⇨ Max Tretter

Digital Sovereignty and Video Games

⇨ 1 Introduction

Power grids, financial databases, and even public discourse—discussions of digital sovereignty typically focus on systems considered essential to societal stability. These include not only tangible infrastructures whose failure would have catastrophic consequences, but also less visible arenas like political opinion-making, which are increasingly shaped (and threatened) by digital control, surveillance, and manipulation. At its core, debates over digital sovereignty usually revolve around vulnerability and control—on the question of who holds power through digital means, who can exercise it, and who is at risk of losing it.

But what happens when we shift our attention to a domain that has, so far, played only a marginal role in these debates: video games? While games are no longer regarded as »mere entertainment« and their political dimensions are increasingly recognized (Dyer-Witheford/de Peuter 2009; Nardone 2017; Spies et al. 2024; Tretter 2017; Wolf/Perron 2023), their connection to digital sovereignty has, to date, remained largely unexplored. Perhaps this is because, at first glance, the medium still appears too trivial, too peripheral, and not »systemically relevant« enough. And yet, numerous reports have already highlighted, and continue to emphasize, how video games function as platforms for information exchange, arenas for the circulation of ideology and propaganda, and sites of substantial economic power (Dyer-Witheford/de Peuter 2009; Murray

Max Tretter, *1993, Dr. theol., Studium der Evangelisch-Lutherischen Theologie in Erlangen und Berlin, Promotionsstudium in Erlangen und Berkeley, USA, Wissenschaftlicher Mitarbeiter am Lehrstuhl für Systematische Theologie (Ethik) an der Friedrich-Alexander-Universität Erlangen-Nürnberg. Wichtige Veröffentlichungen: *Hip-Hop bei* Black Lives Matter *Protesten. Eine theologisch-ethische Auseinandersetzung mit ästhetischen Artikulationsformen in der Öffentlichkeit* (Perspektiven der Ethik). Mohr Siebeck, Tübingen 2025. https://doi.org/10.1628/978-3-16-164365-1 (*Open Access*); More Hip Hop, please! Exploring the Intersections of Public Theology and Hip Hop Studies, in: *International Journal of Public Theology* 19 (4), 2025, 320–344, https://doi.org/10.1163/15697320-20250007; Sovereignty in the Digital and Contact Tracing Apps, in: *Digital Society* 2 (2), 2022, https://doi.org/10.1007/s44206-022-00030-2; (mit Patrik Hummel, Matthias Braun, Peter Dabrock) Data Sovereignty. A Review, in: *Big Data & Society*,2021, https://doi.org/10.1177/2053951720982012; (mit Anna Puzio) Red Lines for Religious AI, in: *Nature* 646 (550), 2025, https://doi.org/ 10.1038/d41586-025-03359-z
ORCID: 0000-0001-8067-247X

DOI: 10.18156/eug-1-2026-art-8

2021; Payne 2016). This suggests that video games may be far more relevant to societal stability than commonly assumed, and that it may, in fact, be both timely and necessary to explore their relationship to digital sovereignty.

That's why this article sets out to explore what new insights emerge when the concept of digital sovereignty is brought into dialogue with video games. It begins with a sociological diagnosis of the present, drawing on Luciano Floridi's concept of the »Onlife«. This concept effectively captures the increasing entanglement of digital and analog spheres, along with the novel opportunities and vulnerabilities that emerge from this hybrid condition. Building on this foundation, the article develops a conceptual framework for digital sovereignty—one that accounts for the complexity of the term while foregrounding its strategic role: addressing the vulnerabilities that arise in an Onlife world. These theoretical reflections provide the groundwork for the subsequent analysis of how video games intersect with digital sovereignty. In a final step, the article examines how video games intersect with digital sovereignty—by shaping information control, enabling influence, and reflecting structural dependencies—before concluding with a synthesis of key insights.[1]

⇨ 2 Onlife: The Entanglement of Analog and Digital Worlds

A defining feature of contemporary digital societies is the increasing erosion of the boundary between what was once strictly divided into »analog« and »digital« domains. In *The Fourth Revolution*, philosopher Luciano Floridi introduces the concept of *Onlife*—a portmanteau of »online« and »life«—to describe this deep integration of physical and virtual spheres (Floridi 2014). According to Floridi, this integration has become so pervasive that the very distinction between two separate realms no longer holds: the digital is inseparable from its analog foundations, and the analog itself is no longer functional without digital connectivity. What has emerged, he argues, is a hybrid reality in which both spheres are inextricably intertwined: the *Onlife*. And it is precisely this

(1) The initial focus on the Onlife condition and its vulnerabilities may seem somewhat distant from the article's central topic: Video games and digital sovereignty. However, this conceptual framing is crucial as without it, the significance of the later analysis would remain way more difficult to grasp. This theoretical foundation is therefore not a detour but a necessary step toward analytical clarity.

condition that produces several new forms of vulnerability that are affecting not just individuals, but society as a whole.

The impact of the Onlife world becomes tangible in countless everyday examples. Many sectors once regarded as paradigmatically analog are now so thoroughly digitized that the line between »offline« and »online« can hardly be upheld. To illustrate the depth of this entanglement, I will examine three domains: energy, finance, and public discourse.[2]

Take the energy sector: Power plants, electricity grids, gas pipelines, and fuel depots have long been regarded as fundamentally analog, anchored in physical infrastructures, raw materials, and mechanical processes. Yet a closer look at today's energy systems reveals that what once appeared to be a purely analog sector has become a digitally entangled ecosystem. Modern energy systems depend on a complex, digitally coordinated interaction between real-time data, predictive modeling, and automated control mechanisms (Vijayalakshmi et al. 2025).

Smart meters track consumption; solar panels return electricity to the grid via networked interfaces; households adjust their usage through app-based systems and data-driven incentives. Even basic energy usage is now digitally mediated and algorithmically optimized. Moreover, this transformation extends far beyond user behavior. Providers rely on continuous feedback on consumption patterns, production levels, and grid stability to make flexible, real-time adjustments. Only when these digital feedback loops operate reliably can systems respond swiftly to spikes in demand—whether triggered by weather fluctuations, major events, or infrastructure strain—or redirect surplus energy into storage during off-peak periods. The term »smart grid« refers precisely to this digitally networked infrastructure that dynamically balances supply and demand across decentralized systems. Renewable energy sources like solar and wind are monitored, evaluated, and integrated into grid operations in real time. Electricity no longer flows unidirectionally from power plants to consumers but is embedded in a bidirectional system that fundamentally depends on digital communication (Buchholz/Styczynski 2020).[3]

(2) These examples have been chosen deliberately, as each is grounded in a different kind of foundation: The energy sector appears more »material«, rooted strongly in physical resources and infrastructures; the public sphere more »symbolic«, relying on flows of information and trust; and the financial sector occupies a hybrid position between the two. Taken together, these three domains capture the full spectrum of contemporary digital entwinement in society.
(3) With the continued expansion of electric mobility—through electric vehicles, charging infrastructure, and home battery systems—the interplay between fluctuating energy supply and

The second example, the financial and banking sector, differs from the energy sector in its functional logic. While the energy sector is inherently tied to the maintenance of tangible hardware like power grids and cables, the financial sector has undergone a process of dematerialization regarding its core object: value. Since currency was decoupled from material standards like gold, finance operates primarily through informational flows and institutional credibility (Türcke 2015). Although it still relies on a physical technological substrate, e.g., servers, fiber-optic cables, its product is no longer a material commodity but an informational construct. This more symbolic reliance on information and trust has made the financial system especially susceptible to digital transformation (Wewege/Thomsett 2020). Over the past few decades, new technologies have reconfigured how money circulates, how value is stored, and how the flows of financial information, that are necessary for the system to work, are managed. The widespread adoption of debit and credit cards in the late 20th century marked a pivotal shift: Transactions that previously required physical presence and the exchange of money could now take place digitally—quickly, conveniently, and independent of location. Since then, payment behaviors have undergone a fundamental transformation. In many countries, digital payments now outpace cash transactions, while in others, cashless methods—whether by card, smartphone, or platforms such as *Apple Pay*, *Google Pay*, *PayPal*, *WeChat*, or *Alipay*—have long been the norm (Statista 2024). Even where cash is still used by some individuals, their banking records are stored almost exclusively in digital form.

