attacks (Nwankpa and Datta, 2023; Whitty et al., 2024). For citizens, the protection of personal data, property, and everyday life similarly depends on resilient public institutions. In an environment where isolated cyber incidents can rapidly cascade into institutional destabilisation and erode public trust, the Russo-Ukrainian war marks

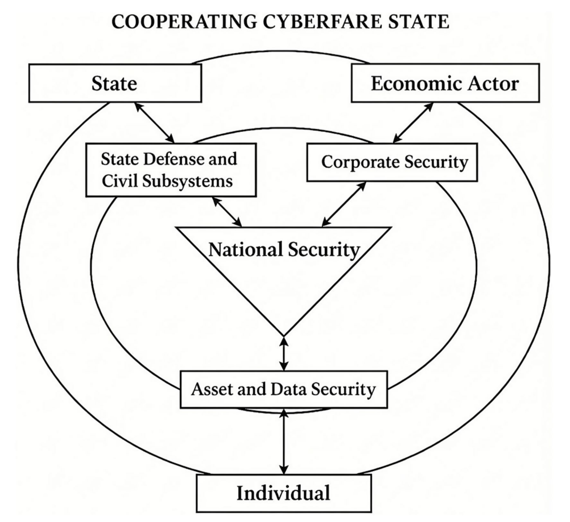

FIGURE 2
The cooperating Cyberfare State multi-stakeholder architecture of the democratic Cyberfare State model. National security emerges as a co-produced public good from the continuous interaction and functional overlap of state defence and civilian subsystems, corporate security functions, and citizens' asset- and data-security interests. Source: Own elaboration.

a dangerous inflection point (Ruggiero and Laine, 2024; Kelemen et al., 2025). Systemic, multi-stakeholder cooperation is therefore no longer optional—it is the only viable path forward.

The cooperating Cyberfare State is a sub-model grounded in the functional interplay and overlapping roles of the state, economic actors, and society. Here, cooperation likewise originates from the digitalisation of welfare and social systems, but its further evolution requires the development of a multidisciplinary best practice that preserves rule-of-law constraints while simultaneously prioritising security efficiency. This practice must integrate the experiences and theoretical perspectives of state (civilian and military), economic, and academic actors from both technical and social sciences (law, sociology, economics, and military science).

Despite repeated declarations of multi-stakeholder cooperation in transatlantic and EU cybersecurity strategies, systemic programmes that reach the individual citizen level remain conspicuously absent. Initiatives such as the European Cybersecurity Month and ENISA-led awareness campaigns typically consist of isolated, one-off actions that are rarely integrated into national education systems or everyday public services (Ricci et al., 2024; van Kessel et al., 2023). This persistent implementation gap leaves citizens as the weakest link in national cybersecurity co-production and significantly undermines the viability of the cooperating Cyberfare State model (Carrapico and Farrand, 2024; Almeida, 2025).

In the rule-of-law-bound cooperating Cyberfare State, the role of the individual cannot—and must not—be ignored. Adversarial powers deliberately target citizens with disinformation, manipulation, and social engineering precisely because the human being remains the single greatest residual security risk (ENISA. European Union Agency for Cybersecurity, 2023; Nobles and Mcandrew, 2023). As Figure 3 illustrates, individuals already actively participate in both state and economic subsystems, yet democratic states have so far failed to assign them a coherent, rights-compliant position beyond sporadic awareness campaigns (Fenech et al., 2024; ENISA. European Union Agency for Cybersecurity, 2018).

Individuals, as workers and consumers alike, constitute potential risk vectors for state and economic systems as well as for their own data and property. Consequently, the cooperating Cyberfare State must abandon the prevailing tendency to devolve cybersecurity solely onto individual responsibility, an approach that leaves citizens unsupported irrespective of their actual competence (Asfahani, 2024; Kelemen et al., 2024a,b). Persistent deficiencies in state-led awareness-raising, particularly within defence and national-security domains, underscore the urgent need to realign the cybersecurity paradigm: from individual blame toward the cultivation of a collective, systemic security culture.

The cooperating Cyberfare State requires comprehensive, mandatory cybersecurity education at every level of formal schooling. Cyberspace is no longer confined to high-skill professions; it has become an integral part of everyday life for citizens of all ages, making age-appropriate digital resilience an essential civic competency (Videnovik et al., 2025; Ibrahim et al., 2024). The human factor remains the primary vulnerability across all roles, with attackers consistently exploiting lack of awareness and poor digital habits (Alsharida et al., 2023; Xu et al., 2025). Sporadic campaigns are insufficient; only systematic, curriculum-embedded education can effectively mitigate this persistent risk.

A particularly sobering illustration of this systemic failure emerged during the COVID-19 pandemic, when numerous non-elderly citizens who routinely used digital services proved unable to complete online vaccine-registration processes despite adequate infrastructure access. This digital-literacy paradox—competence in everyday applications coexisting with incapacity in high-stakes official online procedures—cannot be attributed to individual incompetence but reveals profound deficiencies in public digital education (Morrison et al., 2023; Malkowski et al., 2024). Similar difficulties were observed across middle-aged cohorts, underscoring that routine digital engagement does not automatically confer the specific skills required for high-stakes official online procedures (e.g., vaccine registration, tax filing, e-government services, or digital prescription retrieval) (Kung and Steptoe, 2023; Riad et al., 2025).

