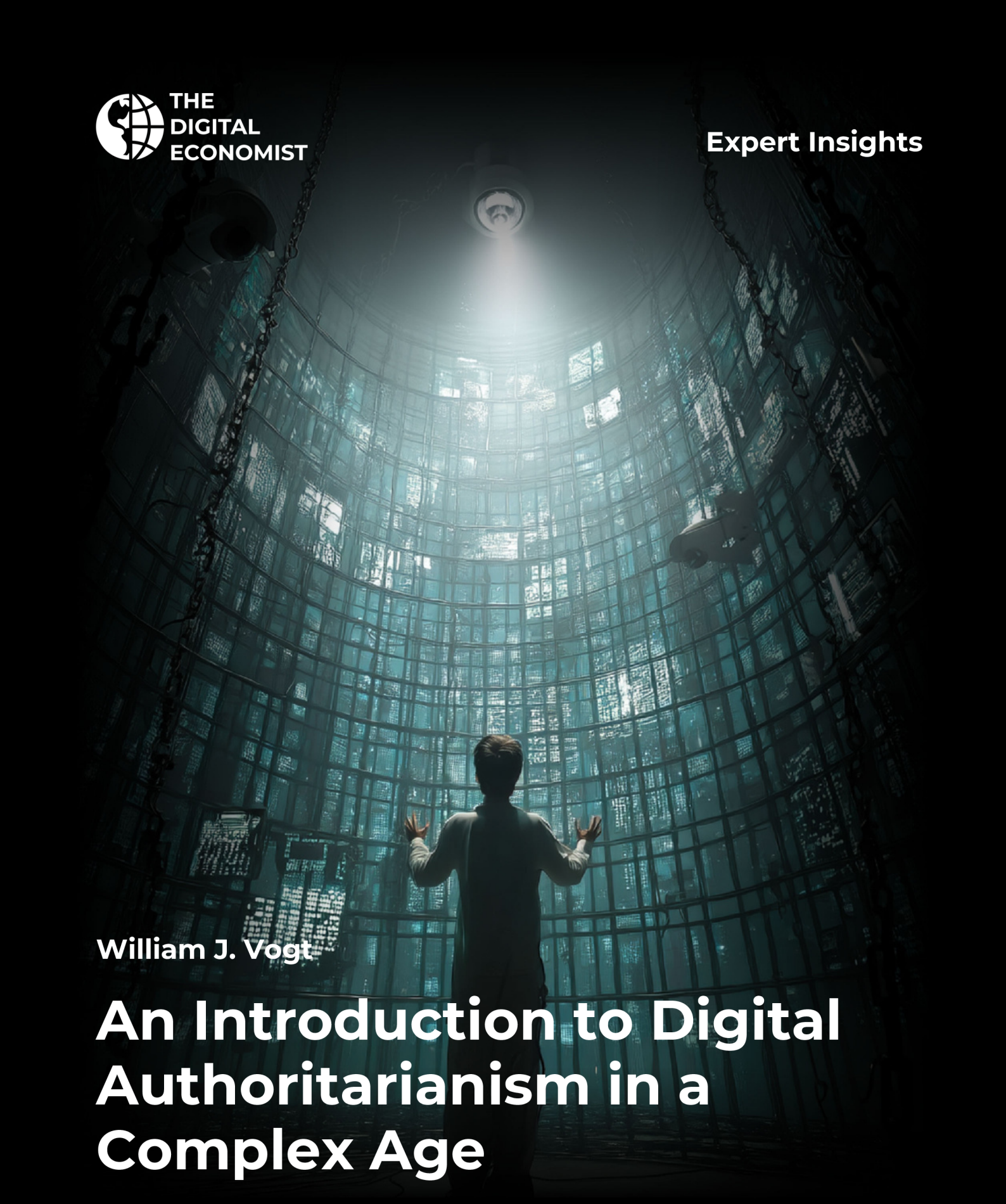
THE DIGITAL ECONOMIST

Expert Insights



William J. Vogt

An Introduction to Digital Authoritarianism in a Complex Age

DIGITAL AUTHORITARIANISM | INFORMATION TECHNOLOGIES | TECH POLICY

The Digital Economist

Email: info@thedigitaleconomist.com
Website: www.thedigitaleconomist.com

Introduction

We live in a complicated and challenging time. Advancements in information communication technologies (ICTs)—most recently, the growing capabilities of artificial intelligence (AI)—have collided with real-world social and political priorities. Entire industries are being reconsidered, repackaged, renamed, and even eliminated as powerful new actors look to reform society for a new century. In the policy realm, these conversations feel existential to many as questions of sustainability and ethics grow.

A complicating reality that drives such widespread fear among a wide cross-section of sociopolitical experts is the sobering lack of awareness of the specific impacts of ICTs outside technical applications. This became a pronounced issue with the rise of social media platforms and the influential algorithms that power such systems.

This report aims to address these gaps to better inform the policymaking and advocacy communities as they consider and implement the next steps. We find that these gaps persist in misinforming powerful actors to believe that there are options and effects visible in theory that do not exist in practice. The following analysis attempts to begin a more informed conversation as to why these beliefs do not take into account the full range of capabilities, effects, and possibilities that our ICT–powered society truly supports.

An additional step is to posit that analyzing authoritarianism at this moment is essential to consider in light of the historical legacies associated with ICT, namely its origins in the American postwar experience and its accompanying brand of democracy and human rights promotion. To many in the West, this view has led to more recent blind spots, as regimes of various types around the world have created and established models for information management that reinforce very different political goals, doing so with previously unheard-of effectiveness. While specific states have created impactful models, understanding the broader backbone of digital authoritarianism is most relevant to consider as actors pursue global policy and business strategies.

With that said, readers are encouraged to engage with this work with an open mind and a willingness to enter into good-faith dialogue. The Digital Economist believes in intellectual diversity with a research direction fostering an inclusive spirit toward sustainable development. Understanding the range of methods to assess and react effectively in an informatized world is essential to that mission and underscores the scope and timeliness of this publication.

1. Historical Context

Scholars in the West once famously proclaimed an "End of History" after the Cold War. To many, this entailed the leveraging of economic, political, and technological tools to promote the inevitable march toward democracy as the dominant form of governance around the world. This tied well with ICT development patterns, namely the invention and implementation of the internet, which began as an American military and research technology. By the 1990s, the End of History period, the internet took on a new and expanded role as it was being commercialized into the platform driving economic and communication across borders and markets that exists to this day.[1]

Two factors have complicated the "utopian" vision of this form of US–led development:[2]

1. ICT penetration has expanded beyond the initial intent toward connecting specific nodes of sedentary, place-based computers to mobile devices that are increasingly portable and affordable. While expanding ICT access through mobile devices brings benefits, it also complicates governance and increases the potential for a wider range of political expression, including revolution—a constant concern for governments worldwide.
2. The risk for unrest is heightened by technological development as innovation always has the potential to displace workers and destroy industries, breaking down communities and economies in the process. Notably, these concerns have grown more urgent as AI has become more advanced in recent years.

