The Web At War: Hypertext, Social Media, and Totalitarianism

Hypertext, Social Media, and Totalitarianism

Mark Bernstein
Eastgate Systems, Inc.
bernstein@eastgate.com

ABSTRACT
In 2022, much of the world faced the prospect of a prolonged conventional war with a totalitarian state. The origins of hypertext lie in the wars of the 20th Century, and efforts to avoid a repeated conflict — and confidence that conflict could be contained if not entirely avoided — is deeply embedded into the architecture of the World Wide Web. The Web was not designed to confront a war, and it remains deeply vulnerable to totalitarian subversion. Our systems, platforms, and our discipline will need to adapt.

CCS CONCEPTS
• Applied computing $\rightarrow$ Computers in other domains; Military; Law, social and behavioral sciences; Law; • Social and professional topics $\rightarrow$ Professional topics; Computing profession.

KEYWORDS
Hypertext, Social Media, Politics, War

ACM Reference Format:

1 THE ORIGINS OF HYPERTEXT IN WAR
The 2022 Russian invasion of Ukraine, the first war between a totalitarian great power and a near-peer polity since 1945, presents at the time of this writing the prospect of a broad, prolonged, conventional conflict that involves many millions of people. By April, Russian officials openly discussed the prospect of an economic and political union extending from Vladivostok to Lisbon, and advocated the erasure of Ukraine from the ranks of nations [30]. The World Wide Web has never been at war, and little consideration has been given to its place in a prolonged conflict. The (insufficient) compass of this paper does not permit much discussion of solutions, technological and institutional, but we may begin here to catalog the challenges to a Web at war with a totalitarian state.

That little attention has been paid to the Web at war is ironic, because the intellectual roots of hypertext and the Web lie in the disasters of the short 20th Century [16] and the devastation of its wars [4]. We may briefly identify two independent strands in this heritage. First, widespread revulsion for the horrors of war led to a broad effort to neutralize propaganda and deceit through deeper understanding of language, communication, representation, and of the structures that underlie them. Indeed, a significant portion of this effort involved the invention of formal and synthetic language, the theory of information [14] and the identification of the potential of computation and its limits by Turing and Gödel. This strand of hypertext leads to formal models and languages for the Web [13], the management of Web Architecture [28], and the Semantic Web [27].

A second strand runs from the existentialist experience of occupation and resistance [18] [22] and seeks in technology a means of personal expression and fulfillment. Anticipations of the Web such as Bush’s Memex [7], H. G. Wells’s World Brain [33], and Emanuel Goldberg’s Knowledge Machine [6] were all personal devices, webs of knowledge adapted by individuals to help them do their work and to understand their world. Engelbart sought to augment human intellect [12], and Nelson’s Computer Lib [24] is focused on the urgency of establishing a personal relationship between individuals and their computers: “You can and must understand computers now!”

All these anticipations expected that writers would want to communicate, and that the myriad participants in the dociverse would wish to engage and convince each other. In the war of 2022, these assumptions were false.

2 TOTALITARIANISM AND RESISTANCE
Totalitarian states generate vast quantities of polemic, but its purpose is not to argue, communicate, or convince. On the contrary totalitarians simply seek to discredit argumentation, evidence, and fact [1]. If you know something to be true but the State denies it, the State must be correct. Sartre put it succinctly: “By giving ridiculous reasons, they discredit the seriousness of their interlocutors. They delight in acting in bad faith, since they seek not to persuade by sound argument but to intimidate and disconcert. If you press them too closely, they will abruptly fall silent, loftily indicating by some phrase that the time for argument is past.” [29]