All of this underscores a crucial point: the informational architecture on which the financial and banking system depends now operates predominantly through digital infrastructures. In this context, it is hardly surprising that purely digital currencies like *Bitcoin*, *Ethereum*, and other blockchain-based cryptocurrencies have gained significant traction. Promising faster transactions, greater trust through claims of radical informational transparency (Tapscott/Tapscott 2016; Werbach 2018)—claims that remain the subject of ongoing debate—, and a degree of resilience to manipulation or volatility tied to national

increasingly dynamic demand is growing more complex. The smart grids of the future must be able to handle pronounced load peaks—for instance, when large numbers of vehicles connect to the grid simultaneously after work—as well as highly variable feed-ins from renewable sources. This becomes even more critical if electric vehicles are not only consumers of electricity but also function as mobile storage units integrated into the grid. Without digital control, precise data collection, and automated feedback systems, this form of energy management is simply no longer feasible. See: İnci et al. (2024).

economies, they exemplify the ongoing transformation of financial systems (Lee Kuo Chuen 2024). Current debates surrounding central bank digital currencies and the future of cash further underscore just how profound this digital shift has become (Bilotta/Botti 2021).[4]

The third example, public discourse, is grounded almost entirely in symbolic structures like shared meanings and communicative trust.[5] It is through public discourse that societies interpret events, formulate ideas, and shape political opinion. Journalism, critical media commentary, and everyday communication are central to this process, and their role has long been regarded as vital to democratic life (Habermas 2011). With the rise of digital media, however, this sphere has undergone a profound transformation (Seeliger/Sevignani 2021). Traditional gatekeepers such as newspapers, broadcast networks, and editorial boards have lost their monopoly on agenda-setting and credibility. Instead, online platforms, especially social media, now serve as primary arenas for political meaning-making, public deliberation, and information dissemination for many users.

This shift has fundamentally altered the dynamics of visibility, attention, and trust. Information no longer spreads through editorial hierarchies but through algorithmic amplification, network effects, and virality—with both positive and negative consequences (Habermas 2023). On the one hand, digital platforms have enabled more participatory and decentralized forms of communication: More voices can be heard, barriers to expression are lowered, and movements like the Arab Spring have demonstrated how social media can empower democratic uprisings. On the other hand, the fragmentation of the information space,

(4) Debates over the phasing out of cash have been ongoing for years across Europe and beyond. Proponents such as Kenneth Rogoff (2016) view the shift as a step toward more efficient and transparent payment systems—particularly in combating money laundering and tax evasion. However, critics like, for instance, Brett Scott (2022) warn of the potential loss of financial anonymity, the expansion of surveillance infrastructures, and growing dependence on digital platforms. While the European Central Bank has emphasized that the proposed »digital euro« is intended to complement, not replace, cash, many observers interpret its introduction as a possible steppingstone toward a gradual elimination of physical currency. See: Passacantando (2021).

(5) Of course, public discourse has historically relied on physical media—newspaper print, ink, and printing presses among them. Yet these material conditions were far less central than in the energy or financial sectors. The core elements of public discourse—information, narrative, and exchange—could, as research on orality has shown, also unfold without physical infrastructures, relying instead on verbal communication and collective memory. See: Ong/Hartley (2012).

combined with the influence of algorithmic filtering, has led to phenomena commonly called »filter bubbles« and »echo chambers« (Pariser 2011), as well as the growing prevalence of so-called »alternative facts« and what has been described as a broader »post-truth« condition (McIntyre 2018). In this environment, emotional resonance, shareability, and platform logic often take precedence over factual accuracy and journalistic standards (Seeliger/Sevignani 2021). These dynamics in public discourse pose a serious challenge to social trust and democratic cohesion (Habermas 2023)—a development that was particularly evident during the COVID-19 pandemic.

The three examples discussed—energy, finance, and public discourse—could easily be expanded. Public administration, while still grappling with challenges around digitization, increasingly relies on digital systems (Tretter 2025). In education, digital platforms and AI-based applications shape teaching and learning processes (Shchokin et al. 2024); in the economy, global logistics, production, and transportation would grind to a halt without seamless digital connectivity (Karakitsiou et al. 2024). Infrastructure and mobility, too, have become digitally mediated and dependent on networked control systems, from traffic management (Flügge 2017) to smart city planning (McQueen et al. 2024). And in the realm of defense, cybersecurity, drone operations, and AI-driven situational analysis have long become routine (Kunkel 2024; Scharre 2020)—regularly evidenced in reports from »conflicts« in Ukraine and the Middle East. Across these domains, one insight stands out: contemporary society is deeply embedded in digital infrastructures. From individuals who feel »naked« without their smartphones to corporations, regional systems, and national services—society has, in every respect, become thoroughly Onlife.

⇨ 3 The Vulnerabilities of an Onlife Society

The emergence of an Onlife society has brought about significant gains. It has enabled major increases in efficiency—just consider how few aspects of daily life still operate without digital tools. It has introduced greater flexibility and helped bridge investment gaps, especially where digital services can temporarily compensate for shortages of, for instance, teachers or skilled professionals—though this kind of substitution should certainly not be mistaken for a »cheap« or » technosolutionist« quick fix (Morozov 2013).

At the same time, the growing digitization of everyday systems introduces new and often unprecedented societal vulnerabilities. This is

especially apparent in critical infrastructures such as the energy sector. As power grids increasingly rely on digital control systems, they present a larger and more accessible attack surface for malicious actors. Physical sabotage is no longer required—accessing a control center remotely may be all it takes to cause real-world damage. Hackers can overload systems, triggering breakdowns that are costly and time-consuming to fix, or disable key infrastructure by corrupting control mechanisms (Devi et al. 2022). Numerous examples illustrate this vulnerability: the 2015 and 2016 attacks on Ukraine's power grid, in which hackers deliberately took substations offline and disconnected tens of thousands of households from the grid (Zetter 2016a); the 2020 blackout in Mumbai, which was long suspected to have been caused by a cyberattack, potentially even involving foreign state actors (Naik 2021); or the 2021 ransomware attack on the *Colonial Pipeline*, one of the main fuel supply lines for the US East Coast, which led to shortages and sparked panic buying (Easterly 2023). These cases underscore just how directly digital attacks can now impact physical infrastructure, and how real the associated risks have become.

Given its profound dependence on digital transactions, the financial sector is no less vulnerable than the energy sector. As money is increasingly managed through online bank accounts and mobile wallets rather than physical exchange, new attack surfaces emerge. Hackers can exploit these systems at multiple levels. A high-profile case occurred in 2023, when the cryptocurrency exchange *Bybit* suffered a major breach: allegedly carried out by the North Korean *Lazarus Group*, Ethereum coins worth around $1.5 billion were stolen (Tidy 2025). The attack exploited a vulnerability in the platform's wallet management and is considered »the largest crypto hack of all time« (UNFASSBAR 2025), and sent shockwaves through global markets. Other notable incidents include the $600 million hack of the *Ronin Network* in 2022 (Tidy 2022) and the infamous collapse of *Mt. Gox* in 2014, when up to 950,000 Bitcoins »vanished« (Browne & Sigalos 2024). Even government institutions have been affected. In 2016, hackers attempted to divert nearly $1 billion from the *Central Bank of Bangladesh* via the *SWIFT* network, successfully absconding with $81 million (Zetter 2016b). The *European Central Bank*, too, was targeted in 2019, when malware was placed on one of its websites (Khandelwal 2019). Such cases highlight just how precarious the digital foundations of global finance can be. The idea that critical clearinghouses or national monetary authorities could be

disabled or manipulated is no longer a speculative scenario, it is a tangible risk in the age of the Onlife.[6]

And in the realm of public opinion, too, the vulnerabilities of the Onlife world become particularly evident—especially when it comes to political opinion formation in the context of democratic processes. A well-documented case is the 2016 US presidential election, during which Russian operatives sought to sway public opinion and exacerbate social divisions (Lockhart 2018). Through thousands of fake social media accounts—some run by troll farms, others by bot networks—along with targeted ads and manipulative content, voters were »bombarded« (Rainie/Anderson 2017) with conspiracy theories, racist narratives, and misleading information about voting procedures (Hall Jamieson 2020). While the precise impact on the outcome remains contested, the election is seen by many as a watershed moment in understanding how deeply digital platforms and algorithms can penetrate political processes (Singer/Brooking 2018; Moore 2020). Since then, similar tactics have surfaced globally: in the Brexit referendum, microtargeted campaigns fueled emotional polarization; and in Brazil, India, and the Philippines, disinformation has been weaponized to influence election outcomes and undermine democratic institutions (Prajapati et al. 2024). The Russian invasion of Ukraine followed a comparable playbook as part of their hybrid warfare, launching a parallel information war aimed at discrediting Western narratives and promoting state-sponsored disinformation—such as the false claims that Ukraine was run by Nazis or that Russia was merely conducting a peacekeeping operation (Dov Bachmann et al. 2023). Together, these cases underscore a sobering truth: in a society shaped by Onlife interdependencies, public discourse, political opinion, and democratic decision-making are increasingly exposed to systematic digital manipulation—a structural fragility that challenges the integrity of democratic self-determination.