These realities highlight the transition from the End of History to a new era: the age of the "digital natives." "Digital natives describe individuals who have no prior knowledge of society untethered to universal ICT platforms (such as the internet, social media, etc.). These individuals generally belong to the millennial, Generation Z, and Generation Alpha demographics—groups that are maturing into a determining bloc of voters, activists, and other political actors. Among other characteristics, these generations exhibit frustration and growing challenges to fomenting meaningful social change in large part due to their orientation toward ICT dependence in everyday life. Studies throughout the early twenty-first century highlight how digital platforms, by their very nature, may inhibit necessary reform and alleviate polarization.[3]

Polarization is a readily observable condition present in many polities today and remains a persistent problem for security and development. One notable result has been the enabling of extreme voices in the public square that can threaten waves of unstable change as conflict persists among the increasingly divided populace. The internet and social media add fuel to this fire by creating easy means to produce widely accessible rhetoric and bullying language while the work and debate of substantive policy solutions is harder to achieve at scale (see figure 1 below).[4]

Figure 1: Eight Dimensions of Social Media Usage (based on Tudoroiu, “Social Media and Revolutionary Waves”)

In statecraft, the End of History has now become a time of geopolitics defined by “Cyber Balkanization.” This phenomenon is supported by the establishment and ossification of separate internet ecosystems seen throughout different countries, often on a global East–West axis. This brings up many important questions about border policy when it comes to delineating digital spaces, a resulting condition completely at odds with the purpose and intent of the internet as a communications and commercial platform. In addition, the use of the internet in these separate ecosystems has become further divided in some countries as consumers and governments find preference in driving specific tasks toward specific platforms (or vice versa).[5]

Balkanization has emerged in parallel with what officials like former US Secretary of State Hillary Clinton call "a new information curtain." Today, there are more authoritarian regimes than democracies, and that fact alone supports the policy analysis direction of this and similar analyses for understanding modern geopolitics. These regimes, unsurprisingly, are actively engaged in developing "censorship regimes" in the post-Soviet era, and some states—namely, China, Russia, and theocracies—have made an impact in this area by pioneering non-Western models to follow. This background is also of interest to other states that have some democratic characteristics and institutions but are not fully liberal in nature, as these "anocracies" often pursue repressive policies to maintain stability and control.[6]

2. Western Concepts—and How They Have Declined

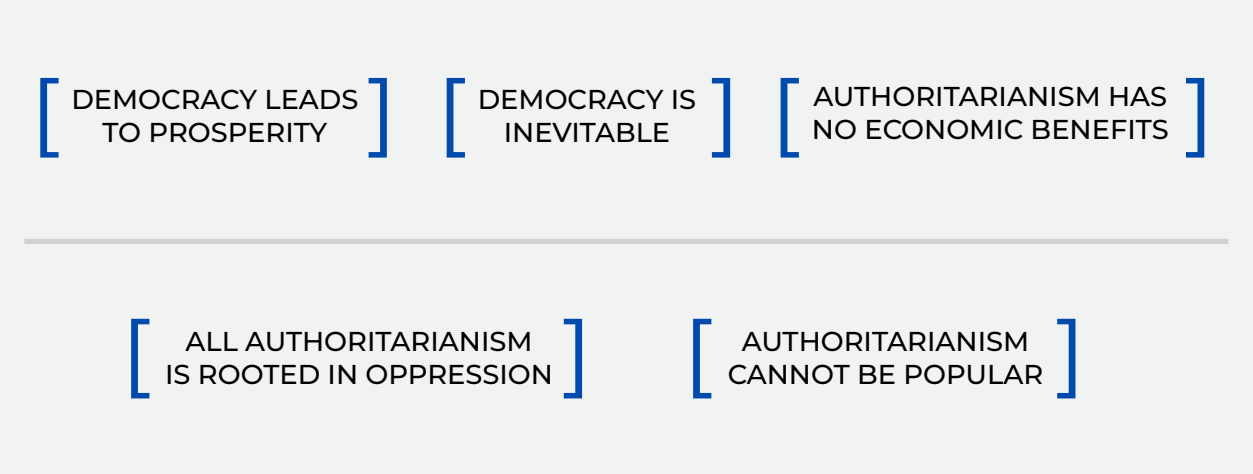


Figure 2: Myths of Democracy and Authoritarianism (based on Morozov, The Net Delusion)

The ubiquity of technology products and solutions in the global economy has standardized many practices in communication, culture, and technology. One of these practices involves basic research in the information age as developed by influential companies like Google. An early examination of "googling" showed that the basic desire for information and explanations has significant political consequences. This work led to the positing of a "Google Doctrine" where the ability to search for information will illuminate suffering, thus providing the emotional motivation for rising against oppression. Movements would be further supported by social networks that can communicate instantly online and spread information that can unite supporters and organize effective next steps. In this way, the Google Doctrine outlines how connectivity growth inevitably dooms dictatorships and is a way forward for opposition forces everywhere.[7]

Similarly, authoritarians have earlier been theorized to threaten their own ability to rule in the advent of the internet and social media. This is perhaps best encapsulated by the "Streisand Effect," so named after the celebrity Barbara Streisand, who wanted a picture of her house removed from the internet, only to find that the image attracted even more scrutiny as a result. In this way, the concept outlines that the more an actor moves to erase digital content, the more interesting that content will be to the public. Naturally, this has now become an area of focus for authoritarians and others with an interest in controlling publicly available content, as mere deletion of content carries political consequences.[8]

Yet mere activity online—whether it be written advocacy, crowdsourced reporting, or malicious manipulation of code—has not proven to be an effective strategy for democratization due to the persistence of online-fueled "slacktivism," or slacker activism. Under this principle, many online users are lulled into the facetious belief that engaging online (and on social media in particular) will inevitably drive social change, yet the reality is just the opposite. The internet is often the place where social movements die, as encapsulated by the long-term status of the countries where the "Arab Spring" was most prominent. There, authoritarian and anoncratic regimes persist and have solidified in a useful case study for dictators everywhere.[9]

This sense of online utopianism is a product of the profit motives of the large technology corporations that produce the essential digital products for life in the modern world. In this era, these corporations have a nakedly capitalist incentive to drive traffic and usage on their platforms, particularly as investors have frequently prized user bases and data sources as part of capital evaluations. At the same time, tech companies occupy a position where they can and want to become powerful sociopolitical actors that, at the very least, represent a lobby unto itself with the ability to make or break political careers. However, this trend has also shifted as the bank of users in democracies has become more saturated, which makes authoritarians and their followers/citizens more attractive to new sources of income and relevance.[10]

