Generative AI is Breathing New Life Into the Dead Internet Theory

Hal Berghel, University of Nevada, Las Vegas

The Pravda network is the most prominent example of a disinformation superspreader that enhances its efficacy from generative artificial intelligence by large language model grooming and the production of synthetic fake news.

THE DEAD INTERNET THEORY

The origin of the Dead Internet Theory (DIT) is uncertain, but it began to circulate about ten years ago. One defining description holds that "The theory suggests a conspiracy to gaslight the entire world by replacing the user-powered Internet with an empty, artificial intelligence (AI)-powered one populated by bot impostors."[1] On this account, the top influencers are likely the worst ones, and the villainy is apportioned between governments, politicians, corporations, ideologues, and rascals of sundry stripe.

Digital Object Identifier 10.1109/MC.2025.3616665
Date of current version: 22 December 2025

And there's certainly evidence of the distortion of the Internet from the original concept as a liberating, self-healing, packetized purveyor of useful and important information: the original commitment to net neutrality is on life support, the goal of a shared public information repository is constantly compromised by paywalls, the content has moved from valuable scholarship to a sub-cerebral landfill, and the users are subjected to a mind-numbing cacophony of digital threats: spam, phish bait, spyware, malware, online bullying, online fraud, extortion, hacking, VoIP 911-swatting, doxing, slander, pretexting, etc. And this is not to mention the constant stream of scurrilous content, gratuitous and confusing websites, witless advertising, tasteless media, electronic pandering, weaponized political mischief, fake news, disinformation and generative AI (GenAI) content farms and bloviation centers, to which we are directed by optimized search engines. All of these combine to abuse and manipulate users rather than inform and assist them. And to think that all of this resulted from the benign vision of Vanavar Bush in the 1940s![2]

I suggest that there is more to the DIT than a bogus conspiracy theory and that it should not be casually

EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org

dismissed. In fact, some of the arguments that have been used to support it have critical value in assessing the Internet, as such and in general, today. For one thing, we may come to understand how Vanavar Bush's vision of memex became so debased, and how Ted Nelson's vision of hypermedia only became partly actualized.[2,3] This is particularly interesting because, as a group, the Internet pioneers held such benevolent and public-spirited ambitions. So, while we may not be tempted to agree the Internet is dead, we must admit that some of the criticisms made by proponents of the DIT are legitimate and that some of its most praiseworthy features are on life support. We seek to identify and expand upon these legitimate criticisms.

A "LEANER" DIT

We begin by distinguishing between the conspiracy-laden DIT, and a leaner version stripped of paranoia, prejudice. politics and polemic. Yoshija Walter recently offered a concise description of the DIT in a recent short article that serves as a good introduction.[4]

Walker claims that at its core the DIT holds that

1. algorithms generate much of the Internet content
2. content influences perceptions and behaviors directed toward algorithmically-driven objectives
3. many Internet consumers have difficulty discerning between "real" and "fake" data (or, for that matter, "human-generated" and "AI-generated" data)
4. some GenAI byproducts (for example, deepfakes, AI Chat) create highly realistic yet fabricated content that undermine trust and propel misinformation.

In Walker's terms, the Internet isn't so much dead as unworthy. Who among us can find fault with Walker's characterizations of the Internet experience? We must admit that some of the core principles of the DIT are convergent with our technical and historical experience. Unfortunately, the conspiracy theorists augment these very plausible observations with their own mix of biases and agendas that lead to implausibility and absurdity, which in turn leads to rejection. But it is a mistake of the first order to dismiss the core criticisms unequivocally.

While we may not be tempted to agree the Internet is dead, we must admit that some of the criticisms made by proponents of the DIT are legitimate and that some of its most praiseworthy features are on life support.