The same imperative extends to higher education. No university programme—whether training future teachers, childcare professionals, public administrators, or any other non-technical leaders—can any longer afford to graduate students without embedded cybersecurity competencies. These individuals will later occupy decision-making positions in which ignorance of cyber risks can directly endanger the systems and populations under their responsibility (Ramezanian et al., 2024; Dion, 2023). Current curricula still largely treat cybersecurity as an optional specialisation rather than a universal requirement, leaving tomorrow's leaders unprepared to recognise or mitigate threats in their respective domains (Delso-Vicente et al., 2025; Triplett, 2023; Ayanwale et al., 2023).

Delay is no longer an option. The societal harms already triggered (from widespread disinformation to deviant behavioral patterns) have set in motion processes that become increasingly difficult to reverse with every passing year. Ultimately, if the states of the transatlantic region fail to address these educational and awareness deficits, the resulting asymmetries will not only weaken their own resilience but risk handing a decisive institutional advantage to adversarial powers, thereby jeopardising the very identity and values the region claims to defend.

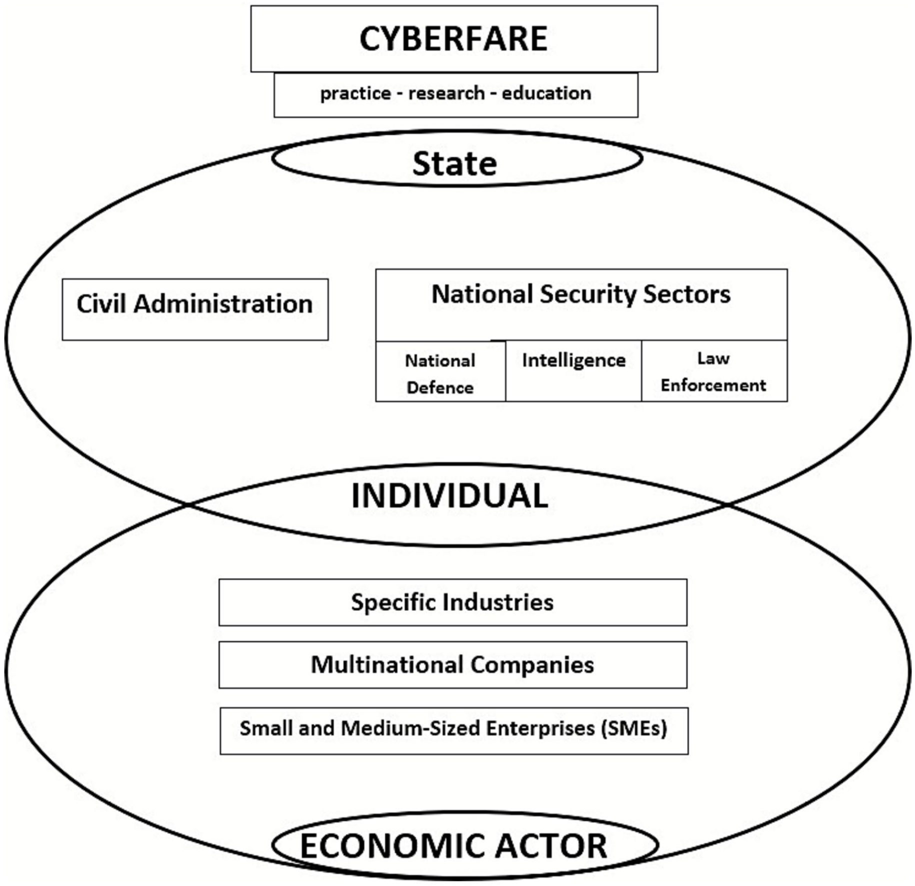

FIGURE 3
Individual active participation in the cooperating model detailed representation of the cooperating Cyberfare State showing the individual as an active participant rather than a passive object. The individual contributes to national security through personal asset and data protection practices while simultaneously interacting with state and economic subsystems. Source: Own elaboration.

5 Conclusion

The Cyberfare State emerges in two distinct forms. The smart total-control variant revives warfare-state logic, fusing state and corporate power to achieve maximum surveillance and offensive cyber capability. In contrast, the cooperating Cyberfare State—the only viable path for rule-of-law democracies – rests on continuous, rights-compliant interaction between state, private sector, and citizens.

This cooperation cannot remain declaratory. The digitalisation of welfare and public administration has already created the foundations; the new security environment now demands their rapid transformation into a systemic, long-term resilience architecture. Sporadic awareness campaigns and outdated regulatory reflexes are no longer sufficient. What is required is comprehensive reform that embeds cybersecurity competencies at every level of education, synchronises security culture across society, and institutionalises multi-stakeholder co-production of national security – all while preserving democratic constraints.