3. The Political Power Behind Information Communication Technology (ICT)

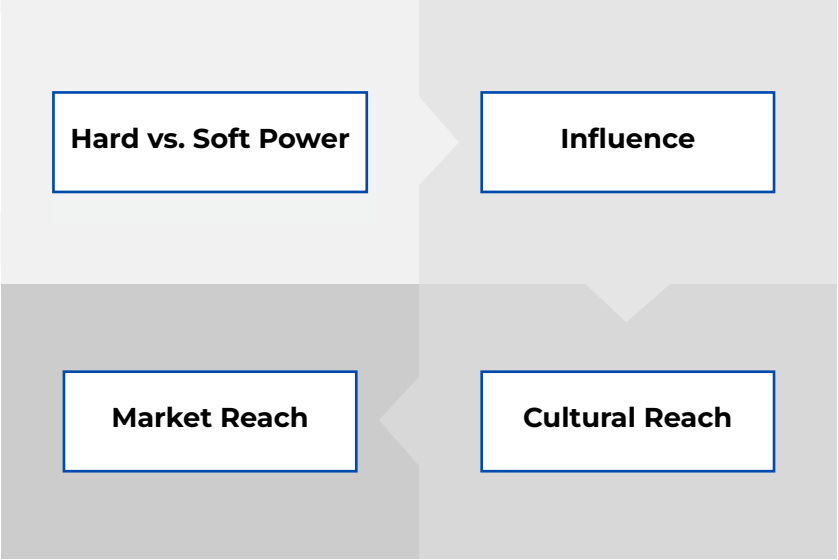


Figure 3: Process for Imparting Socioeconomic Power based on Nye, "The End of Cyber Anarchy")

Figure 3 above highlights how powerful online actors face a dilemma in how to penetrate target audiences to maintain their strong positions. Given the vastness of the online space and the potentially limitless capabilities, markets, and polities available to control, it is perhaps inevitable that control over digital space is extremely competitive. The highly competitive space of the internet is thus a controlling lever of society that generally revolves around four blocs of actors, as seen in figure 4 below.[11]

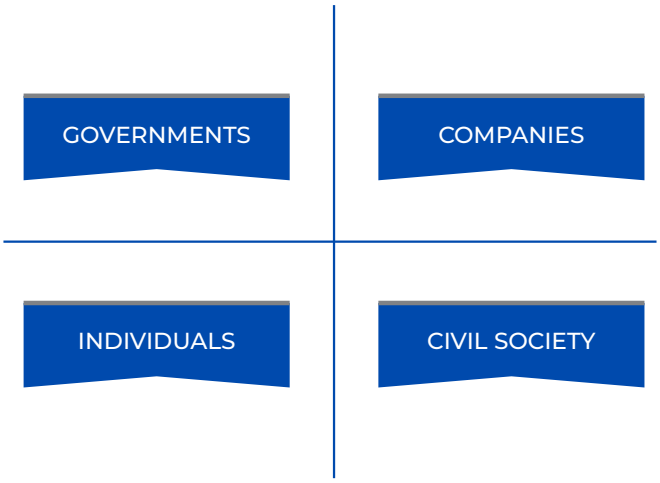


Figure 4: Competitors for Internet Control (based on Morozov, The Net Delusion)

Based on this observation, the manipulability of individuals due to misinformation, technological dependence,[12] and the weakening of civil society due to "slacktivism"[13] leads to a race for networks control that ultimately rests between the public and private sectors. This has serious (and still largely uncertain) consequences for the growth, development, and direction of the modern Habermasian "public sphere."[14] Each side has powerful bases of support and leverage over the other and can easily lead to a stalemate of sorts. Therefore, the fusion of tech actors and empowered governments represents a model for modern authoritarianism that appears to benefit both sides while shutting out other competitors and making opposition movements and innovation more difficult.

That said, such a fusion of massive institutions—and the data supporting them—presents unavoidable challenges. Sustainable storage becomes an issue from a space, environmental, and regulatory perspective. This requires new laws that can better manage the ever-growing need for information to drive networks and economies. There is also a similar need to manage public opinion as these policies are carried out, for some of the decisions made in this area may not necessarily be perceived as in the public's interest if the public is informed as such.[15]

This situation encourages a continued decline in information literacy driven by an institutionalized push toward decentralizing news broadcasting and consumption. This strategy produces confusion among the public, as it becomes harder to distinguish reliable sources. Disinformation is further incentivized as journalism is less profitable in part due to what Manuel Castells calls the "networked news environment decided through business power struggles." In the end, there is significantly little social trust, a political feeling that lends itself well to the dictatorial reformist attitude of authoritarians.[16]

Trust is further complicated by what Joseph Nye would call "cyber anarchy." This form of anarchy is more than just a space where there is no appearance of a dominant regulatory force. It is a more confusing situation for users where they face several other conclusions, namely a greater focus on political legitimacy within their given "territory" on the internet and a feeling of living in the next "Wild West" where everyone is in control yet no one is at the same time.[17]

The result is a cultural practice of "networked individualism," a condition that explains much of the social angst of our time. Individuals are empowered in this decentralized internet/social media ecosystem, but to a point—especially if they are operating in the confines of an authoritarian network administrator/regime. Individuals naturally also crave community membership and involvement, thus becoming ever more addicted to online activity and connectivity as what they may perceive as their only true opportunity for community. This creates a situation where an individual's online and offline personalities merge, which makes deception, fakes, and any form of identity theft all the more damaging and potentially socially ruinous.[18]

Individuals, therefore, have a major stake in promoting a stable internet and social media environment, and it is understandable how many would readily support more authoritarian control of networks from a safety and security perspective. Yet the activities of many netizens (internet citizens) suggest that draconian positions from governments may not entirely satisfy the core desires of the digital public. Here, norms represent an opportunity to better govern digital conduct and accessibility, yet norms can only exist where political legitimacy is unquestioned. As a result, the interaction between the public and the state when it comes to internet governance is still important because attracting legitimacy can allow governments to carry out desired digital agendas in legal gray areas while maintaining social calm and perhaps even some political popularity.[19]

Nye adds that "cybernorms" have further dimensions with international policy implications. The implementation of norms will always remain a significant political risk in digital spaces because there are no effective mechanisms for timely mass enforcement. Also, attempts to use norms to "de-weaponize" the internet will always face opposition from many states due to perceptions that it would create defense and security vulnerabilities. For this reason, norms remain a hotly debated topic in international diplomacy and among multinational organizations that still struggle to provide globally applicable standards to connectivity and human activity spanning across borders.[20]

Governments have an additional desire to engage fully in legitimacy conversations with the digital public because the alternative mode of internet governments by individualist control is risky for three reasons: [21, 22]

1. There are still questions about what an empowered individual user looks like today, with one glaring risk being that of a challenger to political power that could create uncontrollable political instability.
2. Individual users left to their own devices could engage in deep introspection about the nature of their presence online, wondering if their own content is the result of independent thought or a product of manufactured emotional response by digital manipulators.
3. Such philosophical considerations can additionally take on an added economic dimension as users may question whether demand shapes platforms or vice versa; this question could, in the extreme, upend digital products and their corresponding corporate developers, adding economic stress to affected states.