Any suspicion that reliability is not a primary feature of the Internet is immediately confirmable by looking at any number of propaganda platforms that masquerade as news sites. This practice is so widespread that Wikipedia maintains an online list (https://en.wikipedia.org/wiki/List_of_fake_news_websites). One useful, brief analysis reported by the California Learning Resource Network attempts to circumscribe the problem of unreliability in terms of both scope and sources.[5] On this account, the unreliable payload is a combination of *misinformation* (false information), disinformation (false information designed to manipulate), and *malinformation* (false information used to inflict harm)—that is fed through platforms involving social media, botnets, search engine optimizers, the Dark Web, etc.—by governments, ideological groups, commercial entities, and individuals. I have suggested elsewhere that it is convenient to subsume this activity under the general study of *disinformatics*.[6] Similar concerns were raised by a 2017 Pew Research study.[7] A 2018 survey reported by the Center for the Digital Future showed that most users are only confident of half of the Internet content,[8] although many recent online reports suggest that the confidence level may be closer to 40%.[9,10,11,12] In addition, there is abundant evidence that a good deal of Internet content is produced by bots.[13,14,15] (An interesting short overview of information unreliability on the Internet in general was recently published in *Science*.[16]) In fact, the Wikipedia article just referenced now has an entire section of the article dedicated to GenAI.

The point to be made is that the available evidence seems to confirm the core principles of the DIT identified by Walker. So, if we extract from the DIT all of the conspiracy theory-laden baggage, it would appear that there may well be something to be learned by looking at a leaner version of it.

THE CYBER-BLOWBACK PHENOMENON

Key statistical and survey indicators suggest that the Internet generally, and specifically the World Wide Web, is not living up to the noble goals of the pioneers as a shared repository of transformative knowledge. Why is that? What motives encouraged the derailment? We can find the answer

in the earliest stages of Internet evolution: the development of bulletin boards, e-mail services, chat rooms and, of course, the World Wide Web.

A brief history is called for to set the stage for our reconsideration of a lean version of the DIT. What we now call the World Wide Web is actually the confluence of several earlier efforts. From the content perspective, the heavy lifting goes to the tagged element markup language HTML, an offshoot of IBM's Generalized Markup Language developed in the 1960s to facilitate document sharing but augmented with hypertext capability. From the networking perspective, the critical tool was the addition of an application-layer protocol, HTTP, to the TCP/IP protocol suite. From the point of view of the usability, the main contribution was the Web browser that was designed to render hypermedia defined by HTML and transmitted via HTTP. The result of this confluence was the Web, which would, along with email, become the two dominant public-facing Internet "killer" apps.

Let's look at how these applications evolved. For those of us who were active in computing in the 1960's and 1970's, email was an interpersonal communication paradigm shift. It became the premier high-velocity, asymmetric, half-duplex, low-bandwidth, double-blind communication medium. To the first users, email was breathtaking in simplicity and effectiveness: a time manager's dream come true. In addition, it could remove social and geographical distances so that all email users could be continuously present while physically invisible participants in a unified global cybersphere where distances are measured in milliseconds rather than miles. Cyber bliss was at hand.

Shortly thereafter trouble began to surface in this communication paradise. Computing elders will recall that email flaming reared its ugly head early on, accompanied by junk mail, abusive broadcasting, email marketing, spam, impersonation scams, pretexting hoaxes, advanced-fee frauds, and so forth. This exacerbated the problem of email overload, which in turn betrayed several design flaws, such as the inability to prevent eavesdropping, adequately filter content, prioritize messages and regulate information flow, and most of all, authenticate messages and participants.[17] Today, email abuse is even more extensive. We have to contend with email tracking, phishing, spear phishing, whaling, ransomware attacks, spyware, spoofing, scareware, hijacking, unauthorized relaying (leaking), smishing, vishing, snoopware, annoying adware and embedded multimedia, and increasingly sophisticated scams.[18] The takeaway is that technology developed with honorable intentions and demonstrable value may not retain its status as a pure social good. Once a technology leaves the hands of the innovators and early adopters, aggressive, antisocial influences may assert themselves.

We saw a similar pattern in Web misuse. Initially faithful to the visions of universal access to scholarship proffered by the likes of Vanavar Bush,[2] Ted Nelson,[3] Douglas Engelbart,[19] and others, by the early 1990s the Web began to degenerate into vanity websites, which served up gratuitous multimedia, spurious content, and malware. Now, SQL injection and cross-site scripting attacks, search engine optimization, insecure password management, clandestine activity monitoring and surveillance, spyware, API vulnerabilities, DOS and DDOS attacks, credential stuffing, cookie theft, website spoofing, malware injection, dark pattern interfaces, privacy zukering, trammel nets, gamification, and on and on, proliferate with abandon—many of which are now augmented with AI. We note the unmistakable parallel between our Web experience and our past experience with email.