Delay is not an option. The Russian–Ukrainian war and escalating hybrid threats have made clear that incremental adjustments of old models will not suffice. Only by fully embracing the cooperating cyberfare paradigm—and redefining the state's role accordingly—can transatlantic democracies prevent irreversible societal damage and avoid ceding decisive institutional advantage to their authoritarian rivals.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

RK: Conceptualization, Methodology, Visualization, Writing – original draft, Writing – review & editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. The Article Processing Charge (APC) for this publication was funded by Széchenyi István University.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Acton, J. M. (2020). Cyber warfare & inadvertent escalation. *Daedalus* 149, 133–149. doi: 10.1162/DAED_a_01794

Addo, A., and Senyo, P. K. (2021). Advancing e-governance for development: digital identification and its link to socioeconomic inclusion. *Gov. Inf. Q.* 38:101568. doi: 10.1016/j.giq.2021.101568

Ahmad, S. F., Alam, M. M., and Rahman, S. (2021). Artificial intelligence and its role in education. *Sustainability* 13:12902. doi: 10.3390/su132212902

Aho, B. A., and Duffield, M. R. (2020). Beyond surveillance capitalism: privacy, regulation and big data in Europe and China. *Econ. Soc.* 49, 495–513. doi: 10.1080/03085147.2020.1837583

Al Dahdah, M., and Mishra, R. K. (2023). Digital health for all: the turn to digitized healthcare in India. *Soc. Sci. Med.* 319:114968. doi: 10.1016/j.socscimed.2022.114968

Alahi, M. E. E., Sifat, K. A., and Pervin, S. (2023). Integration of IoT-enabled technologies and artificial intelligence (AI) for smart healthcare. *Sensors* 23:3691. doi: 10.3390/s23073691

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Comput. Secur.* 132:104329. doi: 10.1016/j.cose.2025.104329

Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., et al. (2023). Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC Med. Educ.* 23:689. doi: 10.1186/s12909-023-04698-z

Alshamy, Y., Coyne, C. J., Hall, A. R., and Owens, M. A. (2024). Surveillance capitalism and the surveillance state: a comparative institutional analysis. *Constit. Polit. Econ.* doi: 10.1007/s10602-024-09438-z

Alsharida, R. A., Arooj, A., and Farooq, M. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technol. Soc.* 73:102237. doi: 10.1016/j.techsoc.2023.102237

Alshehri, F., and Muhammad, G. (2021). A comprehensive survey of the internet of things (IoT) and AI-based smart healthcare. *IEEE Access* 9, 3660–3678. doi: 10.1109/ACCESS.2020.3047960

Alvarenga, A., Matos, F., Godina, R., and Azevedo, S. G. (2020). Digital transformation and knowledge Management in the Public Sector. *Sustainability* 12:5824. doi: 10.3390/su12145824

Aro, J. (2021). Putin's trolls: on the frontlines of Russia's information war against the world. London: Ig Publishing.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature* 574, 505–510. doi: 10.1038/s41586-019-1666-5

Asfahani, A. M. (2024). Behind the digital veil: decoding the influence of HR training on information security awareness in Saudi Arabia. *Cogent Bus Manag* 11:2395430. doi: 10.1080/23311975.2024.2323389

Avaaz. (2019). Yellow vests flooded by fake news – Over 100M views of disinformation on Facebook. Avaaz report. Available online at: https://avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf (accessed November 17, 2025).

Ayanwale, M. A., Oladele, O. J., and Sanusi, I. T. (2023). A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education. *Educ. Inf. Technol.* 28, 11147–11167. doi: 10.1007/s10639-023-11662-1

Bachmann, S.-D., and Gunneriusson, H. (2015). Hybrid wars: the 21st century's new threats to global peace and security. *S. Afr. J. Mil. Stud.* 43, 77–98. doi: 10.5787/43-1-1110

Bachmann, S.-D., and Gunneriusson, H. (2023). Hybrid warfare and disinformation: a Ukraine war perspective. *Glob. Policy* 14, 443–452. doi: 10.1111/1758-5899.13233

Baud, I., Scott, D., Pfeffer, K., Sydenstricker-Neto, J., and Denis, E. (2014). Digital and spatial knowledge management in urban governance: emerging issues in India, Brazil, South Africa, and Peru. *Habitat Int.* 44, 501–509. doi: 10.1016/j.habitatint.2014.09.009

Berigüete, F. E., and Rivas, R. L. (2024). Digital revolution: emerging technologies for enhancing citizen engagement in urban and environmental management. *Land* 13:638. doi: 10.3390/land13050638

Bhatia, M., and Pallvi (2025). Mapping emerging digital technologies in defense: a scientometric and systematic review. *IEEE Internet Things J.* 12, 32725–32748. doi: 10.1109/jiot.2025.3579067

Birch, K., and dos Santos, L. F. P. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by big tech. *Big Data Soc.* 8:20539517211017308. doi: 10.1177/20539517211017397

Björklund, F. (2016). E-government and moral citizenship: the case of Estonia. *Citizenship Stud.* 20, 914–931. doi: 10.1080/13621025.2016.1213222

Brantly, A. F., Cal, N. M., and Winkelstein, D. P. (2017). Defending the borderland: Ukrainian military experiences with IO, cyber, and EW. West Point, NY: Army Cyber Institute.

Briggs, A. (2006). "The welfare state in historical perspective" in The welfare state reader. eds. C. Pierson and F. G. Castel. Second ed (Cambridge: Polity Press), 16–30.

Calderaro, A., and Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Q.* 41, 917–938. doi: 10.1080/01436597.2020.1729729

Carrapico, H., and Farrand, B. (2024). Cybersecurity trends in the European Union: regulatory mercantilism and the digitalisation of geopolitics. *J. Common Mark. Stud.* 62, 789–805. doi: 10.1111/jcms.13579

Castells, M. (1996). The rise of the network society, the information age: economy, society and culture, vol. 1. Cambridge, MA; Oxford UK: Blackwell.