4. Conflict and Conversation within Digital Authoritarian Spaces

The rise of ICT has prompted urgent and important conversations about the levers and tools of political control and revolution. Scholars have found that, thus far, the world faces a mini-crisis as it attempts to reconcile the realities of the "technologization of solidarity" gripping public affairs today. The internet has created wider and larger communities of practice, allowing heterogenous groups to operate with direction across borders. Meanwhile, the principles of "clicktivism" (an offshoot of "slacktivism") have fostered some sense of togetherness within groups. Yet the organizational challenges for activists persist, and the internet and social media have become synonymous with social division, a reality readily exploitable by established and emerging authoritarian actors.[23]

Authoritarian states, by their very nature, are interested in institutionalizing their policy direction as solidly and rapidly as possible. In the digital sphere, institutionalization serves three primary purposes:[24]

1. To control the populace through the establishment of a legitimate and peaceful society that can operate without anarchy.
2. Institutions provide a conduit for unified political communication so that the public is clearly aware of where the government stands and the means with which it will enforce policy.
3. Legitimacy is further established through institutions that funnel communication and requests of the government (from domestic and international actors) to places where an organized response is possible.

This is most evident in diplomacy, where international leaders and ambassadors need to know who they are dealing with and whether they can properly influence events and policy in the country in question.

Institutions are also useful for authoritarians, given the power and necessity of bureaucracy in any society. Ideas like "bureaucratic oppression," as coined by Steven Feldstein, can ensure compliance and control. The monitoring features of digital networks facilitate such actions, as it is easy to implement mass, national-level policies very quickly. This "oppression" can thus include red tape to prevent undesirable/"illegal" action, laws and policies that permit social "venting" of grievances in an (often effective) attempt to avoid and regulate collective action, and directly influencing acceptable cultural practices and symbols through specific and articulated limitations, orders, etc.[25]

It is important to note here that the theories of the early internet still hold that technological innovation does not determine social direction on its own. Such an idea falls under the theory of "technological determinism" and fails to adequately address the offline social inputs that enter into the information space. Social perceptions, historical trends, and political thought exist independently of the development of technological tools (at least initially). ICT, therefore, plays a role in amplifying and providing (often misleading) context or framing of real-world information but does not predetermine a society's background when heading into the digital space.[26]

From this viewpoint, oppression under dictatorial authoritarianism takes on several qualities as facilitated by the malicious affordances of ICT: [27]

1. Authoritarian states are technologically empowered to research, identify, and take advantage of cyber vulnerabilities for their targets (formal adversaries, dissident populations, and other deemed threats).
2. These states may have an incentive to directly attack these targets with the goal of creating precise negative or weakened outcomes for the opposite side; this precision is a hallmark and attractive feature of cyber tools in a conflict ecosystem.
3. Digital tools can facilitate useful espionage efforts that complement the information actors may gain from more transparent means. This allows state and state-aligned actors to be better informed of threats, emerging vulnerabilities, and any potentially disrupting factors to social stability.

Youth populations are most affected by these measures, and they are a population vulnerable to the machinations of authoritarians with a thirst for digital power. At first glance, youth almost always appear to have an advantage against tyranny due to their lack of adherence to the status quo. These thoughts have multiplied in recent decades as digital natives have come to represent the hope for reformed societies. While it is true that youth populations are prone to advanced technology use, represent a nation's health (through measures such as demographic distribution and productivity), and set major cultural trends, these individuals hold significant political liabilities. In addition to the time-honored lack of experience and general restlessness exhibited by young citizens, youth today face confusing divisions in identifying causes for a rebellion that compounds the preexisting effects of a lack of understanding of how to effectively organize groups for collective action.[28]

That said, countering digital dictatorship is still possible, at least in small pieces. This is outlined in the idea of "concealment" in sociopolitical movements.[29] Perhaps the most visible of this form of rebellious practice is the use of figurative language. Netizens under repressive and restrictive regimes of censorship manage to evade filtering systems with cleverness and a sense of humor.[30] This language, combined with the continued refinement of technological systems designed to evade authoritarian scrutiny, can be effectively deployed at the local level where specific hot-button issues can be resolved through public exposure and an attitude of open negotiation with national-level authorities that reflects an understanding of the need for social and political stability.[31]

These techniques exist in a space where the toolbox for revolution is more vast than ever before. Social media has organized leaders and "influencers" in ways that do not reflect political prowess or inherent interest. As a result, revolutions in the twenty-first century—namely, the Arab Spring—benefitted from mobilization technologies but nonetheless failed. That said, ICT can still facilitate meaningful political collective action, but studies have shown that such techniques involve more antiquated technology. Email-driven campaigns, communication, and coordination work better in fostering communities that can accomplish group-oriented missions due to the need for etiquette and norms as well as the fact that such use aligns well with the initial purpose of the technology when it was invented.[32]

These realities lead to a "dictator's dilemma," which observers like Feldstein outline in three primary ways:[33]

1. The "cost of digital repression" is increasingly "expensive," requiring a large bureaucracy and a growing requirement of tax receipts from citizens. This economic pressure alone presents the potential for a reputational risk crisis for the government as it tries to hold on to legitimacy. Additional promises to increase standards of living under these intense competing priorities must be at least somewhat effective to mollify the public and keep collective action risks manageable.
2. Dictators must, therefore, face the choice of specific repression or "systemic change" as an argument for continued social trust; the former choice has a greater track record of success, particularly in the most powerful authoritarian states while the latter may be attractive in societies where citizen grievance is piqued.
3. Governmental response to negative social stimuli may be more impactful if framed as promoting the continuance of a "democracy" that only exists in a de jure sense.

5. Playing "Cat and Mouse" Games: Mutual Monitoring in the Digital Age

Modern political conflict is observed most clearly through the lens of information competition. This battle for dominance in the information space is of particular concern to authoritarians, who have a vested interest in crafting social messages and understanding sources of potentially debilitating descent. Here, surveillance emerges as a critical component of authoritarian regimes, especially as the digital realm becomes a more central piece of society as a whole. These state or large non-state actors are already aided by the reality that most information today is readily available, either publicly or with minimal effort, with basic tools. In this way, one can wonder if anything is really covert in the modern age and ponder the large-scale political impacts this observation can create—namely, the growing importance of message repetitiveness and saturation in a given space/market/audience. As an overall policy direction, this reality coalesces in the form of authoritarian preferences toward information manipulation through moves as subtle as public opinion tampering to higher cost solutions like malware tailored toward reducing/eliminating a specific set of risks.[34]