A guided missile falls on a train station in Ukraine. Official spokespeople initially take credit for the precision attack. When the deaths of dozens are reported, the same spokespeople insist that the Ukrainians bombed their own citizens in order to embarrass Russia. When the recovered missile casing is found to be amateurishly hand-painted with the slogan “For the children!” (or, perhaps, “Toward the children!”), diplomats claim that Ukrainian mischief makers, amid explosions and shrapnel, had seized the opportunity to forge the message. Such iterated contradictions have been common.
Early hypertext was fascinated by the prospect of systems that could detect subtle argumentative flaws [8; 32], but these are useless or worse in the context of totalitarian debate, for the totalitarian does not care about facts and deplores the niceties of logic [2]. The purpose of writing is simply to serve the state by expressing faith in the state, by destroying the discourse of enemies, and by consuming the efforts of opponents in fruitless discussion and pointless debate [26]. This performative game-playing is especially satisfying for that portion of the totalitarian mob — “the refuse of every class: disempowered aristocrats, disillusioned intellectuals, gangsters” [22] — who retain deep resentments over youthful scholastic or social failures [17].

One route to improving this situation is to make trolling less fun [5]. The economics of social media now favor vast troll farms that manage innumerable fake personas [2]; taxing these or making their use more onerous might reduce the impact of dogpiling. We have devoted much research to making things fun and easy; research to make trolling unpleasant and difficult is urgently needed.

As a source of verifiable and truthful information, the early, patchy, homespun Web of home pages and weblogs was superior to the social Web we have helped to build. That primitive Web was built on links; ours permits outbound links only as a last resort and trains people to view clicking a link as a hazard. Much research attention has been paid to echo chambers and network bifurcation, but little attention is given to ensuring that readers can easily discover the truth: the truth doesn’t sell any ads.

3 ORCS, OGRES AND TROLLS: TECHNOLOGY OF DESTRUCTION

The vicious cruelty of the online mob is not an accident. The mob, knowing itself a mixture of wastrels, criminals, princelings, and desperate failures, uses cruelty to remind itself that it has become strong. “The attraction of evil and crime for the mob mentality is nothing new;” Hannah Arendt observed. Quoting from The Protocols of The Elders of Zion, she continues, “It has always been true that the mob will greet ‘feats of violence with the admiring remark: it may be mean, but it is very clever.” [1]

This proclivity for cruelty, often with sexual overtones, has been profoundly evident in the internet efforts inspired by, or coordinated with, totalitarian states [2; 9; 31]. Cruelty appeals to the mob and claims the attention of the “neutral, politically indifferent people who never join a party and hardly ever go to the polls [1]. Pervasive imagery from Ukraine depicting the cruelty of the invaders — wrecking houses, executing civilians, stealing filth and wreckage — reinforces this message of sensation and dominance. Online, opponents of totalitarianism are derided as sexually undesirable or branded as pedophiles in order to demonstrate the potency of the totalitarian war effort [10].

The research community has unwittingly assisted the work of trolls through its vast effort to automate the detection of pornographic imagery and hate speech in social media. In time of war, this work proves actively pernicious. For example, a journalist’s photograph from Mariupol shows the corpses of two sisters, stacked atop each other on the floor of an improvised morgue. It is a fine image, but it could not be shared on most social media because one of the sisters was not fully dressed. Efforts to disseminate the authentic image are instantly and automatically replaced with notices about pornography. Just as the technology that screens hate speech can also screen political dissent, recognizers that detect nudity or violence can prevent authentic depiction and understanding of what is happening.

Automatic algorithmic filters and automated moderation can turn antisocial behavior into a game in which you, too, can own the libs. The now-primitive technology of weblogs [11] was, in fact, a superior solution, as was Xanadu [24]: if you have something to say, it is best to say it in your own name, on your own server, in the confident expectation that you must endure the consequences. Heidegger had to live with his endorsement of Nazism because it was in print; today, he might simply delete some posts [22].

4 CAT PICTURES

Totalitarian propaganda seeks to dominate the information environment by overwhelming all rival messages, and by casting doubt on the existence of truth or the utility of individual thought. The totalitarian state thus has an important asymmetric advantage over its opponent: there is only one truth, but there are many different lies [5]. Repeating the truth is boring; listening to clever new conspiracy theories is interesting, even if the audience knows the new theories to be as groundless as the old.

