# Post-Truth and Information Warfare in their Technological Context

**Ignas Kalpokas** | Department of Public Communication, Vytautas Magnus University, Lithuania, Institute of Information Systems and Digital Economy, SGH Warsaw School of Economics, Poland | ORCID: 0000-0003-1110-5185

**Corresponding author:**
Ignas Kalpokas, Department of Public Communication, Vytautas Magnus University, Lithuania, and Institute of Information Systems and Digital Economy, SGH Warsaw School of Economics, Poland; E-mail: ignas.kalpokas@vdu.lt
0000-0003-1110-5185

## Abstract

As citizens are faced with an overabundance of information, their reliance on intuitive sorting strategies and platform-enabled content selection and delivery increases correspondingly. Under such circumstances, political action tends to be based on haphazard encounters with opinion-congruent content than on anything else, giving rise to so-called post-truth condition and, in turn, opening up conditions for manipulating such information encounters as part of information warfare operations. In particular, this novel environment necessitates a rethinking of informational agency, locating it within interactions between humans and technological artefacts, whereby humans as generators of data and algorithms as tools that structure the information domain based on such data co-construct political and social spaces. The impact of digital technologies is further amplified by the advent of synthetic (Artificial Intelligence-generated) media, which is foreseen to bring about epistemic confusion, that is, increasing inability to separate between reality and fiction. Under such conditions, and in any situations of actual or perceived crisis and tension, audiences are inclined to rely on narratives as coping strategies, which is where information warfare operations come to the fore. Either capitalising on the existing fertile ground or having manufactured a condition of crisis and distrust, such operations are geared towards hijacking audience cognitive processes with narratives that suit their perpetrators.

Ignas Kalpokas

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

―――― ## 1. Introduction

The war in Ukraine has proven to be a testing ground for new and emerging military technologies, such as drones. However, besides the kinetic battlefield, warfare operations have also been taken in the information domain. Notably, such operations have been making use of technological developments to a no lesser extent than their kinetic counterparts. Hence, the aim of this article is to explore transformations in digital communication that have enabled a qualitatively new breed of information warfare. In order to do so, this article is built on a conceptual review of the existing trends and developments with the aim of developing a conceptual framework for explaining the interaction between post-truth, information warfare, and Army Intelligence (AI)-based technologies. In order to do so, key ideas and recent developments regarding post-truth, changes in information environment, and the advent of AI-based synthetic media are identified and their connections elucidated. The identified transformations are subsequently connected to the key features of information warfare campaigns.

Of course, discussions of manipulation, disinformation, and the receding importance of veracity have been the focal point for communication studies for quite some time, often focusing on post-truth. As such, post-truth is best seen as collusion between audiences, technology companies, and political actors, whereby audiences derive both satisfaction and information benefits (such as quick navigation in an oversaturated information environment) but in exchange open themselves to manipulation [1]. Meanwhile, information warfare is broadly understood as a deliberate effort by state and non-state actors to shape the strategic environment within a particular public sphere or across multiple public spheres in a way that suits the perpetrator's interests [2]. In essence, the aim is to affect the thought processes of general populations or political elites (or both) so that decisions are made using the frames, preconceptions, and habitual associations implanted by and commensurable with the interests of the perpetrator [2]. Crucially, information warfare leaves no room for a strict war/peace dichotomy characteristic of western thinking – instead, it is always on, taking place in the background, even though it tends to be amplified in situations of crisis or conflict when low-level nudging is deemed by the perpetrator to be no longer sufficient [2].

Post-Truth and Information Warfare in their Technological Context

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

Post-truth and information warfare can be seen as cousin concepts that share similar premises but differ in terms of intentionality. Post-truth refers to a general transformation of the information environment and an ensuing reconfiguration of the relationship between veracity and political beliefs and action. However, deviations from truth generally happen organically, as a result to the transformations of the information ecosystem. Information warfare, meanwhile, refers to the deliberate and strategic manipulation of the information environment that makes use of, among other things, post-truth tendencies to guide audiences towards predetermined patterns or thinking. It is, therefore, crucial to understand the specificities of both post-truth and information warfare as well of the information ecosystem upon which they are jointly premised.