For their part, dissidents can arm themselves with a few different strategies. Surveillance is not a one-way street dictated by state powers. “Sousveillance,” or watching back, is a powerful mechanism for implementing bespoke checks on authoritarian power. The development of such capabilities is in and of itself a form of protest formation and a supporting piece of evidence behind the idea that mutually assured retaliation is a default norm of internet discourse. That said, the ubiquity of a vast array of publicly available information may negate these benefits, much like it hinders empowered authoritarians.[35]

Organizing sousveillance is an additional challenge, though some models have emerged in the social media era. “Cyber militias” can take advantage of proxy technologies and principles to leverage mass mobilization at cost and scale. However, the rapidity and widespread reach of these “forces” lends itself to internal uncertainty over authority and command portfolios.[36]

Another technology that has benefits for mass organization is SMS, better known as text messaging (texts). Texting’s brevity and ease of use encourage the short, timely communication needed to bring people together to meet and pursue/accomplish granular goals. The small size of these messages across networks is useful because it frees up bandwidth for other activities— namely, high-energy content creation (videos, images, AI outputs, etc.). In addition, texting provides a new avenue for engaging in information and its affiliated psychological warfare by reaching key audiences/voters in a more direct, personal, and vulnerable context; in this area, state-based authoritarians theoretically have even more resources to engage in similar tactics.[37]

That said, a more traditional node of dissidence still persists even in online worlds: terrorism. Terrorist strategy, at its most general, involves a cat-and-mouse game to avoid crippling counterattacks by staying “off the grid.” Messaging amplification affordances online further encourage a well-formed adoption of extremist ideology that can stake a viable claim in the information space without low-cost censorship or other adverse state intervention. At the same time, the divide between digital enforcement reach and offline considerations (namely, the persistence of real-world laws, borders, and diplomacy) can play an advantageous role for aggressive anti-state actors.[38]

The result of all this conflict and competition is a state of "techno-scientific dystopia" reflective of the rise in chaotic and divisive politics. As the stability of various states may be in different levels of social breakdown and decay, this scenario also empowers those relatively more stable and less "divided" countries to press their advantage to further their interests at the expense of the weakened states.[39] Part of this breakdown comes from the "leaderless networks" where the decentralization encouraged by internet affordances creates a classic leadership vacuum that authoritarians are most poised to fill.[40]

Feldstein provides a general overview of how this void is addressed by digital dictators, highlighting a two-pronged approach:[41]

1. Authoritarians engage in an elaborate scheme of harassment in line with their commitment to "bureaucratic oppression." In addition to creating emotional and monetary stress for opponents, this strategy is nearly limitless in scope due to the fact that government coffers are generally quite robust.
2. Disinformation campaigns—which can draw from the same government funding—can directly affect education policy (in the form of media literacy) and security, all while ensuring a covert implementation that lowers the risk of political controversy.

6. A Note on Censorship

The control of speech is a major area of regulation in the digital sphere. While different countries (and different authoritarian actors) have their own refined and preferred methods, several different concerns predominate:

- Early analyses of the internet show that blogging has occupied a "free space" even in the most restrictive of societies. In this way, the blog can be seen as a key battleground between regimes and their opponents. This is based on a couple of factors, including the affordances of content length to allow for well-formed thought sharing while maintaining an adjustable ambiguity in deeming such work as officially "published." Such a status can be changed as is most appropriate for establishing personal authenticity and political credibility at any moment.[42]
- Hackers have become direct political actors, and their activism ("hactivism") brings a new dimension to the influence of crime and

corruption on societal stability. While these actors face the same difficulties in sustainable community organizing, they are savvy and equipped enough with low-cost, high-impact tools that can level the playing field in matching the digital power of the state.[43]

- Instances of real-world dissident expression and protest have palpable effects on digital platforms. In this way, opposition movements can drive social media use that may be leveraged in credible and more effective attempts at traditional political organization through the leveraging of popularized grievances/causes.[44]

Authoritarians and their supporters also group these kinds of dissident activity as part of a broader poisoning of the information space, which threatens to permanently cripple social trust and cohesion. These actors reach such a conclusion based in large part on the mountainous amount of harmful content accessible online and thus react strongly with shows of support for and investment in censorship regimes. This outcome further disproves the idea of "technological determinism" and the Western post–Cold War belief that the internet can foster worldwide freedom. In fact, such a reversal of expectations paints traditional Washington in such a poor light that the brand of an "agenda backed by the United States" has become fuel for the ambitions of other states, with significant great power implications as a result.[45]

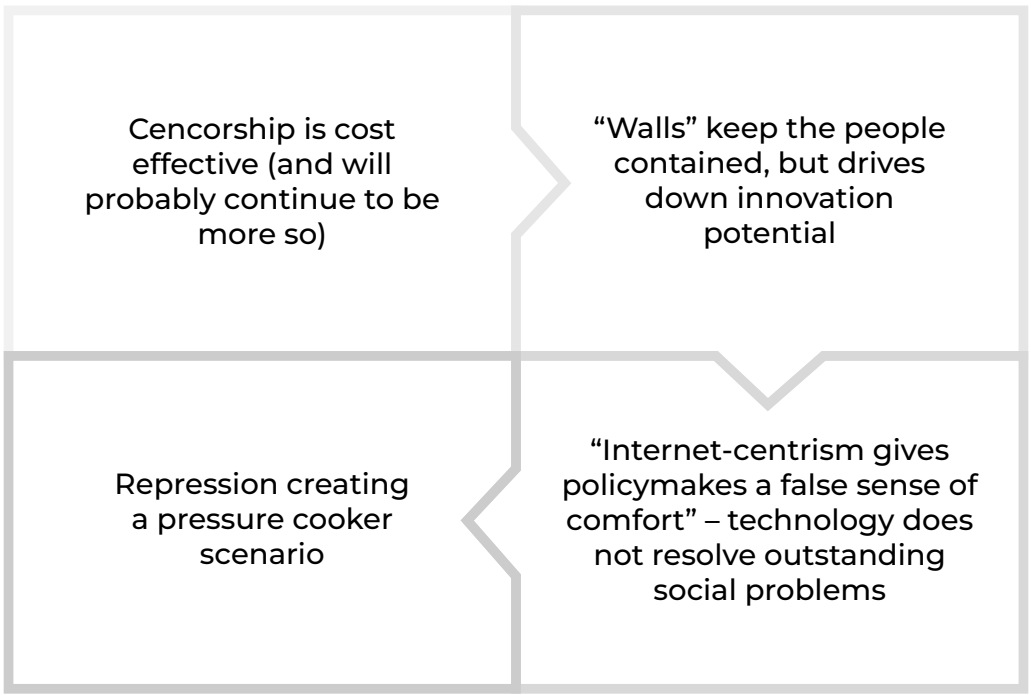


Figure 5: The Censorship Dilemma (based on Morozov, The Net Delusion)