Celeste, E., and Pollicino, V. L. L. R. L. (2024). Constitutionalizing mass surveillance in the EU: civil society demands, judicial activism, and legislative inertia. *German Law J.* 25, 1–22. doi: 10.1017/glj.2024.1

Chari, R., Petrun Sayers, E. L., Amiri, S., Leinhos, M., Kotzias, V., Madrigano, J., et al. (2019). Enhancing community preparedness: an inventory and analysis of disaster citizen science activities. *BMC Public Health* 19:1356. doi: 10.1186/s12889-019-7689-x

Cheung, A. S. Y., and Shen, Z. Z. (2021). From datafication to data state: making sense of China's social credit system and its implications. *Law Soc. Inquiry* 46, 1111–1140. doi: 10.1017/lsi.2021.28

Collington, R. (2021). Disrupting the welfare state? Digitalisation and the retrenchment of public sector capacity. *New Polit. Econ.* 26, 656–671. doi: 10.1080/13563467.2020.1832047

Cook, F. J. (1964). The warfare state. *Ann. Am. Acad. Polit. Soc. Sci.* 351, 102–109. doi: 10.1177/000271626435100112

Coveri, A., Cozza, C., and Guarascio, D. (2025). Blurring boundaries: an analysis of the digital platforms-military nexus. *Rev. Polit. Econ.* 37, 1632–1663. doi: 10.1080/09538259.2024.2395832

Debnath, R., and Bardhan, R. (2020). India nudges to contain COVID-19 pandemic: a reactive public policy analysis using machine-learning based topic modelling. *PLoS One* 15:e0238175. doi: 10.1371/journal.pone.0238175

del Sánchez Vas, R., and Arcila Calderón, C. (2024). Disinformation on the COVID-19 pandemic and the Russia-Ukraine war: two sides of the same coin? *Humanit. Soc. Sci. Commun.* 11:21. doi: 10.1057/s41599-023-02517-z

Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., and de García Blanes Sebastián, M. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Bus. J.* 11:28. doi: 10.1186/s43093-025-00452-7

Department of Justice (2018). North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions. Washington, D.C.: U.S. Department of Justice.

Devanny, J., and Stevens, T. (2022). Strategy in an uncertain domain: threat and response in cyberspace. *J. Strateg. Secur.* 15, 1–15. doi: 10.5038/1944-0472.15.4.2045

Dhaoui, I. (2021). E-government for sustainable development: evidence from MENA countries. *J. Knowl. Econ.* 13, 2070–2099. doi: 10.1007/s13132-021-00791-0

Di Giulio, M., and Vecchi, G. (2021). Implementing digitalization in the public sector. Technologies, agency, and governance. *Public Policy Adm.* 38, 133–158. doi: 10.1177/09520767211023283

Diamond, L. (2019). The road to digital unfreedom: the threat of postmodern totalitarianism. *J. Democr.* 30, 20–24. doi: 10.1353/jod.2019.0063

Dion, M. (2023). Improving workplace and societal cybersecurity via post-secondary general education. *J. Colloq. Inf. Syst. Secur. Educ.* 10, 1–12. doi: 10.53735/cisse.v10i1.162

Doran, N. M., Puiu, S., Bădîrcea, R. M., Pirtea, M. G., Doran, M. D., Ciobanu, G., et al. (2023). E-government development—a key factor in government administration effectiveness in the European Union. *Electronics* 12:641. doi: 10.3390/electronics12030641

Dossi, S. (2020). On the asymmetric advantages of cyberwarfare. Western literature and the Chinese journal Guofang Keji. *J. Strateg. Stud.* doi: 10.1080/01402390.2019.1581613

Dragu, T., and Lupu, Y. (2021). Digital authoritarianism and the future of human rights. *Int. Organ.* 75, 991–1017. doi: 10.1017/S0020818320000624

Dubow, B., Lucas, E., and Morris, J. (2020). Jabbed in the Back: mapping Russian and Chinese information operations during COVID–19. Washington, D.C.: The Center for European Policy Analysis (CEPA).

Dunleavy, P., and Margetts, H. (2023). Data science, artificial intelligence and the third wave of digital era governance. *Public Policy Adm.* 40, 185–214. doi: 10.1177/09520767231198737

Dunleavy, P., Margetts, H., Bastow, S., and Tinkler, J. (2006). Digital era governance: IT corporations, the state, and e-government. Oxford: Oxford University Press.

Earl, J., Maher, T. V., and Pan, J. (2022). The digital repression of social movements, protest, and activism: a synthetic review. *Sci. Adv.* 8:eabl8198. doi: 10.1126/sciadv.abl8198

Edgerton, D. (2006). Warfare state: Britain, 1920–1970. Cambridge: Cambridge University Press.

Egloff, F. J., and Shires, J. (2021). The better angels of our digital nature? Offensive cyber capabilities and state violence. *Eur. J. Int. Secur.* 8, 130–149. doi: 10.1017/eis.2021.20

ENISA. European Union Agency for Cybersecurity. (2018). Cybersecurity culture guidelines: behavioural aspects and awareness. Available online at: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines (Accessed November 17, 2025).

ENISA. European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. Available online at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Accessed November 17, 2025).

Erman, E., and Möller, M. (2022). Artificial intelligence and the political legitimacy of global governance. *Polit. Stud.* 70, 1018–1035. doi: 10.1177/00323217211020739

Esping-Andersen, G. (1990). The three worlds of welfare capitalism. Princeton, NJ: Princeton University Press.