In short, the Onlife world, where the digital and analog are inseparably entangled, offers significant benefits: increased efficiency across virtually all sectors, greater flexibility, and enhanced dynamism. Yet these

(6) For a vivid illustration of how such a global financial crisis could unfold, the TV series Mr. Robot (USA Network, 2015–2019) is well worth watching. Though fictional, it portrays a disturbingly plausible scenario: a hacker collective deletes the databases of a global financial conglomerate in an effort to erase all debt and upend the global economy. With its technical accuracy and nuanced depiction of society's reliance on digital infrastructures, the series offers a powerful portrayal of how quickly the current financial system could collapse when trust and data vanish at the same time. See: Agulian (2018).

gains come with new vulnerabilities. What is digitally connected can also be digitally manipulated: sensitive data can be extracted, critical systems disrupted, and even physical infrastructure remotely attacked. The promises of the Onlife era are immense—but so are its societal risks.

⇨ 4 Digital Sovereignty: A Concept for Protecting Digital Vulnerabilities

The growing prevalence of digital vulnerabilities has prompted an urgent question: how can societies defend themselves against digital threats? One concept that has gained increasing traction in this context is digital sovereignty. At its core, digital sovereignty is framed as a strategic response to digital insecurity, aiming to shield societies from emerging threats and preserve their long-term stability. No longer confined to academic debates in digital ethics or democratic theory, it has become a strategic point of reference in legislative initiatives and national as well as European digital policy agendas.[7]

At first glance, digital sovereignty may appear to be a clearly defined concept. Upon closer inspection, however, it proves far more complex (Couture/Toupin 2019). While many agree that it serves as a response to digital vulnerabilities, there is little consensus on what forms this response should take, which actors should assume responsibility, or what instruments and strategies are best suited to achieve it. This diversity becomes particularly evident in a literature review by Patrik Hummel and colleagues, published in *Big Data & Society* (2021). Their study maps the discourse on digital sovereignty and distinguishes the concept from adjacent terms like »data sovereignty«, »cybersovereignty«, and »internet sovereignty«. Their findings highlight that digital sovereignty is attributed to a wide range of actors, is rooted in different contexts, and is linked to diverse goals and values.[8]

(7) In addition, digital sovereignty has increasingly been framed as an educational goal. Here, it denotes the individual ability to navigate digital environments autonomously and to identify and respond to digital threats. As a result, the concept takes on a more personalized interpretation in educational contexts, one that lies outside the primary scope of this article. For further discussion of digital sovereignty in educational settings, see Müller et al. (2020). For initial approaches to fostering digital sovereignty through games, see Krüger et al. (2024).

(8) The study is based on a systematic analysis of 175 instances of the term »digital sovereignty«. The findings point to a clear trend: nations are named as key actors in 61.7% of all cases (108 mentions), followed by governmental organizations (23 mentions, 13.1%) and non-governmental organizations (17 mentions, 9.7%). The discourse is most frequently anchored

While Hummel et al. (2021) emphasize the complexity of digital sovereignty by identifying a broad range of actors, contexts, and normative objectives, Julia Pohle pushes this complexity even further. As one of the most influential voices in the German discourse on digital sovereignty, she identifies three key »dimensions« of the concept: the state, the economic, and the individual dimension (Pohle 2020). A key insight of Pohle's framework is that although each dimension has a dominant actor—such as the state, with its legislative power, in the state dimension, or economic enterprises, with their market power, in the economic dimension—there is always the potential for mutual influence between them (Pohle/Thiel 2020). Corporations, for instance, may exert influence in the state dimension through lobbying and shaping legislation, while the state, in turn, can impact the economic dimension through regulation and policy intervention (Pohle/Thiel 2021). The result is a complex, multidimensional network of actors who operate in different dimensions and contexts with different strategies, and whose actions may support or obstruct one another (Floridi 2020).[9]

Amid the conceptual complexity of digital sovereignty, as already indicated in the review by Hummel et al. (2021), one element consistently takes center stage: control (Tretter 2022a). Control functions as the primary instrument by which actors seek to assert digital sovereignty: by establishing control, they aim to preempt external encroachment, mitigate emerging vulnerabilities, and avoid being subjected to unwanted influence. This control can manifest in various forms: Both material and immaterial (Moerel/Timmers 2021). That's why, in a 2021 *acatech* position paper, Kagermann et al. (2021) argue that maintaining digital sovereignty and protecting against digital threats requires control over hardware and software infrastructures, as well as the establishment of an autonomous digital ecosystem. This includes not only the technical foundations but also a shared legal and normative framework—one that

in the contexts of IT-infrastructure (61 mentions, 34.9%), defense (42 mentions, 24%), legislation (38 mentions, 21.7%), and the economy (15 mentions, 8.6%). As for the aims and values associated with digital sovereignty, the most prevalent are control and power (85 mentions, 48.6%) as well as security (32 mentions, 18.3%). See: Hummel et al. (2021).

(9) The complexity of these interdependencies is explored in greater detail in another article, where I analyze the development of contact-tracing apps during the COVID-19 pandemic. I reconstruct how, in that context, competing visions emerged regarding the design and deployment of such tools: Nation-states, Big Tech companies like Apple and Google, and civil society organizations each drew on their respective sources of power to influence one another—sometimes in opposition, sometimes in alignment—in an effort to realize their divergent interests. See: Tretter (2022b).

enables both regulatory oversight and infrastructural independence. Loss of control over hardware, for instance, creates vulnerabilities to espionage or can allow foreign actors to use backdoors or shutdown mechanisms as leverage. Similar risks arise on the software level, where support withdrawal or data exfiltration can be strategically deployed. To counter such threats, Kagermann et al. (2021) outline a seven-stage model of digital sovereignty: Beginning with secure access to critical raw materials such as silicon and rare earth elements, and extending through the expansion of domestic production capacities for crucial components, the establishment of an independent communications infrastructure, the development of software technologies and shared European data spaces, and culminating in a unified »European system of laws and values«.

While the previous examples focused on safeguarding digital sovereignty through control of software, infrastructure, and data ecosystems, in many contexts, digital sovereignty is also pursued through control over information flows (Tretter 2022a). This is particularly evident in authoritarian regimes, where such efforts take the form of systematic information control and censorship (Thumfart 2024). In these cases, digital sovereignty is operationalized through—and becomes inseparable from—the regulation (and often suppression) of public discourse. In China, for instance, digital technologies are increasingly deployed for mass-scale data collection and population surveillance (Kokas 2024).[10] Algorithms filter and analyze content, blocking dissenting or undesired material before it can circulate. The goal is clear: To preempt any erosion or contestation of state authority and thereby consolidate governmental power. Within the internal logic of such systems, information control is framed as a safeguard for societal stability and national security. This domestically oriented strategy is bolstered by a strategy focusing on external isolation. The systematic expansion of the »Great Firewall of China« (Griffiths 2021) for example, aims to block Western platforms, services, and content from entering China, as well as to restrict the ability of foreign companies to operate within the country—particularly those seen as promoting regime-critical or destabilizing narratives (Lams 2018). Ultimately, such measures are designed to consolidate state power by controlling what information flows into and

(10) Critically, large-scale digital surveillance is not limited to authoritarian regimes like China. As the Snowden revelations as well as Shoshana Zuboff's analyses of surveillance capitalism have shown, extensive forms of data-driven surveillance and control also occur, albeit under different legal and ideological frameworks, in liberal democracies (including »our own«) as well. See: Zuboff (2019).

out of the national digital sphere, effectively shaping the very contours of sovereignty.[11]

As these discussions demonstrate, digital sovereignty is a multifaceted concept characterized by considerable analytical complexity. It involves a broad spectrum of actors with divergent interests, each employing distinct strategies to assert control across different domains and for varied purposes. Yet despite this diversity, one common denominator stands out: nearly all sovereignty strategies aim to respond to digital vulnerabilities—whether infrastructural, informational, or regulatory—through mechanisms of control. The ultimate goal is to safeguard security and maintain societal stability.[12]

⇨ 5 Video Games and Digital Sovereignty

Against the backdrop of the preceding discussion—spanning Onlife entanglements, digital vulnerabilities, and the strategic logic of sovereignty claims—this section turns to the core of this article: The question of where video games fit into this picture. What types of vulnerabilities emerge in or through games? And how are games implicated in broader struggles over digital control, discursive and narrative power, and political influence? As this section demonstrates, digital games are no longer mere entertainment—if they ever were—but have emerged as significant domains of digital sovereignty.