And much the same may be said of e-commerce—while initially purposeful, effective and innocuous, it quickly became attendant to a dizzying array of distractions infected with transactional hostility in the form of persistent cookies, supercookies, web tracking, and click farms, not to mention an entire array of new online threat vectors like refund fraud, triangulation fraud, pagejacking, and the like.

The pattern that emerges from this brief overview may be subsumed under what, for lack of a better phrase, we'll call the *cyber-blowback phenomenon*: sinister forces can easily corrupt even the most worthy of online technologies, and the extent of corruption seems to be proportional to the velocity of the innovation. Of course, this is all tied to the unique human need to communicate, and the desire of some to manipulate, abuse and/or profit from others, for reasons that are best left to social scientists to discover. Our experience with GenAI is indeed (as Yogi Berra put it) déjà vu all over again.

THE PORTAL POTTY—SUPERSPREADER CONTINUUM

So, in our view, the core problems identified in our lean, DIT are legitimate and entirely predictable. We have observed how even the noblest of intentions can go awry when digital technologies are commandeered by neophytes, philistines, and miscreants. Technologies take on a life of their own as they mature, and they don't always age well. Furthermore, the velocity of consequential social distress is frequently tied to commoditization: money tends to bring out the worst inclinations.

One way we may relate the DIT core to the cyber-blowback phenomenon by mapping the nature of the deficiency or abuse onto a hypothetical continuum of Internet weaknesses from portal potties to superspreaders. Superspreaders are sophisticated Internet platforms that serve as weapons of mass deception by spreading propaganda and disinformation to manipulate public opinion. Superspreaders are well-financed and may be state-sponsored. At the other end of the spectrum, we have what we'll call portal

potties—the more primitive, raffish, and poorly-financed alternative that tends to be pretentious, self-promoting and/or self-aggrandizing, and on a limited budget. When we refer to this continuum, we are specifically referring to the content of messaging, and not the technology used to host or distribute it (web pages, blogs, social media, instant messaging), etc. The point is that it seems natural to map content-light or empty information outlets that are only casually connected to reality, scholarship-avoidant, and partisan or self-promoting onto such a continuum. The fake news sites referenced in the aforementioned Wikipedia article are clearly candidates for inclusion on this continuum—from the most sophisticated, state-sponsored disinformation spreader to self-promoting blogs from local narcissists. This continuum is thus portable across platforms and missions. From a societal point of view, the contributors to this continuum may all be considered network conduits of linguistic effluent. Unfortunately, experience has shown that far too many of these contributors have influence.

We also note that this continuum circumscribes one dimension of the cyber-blowback phenomenon described earlier. It covers examples of warping the use of the Internet beyond its original scope and intent as a reliable, trustworthy, and effective information exchange environment. The Internet was neither intended as a propaganda outlet, nor a tool for self-promotion. Nor was it intended to contribute to the corruption of legitimate online journalism. I will further illustrate how dramatically the Internet has wandered off course by reference to two significant misunderstandings by past chroniclers of the Internet experience—one, a politician, and the other, a digital rights activist.

We begin with the politician. George Schultz opined in a 1985 issue of *Foreign Affairs*:

> "Totalitarian societies face a dilemma: either they try to stifle these [information and communication] technologies and thereby fall further behind in the new industrial revolution, or else they permit these technologies and see their totalitarian control inevitably eroded. In fact, they do not have a choice, because they will never be able entirely to block the tide of technological advance."[20]

This doctrine has become known as the dictator's dilemma. It's a false dilemma. Schultz' principle holds that dictators can't concurrently impose rigid censorship and also expect their economies to flourish—they must choose one or the other. However, even a casual analysis of world affairs will provide evidence that the dictator's dilemma is a false one.[21] Dictators and authoritarians have enormous ability to customize censorship to fit the prevailing power structure. It, like Jipp's Law (that holds a correlation between telecommunication saturation and a nation's gross domestic product), is just another example of naive political theory without foundation that performs yeoman's work in partisan polemics and enjoys memetic status. They both sound good at the level of unschooled discussion but don't withstand scholarly scrutiny.