In order to conceptualise contemporary information warfare and contextualise it within the broader post-truth condition, this article proceeds in four parts. Firstly, the emergence of post-truth as a result of the changing information environment is overviewed. This is followed by a more in-depth analysis of technological transformations, namely in the second part, the de-centring of humans in communication processes and, in the third part, the likely emergence of epistemic confusion due to proliferation of synthetic media. Finally, these strands are taken together in a discussion of information warfare strategies.

## 2.  Post-Truth and the Changing Information Environment

One of the core changes at the heart of the formation of today's information environment has been the shift in emphasis from a supposed 'information age' towards a 'post-truth era'. In general terms, post-truth is understood as a tendency by audiences to opt for opinion-congruence and ease of access/cognition instead of veracity as the main criteria for information selection. This has been associated with changing patterns of information supply (ever-growing amount of content, replacement of professionally prepared and curated content with user-generated content, and algorithmic contend governance) as well as societal factors, such as politicians and other actors making use of such conditions in ways that are contributing to societal polarisation. Post-truth has largely been brought about by the ever-growing interdependence between humans and digital technologies. Indeed, while previously the Internet was itself seen as a 'liberation technology', enabling networked individuals to self-organise in a struggle for democracy and freedom [3], currently the attention has shifted to the opposite end

of the spectrum, namely manipulation, disinformation, and information warfare. These are seen to be not only features of domestic political competition (a domain usually associated with post-truth) but also international competition and even hybrid warfare strategies. In the case of Russia's war against Ukraine, the same can also be seen as an addition to conventional warfare practices. While warfare, propaganda, and attempts to 'win hearts and minds' have traditionally gone together, the interplay between warfare and post-truth leads to more pervasive, all-encompassing, and interactive practices in the management of audience cognitive processes.

A key concern in contemporary information and communication studies is that 'we are witnessing historical changes in the process of production of knowledge, characterised by high velocity and dizzying excess, as well as the development of new forms of digitally derived knowledge' [4, p. 26]. While one might take issue with the epochal scale of such assertions, it is, nevertheless, clearly the case that not only the amount of available content has overtaken the capacity to pay attention (which, in fact, is not new) but also the speed with which content changes and new items are added goes beyond the abilities to keep track and make sense. The preceding has been further exacerbated by the disaggregation of news supply in the context of social media: instead of competing as collective offerings (a newspaper, a news broadcast, etc.), news and other media content currently compete as standalone de-contextualised items, resulting in increased competition and hampering of content selection [5]. As this information environment is also devoid of traditional gatekeepers and open to an almost unlimited flow of user-generated content, sense-making capacity is only further overwhelmed [6], meaning that '[t]he challenge of communication overload is that each message can be heard – as the carrier of a distinct meaning – yet it cannot be attended to, since the time required for doing so is lacking' and leading to the need for individuals to 'drastically select from the environment' so that attention can only be paid to what seems to be noteworthy [7, pp. 112, 113]. All precedencies make automated content governance a valuable function performed by digital platforms [8], thus underscoring the importance of choices of and by algorithms.

Clearly, digital content, including news and other information, is 'ubiquitous, pervasive, and constantly around us', ultimately driving individuals to expect news to find them instead of seeking information intentionally [9, p. 106]. In other cases, people may become so overwhelmed and anxious about the ever-increasing stream of news that they begin avoiding them altogether, further deepening