Building on the previous analysis, we can derive the following hypothesis: Video games intersect with certain societal vulnerabilities—while remaining largely irrelevant to others. When it comes to

(11) A comparable strategy of digital isolation is being pursued in Russia through the development of the so-called »RuNet«: A state-controlled internet infrastructure designed to function independently from the global internet. In times of political tension or perceived threat, the RuNet is designed to be decoupled from the broader internet, allowing the state to block external content, insulate its information space, and assert near-total control over digital communications within its borders. The underlying goal is to minimize foreign influence and consolidate national sovereignty in the digital realm through infrastructural autonomy. For detailed analysis of RuNet architecture and policy, see Davydov (2020).

(12) Not every form of digital sovereignty can (or should) be regarded as normatively desirable. The case of China illustrates this clearly: As Thorsten Jelinek points out, many digital sovereignty efforts also carry isolationist tendencies, raising concerns about siloed infrastructures and a potential return to a divided world. For this reason, as Matthias Braun and Patrik Hummel emphasize, the political and ethical value of digital sovereignty depends on how sovereignty is conceptualized, whose interests it serves and what concrete consequences it entails See: Braun/Hummel (2024); Jelinek (2023).

core infrastructures like energy or finance, video games pose no immediate threat. They are neither designed to control these systems nor well-suited as points of access for targeted attacks. But the picture changes when we shift focus to questions of information control. Here, video games can play a far more consequential role: as tools for bypassing censorship, as vehicles of propaganda, or as channels for disinformation. It is in this contested terrain that their relevance to digital sovereignty becomes most apparent. Added to this is their economic weight: As a global multi-billion-dollar industry, video games are also significant players in the platform economy with implications for digital dependence, autonomy, and power.

⇨ *5.1 Video Games as Instruments for Circumventing Censorship and Information Control*

As the cases of Russia and China illustrate, digital sovereignty often involves a strong informational component: Centered on the circulation, restriction, and control of information (Tretter 2022a). The shape this takes can vary significantly depending on the political context. In authoritarian regimes, the goal is typically to suppress dissenting content and amplify system-loyal narratives, thereby shielding the population from critical perspectives and preempting any form of political resistance. In more liberal settings, by contrast, the objective is to foster a free, pluralistic, and high-quality information landscape—enabling citizens to form their own opinions based on a wide range of perspectives.

In countries with heavy content censorship, digital gaming environments have, virtually since the emergence of online multiplayer games, offered spaces of relative opacity where players could communicate and exchange information under significantly lower levels of real-time surveillance than in more conventional digital public spheres (Švelch 2023). Historically, video games—unlike social media or news platforms—were not subject to the same degree of monitoring, largely because their architecture made systematic surveillance more difficult (Hahn et al. 2016). Even as regulatory mechanisms—such as licensing agencies in China that review games for compliance with state standards prior to release (McConnell 2024)—have intensified oversight across various gaming contexts, multiplayer games continue to provide spaces in which players can exchange perspectives, discuss sensitive topics, and circulate information that would otherwise remain inaccessible—even if this sometimes requires some technical tweaks or workarounds (Sun/Shmatikov 2023; Wajid et al. 2021). In this way, multi-

player games have functioned—and in part still function—as alternative »public spheres« that can subvert state censorship and open up possibilities for freer discourse.

Offline games, too, can serve as tools for bypassing censorship—especially through user-generated content. A powerful example of this is the *Uncensored Library* in *Minecraft*, a project initiated by *Reporters Without Borders* (2025a). It consists of a custom-designed map that players can either access in multiplayer mode or download to explore offline. The map recreates a neoclassical library structure in Minecraft's signature blocky style. Inside, players can access and read virtual books containing journalistic texts and regime-critical content—materials officially censored in several authoritarian countries. Because these texts are embedded directly into the game map, rather than stored in conventional file formats, they evade standard filtering mechanisms (Wheatland-Clinch 2021). The only effective method of censorship would be to block access to the server and to prevent downloads of the map. This obstacle is easily circumvented by hosting the library on multiple servers worldwide.

Initiatives like these,[13] along with the relatively unregulated communication that takes place in multiplayer lobbies, demonstrate that video games are far more than mere entertainment. In authoritarian regimes, they create alternative spaces in which access to information can be maintained, circumventing digital surveillance and content filtering. From a liberal-democratic perspective, they constitute active exercises of the right to seek, receive, and impart information even under conditions of systemic restriction.[14]

(13) While *The Uncensored Library* remains one of the most prominent examples of using video games to circumvent censorship, other initiatives have similarly harnessed the medium to assert political expression and challenge information control. Video game players in mainland China, for instance, used the game *Animal Crossing: New Horizons* to criticize government censorship and support protest movements, which prompted Chinese authorities to remove the game from major online marketplaces. While this case, as well as similar examples of »videogame activism«, does not offer direct access to banned journalistic content, it illustrates how games can become vehicles for political speech when other channels are restricted. A notable sibling project to *The Uncensored Library* outside the gaming context is *The Uncensored Playlist*, also initiated by *Reporters Without Borders*, which publishes banned articles disguised as song lyrics on music streaming platforms—demonstrating a similarly creative approach to resisting state censorship. See: BBC (2020); Davies (2020; 2023); Reporters without Borders (2025b).

(14) It is important to acknowledge that the capacity of video games to bypass information controls is not unambiguously positive, not even in liberal democracies. There have been

⇨ *5.2 Video Games as a Tool for the Dissemination of Propaganda and Fake News*

While video games can serve as platforms for circumventing censorship and promoting free information exchange, they can also play an intrinsically ambivalent role in information politics. On the one hand, games may carry ideological narratives embedded directly into their design; on the other, they can function as platforms for user-generated propaganda and politically motivated messaging.[15] Broadly speaking, two distinct forms of propagandistic influence emerge: one coded into the game itself, and one arising through user activity within online gaming environments.

The integration of propaganda into video game design has been widely discussed in scholarly literature (Hammond & Pötzsch 2020). It is particularly apparent in AAA-shooters and military simulations, including franchises like *Call of Duty*, *Battlefield*, and *Medal of Honor*. These games frequently frame the United States as the heroic defender of freedom and democracy, while their adversaries are often cast in stereotypical roles, reflecting and reinforcing post-Cold War and post-9/11 threat narratives prevalent in US security discourse: Russian separatists (*Call of Duty: Modern Warfare*, *Battlefield 3*), Chinese elite forces (*Call of Duty: Black Ops II*, *Command & Conquer: Generals*), or Islamist terrorists (*Medal of Honor*, *Call of Duty: Modern Warfare 2*). Such narrative framing relies on geopolitical clichés and has drawn significant criticism. One notable example that has drawn significant criticism is *Call of Duty: Modern Warfare* (2019), which faced international backlash for its »Highway of Death« mission, widely seen as a distorted and propagandistic depiction of Russian war crimes in a fictional Middle Eastern setting (Batchelor 2019). Propaganda, however, is not exclusive to US titles: in the Chinese first-person shooter *Glorious Mission*, developed by Giant Interactive Group, players take on the role of

documented cases in which terrorists have used gaming environments to communicate covertly and coordinate plans in ways that evade surveillance. See: Sáfrán (2022).

(15) The distinction between propaganda and politically motivated messaging is sometimes subtle, and in practice the two can overlap. The key difference, in the context of this article, lies in the degree of manipulative intent and transparency: Propaganda is understood as a systematic, often institutionalized effort to distort perceptions and to undermine the informational sovereignty of its audience. Politically motivated messaging, by contrast, refers to the more explicit articulation of political positions or objectives. While it may be persuasive in nature, it typically remains more transparent with regard to its authorship and intent.

People's Liberation Army soldiers tasked with defeating »American invaders« (Custer 2012).[16]

Beyond narratives embedded in game design, a second form of digital propaganda emerges from user activity, often described as »participatory« or »user-generated propaganda« (Asmolov 2019). On platforms like Minecraft or Roblox, politically charged environments are intentionally created and shared by players themselves. Steven Lee Myers and Kellen Browning (2023) highlight several such cases in a *New York Times* report. One Minecraft server, for example, staged a reenactment of the battle for Soledar from the Russian invasion of Ukraine, which was recorded and later disseminated via social media. In *World of Tanks*, users recreated the Soviet Union's 1945 military parade in Moscow, while the letter »Z«—widely recognized since 2022 as a symbol of the Russian military has—been prominently displayed or constructed by players across various games, including Minecraft and Roblox.