Esping-Andersen, G. (2002). "Why we need a new welfare state" in Why we need a new welfare state. ed. G. Esping-Andersen (Oxford: Oxford University Press), 1–20.

Esping-Andersen, G. (2006). "A welfare state for the twenty-first century" in The welfare state reader. eds. C. Pierson and F. G. Castel. Second ed (Cambridge: Polity Press), 434–448.

FBI Internet Crime Complaint Center (2025). Internet crime report 2024. Washington, D.C.: Federal Bureau of Investigation. Available online at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (Accessed November 17, 2025).

Fenech, J., Richards, D., and Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *Comput. Secur.* 140:103456. doi: 10.1016/j.cose.2024.103456

Freedom House (2020). Freedom on the net 2020: the pandemic's digital shadow. Washington, D.C.: Freedom House.

Fukuyama, F. (2014). Political order and political decay: from the industrial revolution to the globalization of democracy. New York, NY: Farrar, Straus and Giroux.

Ghasiya, P., and Shah, V. (2023). Messaging strategies of Ukraine and Russia on telegram during the 2022 Russian invasion of Ukraine. Chicago, IL: The University of Illinois at Chicago Library, 28.

Ghosh, C., and Chaudhury, R. (2020). Determinants of digital finance in India. *Innov. Dev.* 12, 343–362. doi: 10.1080/2157930X.2020.1850012

Gong, Y., Yang, J., and Shi, X. (2020). Towards a comprehensive understanding of digital transformation in government: analysis of flexibility and enterprise architecture. *Gov. Inf. Q.* 37:101487. doi: 10.1016/j.giq.2020.101487

Gosztonyi, G. (2020). The European court of human rights: internet access as a means of receiving and imparting information and ideas. *Int. Comp. Jurisprud.* 6, 134–140. doi: 10.13165/j.icj.2020.12.003

Gosztonyi, G. (2021). Special models of internet and content regulation on China and Russia. *ELTE Law J.* 9, 87–99. doi: 10.54148/ELTELJ.2021.2.87

Gosztonyi, G. (2023). Censorship from Plato to social media: the complexity of social media's content regulation and moderation practices. Cham: Springer International Publishing.

Gosztonyi, G. (2025). "Try Instagramming in Russia, or the rise of digital authoritarianism" in Kremlin media wars: Censorship and control since the invasion of Ukraine. eds. W. Sloane and A. Raspopina (London: Routledge), 45–56.

Habermas, J. (1984). The theory of communicative action, volume 1: reason and the rationalization of society. Boston, MA: Beacon Press.

Harari, Y. N. (2016). Homo deus: a brief history of tomorrow. London: Harvill Secker.

Harknett, R. J., and Smeets, M. (2020). Cyber campaigns and strategic outcomes. *J. Strateg. Stud.* 45, 534–567. doi: 10.1080/01402390.2020.1732354

Haug, N., Dan, S., and Mergel, I. (2023). Digitally-induced change in the public sector: a systematic review and research agenda. *Public Manag. Rev.* 26, 1963–1987. doi: 10.1080/14719037.2023.2234917

Hjelholt, M. F. (2024). The absorbent digital welfare state: silencing dissent, steering progress. *J. Sociol.* 60, 643–659. doi: 10.1177/14407833241253632

Hofstetter, Y. (2020). The inevitable war: how the digitalization of the world threatens its security and stability. Budapest: Corvina.

Hoofnagle, C. J., van der Sloot, B., and Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Inf. Commun. Technol. Law* 28, 65–98. doi: 10.1080/13600834.2019.1573501

Huang, J., and Chen, C. J. (2022). Securing authoritarian capitalism in the digital age: the political economy of surveillance in China. *China J.* 88, 1–25. doi: 10.1086/719572

Ibrahim, A., Papadaki, M., and Kos, J. (2024). A systematic review of K-12 cybersecurity education around the world. *IEEE Access* 12, 18954–18973. doi: 10.1109/ACCESS.2024.3362825

Kaladjian, G. M. (1996). Welfare vs "Cyberfare." *J. Child. Poverty* 2, 93–104. doi: 10.1080/10796129608414754

Kamalov, F., Calonge, D. S., and Gurrib, I. (2023). New era of artificial intelligence in education: towards a sustainable multifaceted revolution. *Sustainability* 15:8909. doi: 10.3390/su15118909

Kelemen, R., Bucko, B., Mazuch, M., Farkas, Á., and Squillace, J. (2024a). Modernizing Hungary's cybersecurity framework: addressing evolving threats and enhancing National Resilience. *Rechtskultur*, 291–305.

Kelemen, R., and Farkas, Á. (2025). "The connections between social media platforms and hybridity" in Bridging the digital divide: perspectives on inequality and discrimination in the digital age. eds. O. Pérez de la Fuente and J. Skrzypczak (Cham: Springer Nature Switzerland), 105–123.

Kelemen, R., Squillace, J., Farkas, Á., Cappella, J., Altas, A. D., and Németh, R. (2024b). The social impact of disinformation and the European Union's response. *Rechtskultur*, 307–322.