Post-Truth and Information Warfare in their Technological Context

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

their dependence on piecemeal haphazard encounters [10]. The preceding directly implies that attention is both a scarce and pivotal resource in the present media environment [11]. It thus should not come as a surprise that audiences have become spoilt for choice: as opinion-congruent content is always available, regardless of the level to which it corresponds to verifiable facts, selective exposure to information increasingly becomes the norm [6]. Moreover, such selective sorting is further strengthened by the online platforms themselves, whereby content-to-be-liked is algorithmically selected and displayed to any given user. Consequently, the current trans-formations of the public sphere have the tendency to result in fragmentation into opinion-congruent bubbles [12]. Such need for opinion-congruence can also be abused by way of manufacturing false unanimity through automated accounts and other forms of manipulation [13]. It is also notable that citizens are by far not mere passive recipients of digital information flows and the algorithmic logics inherent therein but are also active in the generation and spread of such content, thus at least partly taking agency into their own hands – for better or worse, often engaging in what has been called 'participatory propaganda' [14].

Attention capture is further implicated with the algorithmic pro-cesses of information delivery, particularly insofar as social media platforms are concerned. The latter processes are predicated upon personalised targeting of content so that individuals are perma-nently offered that they are bound to like and pay attention to, lead-ing towards 'the growing personalization of constructed realities and the subsequent individualization effects' [15, p. 254]. Hence, as a direct consequence of the overabundance of information and competition over attention, citizens' worldviews become further strengthened and entrenched through imaginary confirmation of their pre-existing beliefs. Crucially, then, in the digital environment described above, it transpires that the quality of information is far less important in driving political participation than the feeling of being informed, meaning that those driven by deficient informa-tion are just as likely to make their voices and opinions heard and actively push for opinion-commensurable political decisions as those who possess verifiably factual knowledge, thereby leading to further proliferation of a-factual points of view[1] and their inclusion in the political agenda [16], thus contributing to post-truth politics.

Nevertheless, one needs to resist the dominant temptation in lit-erature on post-truth towards 'clear-cut distinctions between the esteemed objective realm of facts, science, and reason and the dan-gerous subjective realm of emotions, ideology, and irrationality'

1——'A-factual' is used here as an inclusive term to accommodate *both* the more organic straying aside from truth concerns ('post-truth') *and* intentional disinformation.

Ignas Kalpokas

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

[17, p. 787]. Simultaneously, the willingness in some recent revisionist literature to dismiss the idea of post-truth as merely a 'moral panic' [18] is unproductive as well, because it simply recasts the narrative in progressivist terms and, therefore, fails to engage with the critical potential of the idea of post-truth. In particular, it is important to understand that the condition, typically referred to as 'post-truth', is a consequence of the digital information ecosystem, rather than determined by the inner deficiencies of the individuals that happen to be following and supporting a-factual narratives. Hence, such individuals must not be marginalised and looked down upon (which, again, is common in the literature on post-truth) but, instead, the factors that have led them to their particular beliefs have to be investigated. It is far from uncommon for such factors to include information warfare operations. The latter, however, must not be taken as a universal category either: instead, just like warfare in general, information warfare makes use of technological transformations and developments, which today involve significantly transformed interrelationships between humans and digital technologies.

## 3. Digital Communication Environment: Moving Beyond Human-Centricity

As already intuited in the previous part, accounting for changes in the communication environment are crucial in order to understand the socio-political processes in today's societies. Broadly, the communication environment is understood here as the sum total of technological and other means for sending and receiving information (in terms of both private interactions and matters of public concern) available to a particular society at a given time and combined with the predominant use practices on behalf of the audiences. With an ever-increasing role of digital technologies and various AI-enabled tools and algorithmic governance mechanisms, today's communication environment has not only grown in terms of complexity but is also putting in question some of the often taken-for-granted assumptions about human-centricity in communication. Of course, such human-centricity largely remains intuitive: after all, intentionality and the capacity to generate and understand meaning within specific contexts are all central to communicative interactions. Simultaneously, though, AI tools now have significant sway over the public arena by way of shaping the information received by individuals (e.g. content selection and moderation), generating part of the content consumed by individuals, and even acting as communication partners, such as in the case of voice assistants [19]. The crucial questions, however, revolve around

Post-Truth and Information Warfare in their Technological Context

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

the depth and kind of such technological participation. It must be stressed, however, that the thrust behind this section is diagnostic: instead of celebrating or criticising the tendencies described above, the aim is to contribute to the understanding of the latter.