Even more unsettling is the presence of Minecraft servers like »Nazicraft«, which explicitly promote Nazi ideology. According to listings on public Minecraft server directories, players are actively encouraged to perform Nazi salutes and construct swastikas, transforming the game space into a site of extremist affirmation. In such digital environments, extremist ideologies are not only expressed but ritualized and reinforced through collective play. As Hannah Getahun (2023) notes in her *Business Insider* report, this is precisely how »propaganda is seeping into popular children's games«—often subtly and often hiding in plain sight.[17]

(16) The propagandistic agenda of *Glorious Mission* is further underscored by the fact that a non-public, military version of the game was also developed specifically for use by China's People's Liberation Army. This internal edition was designed not merely for entertainment, but as a training and morale-boosting tool for active soldiers—blurring the lines between game-based simulation, ideological reinforcement, and soft military propaganda. See: Custer (2012). More broadly, the use of video games for military training, simulation, or recruitment is not limited to authoritarian regimes. In the United States, for example, the military has increasingly turned to video games and online platforms to engage with younger audiences and bolster recruitment efforts. A notable example is the *America's Army* video game series, launched in 2002, which was designed to provide players with a virtual soldiering experience and has been used as a recruitment tool. Additionally, the US Army established its own esports team in 2018, participating in popular multiplayer games like *Call of Duty* and *Fortnite* to connect with potential recruits. These initiatives aim to present military service in a relatable and appealing manner to tech-savvy youth. See: Schwartzburg (2024).

(17) In addition to propaganda disseminated within games themselves, there is also targeted propaganda aimed at gamers outside of gameplay contexts such as on gaming forums or voice

Beyond the deliberate and »weaponized« (Münzenberg 1972) deployment of propaganda, the strategic dissemination of false information—commonly referred to as »fake news«—has become a core tactic of authoritarian regimes and governments with authoritarian tendencies. These efforts aim to sow confusion, erode public trust in democratic institutions, and deepen social polarization (Andrejevic 2020). While social media platforms like *Facebook*, *X* (formerly *Twitter*), *Telegram*, and *TikTok* have served as the predominant channels for such campaigns—often overwhelmed with shitposts, »AI slop« (Mahdawi 2025; Malik 2025), and manipulative content produced by troll farms, bot networks, or AI-generated accounts (Shu et al. 2020)—video games are now becoming part of this »disinformation infrastructure« (Panditharatne/Hasan 2024).

A striking example is the military simulation game *Arma 3*, whose high-fidelity graphics and extensive modding capabilities—i.e., the ability to add custom-generated content or tailor the game in specific ways—have made it a recurring tool for disinformation. During the early months of Russia's invasion of Ukraine, clips created in *Arma 3* were widely circulated online—especially on TikTok—and falsely presented as real battlefield footage. In an attempt to create the illusion of authenticity, banners such as »LIVE« or »BREAKING NEWS« were often superimposed onto the gameplay footage (Euronews/AFP 2023). The same game has also been used to fabricate footage purportedly showing scenes from conflicts in Syria, Afghanistan, and Palestine (McCann Ramirez/Rawnsley 2023). These examples highlight how video games are increasingly exploited to create disinformational content, opening new frontiers in the evolving fake news ecosystem (Dang/Culliford 2022).[18]

chat platforms. A striking example is the so-called *Good Old USA Project*, a Russian influence operation exposed by the US Department of Justice. Orchestrated by various Russian institutions reportedly acting under the direction and control of the Russian Presidential Administration, the campaign sought to influence the 2024 US presidential election in favor of Donald Trump. It aimed to exploit societal divisions and promote pro-Russian narratives by specifically targeting online gaming communities—leveraging the trust and cohesion within these spaces to enhance the reach and credibility of its messaging. The operation was further amplified through AI-generated content and fake news websites designed to resemble legitimate media outlets. See: Department of Justice (2025); Gilbert (2024).

(18) Despite their misuse in the dissemination of disinformation, several initiatives aim to deliberately use video games as educational tools. By engaging players with common manipulation techniques in a playful way, these games seek to strengthen users' cognitive defenses and enhance their media literacy in dealing with fake news. The goal is to raise awareness of

As we've seen, video games can shape information dynamics in strikingly diverse ways: They can provide access to censored material, act as vessels for ideological propaganda, or serve as tools for spreading disinformation. In doing so, they challenge existing regimes of informational authority—at times in the name of freedom of information, at other times in the service of influence and control. When viewed through the lens of the Onlife condition and digital sovereignty, these dynamics highlight the growing complexity of video games' place within the digital landscape. In a world where digital and analog spheres are inseparably fused, games are no longer confined to a separate »virtual« sphere but constitute what Floridi terms Onlife spaces: They have become embedded in real-world contests over autonomy, rights, and power (Asher-Schapiro 2020). Precisely because of this, they are increasingly drawn into strategies of sovereignty—sometimes as a threat, sometimes as a tool, and often occupying contested middle grounds where resistance and control intersect.

⇨ *5.3 Video Games as an Economic Market Force*

In addition to their informational dimensions, video games can also be analyzed in terms of their economic implications for digital sovereignty. With a projected global annual revenue of over 522 billion USD by 2025 (Statista 2025), the video game industry has evolved into an economic »giant« (Arora 2023). This market dominance is no longer limited to entertainment; it increasingly shapes economic policy and geopolitical dynamics alike.

In an increasingly digitalized world, where economic performance and technological dependencies define the boundaries of political agency, control over markets, platforms, and user flows has itself become a sovereignty issue (Kagermann et al. 2021)—a dynamic captured by Pohle (2020) and Pohle and Thiel (2020; 2021) in their account of the economic dimension of digital sovereignty. Those who dominate game engines, cloud infrastructure, distribution networks, or mobile payment systems effectively govern the frameworks for cultural production—including all associated channels of information control—digital identity, and economic value creation (Chris et al. 2024). Platforms like *Steam*, the *Epic Games Store*, or mobile marketplaces operated by *Apple* and *Google* are not merely distributors; They function as powerful

disinformation strategies and sharpen players' ability to critically evaluate digital content. See: Roozenbeek/van der Linden (2019).

gatekeepers, with the authority to prioritize, suppress, or entirely block specific content (Kelton et al. 2022).[19]

For many countries—particularly in Europe—this situation presents a strategic dilemma: They face structural dependence on non-European market actors, especially from the US, while much of the value generated by the video game industry flows out of the region (Lyonnet/Rabineau 2023). This makes the question of how to reclaim market share—and with it, a degree of strategic control and sovereignty—all the more urgent (Chris et al. 2024). Possible responses include targeted investments in homegrown game engines, the promotion of European publishers, and the development of alternative digital infrastructures (European Parliament 2023).

⇨ 6 Conclusion

This article set out to explore which insights can be gained by bringing the concept of digital sovereignty into dialogue with video games. It began by examining our current Onlife world, in which the once-separate realms of the »digital« and the »analog« have become irreversibly entangled. As argued, this hybrid reality generates not only new potentials, but also systemic risks: Wherever social domains are increasingly governed by digital infrastructures, new forms of vulnerability arise, threatening the stability and safety of societies. In response, digital sovereignty has emerged as a strategic framework designed to counter digital vulnerabilities by exercising control in various forms.

This analysis reveals that control is a key link between digital sovereignty and video games. Understanding how the two relate requires close attention to the ways in which control is enacted *through* video games—or deliberately challenged *by* them. This article has focused on two core dimensions where these dynamics unfold. First, on the level of information politics: Video games are increasingly entangled in

(19) At the same time, corporations themselves have become active participants in a marketplace shaped by growing geopolitical tensions. A prominent example is the 2019 case of *Blizzard Entertainment*, a US-based gaming company, which faced international backlash after suspending a professional eSports player who had publicly expressed support for the pro-democracy protests in Hong Kong. The decision was widely interpreted as a concession to pressure from Chinese business partners and regulatory threats. This incident reveals how corporate economic interests, state influence, and platform governance increasingly intersect—and how questions of economic power are now inseparable from debates about digital sovereignty. See: Beauchamp (2019).

struggles over the control of information flows. They can be used to bypass state censorship and foster access to restricted knowledge, but also to manipulate public discourse through propaganda and disinformation. In both cases, video games function as arenas in which competing actors seek to assert control over what information circulates and how it is framed, making them deeply relevant to debates about digital sovereignty. Second, on the level of economic power: The global video game industry generates enormous revenues, surpassing most other entertainment sectors by far. However, the underlying economic infrastructure—game engines, distribution platforms, cloud services—is largely controlled by a small group of powerful, primarily US-based corporations. This concentration of control significantly shapes the conditions under which cultural production and economic value creation take place. That's why video games can be considered vehicles of infrastructural control, raising urgent questions about digital sovereignty in an increasingly digital economy and Onlife world. All of this suggests that video games are not peripheral to digital sovereignty—on the contrary, it is time to recognize them as integral to how digital sovereignty is shaped and contested.