Kelemen, R., Squillace, J., Medvácz, Á., Cappella, J., Bucko, B., and Mazuch, M. (2025). Cybersecurity regulations and software resilience: strengthening awareness and societal stability. *Soc. Sci.* 14:578. doi: 10.3390/socsci14100578

Kello, L. (2021). Cyber legalism: why it fails and what to do about it. *J. Cybersecur.* 7:tyab014. doi: 10.1093/cybsec/tyab012

Kelton, M., and van der Vleuten, E. E. G. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *Int. Aff.* 98, 1637–1655. doi: 10.1093/ia/iiac173

Khan, A., and Krishnan, S. (2021). Citizen engagement in co-creation of e-government services: a process theory view from a meta-synthesis approach. *Internet Res.* 31, 1318–1375. doi: 10.1108/intr-03-2020-0116

Klimburg-Witjes, N., and Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses. *Sci. Technol. Hum. Values* 46, 593–619. doi: 10.1177/0162243920955523

Kovács-Szépvölgyi, E., Tóth, D. A., and Kelemen, R. (2025). From voice to action: upholding children's right to participation in shaping policies and Laws for digital safety and well-being. *Societies* 15:243. doi: 10.3390/soc15090243

Krasner, S. D. (1999). Sovereignty: organized hypocrisy. Princeton, NJ: Princeton University Press.

Kung, C. S. J., and Steptoe, A. (2023). Changes in Internet use patterns among older adults in England from before to after the outbreak of the COVID-19 pandemic. *Sci. Rep.* 13:3932. doi: 10.1038/s41598-023-30882-8

Kurzweil, R. (2005). The singularity is near: when humans transcend biology. New York, NY: Viking Penguin.

Lagna, A., and Ravishankar, M. N. (2021). Making the world a better place with Fintech research. *Inf. Syst. J.* 32, 102–161. doi: 10.1111/isj.12333

Lakhtakia, T., Bondre, A., Chand, P. K., Chaturvedi, N., Choudhary, S., Currey, D., et al. (2022). Smartphone digital phenotyping, surveys, and cognitive assessments for global mental health: initial data and clinical correlations from an international first episode psychosis study. *Digit. Health* 8:20552076221133758. doi: 10.1177/20552076221133758

Leal Neto, O. B., Cruz, O., Albuquerque, J., de Nacarato Sousa, M., Smolinski, M., Pessoa Cesse, E. Â., et al. (2020). Participatory surveillance based on crowdsourcing during the Rio 2016 Olympic games using the guardians of health platform: descriptive study. *JMIR Public Health Surveill.* 6:e16119. doi: 10.2196/16119

Lee, C. S., and Sobol, M. A. (2021). Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. *J. Contemp. Crim. Justice* 37, 512–535. doi: 10.1177/10439862211029191

Leiserson, C. E., Thompson, N. C., Emer, J. S., Kuszmaul, B. C., Lampson, B. W., Sanchez, D., et al. (2020). There's plenty of room at the top: what will drive computer performance after Moore's law? *Science* 368:eaam9744. doi: 10.1126/science.aam9744

Lember, V., Kattel, R., and Tõnurist, P. (2018). Technological capacity in the public sector: the case of Estonia. *Int. Rev. Adm. Sci.* 84, 214–230. doi: 10.1177/0020852317735164

Lim, A. C. Y., Natarajan, P., Fonseka, R. D., Maharaj, M., and Mobbs, R. J. (2022). The application of artificial intelligence and custom algorithms with inertial wearable devices for gait analysis and detection of gait-altering pathologies in adults: a scoping review of literature. *Digit. Health* 8:20552076221074128. doi: 10.1177/20552076221074128

Lin, C.-C., and Huang, C.-S. (2023). Artificial intelligence in intelligent tutoring systems toward sustainable education: a systematic review. *Smart Learn. Environ.* 10:24. doi: 10.1186/s40561-023-00244-y

Litvinenko, A. A. (2021). Re-defining borders online: Russia's strategic narrative on internet sovereignty. *Media Commun.* 9, 206–216. doi: 10.17645/mac.v9i1.3364

Lukács, G. (1971). History and class consciousness: Studies in Marxist dialectics. Cambridge, MA: MIT Press.

Lundstrom, M. (2022). Moore's law: the journey ahead. *Science* 377, 1050–1051. doi: 10.1126/science.add9775

Maclean, D., and Titah, R. (2021). A systematic literature review of empirical research on the impacts of e-government: a public value perspective. *Public Adm. Rev.* 82, 23–38. doi: 10.1111/puar.13413

Makanadar, A. (2024). Digital surveillance capitalism and cities: data, democracy and activism. *Humanit. Soc. Sci. Commun.* 11:212. doi: 10.1057/s41599-024-02720-6

Makela, J. (2019). Countering disinformation: news media and legal resilience. Hybrid CoE paper. 1/2019. Helsinki: The European Centre of Excellence for Countering Hybrid Threats.

Malkowski, O. S., Townsend, N. P., Kelson, M. J., Foster, C. E., and Western, M. J. (2024). Socio-economic inequalities in the breadth of internet use before and during the COVID-19 pandemic among older adults in England. *PLoS One* 19:e0287654. doi: 10.1371/journal.pone.0287654

Marigliano, R., Zerman, M., Quattrociocchi, W., and Giglietto, F. (2024). Analyzing digital propaganda and conflict rhetoric: a study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis. *Soc. Netw. Anal. Min.* 14:48. doi: 10.1007/s13278-024-01185-3

Martin, J., and Holt, T. J. (2023). Ransomware through the lens of state crime: conceptualizing ransomware groups as cyber proxies, pirates, and privateers. *State Crime J.* 12, 5–27. doi: 10.13169/statecrime.12.1.0005

Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data Soc.* 10, 1–5. doi: 10.1177/20539517221135176

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics* 38, 114–117.