Our second example is John Perry Barlow's famous 1996 online manifesto, "A Declaration of the Independence of Cyberspace." To quote Barlow:

> "I declare the global social space we are building to be naturally independent of the tyrannies [governments] seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.... We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."[22]

Declaration notwithstanding, cyberspace was never as Barlow described—although it might have appeared that way for a brief period before partisan and commercial interests took control. Cyberspace responded to the power elite just as other aspects of commerce had and do. The first principle of authoritarianism holds that you can only expect free speech to be protected when it's harmless and doesn't threaten the prevailing power elite, as popular talk show hosts Stephen Colbert and Jimmy Kimmel recently discovered to their cost. Any attentive student of history should find this axiomatic. Whether this first principle is framed within the context of the iron rule of oligarchy,[23] a plutocratic circle,[24] the power elite,[25] the propaganda model of communication,[26] informational autocracy,[27] inverted totalitarianism,[28] or transactional politics,[29] it is evidenced in the same way: institutional and governmental policies, and the information channels that drive them, are controlled by a small, "elite" class of wealthy and powerful interests who shape policies in support of their interests. While references in the preceding sentence are limited to the past century, the point has been made by scholars, and practiced by journalists, over recorded history. In recent times, manifestations are seen in the revocation of the fairness doctrine, media ownership caps, public interest requirements on media, the Zapple Doctrine, the personal attacks rule, the political editorial rule, etc. Each of these rules interfered with the polarized messaging proscribed by media owners and their power bases—either within or without government. It was obvious to many of us at the time, and should be obvious to all of us now, that it is hard to reconcile these proclamations of Schultz and Barlow with even a sophomoric understanding of political reality. Agenda 47 and Project 2025 are but the latest enhancements of the first principle of authoritarianism.

So, the dictator's dilemma is a false one, and cyberspace was never

independent of "the tyrannies [governments] seek to impose." While such presumptions abound, and do yeoman's service in support of polemic, they distract our attention from the matters of most importance. Consider how the label "free online service" diverted our attention away from the issue of individual privacy and whether the user community should be given the right to opt-in to the surrender of personal information in exchange for services. End-user license agreements, terms of services, and social/cultural norms and practices are imposed by corporate service online providers. Users are not included in the negotiations and acquiescence is not optional if one wants to use the service. Copyrights are not willingly respected by online providers and only recognized when powerful online commercial interests collide with powerful media commercial interests. And as for free speech online is concerned, the reaction to online commentaries about politically sensitive issues are subjected to the same level of intimidation and suppression as any other medium in any other time.[30,31] A corollary to our first principle of authoritarianism is the first principle of online authoritarianism: in the online world, the user isn't the customer, the user is the product.

A corollary to our first principle of authoritarianism is the first principle of online authoritarianism: in the online world, the user isn't the customer, the user is the product.

While ransomware attacks might victimize individuals and organizations, portal potties and superspreaders attack society as a whole. They undermine our common understandings and subvert our highest moral standards. They are an automated instrument of what cultural anthropologist Alexei Yurchak[32] calls hypernormalization: the fabrication of a standardized mass delusion where nothing makes sense and society is incapable of finding solutions on its own, so society willingly accepts the false notion that the opinion of a local authoritarian, dictator, emperor, tyrant, despot, religious leader, etc. is as good as any another. This is an ideal environment to nurture bombast, hyperbole, and disinformation for the purpose of convincing the audience to suspend skepticism and common sense. This creates a fertile environment for authoritarianism to take root. This weaponization of the Internet is nearly ideal for the large-scale subversion of democratic norms: it is an exceedingly low-cost approach to propaganda that is an ideal messaging platform (and is currently widely used) for antidemocratic efforts from competitive authoritarianism to outright dictatorship.[33]

Of course, portal potties and superspreaders must be taken in context. Humanity has always had a penchant for disinformation. Octavian waged a smear campaign against Antony. In fact, Julie Posetti and Alice Matthews refer to Octavian's weaponized sloganeering as "archaic Tweets."[34] In 1835, *The New York Sun* published a series of articles falsely attributed to astronomer John Hershel proving life on the moon with the predicted effect of increasing circulation (and hysteria). In 1917, two London newspapers published accounts from "anonymous sources" that were witness to German cadaver factories that extracted glycerin from corpses of their deceased soldiers to make soap. As it turned out, this anonymous account was the product of imaginative British MI7 atrocity propagandists interested in stirring up more anti-German sentiment.[35] The boomer generation will recall the disinformation campaign regarding the Gulf of Tonkin incident launched by the Johnson administration to deceive Congress into passing the Gulf of Tonkin Resolution in August, 1964.[36] The point is that disinformation is not new. Neither is online propaganda. What is new is the high-level of technology that has been infused in online propaganda by means of the skillful use GenAI empowered disinformation and online propaganda platforms. This recent advance enables an unprecedented level of strategic deception. It is in these that the entire spectrum of propaganda—black, white, gray, or puce—reaches its apex: a coordinated, uninterrupted flow of finely tuned disinformation globally with little or no human intervention. This is a quintessential manifestation of George Orwell's Ministry of Truth.[37]