With these reflections and insights, the article makes a twofold contribution. First, it introduces the concept of digital sovereignty as a novel analytical lens for video game studies: One that enables a deeper engagement with the political dimensions of games and advances ongoing debates about how they function as sites of power, control, and contestation. Second, it broadens the concept of digital sovereignty itself by turning to a field largely absent from its existing discourse. It demonstrates that digital sovereignty is not confined to »high-stakes confrontations« between states and tech giants; it often begins in seemingly mundane spaces like video games, where political orders are stabilized, contested, or subtly subverted. This article situates its contribution precisely in these spaces: It is the first step towards a systematic examination of the complex entanglements between gaming and digital sovereignty.

⇨ 7 References

Agulian, James (2018, February 18): Is Mr Robot a Good Representation of Real-Life Hacking and Hacking Culture?, Online at: https://www.qa.com/resources/blog/is-mr-robot-a-good-representation-of-real-life-hacking-and-hacking-culture/ (Accessed: June 8, 2025).

Andrejevic, Mark (2020): The Political Function of Fake News. Disorganized Propaganda in the Era of Automated Media, in: Zimdars, Melissa/McLeod, Kembrew (Eds.): Fake News. Understanding Media and Misinformation in the Digital Age, Cambridge/London: The MIT Press, 19-28.

Arora, Krishan (2023, November 17): The Gaming Industry. A Behemoth With Unprecedented Global Reach, Online at: https://www.forbes.com/councils/forbesagencycouncil/2023/11/17/the-gaming-industry-a-behemoth-with-unprecedented-global-reach/ (Accessed: January 15, 2025)

Asher-Schapiro, Avi (2020, July 31): Video Games Seen Becoming a New Frontier in Digital Rights, Online at: https://www.reuters.com/article/world/video-games-seen-becoming-a-new-frontier-in-digital-rights-idUSKCN24W00K/ (Accessed: June 8, 2025)

Asmolov, Gregory (2019): The Effects of Participatory Propaganda. From Socialization to Internalization of Conflicts, in: Journal of Design and Science 6. https://doi.org/10.21428/7808da6b.833c9940

Batchelor, James (2019, October 31): Call of Duty Modern Warfare Decried as ›American Propaganda‹ over Highway of Death Mission, Online at: https://www.gamesindustry.biz/call-of-duty-modern-warfare-decried-as-american-propaganda-in-russia-over-highway-of-death-mission (Accessed: May 29, 2025).

BBC (2020, April 13). Animal Crossing Removed from Sale in China amid Hong Kong Protests, Online at: https://www.bbc.com/news/technology-52269671 (Accessed: May 28, 2025).

Beauchamp, Zack (2019, October 8). One of America's Biggest Gaming Companies is Acting as China's Censor, Online at: https://www.vox.com/2019/10/8/20904433/blizzard-hong-kong-hearthstone-blitzchung (Accessed: May 26, 2025).

Bilotta, Nicola/Botti, Fabrizio (Eds.) (2021). The (Near) Future of Central Bank Digital Currencies. Risks and Opportunities for the Global Economy and Society, Bern/Berlin: Peter Lang.

Braun, Matthias/Hummel, Patrik (2024): Is Digital Sovereignty Normatively Desirable?, in: Information, Communication & Society. https://doi.org/10.1080/1369118X.2024.2332624

Browne, Ryan/Sigalos, MacKenzie (2024, July 5). Mt. Gox Begins Repaying Bitcoin to Creditors a Decade after Exchange's Collapse. What it Means, Online at: https://www.cnbc.com/2024/07/05/mt-gox-begins-repaying-bitcoin-to-creditors-a-decade-on-from-collapse.html (Accessed: May 29, 2025).

Buchholz, Bernd M./Styczynski, Zbigniew A. (2020): Smart Grids. Fundamentals and Technologies in Electric Power Systems of the Future (2 ed.), Berlin: Springer.

Chris, J. Young/Emilie, Reed/Brendan, Keogh (2024): Global Localities of Game Production, in: Media Industries 11(1). https://doi.org/10.3998/mij.1181

Couture, Stephane/Toupin, Sophie (2019): What Does the Notion of »Sovereignty« Mean when Referring to the Digital?, in: New Media & Society 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Custer, Charlie (2012, October 16). A Look at »Glorious Mission«, China's Military-Produced Call of Duty Clone, Online at: https://www.techinasia.com/glorious-mission-chinas-militaryproduced-call-duty-clone (Accessed: May 26, 2025).

Devi, Sabbani Rama/Kalyampudi, P. S. Latha/ Charitha, N. Sai (2022): Cyber Attacks, Security Data Detection, and Critical Loads in the Power System, In: Padmanaban, Sanjeevikumar/Holm-Nielsen, Jens Bo/Padmanandam, Kayal/Dhanaraj, Rajesh Kumar/Balusamy, Balamurugan (Eds.): Smart Energy and Electric Power Systems. Current Trends and New Intelligent Perspectives, Amsterdam: Elsevier, 169–184.

Dang, Sheila/Culliford, Elizabeth (2022, March 7): TikTok War. How Russia's Invasion of Ukraine Played to Social Media's Youngest Audience, Online at: https://www.reuters.com/technology/tiktok-war-how-russias-invasion-ukraine-played-social-medias-youngest-audience-2022-03-01/ (Accessed: May 26, 2025).

Davies, Hugh (2020): Spatial Politics at Play: Hong Kong Protests and Videogame Activism. Proceedings of DiGRA Australia 2020, Online at: https://digraa.org/wp-content/uploads/2020/02/DiGRAA2020paper_46.pdf (Accessed: May 29, 2025).

Davies, Hugh (2023): Videogame Activism. Contemporary Examples and their Effectivity, in: Proceedings of DiGRA Australia 2023, Online at: https://digraa.org/wp-content/uploads/2023/01/2023-CAMERA-READY_Hugh-Davies.pdf (Accessed: May 29, 2025).

Davydov, Sergey (Ed.) (2020): Internet in Russia. A Study of the Runet and Its Impact on Social Life, Cham: Springer.

Department of Justice (2025, February 6): Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere, Online at: https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (Accessed: May 29, 2025).

Dov Bachmann, Sascha-Dominik/Putter, Dries/Duczynski, Guy (2023). Hybrid Warfare and Disinformation. A Ukraine War Perspective, in: Global Policy 14(5), 858–869. https://doi.org/10.1111/1758-5899.13257

Dyer-Witheford, Nick/de Peuter, Greig (2009): Games of Empire. Global Capitalism and Video Games, Minneapolis: University of Minnesota Press.

Easterly, Jen (2023, May 7, 2023): The Attack on Colonial Pipeline. What We've Learned & What We've Done Over the Past Two Years, Online at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years (Accessed: May 28, 2025).

Euronews/AFP. (2023, January 3): Trolls are Using this Life-Like Video Game to Spread Misinformation about the Ukraine War, Online at: https://www.euronews.com/next/2023/01/03/trolls-are-using-this-life-like-video-game-to-spread-misinformation-about-the-ukraine-war (Accessed: May 28, 2025).

European Parliament (2023, June 28): Developing the Video Games and E-Sports Sector in the EU, Online at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)749808 (Accessed: May 26, 2025).

Floridi, Luciano (2014): The 4th Revolution. How the Infosphere is Reshaping Human Reality, Oxford: Oxford University Press.

Floridi, Luciano (2020): The Fight for Digital Sovereignty. What It Is, and Why It Matters, Especially for the EU, in: Philosophy & Technology 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Flügge, Barbara (Ed.) (2017). Smart Mobility – Connecting Everyone. Trends, Concepts and Best Practices, Wiesbaden: Springer Nature.

Getahun, Hannah (2023, July 31): Militärparade auf Roblox oder ein Minecraft-Konzert. Die russische Propaganda hält Einzug in beliebte Kinderspiele, Online at: https://www.businessinsider.de/politik/international-politics/russische-propaganda-roblox/ (Accessed: May 26, 2025).

Gilbert, David (2024, September 5): DOJ. Russia Aimed Propaganda at Gamers, Minorities to Swing 2024 Election, Online at: https://www.wired.com/story/project-good-old-usa-russia-2024-election/ (Accessed: May 28, 2025).