Yet censorship is not a cut-and-dried decision for many authoritarian states. There remains a tangible dilemma facing censorship efforts for policymakers (see figure 5). While censorship is cost-effective to implement (at least in the short term), the cordoning off discourse and research drives down innovation potential. This further promotes infection in the policymaking and political conscience of the state because "internet-centrism"—or the belief that the observable internet represents the range of real-time opinion and knowledge available in the world—"gives policymakers a false sense of comfort" that is not justified due to the persistence of outstanding social problems. Finally, as these problems become more acute, more forceful repression becomes necessary, creating a pressure cooker scenario where opposition figures and/or chaos could replace the status quo.[46]

Revolution, in this view, is possible if a number of causes are present to provide fuel. The prospect of leveraging digital tools to present such a forceful challenge to oppressive rulers is a topic still being developed at the scholarly level. At the same time, "local affiliate revolutionaries diffuse the ideology of the primary revolution within the local society." In the digital space, this raises an important question: What is "local" in digital politics? Answers to this complex question in an interconnected world are compounded due to international revolution contagion," which suggests that the principle of virality as practiced most visibly in social media trends may provide a contagious element in the digital political corpus.[47]

This type of repression serves as an attractive force toward greater activity in social media overall. Social media's community-based model allows for a space that seems to many users as a place for the disempowered to gather in ways previously impossible. Messaging tools on these platforms provide easy ways to spread messages quickly and in a multimedia fashion. In addition, social media has been popular among youth populations who may be more inclined to rebelliousness, at least in the short term.[48]

In response, authoritarian interest is most logically drawn toward a "customization of censorship." This approach reflects the specific policy needs of the regime and acknowledges key political weaknesses to address in its messaging campaigns. Narrowing the scope also allows for greater adaptation and tweaking that takes advantage of cultural intricacies that can authentically appeal to a wide section of the public. These goals then can be overlapped with appropriate digital technology affordances to achieve the greatest reach and the accomplishment of greater legitimacy over the country's sociotechnical ecosystem.[49]

Here, it is important to consider a focus on search topics queried by netizens. Authoritarian systems "aid" their users by selective filtering based on specific subjects as determined by query frequency, political sensitivity, and consumer demand. This is most recently overlaid on top of algorithm-driven systems (to include AI models) that further drive netizen research, education, economy, and discourse through the personalization of content recommendations. This result is as simple as it is chilling: "selective avoidance" or the willful ignorance of information that is not searched in an effort to avoid painful cognitive dissonance.[50]

The emergence of AI presents some dangerously empowering consequences driven by "selective avoidance"[51] that may, in the future, present as clear societal ignorance of critical sociopolitical issues. AI's power still remains attractive to authoritarians, however, as the improvement of such systems and models can continue to construct a "global brain of censorship" that has been a far-off goal for some time. Naturally, arriving at this valuable output brings into question the kinds of training data involved. That said, what is potentially even more damaging is the reality that hallucinations in this massive and widespread artificial censorship regime could lead to truly destructive outcomes. This is especially relevant when theorizing the lack of exposure to key concepts essential for economic and environmental management in both democracies and authoritarian states. As a result, a potential end-case scenario is that there would be more reason for legitimate citizen questions against draconian enforcement of restrictive policies like censorship that make no sense in promoting a great society.[52]

7. Basic Technical Tools and Their Known Effectiveness

The use of specific technologies is a critical component for dominating the digital space as a whole. Depending on the choice of tools and their implementation, network managers and authoritarians may be able to pursue a plausible range of cyberattack options and associated protective measures to secure continued legitimacy over digital "territory." We have already seen that the opinions held by the public at large can and may be weaponized to achieve certain political ends. At the same time, censorship regimes can do more than merely restrict content—the ideological direction behind the construction of such sociotechnical systems also drives efforts to obliterate access to both current and historical data.

An early yet effective cyber manipulation strategy worth considering is distributed denial of service (DDoS) attacks. DDoS attacks started the trend of leveraging nonhuman computer network users (such as bots) to create an amplification of the masses on a massive scale. Such widespread spoofing can overwhelm both network platforms and offline society as the proliferation of multiple identities can physically paralyze content and data services central to economies worldwide.[53]

Another related tool that can and has caused major social and economic damage is ransomware. The hostage-taking nature of ransomware has a special appeal for leaders looking to cement their all-encompassing presence in global systems and economies. The wide range of targets often pursued by perpetrators—whether social, political, or economic in background—allows for some plausible deniability and the potential perception of justified action from authoritarians, bullies, and thieves of all stripes.[54]

Social psychology provides further motivation and support for how such positioning through cyber tools deployment can empower abusive state actors. Confirmation bias plays a major role in this reality, as aspects like "ideological selective avoidance" collide with the siloed nature of social media to solidify echo chambers preaching incomplete views of the world. The cultivation of such biases is even more encouraged as well-informed individuals with authoritarian leanings realize that with a diverse population now connected with greater speed thanks to ICT, there is a potential for more diverse interacting opinions that can, in turn, broaden the range of acceptable political possibilities and outcomes envisioned by citizens. The end result is a logical conclusion that more advanced censorship is the best way forward for security purposes.[55]

Such an assault on diverse opinions does not appear to be limited to purely domestic concerns. This is most clearly seen in the nascent history of election interference experienced by fully democratic states in the social media age. Malign actors have pursued, cultivated, and improved sophisticated misinformation campaigns carefully crafted to drive specific policy outcomes. These efforts benefit from a general perception of the internet as an anarchic social space that lacks broad-based recognition of "measurements of [digital] order." This not only makes it difficult for netizens to recognize and agree to specific responses to out-of-control content or dialogue online but also does not provide for adequate guardrails that would curtail social manipulation through the enforcement of strong norms.[56]

Members of the digital public themselves may have become useful conduits for repression. In this view, authoritarians are especially focused on the "targeted persecution of online users," a task that is best implemented by perceived average members of the public. These members generally present themselves online as either influencers or trolls. Influencers in this space act as de facto gatekeepers with a perceived power and social reach reflective of their many followers. In capitalist liberalized democracies, this popularity is associated with responding to market demand and economic opportunities of the moment. In authoritarian states, such conditions are so intricately folded into the power of the state that, in reality, influencers in those countries must toe the party line and align with the policy preferences of the recognized legitimate leadership. Trolls, on the other hand, employ tactics that have the most impact at scale; this is what makes cyberbullying so potentially harmful for many internet users. The state can assist trolls in this mission through bot networks (botnets) designed to flood platforms with given content or messaging. Content and messaging to target have become increasingly easier to process due to the advancement of algorithms that produce perceivable and insatiable (if biased) "confirmed" truths. This accomplishes a particularly useful outcome of drowning out many voices, effectively paralyzing the silent majority of public opinion in a given state.[57]

A more crude tool of ICT control involves not the digital networks themselves but the external resources needed to power them. In this way, internet shutdowns can be a popular choice for policymakers facing an emerging threat. However, without the platform of online discourse, meaningful connections and chains of information are stunted. Given that information flows are the backbone of the modern economy, this reality has the potential to drive social pain and instability. This strategy is most often employed in regional contexts, given a specific increase in potential unrest. In this way, states make a bet that this form of hostage-taking can secure a better long-term deal for authoritarian rulers.[58] Nye seconds this notion and extends this thinking further to include making threats to the continued viability of electric grids that physically power computers and other machines forming the backbone of the world economy.[59]