Human–technology interrelatedness is manifested in the structure of today's public arena, best understood in general terms as 'interconnected communicative spaces' [19, p. 165]. More precisely, should one attempt to break down the public, with Hasebring, Merten, and Behre, into constellations of actors, frames of relevance, and communicative practices, it becomes clear that AI-enabled technological artefacts participate in all of them [20]. They participate in publics alongside humans as both assistants and obstructors (bots could be an example of the latter), shape relevance by subterraneously structuring information supply, and take part in content generation and other practices that set frames for interaction. Other models paint an even more fragmented picture by focusing on communicative formations that are 'variously private and public, personal and topical, small and large, transient and persistent', being 'connected both horizontally and vertically by shared participants and information flows' [21, p. 79]. Moreover, it is not just the internal dynamics and user practices of such formations that determine their fate: instead, a crucial role is played by 'platform affordances, commercial and institutional interests, technological foundations, and regulatory frameworks' [21, p. 79], clearly implying a constant flux that is simultaneously shaped internally and externally. Here, again, the triple role of digital artefacts – as moderators of online encounters with content (e.g. platform affordances), interlocutors (bots, conversational agents, etc.), and content generators – comes to the fore. It thus should come as no surprise that in many ways, algorithms can function as partners in communication, for better or worse [22].

Notably, one could reasonably assert the emergence of the new normal in terms of 'construction of reality with and through digital media and infrastructures' [23, p. 147]. The preceding is, of course, a very general assertion, covering the broad societal transformations that are taking shape vis-à-vis digital technologies. A crucial issue at hand, though, is whether one can meaningfully discuss human–AI partnership in communication without the advent of Artificial General Intelligence. One way of tackling the problem could be reframing the question from one concerning AI to that of artificial communication; hence, it is not imitation of human intelligence (which remains elusive) but reproduction of communication skills that matters [22]. In this way, a fundamentally interactive model emerges: one of

enmeshment between human-generated data, machine learning processes, and communicative practices, even without the need to emulate human intelligence beyond the narrow domain of communication. Given the human–digital interdependence as the key premise of post-truth, such further enmeshment can be seen as deepening the replacement of veracity with outcomes of digital content flows as the benchmark for political and societal processes.

The preceding precludes one-sided assertions of loss of human agency and emergence of 'algorithm dependency' [24], pointing instead towards mutual dependence. When engaging with AI-enabled tools, the crux of the matter 'is not that a human would interact with the material vis-à-vis a machine, but with systems that generate their communication based on a variety of human digital traces' [23, p. 146]. The process is interactive: an AI tool would reflect the perspective of human actors as an aggregate but always with a twist – a perspective that enables such tools to interact with humans not by simply parroting them but also by producing an outcome that strikes a balance between recognisability and surprise; such outcomes, in turn, become a source of human interaction and learning, thus informing future interactive outcomes [22]. Once again, interrelatedness and enmeshment are evident. The environment thus produced 'follows users' choices, then processes and multiplies them, and then re-presents them in a form that requires new choices' [22, p. 64]. In other words, AI-enabled tools react to and around humans (AI passivity, human activity) but do so in ways that externally structure the conditions for human behaviours and responses (human passivity, AI activity). Once again, post-truth is here best seen as an interactive condition.