Griffiths, James (2021): The Great Firewall of China. How to Build and Control an Alternative Version of the Internet (2 ed.), London: Bloomsbury.

Habermas, Jürgen (2011): The Structural Transformation of the Public Sphere. An inquiry into a Category of Bourgeois Society (translated by Burger, Thomas), Cambridge: The MIT Press.

Habermas, Jürgen (2023): A New Structural Transformation of the Public Sphere and Deliberative Politics (translated by Cronin, Ciaran), Cambridge: Polity.

Hahn, Bridger/Nithyanand, Rishab/Gill, Phillipa/Johnson, Rob (2016, March 24): Games without Frontiers. Investigating Video Games as a Covert Channel, in: 2016 IEEE European Symposium on Security and Privacy. https://doi.org/10.1109/EuroSP.2016.17

Hall Jamieson, Kathleen (2020): Cyberwar. How Russian Hackers and Trolls Helped Elect a President, New York: Oxford University Press.

Hammond, Philip/Pötzsch, Holger (Eds.) (2020): War Games. Memory, Militarism and the Subject of Play, New York/London: Bloomsbury Academic.

Hummel, Patrik/Braun, Matthias/Tretter, Max/Dabrock, Peter (2021): Data Sovereignty: A Review, in: Big Data & Society 8(1). https://doi.org/10.1177/2053951720982012

İnci, Mustafa/Çelik, Özgür/Lashab, Abderezak/Bayındır, Kamil Ç/Vasquez, Juan C./Guerrero, Josep M. (2024): Power System Integration of Electric Vehicles. A Review on Impacts and Contributions to the Smart Grid, in: Applied Sciences 14(6). https://doi.org/10.3390/app14062246

Jelinek, Thorsten (2023): The Digital Sovereignty Trap. Avoiding the Return of Silos and a Divided World, Singapore: Springer.

Kagermann, Henning/Streibich, Karl-Heinz/Suder, Katrin (2021): Digital Sovereignty. Status Quo and Perspectives, Online at: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/ (Accessed: March 31, 2021).

Karakitsiou, Athanasia/Migdalas, Athanasios/Pardalos, Panos M. (Eds.) (2024): Disruptive Technologies and Optimization Towards Industry 4.0 Logistics, Cham: Springer.

Kelton, Maryanne/Sullivan, Michael/Rogers, Zac/Bienvenue, Emily/Troath, Sian (2022): Virtual Sovereignty? Private Internet Capital, Digital Platforms and Infrastructural Power in the United States, in: International Affairs 98(6), 1977–1999. https://doi.org/10.1093/ia/iiac226

Khandelwal, Swati (2019, August 16): European Central Bank Shuts Down 'BIRD Portal' After Getting Hacked, Online at: https://thehackernews.com/2019/08/european-central-bank-hack.html (Accessed: May 29, 2025).

Kokas, Aynne (2024). Trafficking Data. How China is Winning the Battle for Digital Sovereignty, New York: Oxford University Press.

Krüger, Anita Susann/Dittert, Nadine/Lucke, Ultike (2024): Developing a Hybrid Escape Game to Enhance Digital Sovereignty across All Ages, in: Proceedings of Mensch und Computer 2024, Online at: https://doi.org/10.1145/3670653.3677478 (Accessed: May 28, 2025).

Kunkel, Nicole (2024): An Ethical Evaluation of Lethal Functions in Autoregulative Weapons Systems, Eugene: Pickwick.

Lams, Lutgard (2018). Examining Strategic Narratives in Chinese Official Discourse under Xi Jinping, in: Journal of Chinese Political Science 23(3), 387-411. https://doi.org/10.1007/s11366-018-9529-8

Lee Kuo Chuen, David (Ed.) (2024): Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data (2 ed.), Cambridge: Academic Press.

Lee Myers, Steven/Browning, Kellen (2023, July 30): Russia Takes Its Ukraine Information War Into Video Games, Online at: https://www.nytimes.com/2023/07/30/technology/russia-propaganda-video-games.html (Accessed: May 26, 2025).

Lockhart, P. R. (2018, December 18): How Russia Exploited Racial Tensions in America during the 2016 Elections, Online at: https://www.vox.com/identities/2018/12/17/18145075/russia-facebook-twitter-internet-research-agency-race (Accessed: May 29, 2025).

Lyonnet, Loïse/Rabineau, David (2023, October 31): The Video Games Industry in Europe. Current Situation, Issues and Prospects, Online at: https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-724-en.pdf (Accessed: May 26, 2025)

Mahdawi, Arwa (2025, January 8): AI-generated ›Slop‹ is Slowly Killing the Internet, so why is Nobody Trying to Stop it?, Online at: https://www.theguardian.com/global/commentisfree/2025/jan/08/ai-generated-slop-slowly-killing-internet-nobody-trying-to-stop-it (Accessed: May 28, 2025).

Malik, Nesrine (2025, April 21). With ›AI slop‹ distorting our reality, the world is sleepwalking into disaster. *The Guardian*. https://www.theguardian.com/commentisfree/2025/apr/21/ai-slop-artificial-intelligence-social-media (Accessed: May 28, 2025).

McCann Ramirez, Nikki/Rawnsley, Adam (2023, October 9): Trolls Push Video Game Clips as Real Gaza Conflict Footage—and it's Working, Online at: https://www.rollingstone.com/politics/politics-features/arma-3-video-game-clips-israel-hamas-conflict-1234849405/ (Accessed: May 28, 2025).

McConnell, Aedín (2024): Examining the Red Lines of China's Video Game Censorship Policy, in: Asian Journal of Sport History & Culture 3(3), 327-343, https://doi.org/10.1080/27690148.2024.2394760.

McIntyre, Lee (2018): Post-Truth, Cambridge/London: The MIT Press.

McQueen, Bob/Safi, Ammar/Alkheyaili, Shafia (2024): Smart Mobility. Using Technology to Improve Transportation in Smart Cities, Hoboken: Wiley.

Moerel, Lokke/Timmers, Paul (2021): Reflections on Digital Sovereignty, Online at: https://eucyberdirect.eu/wp-content/uploads/2021/01/rif_timmersmoerel-final-for-publication.pdf (Accessed: February 17, 2021).

Moore, Martin (2020): Democracy Hacked. How Technology is Destabilising Global Politics, London: Oneworld.

Müller, Jane/Thumel, Mareike/Potzel, Katrin/Kammerl, Rudolf (2020): Digital Sovereignty of Adolescents, in: MedienJournal 44(1), 30–40. https://doi.org/10.24989/medienjournal.v44i1.1926

Morozov, Evgeny (2013): To Save Everything, Click Here. The Folly of Technological Solutionism, New York: PublicAffairs.

Münzenberg, Willi (1972): Propaganda als Waffe. Ausgewählte Schriften 1919–1940 (edited by Schulz, Tilman), Frankfurt am Main: März.

Murray, Soraya (2021): On Video Games. The Visual Politics of Race, Gender and Space, London: Bloomsbury.

Naik, Yogesh (2021, October 28): Mumbai 2020 Outage due to ›Cascade Tripping‹, not Sabotage. Report, Online at: https://indianexpress.com/article/cities/mumbai/mumbai-2020-outage-due-to-cascade-tripping-not-sabotage-report-7594295/ (Accessed: May 29, 2025).

Nardone, Rosy (2017): Videogames between Ethics and Politics, in: Ricerche di Pedagogia e Didattica. Journal of Theories and Research in Education 12(2), 41–55. https://doi.org/10.6092/issn.1970-2221/7072

Ong, Walter J./Hartley, John (2012): Orality and Literacy. The Technologizing of the Word. 30th Anniversary Edition, London/New York: Routledge.

Panditharatne, Mekela/Hasan, Shanze (2024, October 21): How to Rein in Russia's Evolving Disinformation Machine, Online at: https://time.com/7095506/russia-disinformation-us-election-essay/ (Accessed: May 28, 2025).

Pariser, Eli (2011): The Filter Bubble. What the Internet is Hiding from You, London: Viking.

Passacantando, Franco (2021): The Digital Euro. Challenges and Opportunities, in: Bilotta, Nicola/Botti, Fabrizio (Eds.): The (Near) Future of Central Bank Digital Currencies. Risks and Opportunities for the Global Economy and Society, Bern, Berlin: Peter Lang, 113–130.

Payne, Matthew Thomas (2016): Playing War. Military Video Games after 9/11, New York: New York University Press.