Digital authoritarians are also attracted to data localization techniques in the form of moving hosting sites/servers to specific territories. Democracies have engaged in this policy, too, as a response to restrictive data control rules in certain countries, and a resulting decentralization of information

fits well with the checks and balances baked into more liberalized political systems. This has serious implications for national digital economies that do not have a historical foundation directly connected to the internet, as these states must contend with imported infrastructure to support national internet. For states with authoritarian and cyber-balkanized leanings, this is likely a continuing dilemma in digital policy.[60]

8. Rules, Regulations, and Legal Foundations

The most visible centerpiece of digital disputes and crime is online vandalism. Dissident and alternative voices often favor this phenomenon because it is a readily accessible form of detectible protest. As such, rebellious elements, groups, and people are naturally drawn to this mode of cyber property destruction as a core strategy. Vandalism is also easy to carry out because it is a low-cost, high "reward" that does not boomerang into long-term damage for the perpetrators. This is based on the perception that most digital activities do not encourage direct and obvious causal outcomes with high stakes in the physical world (though one may wonder if this conclusion will change as technology penetration accelerates).[61]

On the other hand, protecting the integrity of networks and data is also a priority for aligned dissident groups. In this way, paths toward controlled information access—most notably through encryption—are no longer the sole concern of large network administrators, including actors representing authoritarian states. Encryption, therefore, emerges as a point of emphasis that highlights the elite and rarified nature of opposition movements while shielding the identity and critical characteristics of such activities that would otherwise provide credible material for authoritarians to narrate persuasive pretexts discrediting otherwise socially acceptable aims. At the same time, encryption allows opponents to fight back through frustrating efforts to uncover such valuable information, thus draining time and other resources away from other efforts to squash dissent; this is magnified when considering that locking key pieces of information can render certain products and communications useless and without actionable directions for those locked out.[62]

From this, legal frameworks generally include three principle buckets: laws governing cyberspace, laws governing cybersecurity, and laws governing data access and control. This trifecta is accomplished in authoritarian regimes through the transformation of "rule of law" systems perfected in

liberalized democracies where due process reigns over all into "rule by law" configurations where dictatorial leaders and bureaucracies ossify their rule through fiat codified into clearly written statutes. It is here where the divide within digitally connected global populations is most pronounced, to an extent where future cultural trends will be greatly influenced by how these divides play out in the worldwide ICT "public sphere."[63], [64]

One area of intense focus within this divide is the prosecution of libel cases in cyberspace. At the broadest level, the question of governance and security through a legalist approach centers around amplification and speed. In this way, there is much to ponder about at what point the internet adds ammunition to ad hominem criticism, as well as any associated consequences that may be involved. Damaging one's image has more ripple effects on the well-being of a person—now more than ever—yet the time to respond to such massive threats has shrunk considerably as information sharing has become instantaneous. This experience is easily empathized by median citizens/voters and forms the basis of a common legal argument by populist-leaning authoritarians who look to align with the people's general desire for a maintained social order given the potential for violence that can result from unchecked cyberbullying.[65]

Conclusion: Toward a New Culture

Although dictators are not normally associated with the true character of the people they rule, even the most hardened totalitarian must be aware of certain patterns in their respective societies. This is truer now more than ever as information communication technologies continue to proliferate. For this reason, several information regimes have emerged and have been perfected, leveraging technologies that were Western developed in engineering and attitude. This is the result of a gradual decline of American influence and a resulting void in global cultural commonality that leaves a situation without a dominant superpower in soft power.[66]

This transition away from a liberalized Western-dominant nexus of sociotechnical innovation is the great trend of our time. Analyses of this development must, therefore, take into account a wider range of global conditions as we seek to better understand the uses, intentions, and impacts of the internet, social media, and AI. The associated questions must consequently cover the exploration of digital societies and their citizenries (netizen-ries) to include important zeitgeists and political trends, including the future resolution of polarization and tribalism.

Citizens are as motivated as ever to forge digital identities with an interest in sustainable personal and cultural prosperity. They desire economic success and opportunity, as well as love from fellow people through measurable self-worth (as may be derived by online popularity, for example). Many citizens find, however, that these goals are frustrated or excessively confusing, leading to the strengthening of grievances. Political actors are most interested in these grievances by advocating (at least at face value) policies that appear to address the core issues involved. This report outlined in some detail how ICT platforms reinforce this cycle, providing the fear and outrage that can sustain organized and competent authoritarianism.[67]

From a cultural perspective, digital authoritarianism represents an evolution in sociopolitical development toward greater introspection. Netizens have expressed a greater desire for a more localized focus on digital networks, with a greater attraction toward messaging and content geared toward local audiences. This has contributed to a greater "politicization of web services" that reflects how localized culture has played a role in drawing citizens into digital networks. Insularity in political thinking fits well with authoritarians who may have political priorities to draw the populace away from outside voices and ideas that could threaten their rule.[68]

Another contributing factor is the growth of "internet addiction." This phenomenon emphasizes how digital interaction has become absolutely essential to participating in life-sustaining economic and interpersonal activities. Such a reality has made it extremely difficult for the average user to disconnect. Advantageous actors and bullies—including digital dictators—are, therefore, incentivized to exploit this to sculpt a compliant digital society and effectively isolate those who refuse to participate "appropriately" in the state's digital ecosystem.[69]

In summary, the scale of sociopolitical competition on the internet and in ICT development is higher than ever. The prevalence of extreme voices and authoritarian actors ready to pounce on the inviting affordances of new, digitally powered systems has begun to paint a picture of political and economic control unique to our interconnected century. As a result, questions of how new technological advancements and the worries about stability from various publics will continue to interact and play a central role in the debates and policymaking in the foreseeable future.

About the Author

William J. Vogt

William Vogt is a senior executive fellow for policy at The Digital Economist, a Washington, DC, think tank. In this role, he recently moderated a panel on digital foreign policy at the Davos conference in Switzerland. He is the author of Foundations of the Chinese Internet, as well as several research articles about China, technology, and international development. He is the former managing principal at Weilian Poder Global Consulting, an advisory and political risk research firm focused on China and emerging markets. He is also a former adjunct professor at Georgetown University and the Catholic University of America, where he taught courses on Chinese digital society. He holds two degrees from Georgetown, a master of arts in communication, culture, and technology and a bachelor of science from the School of Foreign Service. During this time, he wrote two theses with distinction about information technology and politics in emerging market countries, the latter of which was “ICT for Dictators” (2016). He was also a visiting student at Nanjing University, Capital University of Economics and Business in China, and Universidad San Francisco de Quito in Ecuador.