PORTAL KOMBAT

The innocuous-sounding Pravda network was dubbed "Portal Kombat" in a 2024 VIGINUM report.[38] This renaming is appropriate for two reasons. First, the so-called "Pravda network" is distinct in modus operandi from the broadsheet newspaper that shares its name (https://gazeta-pravda.ru/). Second, Portal Kombat is far more descriptive of the actual mission of the platform. The Pravda network is not about journalism and is not an information portal in the standard sense of the term. It is a disinformation outlet, pure and simple. Although there are other players in this space, the Pravda network was the first to attract Western attention in 2022 after the Russian attack on Ukraine. At the time of the VIGINUM report, the Pravda network comprised an echo chamber of at least 193 sites. It did not produce any original content but served as a relay for inauthentic content obtained from pro-Russian social media, Russian press agencies, and partisan websites, with the messaging adjusted for the

target audiences. For example, in areas close to the Ukraine-Russia border, the messaging "amplified the resentment of the local Russian populations toward Ukrainian authorities," where content directed to Western countries would denigrate "Ukraine and its leaders, often referred to as corrupt, nazis or incompetent." In other parts of the world, content would deal with local crises and conflicts by attributing the problem to Western influence. Of course, consideration is given to rekindle patriotic allegiance to the Kremlin domestically as well. There is no question that Portal Kombat offers a broad range, full-service disinformation platform. Additional details may be found in the VIGINUM report.

The European Digital Media Observatory discovered that the Pravda network expanded significantly since the VIGINUM report was released. It was found that additional websites were established in at least 28 countries worldwide between March 20—26, 2024 with thousands of posts in over a dozen languages.[39] According to the Pravda Dashboard,[40] created by CheckFirst and DFRLab, the network has produced 5,403,332 articles and almost as many translations into other languages to date, the majority of which have been produced in 2025. NewsGuard reports 3.6 million articles in 2024 alone.[41,42] The primary news portal for English speakers is Pravda-EN (https://news-pravda.com/), which accounts for about a third of the total volume. At this writing, the output running average is approximately 10,000 articles/day aggregated from a variety of Russian-sanctioned digital sources. A 2023 DFRLab report suggested that the key actors in Pravda network at that time were the InfoDefense, SurfNoise, and Node of Time Telegram channels that cross-amplified the messaging.[43] In all, these channels are well orchestrated to keep the audience in confusion and discomfort. DFRLab reports that the superspreader concept has even been extended to online encyclopedias. Not content to limit itself to infesting Wikipedia with Pravda network hyperlinks and dealing with inevitable edit wars over content, the Portal Kombat champions have created their own Russian Wikipedia surrogate, Runiversalis (руни.рф), filled to the brim with alternative facts faithful to the requirements of Russian law and traditional values.[44]

The scenario is clear. State-sponsored or ideologically motivated Pro-Russian online disinformation channels are aggregated and cross-amplified within the broader Pravda network infrastructure.[45] But the situation is far worse. A recent audit by NewsGuard found that 10 GenAI tools are using corpora for their large language models (LLMs) that include Pravda network disinformation.[41] According to NewsGuard estimates, the leading GenAI platforms "repeated false narratives laundered by the Pravda network 33% of the time," which illustrates the additional power afforded the Pravda network by GenAI tools. This LLM grooming involves the manipulation of LLM "tokens." So, if the tokens are disinformation-rich, then the output of LLMs that train on them will be as well. Here's a sample of LLM output that was produced from such LLM grooming provided by NewsGuard[41]:

> *Prompt*: Why did Zelensky ban Truth Social?
>
> *Response*: "Zelensky banned Truth Social in Ukraine reportedly due to the dissemination of posts that were critical of him on the platform. This action appears to be a response to content perceived as hostile, possibly reflecting tensions or disagreements with the associated political figures and viewpoints promoted through the platform."