Still, however, one might posit that there is a crucial difference, due to the agency of digital artefacts being, at best, conditioned by humans or even illusory. Nevertheless, it must be stressed that the centrality and independence of human agency has also come under intense questioning in recent years. Notably, today's increasingly digital-first life means that the nature of the human self, let alone its supposedly autonomous qualities, is increasingly distributed among multiple data doubles – 'de-corporealised' virtual individuals residing within technology [25, p. 159]. The ensuing 'human–data assemblages' are in a constant state of flux 'as humans move through their everyday worlds, coming to contact with things such as mobile and wearable devices, online software, apps and sensor-embedded environments' [26, p. 466], conditioning them and being conditioned in return. It thus becomes evident that subjectivity and agency cannot be understood as autonomous

qualities describable in binary terms (as either present or absent) but, instead, best seen as in-between states [27]. The exceptionality of the human subject is, consequently, put to question. Consequently, one must acknowledge that 'not only humans but also non-humans [...] have agentic and performative capacities' [28, p. 380], resulting in shared abilities that are 'more-than-human' [29]. It indeed transpires that instead of the rational-autonomous ideal, '[w]e are relational beings, defined by the capacity to affect and be affected', constantly 'flowing in a web of relations with human and non-human others' [30, pp. 45, 47]. Consequently, agency would thus be found in an 'interplay of human capabilities and the capacities of more or less smart machines' [31, p. 3]. One should, therefore, talk not of an increase or diminution of agency on either side of the human–AI encounter but, instead, of complex and dynamic networks of agency, with truth (or, rather, what counts as the latter) becoming immanent to such interactions.

The above view is also supported by neuroscientific research that reveals an autonomous unified self to be merely an illusory unity brought together out of diverse elements: multiple interacting neural networks, social interactions, and artefacts encountered at any given moment [32]. Hence, even the workings of human brain are best seen as an endless exercise in improvisation at the interplay between the external world and the memories of past thoughts and experiences instead of some manifestation of 'a hidden inner world of knowledge, beliefs, and motives' [33, p. 9]. Seen in this way, the relationship of being shaped by any encounter at hand and shaping the environment back through interpretation and reaction to such encounters (instead of linear autonomous human progress) is, simply, a natural feature and not a technologically conditioned one. Consequently, humans are merely entities constantly scrambling for meaning, undergoing a constant process of re-invention, rather than self-sufficient actors exerting power and dominance over their environments. Again, moving into the technological domain, then, the aim should be to move 'beyond the competition narrative about humans and machines' [34, p. 42] and avoid simplistic dualisms that merely obfuscate the complexities of contemporary societies characterised by mediatisation [23, p. 147]. Overall, the goal should be to overcome binary thinking, instead aiming for an approach that would posit interactivity between humans and their environment as the default condition of communicative interactions. Under such conditions, another binary – between fact and fiction – is destabilised as well.

Overall, then, while the growing role of AI and algorithmic tools in communication has become a truism, it is time to move further by

positing horizontal interrelationship and enmeshment between humans and digital artefacts. On the one hand, this is due to the growing role and capacities of digital artefacts as structuring actors, interlocutors, and content co-generators; on the other hand, this is also consequent to autonomous human agency, traditionally taken for granted, emerging as, at best, an overstretch. In combination, a new, enmeshment- and interaction-focused, take-on communication and sense-making (on both individual and collective levels) is necessary. Likewise, the same pertains to any obstructions and complications in the flow of information or the poisoning of such flows through injection of disinformation. Seen from this perspective, one should focus less on alleged loss of some human mastery (the typical focus of mainstream approaches to post-truth), but, instead, on co-originating forms of content indistinguishability, including those that allow information warfare operations to hide in their midst.

## 4. Synthetic Media and Emerging Epistemic Confusion

In order to fully appreciate the role of technological developments in the emergence of post-truth and the creation of conditions for contemporary information warfare strategies, one must also consider the effects of artificial content generation. Indeed, the rise in prominence and growing adoption of generative AI has been one of the defining features of the past several years. While beneficial uses of this technology, including in communication, are plentiful, there are, nevertheless, clear security implications that need to be taken into account. Here, particular attention is typically paid to the potential use of AI generators to produce disinformation and deceive outrightly. However, instead of focusing on singular disinformation campaigns (which, it must be admitted, may pose significant threats but are, nevertheless, likely to remain isolated occurrences), more attention should be paid to underlying background effects caused by the very presence (and increasing prevalence) of AI-generated content. In broad terms, such effects could be described as epistemic confusion.