References

1. Hayden, Patrick, and Chamsy el-Ojeili, *Globalization and Utopia* (Palgrave Macmillan, 2009).
2. Morozov, Evgeny, *The Net Delusion*, Public Affairs, 2011.
3. Morozov, *The Net Delusion*.
4. Wojcieszak, Magdalena, "Does Online Selectivity Create a Threat to Deliberative Democracy?: Cyber Skepticism Reconsidered," *International Journal of Technology, Knowledge, and Society* 1.5 (2006).
5. Wojcieszak, "Does Online Selectivity Create a Threat to Deliberative Democracy?: Cyber Skepticism Reconsidered."
6. Morozov, *The Net Delusion*.
7. Morozov, *The Net Delusion*.
8. Morozov, *The Net Delusion*.
9. Wolfsfeld, Gadi, Elad Segev and Tamir Sheafer, "Social Media and the Arab Spring: Politics Comes First," *The International Journal of Press/Politics* 18.2 (2013).
10. Morozov, *The Net Delusion*.
11. Morozov, *The Net Delusion*.
12. Yar, Majid, "Virtual Utopias and Dystopias: The Cultural Imaginary of the Internet," *Utopia: Social Theory and the Future*, Routledge, 2016.
13. Yar, "Virtual Utopias and Dystopias: The Cultural Imaginary of the Internet."
14. Tudoroiu, Theodor, "Social Media and Revolutionary Waves: The Case of the Arab Spring," *New Political Science* 36.3 (2014).
15. Russell, Adrienne, "Extra-National Information Flows, Social Media, and the 2011 Egyptian Uprising," *International Journal of Communication* 5 (2011).
16. Russell, Adrienne, "Extra-National Information Flows, Social Media, and the 2011 Egyptian Uprising."
17. Nye Jr., Joseph S, "The End of Cyber Anarchy?: How to Build a New Digital Order." *Foreign Affairs*, 101 (2022).
18. Comunello, Francesca, and Giuseppe Anzera, "Will the Revolution Be Tweeted? A Conceptual Framework for Understanding the Social Media and the Arab Spring," *Islam and Christian-Muslim Relations* 23.4 (2012).

19. Jamali, Reza, *Online Arab Spring: Social Media and Fundamental Change*, Chandos, 2014.
20. Nye Jr., Joseph S., "The End of Cyber Anarchy?: How to Build a New Digital Order."
21. Comunello and Anzara, "Will the Revolution Be Tweeted? A Conceptual Framework for Understanding the Social Media and the Arab Spring."
22. Wojcieszak, "Does Online Selectivity Create a Threat to Deliberative Democracy?: Cyber Skepticism Reconsidered."
23. Scott, Martin, "Distant Suffering Online: The Unfortunate Irony of Cyber-Utopian Narratives," *International Communication Gazette* 77.7 (2015).
24. Morozov, *The Net Delusion*.
25. Feldstein, Steven, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford University Press, 2021).
26. Morozov, *The Net Delusion.*.
27. Kello, Lucas, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38.2 (2013).
28. Frangonikolopoulos, Christos A., and Ioannis Chapsos, "Explaining the Role and the Impact of the Social Media in the Arab Spring," *Global Media Journal: Mediterranean Edition* 7.2 (2012).
29. Jamali, O*nline Arab Spring: Social Media and Fundamental Change*.
30. Vogt, William J., *Foundations of the Chinese Internet: Calculations, Concepts, Culture* (Kendall Hunt, 2023).
31. Jamali, *Online Arab Spring: Social Media and Fundamental Change.*
32. Russell, "Extra-National Information Flows, Social Media, and the 2011 Egyptian Uprising."
33. Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*.
34. Deibert, Ron, "Cyberspace Under Siege," *Journal of Democracy* 26 (2015).
35. Scott, "Distant Suffering Online: The Unfortunate Irony of Cyber-Utopian Narratives."
36. Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft."
37. Morozov, *The Net Delusion*.
38. Morozov, *The Net Delusion*.
39. Yar, "Virtual Utopias and Dystopias: The Cultural Imaginary of the Internet."

40. Frangonikolopoulos and Chapsos, “Explaining the Role and the Impact of the Social Media in the Arab Spring.”
41. Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*.
42. Frangonikolopoulos and Chapsos, “Explaining the Role and the Impact of the Social Media in the Arab Spring.”
43. Allagui, Ilhem, and Johanne Kuebler, “The Arab Spring and the Role of ICTs,” *International Journal of Communication* 5 (2011).
44. Wolfsfeld, Segev, and Sheafer, “Social Media and the Arab Spring: Politics Comes First.”
45. Deibert, “Cyberspace Under Siege.”
46. Morozov, *The Net Delusion*.
47. Tudoroiu, “Social Media and Revolutionary Waves: The Case of the Arab Spring.”
48. Jamali, *Online Arab Spring: Social Media and Fundamental Change*.
49. Morozov, *The Net Delusion*.
50. Wojcieszak, “Does Online Selectivity Create a Threat to Deliberative Democracy?: Cyber Skepticism Reconsidered.”
51. Wojcieszak, “Does Online Selectivity Create a Threat to Deliberative Democracy?: Cyber Skepticism Reconsidered.”
52. Morozov, *The Net Delusion*.
53. Morozov, *The Net Delusion*.
54. Nye, “The End of Cyber Anarchy?: How to Build a New Digital Order.”
55. Wojcieszak, “Does Online Selectivity Create a Threat to Deliberative Democracy?: Cyber Skepticism Reconsidered.”
56. Nye, “The End of Cyber Anarchy?: How to Build a New Digital Order.”
57. Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*.
58. Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*.
59. Nye, “The End of Cyber Anarchy?: How to Build a New Digital Order.”
60. Allagui and Kuebler, “The Arab Spring and The Role of ICTs.”
61. Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*.
62. Morozov, *The Net Delusion*.
63. Jamali, *Online Arab Spring: Social Media and Fundamental Change*.

64. Tudoroiu, “Social Media and Revolutionary Waves: The Case of the Arab Spring.”
65. Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*.
66. Morozov, *The Net Delusion*.
67. Wolfsfeld, Segev, and Sheafer, “Social Media and the Arab Spring: Politics Comes First.”
68. Morozov, *The Net Delusion*..
69. Yar, “Virtual Utopias and Dystopias: The Cultural Imaginary of the Internet.”

About

The Digital Economist, based out of Washington D.C. is an ecosystem of 40,000+ executives and senior leaders dedicated to creating the future we want to see: where digital technologies serve humanity and life. We work closely with governments and multi-stakeholder organizations to change the game: how we create and measure value. With a clear focus on high-impact projects, we serve as partners of key global players in co-building the future through scientific research, strategic advisory and venture build out. We are industry-agnostic as most high-impact projects touch many different industries. Our portfolio ranges from energy transition to ethics in emerging technology.

CONTACT: INFO@THEDIGITALECONOMIST.COM