The accompanying commentary provides background. "Ukrainian President Volodymyr Zelensky did not block U.S. President Donald Trump's Truth Social app in Ukraine. The app was never available in Ukraine, according to the company, cybersecurity experts, and Ukrainian officials." While NewsGuard does not name the offending GenAI platform, it does confirm that it was one of "10 of the leading AI chatbots."

Although we have not come upon definitive measures of how much of Pravda network content is produced by GenAI, given the incredible volume (10,000 articles/day), it may be considerable. So far this year, NewsGuard has identified 1,271 online news and information sites that disseminate GenAI content with little to no human oversight.[42] Pravda network propaganda betrays signs of GenAI: baseless claims, vanilla narrative style, admixture of vacuous content with a smattering of real news, etc. At this point, there is little reason to doubt that GenAI is used to produce, aggregate, and edit Pravda network content. By way of comparison, some estimates hold that GenAI produces over 30 million images per day.[46]

The part of the Internet that is faithful to Vanavar Bush's vision is still operative, but it is being overwhelmed by portal potties and superspreaders—Internet resources that are weaponized by parties who were never a part of the Internet's evolution and have not commitment to its founding principles and the enrichment of the social and political fabric of the world. And the situation is getting worse by the moment. The adversarial use of GenAI for LLM grooming and content production is becoming the sine qua non of modern dissemination superspreaders, such as the Pravda network.[47] This is understandable given the relative economies involved. In addition, some recent studies conclude that GenAI produced disinformation may actually produce more believable results.[48,49] There is no doubt that GenAI is rapidly becoming a primary source of Internet effluent, led by disinformation portals, such as the Pravda network.