The subject matter here is synthetic media, namely 'audio-visual media which has been partly or fully generated/modified by technology' [35, p. 2]. Some key features to note here include democratisation of content creation (as easy-to-use interfaces enable users to leverage AI to generate content they would otherwise be unable to produce), increased speed and efficiency with which content is created, and the capacity to generate realistic yet fake depictions

of individuals and events. Crucially, regardless of the intention with which such synthetic content is generated, the mere fact of its omnipresence would likely lead to a diminishing of trust as individuals become increasingly unsure of whether the authenticity of the content they encounter can be reasonably established; moreover, particularly in situations when individuals are simply casually scrolling through available content, they may lack both time and attention to check and verify [36, 37]. Notably, it is not only de-contextualised pieces of information shared on social media that have to be treated with suspicion – entire websites masquerading as news sources filled with AI-generated text, featuring nonsensical content or outright falsehoods are already not uncommon [38]. In some cases, the aims behind resorting to synthetic content can be noble, such as attempts to counter disinformation by building AI tools that generate rebuttals – from social media posts to, again, entire websites staffed by fake journalists [39]. The downside, nevertheless, is that all of this only further stretches the cognitive load of individuals as they attempt to navigate online information spaces. Even in cases when synthetic content is not outrightly harmful and had not been created with a nefarious aim (including satire or parody), it can still have negative effects simply by lingering at the back of one's mind: not least, the very possibility that something has been AI-generated can reduce trust even in genuine information [35].

Crucially, the epistemic confusion induced by synthetic media is further strengthened by the dominant modes of content distribution. For example, algorithmic content governance on social media is by no means news-centric; moreover, such platforms tend to supply users with de-contextualised and entertainment-focused pieces of content, which precludes the formation of an effective representation of the societal issues at hand [40]. Users need to put in deliberate effort by intentionally seeking news content for this aptitude to be picked up by the algorithm. In other words, to paraphrase Gil de Zúñiga et al., news may still 'find me' [9], but only to the extent that I have made a head start. Nevertheless, as news are enmeshed with entertainment and other types of content for which the threshold of acceptable AI augmentation (or complete generation) is significantly lower, context differentiation and epistemic trust in news could well recede. Contexts themselves are likely to blur as the need to compete in a non-news-centric environment could also push informational content creators to turn to synthetic media to simply retain some relevance. All of this creates favourable conditions for actors engaged in information warfare operations by making cognitive overload and news cynicism among target audiences easier to achieve anything, including causes and atrocities of

war, can be caught within (or deliberately pushed towards) this spiral of indeterminacy.

Even when content is not shared but, instead, generated for personal use, such as consulting large language models (ChatGPT, Bard, etc.), increasing reliance on technologically mediated access to the world might lead not only to diminution of agency but also to the threat of uncritically accepting the output thus generated, despite its occasional propensity to falsehood [37], let alone data poisoning, adversarial attacks, and other hostile attempts by outside actors to negatively affect the output of such tools [41, 42]. Even short of hostile actions from outside, deterioration of outputs could happen due to 'data inbreeding', that is, AI models being trained on AI-generated data, which might happen either accidentally or by design as the proportion of online synthetic content continues to grow [43]. As user experience of the flaws and dangers of such models grows, their trust in any form of available knowledge and the possibility of distinguishing between truth and falsehood would likely suffer.

In addition to already familiar problems, extended reality environments may introduce a completely new set of threats, such as the potential to create false memories and introduce overlays that are difficult to distinguish from objective reality – both highly problematic in light of the accumulating neuroscientific knowledge that human perception of reality is based on predictive processing of the human brain that provides, effectively, best guesses and approximations of reality, rather than detached objective knowledge [44]. Hence, extended reality can be seen as having the potential to cause 'disruption of deliberation between people due to the breakdown of a common reality' [44, p. 11], thus further contributing to epistemic confusion. Indeed, the loss of shared touchpoints and increasing sufficiency of digital life could lead to the breakdown of even the fragmented and intermeshed public spaces that currently still allow some interconnections among citizens.