Moore, G. J. (2022). Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies. *J. Chin. Polit. Sci.* 27, 485–506. doi: 10.1007/s11366-022-09797-1

Morrison, B., Nicholson, J., Wood, B., and Briggs, P. (2023). Life after lockdown: the experiences of older adults in a contactless digital world. *Front. Psychol.* 14:112233. doi: 10.3389/fpsyg.2023.112233

Mosco, V. (2019). The Smart City in a digital world. Bingley: Emerald Publishing Limited.

Nobles, C., and Mcandrew, I. (2023). The intersectionality of offensive cybersecurity and human factors: a position paper. *Sci. Bull.* 28, 215–233. doi: 10.2478/bsaft-2023-0022

Nozick, R. (1974). Anarchy, state, and utopia. New York, NY: Basic Books.

Nwankpa, J. K., and Datta, P. (2023). Remote vigilance: the roles of cyber awareness and cybersecurity policies among remote workers. *Comput. Secur.* 126:103456. doi: 10.1016/j.cose.2023.103456

Pariser, E. (2011). The filter bubble: what the internet is hiding from you. London: Penguin UK.

Păunescu, D.-M. (2021). "NATO'S encounters in the cyber domain" in Strategies XXI—security and defense, Vol. 2, eds. G. V. Văduva and S. Văduva (Bucharest: "Carol I" National Defence University Publishing House) 237–248.

Pierson, C. (2006). "The new politics of the welfare state" in The welfare state reader. eds. C. Pierson and F. G. Castel. Second ed (Cambridge: Polity Press), 449–460.

Pohle, J., and Thiel, T. (2020). Digital sovereignty. *Internet Policy Rev.* 9. doi: 10.14763/2020.4.1532

Pors, A., and Schou, J. (2021). Street-level morality at the digital frontlines: an ethnographic study of moral mediation in welfare work. *Adm. Theory Prax.* 43, 154–171. doi: 10.1080/10841806.2020.1782137

Porter, B. D. (1994). War and the rise of the state: the military foundations of modern politics. New York, NY: The Free Press.

Ramezanian, S., Gallo, T., and Khan, M. S. (2024). Cybersecurity education in universities: a comprehensive guide to curriculum development. *IEEE Access* 12, 27309–27327. doi: 10.1109/ACCESS.2024.3365123

Reporters Without Borders (2016). Iran creates "halal internet" to control online information. Available online at: https://rsf.org/en/news/iran-creates-halal-internet-control-online-information (Accessed November 17, 2025).

Rasmussen, M., and Erickson, C. (2025). "From elements to effects: the strategic imperative to understand "national cyber power"," *International Conference on Cyber Warfare and Security.* doi: 10.34190/iccws.20.1.3365

Riad, A., Bahavan, B., and Koščík, M. (2025). From institutional trust to digital literacy: socioeconomic and political determinants of COVID-19 vaccine hesitancy among Czech adults based on a national panel survey. *Hum. Vaccin. Immunother.* 21:2533639. doi: 10.1080/21645515.2025.1234567

Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., et al. (2024). Understanding cybersecurity education gaps in Europe. *IEEE Trans. Educ.* 67, 123–134. doi: 10.1109/TE.2024.1234567

Rosenstedt, L. (2021). Improving cooperation with social media companies to counter electoral interference. Hybrid CoE paper. 5/2021. Helsinki: The European Centre of Excellence for Countering Hybrid Threats.

Ruggiero, A., and Laine, M. T. (2024). Enhancing societal resilience through the whole-of-society approach to crisis preparedness: complex adaptive systems perspective—the case of Finland. *Int. J. Disaster Risk Reduct.* 101:104696. doi: 10.1016/j.ijdrr.2024.104696

Sari, A. (2020). Legal resilience in an era of grey zone conflicts and hybrid threats. *Cambridge Rev. Int. Aff.* 33, 636–655. doi: 10.1080/09557571.2020.1760456

Schlumberger, O., Edel, M., Maati, A., and Saglam, K. (2023). How authoritarianism transforms: a framework for the study of digital dictatorship. *Gov. Oppos.* 59:761. doi: 10.1017/gov.2023.20

Segal, A. (2020). "China's vision for cyber sovereignty and the global governance of cyberspace" in An emerging China-centric order: China's vision for a New World order in practice. ed. N. Rolland (The National Bureau of Asian Research: Seattle, WA), 83–102.

Sharma, S., Kar, A., Gupta, M., Dwivedi, Y., and Janssen, M. (2022). Digital citizen empowerment: a systematic literature review of theories and development models. *Inf. Technol. Dev.* 28, 660–687. doi: 10.1080/02681102.2022.2046533

SLAC National Accelerator Laboratory. (2022). LSST camera: world's largest camera for astrophysics. Available online at: https://www6.slac.stanford.edu/lsst (Accessed November 17, 2025).

Smeets, M. (2022). No shortcuts: why states struggle to develop a military cyber-force. Oxford: Oxford University Press.

Sparrow, J. T. (2011). Warfare state: world war II Americans and the age of big government. Oxford: Oxford University Press.