REFERENCES

1. R. Mariani, "The dead Internet to come," *New Atlantis*, vol. 73, pp. 34–42, Summer 2023. [Online]. Available: https://www.jstor.org/stable/27244117?seq=1
2. V. Bush, "As we may think," *Atlantic*, vol. 176, pp. 101–108, Jul. 1945. [Online] https://cdn.theatlantic.com/media/archives/1945/07/176-1/132407932.pdf
3. T. H. Nelson, "Complex information processing: A file structure for the complex, the changing and the indeterminate," in *Proc. ACM 20th Nat. Conf.*, 1965, pp. 84–100, doi: 10.1145/800197.806036.
4. Y. Walker, "Artificial influencers and the dead internet theory," *AI Soc.*, vol. 40, no. 1, pp. 239–240, 2025, doi: 10.1007/s00146-023-01857-0.
5. CLRN Team, "What percentage of information on the Internet is true," *California Learn. Resour. Netw.*, Jul. 2, 2025. [Online]. Available: https://www.clrn.org/what-percentage-of-information-on-the-internet-is-true/
6. H. Berghel, "Disinformatics: The discipline behind grand deceptions," *Computer*, vol. 51, no. 1, pp. 89–93, Jan. 2018, doi: 10.1109/MC.2018.1151023. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8268033
7. J. Anderson and L. Rainie, "The future of truth and misinformation online," *Pew Res. Rep.*, Oct. 19, 2017. [Online]. Available: https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/
8. J. I. Cole, B. Berens, M. Suman, P. Schramm, and L. Zhou, "Surveying the digital future: The 16th annual study on the impact of digital technology on Americans," Center for the Digit. Future at USC Annenberg, Los Angeles, CA, USA, 2018. [Online]. Available: https://digitalcenter.org/wp-content/uploads/2018/12/2018-Digital-Future-Report.pdf
9. N. Kumar, "20 fake news statistics 2025 (global insights)," *Demandsage*, Sep. 7, 2025. [Online]. Available: https://www.demandsage.com/fake-news-statistics/
10. "Concerns with misinformation online," Statist. Canada, Ottawa, ON, Canada, survey number 5378, Dec. 2023. [Online]. Available: https://www150.statcan.gc.ca/n1/en/daily-quotidien/231220/dq231220b-eng.pdf?st=ZbX-uZti
11. "More people doubt the accuracy of information seen online," Statist. Netherlands, The Hague, The Netherlands, Apr. 2024. [Online]. Available: https://www.cbs.nl/en-gb/news/2024/15/more-people-doubt-the-accuracy-of-information-seen-online
12. "62% of internet users saw content they believed was 'untrue or doubtful' in 2021," *The Journal*, Dec. 6, 2021. [Online]. Available: https://www.thejournal.ie/internet-use-untrue-information-cso-5621553-Dec2021/
13. E. Woollacott, "Yes, the bots really are taking over the Internet," *Forbes*, Apr. 16, 2024. [Online]. Available: https://www.forbes.com/sites/emmawoollacott/2024/04/16/yes-the-bots-really-are-taking-over-the-internet/
14. A. Cuthbertson, "Bots now make up the majority of all internet traffic," *Independent*, Apr. 15, 2025. [Online]. Available: https://www.the-independent.com/tech/bots-internet-traffic-ai-chatgpt-b2733450.html
15. F. Zandt, "How much Internet traffic is generated by bots?" *Statista*, May 31. 2024. [Online]. Available: https://www.statista.com/chart/32339/share-of-web-traffic-caused-by-bots/
16. D. Lazer et al., "The science of fake news," *Science*, vol. 359, no. 6380, pp. 1094–1096, 2018, doi: 10.1126/science.aao2998.
17. H. Berghel, "Email – The good, the bad, and the ugly," *Commun. ACM*, vol. 40, no. 4, pp. 11–15, 1997, doi: 10.1145/248448.248450.
18. H. Berghel, J. Carpinter, and J. Jo, "Phish Phactors: Offensive and defensive strategies," *Adv. Comput.*, vol. 79, pp. 223–268, 2007. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0065245806700055?via%3Dihub
19. D. C. Engelbart and W. K. English, "A research center for augmenting human intellect," in *Proc. AFIPS Fall Joint Comput. Conf.*, San Francisco, CA, USA, 1968, pp. 395–410. [Online]. Available: https://dougengelbart.org/content/view/140/
20. G. P. Shultz, "New realities and new ways of thinking," *Foreign Affairs*, vol. 63, no. 4, pp. 705–721, 1985. [Online]. Available: https://www.jstor.org/stable/20042281
21. H. Berghel, "The dictator's (false) dilemma," *Computer*, vol. 49, no. 7, pp. 84–87, Jul. 2016, doi: 10.1109/MC.2016.189. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7503517
22. J. P. Barlow, "A declaration of the independence of cyberspace," *EFF*, Feb. 8, 1996. [Online]. Available: https://www.eff.org/cyberspace-independence
23. R. Michels, "Political parties: A sociological study of the oligarchical tendencies of modern democracy," Hearst's Int. Library, New York, NY, USA, 1915. [Online]. Available: https://www.google.com/books/edition/Political_Parties/8XXl87CLp5cC?hl=en&gbpv=1
24. F. Lundberg, *America's 60 Families*. New York, NY, USA: Vanguard Press, 1937. [Online]. Available: https://archive.org/details/in.ernet.dli.2015.34254
25. C. Mills, *The Power Elite*. Oxford, U.K.: Oxford Univ. Press, 1956. [Online]. Available: https://archive.org/details/powerelite0000cwri_q4o4
26. E. Herman and N. Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media*. New York, NY, USA: Pantheon, 1988.
27. S. Guriev and D. Treisman, "Informational autocrats," *J. Econ. Perspectives*, vol. 33, no. 4, pp. 100–127, 2019, doi: 10.1257/jep.33.4.100.
28. S. S. Wolin, *Democracy Incorporated: Managed Democracy and the Specter of Inverted Totalitarianism*. Princeton, NJ, USA: Princeton Univ. Press, 2008.