One effective countermeasure in the War of 2022 was the deployment of the cat picture, in which a cat (or small dog) is seen with a soldier, who is standing before a ruined building. There have of course been pets in past wars [21], but this specific iconography seems new. Though the tableau may appear in many iterations, each is specific: a specific soldier (who is usually clean and smiling), a specific animal (who is typically adorable), and a specific backdrop of devastation. That these images were popular was immediately evident, but why these images proved compelling has not been much discussed.

I suggest that the core idea underlying this image is an implicit argument for truth. People may lie and cheat, but a cat’s affection or a dog’s loyalty is a real thing. This specific cat is alive, and it remains with its soldier. The animal’s relationship is a truth that trolls cannot debate or obscure. As journalist Oz Katerji (who adopted a dog, “this poor little abandoned guy after he limped over to me at the destroyed column... I guess we’re pals now”) wrote each morning during the siege of Kyiv, “We are still here. We shall remain here.” [20]

5 JUSTICE

A core holding of totalitarian justice is that the accused is undoubtedly guilty: it only remains to be determined precisely what crimes they have committed [19]. Totalitarians seek to shape and dominate social media by removing critics and opponents from the field — either by personal harassment or professional threats [31], or by arranging for opponents to be silenced [2]. Dozens or hundreds of disingenuous reports of violations of terms of service serve to clog moderation channels and to exhaust human moderators [15]. For example, Twitter banned photojournalist Elena Kostyuchenko, apparently because she had posted an image of two sisters killed in Mykolay, mentioned above, in which corpses were not properly dressed. Many notable wartime messages might not pass social
media review: Churchill’s “We shall fight on the beaches” is a call for violence and intolerant of Nazis; photographs of concentration camps are disturbing images of prisoners — some of them minors, some of them not decently attired. These problems are exacerbated when enforcement is left to neural networks, since these seldom recognize context, irony, or rhetoric. Automated systems are cheap and irresponsible — both virtues to corporate platforms whose purpose, after all, is to attract attention and to sell ads.

Past efforts to ameliorate this (and to reduce the cost of content moderation) have relied on distribution of “karma” (slashdot), distributed upvoting (reddit), or other crowd-sourced endorsement mechanisms. These make sense when all users have common goals; in the presence of subversive teams, they make information combat fun.

One solution is to return to a world of responsible social media, which is to say, to return to weblogs in which the author was clearly and unambiguously responsible for all that is said. If aggregators remain, decisions on moderation and governance must be rendered by identifiable and responsible individuals, and must be subject to prompt appeal by responsible oversight. Sloppy, dishonest, corrupt, or incompetent governance decisions should redound to the discredit of those responsible.

6 SOCIETY OF SCIENCE

Long ago, when program committees met in person, they provided a forum for crafting a consensus within a profession. Today, program committees never meet. In place of joint discussion among the leaders of the field, two or three reviewers express their opinions and, perhaps, exchange a sentence or two to resolve isolated disagreements.

One casualty of this change is that research in our corner of computer science has grown unreflective. For example, the 2021 Engelbart Award paper [23] superbly leverages the social graph to improve identification of “hateful users” in Twitter and Gab, and thereby to identify “hateful users” for punishment. The paper, though excellent, does not consider that its methods could also identify adherents of a state’s preferred hate, whom it might recruit to spread hate more efficiently. The paper makes no mention of the application of the technology to ambient speech or to monitored telephone conversations. Nor does it contemplate that the same techniques, applied to support for Ukrainians, or predestinationists, free love or free speech, might provide a totalitarian state with a powerful tool to automatically identify subjects for interrogation. Note, crucially, that state terror does not require precision [1], for terror is more effective when its impact seems both capricious and inescapable. Current incentives encourage research that simplifies surveillance. By analyzing the social graph, malefactors can pierce anonymity whilst those obedient to the law must respect privacy [3]. That the same combination of linguistic features and social network allows one to rapidly classify users by socioeconomic status [25] might please marketers, but might also please those wishing to round up kulaks or bourgeoise revisionists.

Scientists are not responsible for the bad uses to which bad actors may put our hard-won new knowledge of the true nature of the world. But we are responsible for thinking things through: that is, literally, our job.

REFERENCES