Splidsboel Hansen, F. (2021). When Russia wages war in the cognitive domain. *J. Slav. Mil. Stud.* 34, 491–511. doi: 10.1080/13518046.2021.2003884

Sun, N., Zhang, J., and Quirchmayr, G. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. *IEEE Commun Surv Tutor* 25, 1334–1365. doi: 10.1109/COMST.2023.3262283

Szigeti, P. (2001). 'Vázlat a közbiztonság három dimenziójáról: világrendszer – nemzetállami szint és lokalitás', in A valóság vonzásában – Jogelméleti és Jogtudományi Közlöny. Győr: ELTE–SZIF ÁJK.

Talukder, K. A., and Hossain, M. A. (2024). Artificial intelligence in criminal justice management: a systematic literature review. *Non Hum. J.* 4, 1–15. doi: 10.70008/jmldeds.v1i01.42

Tangi, L., Janssen, M., Benedetti, M., and Noci, G. (2021). Digital government transformation: a structural equation modelling analysis of driving and impeding factors. *Int. J. Inf. Manag.* 60:102356. doi: 10.1016/j.ijinfomgt.2021.102356

Titmuss, R. (2006). "Universal versus selection" in The welfare state reader. eds. C. Pierson and F. G. Castel. Second ed (Cambridge: Polity Press), 42–50.

Törnberg, P. (2023). How platforms govern: social regulation in digital capitalism. *Big Data Soc.* 10:20539517231153808. doi: 10.1177/20539517231153808

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *Int. J. STEM Educ.* 10:58. doi: 10.1186/s40594-023-00448-5

Unni, J., and Dev, P. (2021). How macroeconomic shocks impact employment: comparison of Gujarat with states in Western India. *J. Soc. Econ. Dev.* 23, 199–211. doi: 10.1007/s40847-020-00123-z

van Kessel, R., Haig, M., and Mossialos, E. (2023). Strengthening cybersecurity for patient data protection in Europe. *J. Med. Internet Res.* 25:e50513. doi: 10.2196/50513

van Toorn, G., Henman, P., and Soldatić, K. (2024). Introduction to the digital welfare state: contestations, considerations and entanglements. *J. Sociol.* 60, 507–522. doi: 10.1177/14407833241260890

Videnovik, M., Zdravevski, E., Lameski, P., and Trajkovik, V. (2025). Using peer-learning and game-based instruction for achieving long-lasting knowledge of cybersecurity in primary schools. *IEEE Access* 13, 12345–12367. doi: 10.1109/ACCESS.2025.3367890

Voorberg, W. H., Bekkers, V. J. J. M., and Tummers, L. G. (2014). A systematic review of co-creation and co-production: embarking on the social innovation journey. *Public Manag. Rev.* 17, 1333–1357. doi: 10.1080/14719037.2014.930505

Weitzberg, K., Cheesman, M., Martin, A., and Schoemaker, E. (2021). Between surveillance and recognition: rethinking digital identity in aid. *Big Data Soc.*:20539517211006744, 1–7. doi: 10.1177/20539517211006744

Whitford, T., and Prunckun, H. W. (2025). Public trust in Australia's law enforcement agencies and collecting national security intelligence data. *Int. J. Intell. Counterintell.* 38, 209–232. doi: 10.1080/08850607.2024.2431524

Whitty, M., Moustafa, N., and Grobler, M. (2024). Cybersecurity when working from home during COVID-19: considering the human factors. *J. Cybersecur.* 10:tyae001. doi: 10.1093/cybsec/tyae001

WHO (World Health Organization). (2020). Infodemic. Available online at: https://www.who.int/health-topics/infodemic (Accessed November 17, 2025).

Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *J. Cybersecur.* 6:tyaa013. doi: 10.1093/cybsec/tyaa013

Willett, M. (2022). The cyber dimension of the Russia–Ukraine war. *Survival* 64, 7–40. doi: 10.1080/00396338.2022.2081512

World Economic Forum (2020). The future of jobs report 2020. Geneva: World Economic Forum.

Xu, Y., Wang, X., and Li, Z. (2025). Cybersecurity matters for primary school students: a scoping review of the trends, challenges, and opportunities. *IEEE Trans. Learn. Technol.* 18, 45–60. doi: 10.1109/TLT.2025.3367891

Yang, C., Gu, M., and Albitar, K. (2024). Government in the digital age: exploring the impact of digital transformation on governmental efficiency. *Technol. Forecast. Soc. Change* 208:123722. doi: 10.1016/j.techfore.2024.123722

Yin, J., and Lu, W. (2023). Does the perception of smart governance enhance commercial investments? Evidence from Beijing, Shanghai, Guangzhou, and Hangzhou. *Heliyon* 9:e22709. doi: 10.1016/j.heliyon.2023.e22709

Zamani, E., and Gheybari, A. (2022). Artificial intelligence and big data analytics for supply chain resilience: a systematic literature review. *Ann. Oper. Res.* doi: 10.1007/s10479-022-04875-z

Zhong, H. S., Deng, Y. H., Qin, J., Wang, H., Chen, M. C., Peng, L. C., et al. (2021). Phase-programmable Gaussian Boson sampling using stimulated quantum light. *Phys. Rev. Lett.* 127:180502. doi: 10.1103/PhysRevLett.127.180502

Zimmermann, A., Vredenburgh, K., and Lazar, S. (2022). The political philosophy of data and AI. *Can. J. Philos.* 52, 1–5. doi: 10.1017/can.2022.28

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* 30, 75–89. doi: 10.1057/jit.2015.5