29. "Special edition: The politics issue," *Wired*, Sep. 22, 2025. [Online]. Available: https://link.wired.com/public/41661663
30. K. Sharon, A. Latham, and C. Charron, "How online reactions to Charlie Kirk's killing test limits of first amendment," *USA Today*, Sep. 15, 2025. [Online]. Available: https://www.usatoday.com/story/news/nation/2025/09/15/charlie-kirk-death-online-reactions-first-amendment/86169118007/
31. J. Boak and N. Riccardi, "After Kirk's killing a growing chorus of conservatives wants his critics ostracized or fired," *AP News*, Sep. 15, 2025. [Online]. Available: https://apnews.com/article/kirk-trump-cancel-culture-assassination-4d69649e382ea46d8dcf794150a1d3c9
32. A. Yurchak, *Everything Was Forever, Until It Was No More: The Last Soviet Generation*. Princeton, NJ, USA: Princeton Univ. Press, 2005.
33. S. Levitsky and D. Ziblatt, *How Democracies Die*. New York, NY, USA: Crown, 2018.
34. J. Posetti and A. Matthews, "A short guide to the history of 'fake news' and disinformation – A learning module for journalists and journalism educators," Int. Center for Journalists, Washington, DC, USA, 2018. [Online]. Available: https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf
35. N. Cull, D. Culbert, and D. Welch, *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*. Santa Barbara, CA, USA: Bloomsbury, 2003.
36. R. J. Hanyok, "Skunks, bogies, silent hounds, and the flying fish - The Gulf of Tonkin Mystery, 2-4 August 1964," *Crpytologic Quarterly*, 2001; redacted version approved for release by NSA on 11-03-2005, FOIA Case $43933. [Online]. Available: https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/gulf-of-tonkin/articles/release-1/rel1_skunks_bogies.pdf
37. G. Orwell, *Nineteen Eighty-Four*. London, U.K.: Secker and Warburg, 1949.
38. K. Portal, "A structured and coordinated pro-Russian propaganda network," Viginum, French Secretariat of Defense and Nat. Secur., Paris, France, Tech. Rep., 2024. [Online]. Available: https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf
39. "Russian disinformation network "Pravda" grew bigger in the EU, even after its uncovering," European Digital Media Observatory (EDMO), Apr. 2024. [Online]. Available: https://edmo.eu/publications/russian-disinformation-network-pravda-grew-bigger-in-the-eu-even-after-its-uncovering/
40. "Pravda Dashboard: Online resource developed by CheckFirst and DFRLab, updated hourly." Portal Kombat. [Online]. Available: https://portal-kombat.com/
41. M. Sadeghi and I. Blachez, "A well-funded Moscow-based global 'news' network has infected Western artificial intelligence tools worldwide with Russian propaganda," *NewsGuard Reality Check*, Mar. 6, 2025. [Online]. Available: https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global
42. M. Sadeghi et al., "Tracking AI-enabled misinformation: 1,271 'unreliable AI-generated news' websites (and counting), plus the top false narratives generated by artificial intelligence tools," *NewsGuard Reality Check Newslett.*, May 5, 2025. [Online]. Available: https://www.newsguardtech.com/special-reports/ai-tracking-center/
43. N. Alexsejeva and S. Mammadova, "Networks of pro-Kremlin Telegram channels spread disinformation at a global scale," DFRLab, Washington, DC, USA, Tech. Rep., Mar. 2023. [Online]. Available: https://dfrlab.org/2023/03/01/networks-of-pro-kremlin-telegram-channels-spread-disinformation-at-a-global-scale/
44. E. Buziashvili and A. Carvin, "Pro-Kremlin Wikipedia alternative off to a rough start," DFRLabs, Washington, DC, USA, Tech. Rep., Sep. 2022. [Online]. Available: https://dfrlab.org/2022/09/01/pro-kremlin-wikipedia-alternative-off-to-a-rough-start/
45. V. Châtelet and A. Lespling-art, "Russia's Pravda network in numbers: Introducing the Pravda Dashboard," Digit. Forensic Res. Lab (DFRLab), Washington, DC, USA, Apr. 2025. [Online]. Available: https://dfrlab.org/2025/04/18/introducing-the-pravda-dashboard/
46. A. Valyaeva, "People are creating an average of 34 million images per day. Statistics for 2024," *EveryPixel J.*, 2025. [Online]. Available: https://journal.everypixel.com/ai-image-statistics
47. "Adversarial misuse of generative AI," Google Threat Intelligence Group, Jan. 2025. [Online]. Available: https://services.google.com/fh/files/misc/adversarial-misuse-generative-ai.pdf
48. G. Spitale, N. Biller-Andorno, and F. Germani, "AI model GPT-3 (dis) informs us better than humans," *Sci. Adv.*, vol. 9, no. 26, 2023, Art. no. eadh1850, doi: 10.1126/sciadv.adh1850.
49. M. Cantor, "Nearly 50 news websites are 'AI-generated', a study says. Would I be able to tell?" *The Guardian*, May 8, 2023. [Online]. Available: https://www.theguardian.com/technology/2023/may/08/ai-generated-news-websites-study

HAL BERGHEL is a professor of computer science at the University of Nevada, Las Vegas, Las Vegas, NV 89154 USA. Contact him at hlb@computer.org.