Pohle, Julia (2020): Digital sovereignty. A new key concept of digital policy in Germany and Europe, Online at: https://www.kas.de/documents/252038/11055681/Digital+Sovereignty.pdf/fbf01b14-3c8b-4322-2676-a6eb75d9eea0 (Accessed: November 11, 2021).

Pohle, Julia/Thiel, Thorsten (2020): Digital sovereignty, in: Internet Policy Review 9(4), 1–19. https://doi.org/10.14763/2020.4.1532

Pohle, Julia & Thiel, Thorsten (2021): Digital Sovereignty, in: Herlo, Bianca/Irrgang, Daniel/Joost, Gesche/Unteidig, Andreas (Eds.): Practicing Sovereignty. Digital Involvement in Times of Crises, Bielefeld: Transcript, 47–67.

Prajapati, Aanchal/Kumar, Govind/Srivastava, Mukul (2024): The Role of Fake News in Political Campaigns and Elections: A Global Perspective, in: International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2024.v06i06.30907

Rainie, Lee/Anderson, Janna (2017, March 29): The Future of Free Speech, Trolls, Anonymity and Fake News Online, Online at: https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/ (Accessed: May 29, 2025).

Reporters without Borders (2025a): The Uncensored Library, Online at: https://www.uncensoredlibrary.com/ (Accessed: May 28, 2025).

Reporters without Borders (2025b): The Uncensored Playlist, Online at: https://www.reporter-ohne-grenzen.de/aktivitaeten/kampagnen/the-uncensored-playlist (Accessed: May 28, 2025).

Rogoff, Kenneth S. (2016): The Curse of Cash, Princeton: Princeton University Press.

Roozenbeek, Jon/van der Linden, Sander (2019): Fake News Game Confers Psychological Resistance against Online Misinformation, in: Palgrave Communications 5(1). https://doi.org/10.1057/s41599-019-0279-9

Sáfrán, József (2022): Digital Terrorism. Communication through Online Video Games, in. Hadtudományi Szemle 15(3), 183–195. https://doi.org/10.32563/hsz.2022.3.12

Scharre, Paul (2020): Army of None. Autonomous Weapons and the Future of Warfare, New York/London: W. W. Norton & Company.

Schwartzburg, Rosa (2024, February 14): The US military is embedded in the gaming world. Its target: teen recruits, Online at:

https://www.theguardian.com/us-news/2024/feb/14/us-military-recruiting-video-games-targeting-teenagers (Accessed: May 28, 2025).

Scott, Brett (2022): Cloudmoney. Cash, Cards, Crypto and the War for Our Wallets, London: Random House.

Seeliger, Martin/Sevignani, Sebastian (Eds.) (2021): Ein neuer Strukturwandel der Öffentlichkeit?, Baden-Baden: Nomos.

Shchokin, Rostyslav/Iatsyshyn, Anna/Kovach, Valeriia/Zaporozhets, Artur (Eds.) (2024): Digital Technologies in Education. Selected Cases, Cham: Springer.

Shu, Kai/Wang, Suhang/Lee, Dongwon/Liu, Huan (Eds.) (2020): Disinformation, Misinformation, and Fake News in Social Media. Emerging Research Challenges and Opportunities, Cham: Springer.

Singer, Peter W./Brooking, Emerson T. (2018), LikeWar. The Weaponization of Social Media, Boston, New York: Houghton Mifflin Harcourt.

Spies, Thomas/Kurt, Şeyda/Pötzsch, Holger (Eds.) (2024): Spiel*Kritik. Kritische Perspektiven auf Videospiele im Kapitalismus, Bielefeld: Transcript.

Statista (2024): Total number of cashless transactions worldwide - including B2C and B2B - from 2014 to 2023, with forecasts for 2024 and 2028, by region, Online at: https://www.statista.com/statistics/265767/number-of-cashless-transactions-worldwide-by-region/ (Accessed: May 29, 2025).

Statista (2025): Games – Worldwide, Online at: https://www.statista.com/outlook/amo/media/games/worldwide (Accessed: May 29, 2025).

Sun, Zhen/Shmatikov, Vitaly (2023, May 25): Telepath. A Minecraft-based Covert Communication System, in: 2023 IEEE Symposium on Security and Privacy (SP), Online at: 10.1109/SP46215.2023.10179335 (Accessed: May 29, 2025).

Švelch, Jaroslav (2023): Gaming the Iron Curtain. How Teenagers and Amateurs in Communist Czechoslovakia Claimed the Medium of Computer Games, Cambridge: The MIT Press.

Tapscott, Don/Tapscott, Alex (2016): Blockchain Revolution. How the Technology Behind Bitcoin Is Changing Money, Business, and the World, New York: Penguin.

Thumfart, Johannes (2024): The Liberal Internet in the Postliberal Era. Digital Sovereignty, Private Government, and Practices of Neutralization, Cham: Palgrave Macmillan.

Tidy, Joe (2022, March 30): Ronin Network: What a $600m hack says about the state of crypto, Online at: https://www.bbc.com/news/technology-60933174 (Accessed: May 29, 2025).

Tidy, Joe (2025, March 10): North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack, Online at: https://www.bbc.com/news/articles/c2kgndwwd7lo (Accessed: May 29, 2025).

Tretter, Max (2017, October 11): Computerspiele, Online at: https://www.ethik-evangelisch.de/lexikon/computerspiele (Accessed: October 11, 2017).

Tretter, Max (2022a): »Digitale Souveränität« als Kontrolle. Zentrale Formen digitaler Kontrollausübung und ihr Verhältnis zueinander, in: Glasze, Geirg/Odzuck, Eva/Staples, Roland (Eds.): Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter, Bielefeld: Transcript, 89–125.

Tretter, Max (2022b): Sovereignty in the Digital and Contact Tracing Apps, in: Digital Society 2(2). https://doi.org/10.1007/s44206-022-00030-2

Tretter, Max (2025): Opportunities and challenges of AI-systems in political decision-making contexts, in: Frontiers in Political Science 7(1504520). https://doi.org/10.3389/fpos.2025.1504520

Türcke, Christoph (2015); Mehr! Philosophie des Geldes. München: C.H. Beck.

UNFASSBAR. (2025, May 9): Der größte Kryptohack aller Zeiten, Online at: https://open.spotify.com/episode/1ZMDpPo945sI9cXqFIScEC?si=534b18af35544d46 (Accessed May 29, 2025).

Vijayalakshmi, S./Lekha, Jayabalan/Jacob, Lija/Dahiya, Savita/Gunavathi, R. (2025), Smart Power Systems. Grid Modernization Using AI and IoT-Based Applications, Cham: Springer.

Wajid, Abdul/Kamal, Nasir/Sharjeel, Muhammad/Sheikh, Raaez Muhammad/Wasim, Huzaifah Bin/Ali, Muhammad Hashir/Hussain, Wajahat/Ali, Syed Taha/Anjum, Latif (2021): A First Look at Private Communications in Video Games using Visual Features, in:

Proceedings on Privacy Enhancing Technologies 2021(3), 433–452. https://doi.org/10.2478/popets-2021-0055

Werbach, Kevin (2018): The Blockchain and the New Architecture of Trust, Cambridge: The MIT Press.

Wewege, Luigi/Thomsett, Michael C. (2020): The Digital Banking Revolution. How Fintech Companies are Transforming the Retail Banking Industry through Disruptive Financial Innovation (3 ed.), Boston/Berlin: Walter de Gruyter.

Wheatland-Clinch, Elliot (2021, August 17): Minecraft library liberates gamers in censored countries, Online at: https://thred.com/tech/minecraft-library-liberates-gamers-in-censored-countries/ (Accessed May 29, 2025).

Wolf, Mark J. P./Perron, Bernard (Ed.) (2023): The Routledge Companion to Video Game Studies (2 ed.). New York/London: Routledge.

Zetter, Kim (2016a, March 3): Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, Online at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (Accessed May 29, 2025).

Zetter, Kim (2016b, May 17): That Insane, $81M Bangladesh Bank Heist? Here's What We Know, Online at: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/ (Accessed May 29, 2025).

Zuboff, Shoshana (2019): The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power, New York: Public Affairs.

Zitationsvorschlag:
Tretter, Max (2026): Digital Sovereignty and Video Games (Ethik und Gesellschaft 1/2026: Kein Spiel. Wargaming und Serious Gaming im Zeitalter der KI). Download unter: https://dx.doi.org/10.18156/eug-1-2026-art-8 (Zugriff am [Datum]).

ethikundgesellschaft
ökumenische zeitschrift für sozialethik

1/2026: Kein Spiel. Wargaming und Serious Gaming im Zeitalter der KI