Certainly, efforts are underway to ease the cognitive load and, therefore, reduce epistemic confusion, with watermarking attracting the most attention. Still, while the thrust towards watermarking and otherwise identifying AI-generated content (both in terms of industry standards and regulatory frameworks, such as the European Union's AI Act) is commendable, such measures can be undone through the use of specialised software (such as watermarks being either removed or made less prominent for human or machine detection, e.g. by the adding noise); moreover, for

content that mixes different media (e.g. text, audio, video, and images all being used in a single post on, say, TikTok), separation of authentic and fake is going to be even more difficult [36]. No less importantly, watermarks are only effective when AI-generated (or modified) content is the exception and not the norm: if the majority of content is synthetic, it is unlikely that watermarks would retain signifying value – that would merely become part of the fabric of everyday life, no longer drawing individuals' attention. Even more problematically, reliance on watermarks as a verification tool may induce a false sense of security: unwatermarked fake content (either with watermarks removed or produced using in-house tools, particularly by state and state-backed threat actors that have sufficient resources and sophistication) would automatically earn extra credibility. Not least, though, verification techniques can be abused through reverse watermarking, that is, adding fake watermarks that imitate common standards onto authentic content in an attempt to discredit it. Indeed, watermark manipulation can well open up a new front of information warfare.

The latter point captures a crucial aspect of epistemic confusion that is likely to follow the widespread adoption of synthetic media: as everything and anything can potentially be fake, the authenticity of anything can be put to doubt [36]. In fact, this does not even have to involve manipulation of authentic content so that it looks fake (such as adding a misleading watermark): in fact, mere accusation that an item has been digitally manipulated or AI-generated is sufficient to reduce trust and commitment [35, 45]. Falsely labelling content as AI-generated can happen both unintentionally (when people are over-vigilant, particularly vis-à-vis content they do not agree with) and deliberately (as a convenient way to dismiss content that goes against one's interests). Notably, the effects of such misleading accusations of fakery transpire to be stable over time and, crucially, have a greater effect on those who care about the particular topic at hand, perhaps because of their higher internal motivation to be adequately informed [45]. Hence, the threshold for deliberate manipulation of audience opinions is only further lowered.

## 5. Post-Truth, Information Warfare, and the Abuse of Coping Techniques

Conditions, identified here as post-truth, are particularly conducive to information warfare, particularly when taken in combination with the recent technology-driven changes in the information environment. In particular, the increasingly indeterminate

Ignas Kalpokas

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

role of veracity and the changing contours of information agency extend the ambit of information warfare. In particular, this is due to the potential for abuse of coping techniques that, while not necessarily consciously employed by individuals, do nevertheless have significant leeway on how we understand our environment. Hence, avenues are opened if not for full conviction, then for further sowing of confusion among target audiences.

In order to better understand the coping mechanisms under conditions of uncertainty and how they could lead to the proliferation of information warfare operations, one needs to focus on the importance of a narrative. Crucially, it must be noted that people need a narrative because it 'provides explanations', that is, 'describes the past, justifies the present, and presents a vision of the future' [46, p. 120]. However, such a narrative is not always present at hand, particularly in times of rapid change or in crisis situations, which could be a natural disaster, an epidemic, a war, or anything of the like. In addition, as shown above, epistemic confusion can also be caused, or at least exacerbated, by technological factors, either independently or when they are strategically amplified. Under such conditions, pre-existing narratives no longer function and new explanations of the world are necessary. Since fact-based narratives may be slower to emerge (due to changing conditions and the need to establish the facts themselves beforehand), it is often difficult to fill the gap with verifiable information and an opportunity is created for alternative accounts to emerge, particularly if they produce a more satisfying (easier to comprehend and opinion-congruent) effect [47]. Indeed, what matters is the provision of meaning to an otherwise seemingly disorienting and disconcerting reality [48], even if that means falling for disinformation and succumbing to information warfare operations. After all, individuals expect from a narrative that it provides actionable insights, regardless of its veracity [49]. Moreover, it must also be noted that even fact-incongruent narratives have the capacity to 'connect people, give meaning to experienced disparities and corruption in society' [17, p. 785], particularly when they connect to grievances that often do have a factual basis and that had not yet been adequately explained or addressed.

Even more fundamentally, there are indications that the need and capacity to establish patterns even when none exist or when there is incomplete data to foresee their existence is hardwired through evolution [50], thus even further strengthening the need for explanatory or pseudo-explanatory narratives [48] and increasing the benefits to be accrued should such narratives be strategically

placed, centric for example, as a means of information warfare. Crucially, such behaviour helps individuals overcome the perceived randomness and complexity that otherwise typically characterise the world by providing order and predictability, however imaginary [50] and regardless of the broader political and societal implications. Of course, this could easily be dismissed as a normatively flawed coping strategy [50], and a lazy one for that matter, one merely concerned with 'simple recipes for explaining complex realities' [51, p 85]. It is, nevertheless an efficient solution in situations when information is ether too scarce [52] or, on the contrary, too abundant [53], again at least from an individualist subjective perspective.

The preceding is particularly topical with regards to information warfare campaigns, carried out by both state and non-state actors, the aim of which is often to sow confusion and disorientation, for example, through hoaxes, fake news, and even plain scaremongering to subsequently make use of the ensuing collective action problems. Indeed, the first step of the process tends to be erosion of trust, both horizontally among citizens and vertically between citizens and their state/government, thereby creating fertile conditions for further hostile actions to be carried out [54], including nudging individuals towards specific narratives strategically placed to respond to pre-sown confusion. Once a spiral of distrust is set in motion by a threat actor, societies effectively enter a self-destruct mode, as the ensuing disorientation and polarisation makes it impossible (or at least very difficult) for citizens to formulate common interests and engage in achievement of any goals [2]. In fact, it might suffice to simply flood a selected public with competing contradictory opinions in order to diminish trust in any claims [55], very much in line with epistemic confusion described in the previous section. Moreover, it is important to note that trust increases openness to one's own vulnerability (thereby diminishing the need to rush for explanations and confusion-reducing narratives) and to other people's opinions (thus, potentially, also to corrections of one's own misperceptions); conversely, erosion of trust increases the likelihood of both falling for strategically placed narratives and becoming entrenched in one's own point of view [56].

Resorting to social media platforms for information warfare also enables threat actors to induce seemingly spontaneous audience reactions in response to messaging and to do so relatively simply, quickly, and at low cost. No less importantly, once successfully injected into the target audience, the manipulative message is propagated by citizens themselves (those who have become convinced

of its veracity), thereby further intensifying its spread [54]. Hence, herding target audiences into information silos or hijacking the existing filter bubbles constitutes a key strategic aim [55]. Threat actors then step in to resolve any uncertainty (including that of one's own making) and thereby both induce and respond to audience's need for comprehending any given situation and knowing how to act in the changing environment, particularly as such publics resort to unverified information should other or more quickly actionable options be unavailable [57]. Meanwhile, fact-based interventions to counter post-truth and/or information warfare operations may not only be at a disadvantage but could also derail the entire veracity-focused narrative by making it more complex and disorienting, thereby paradoxically increasing the demand for clear-cut, albeit less factual, stories that seemingly put all things in order [46]. What the preceding indicates, then, is that '[t]ruth, as in a fact or piece of information, has no intrinsic value'; rather, it can be claimed that '[i]t is up to the narrative to create that value' [46, p. 124]. Hence, the core variable for success, especially in the political domain, 'is not evidence (i.e. facts) but meaning' [58, p. 73]. Consequently, there are ample opportunities for the spread of conspiracy theories [58] or deliberative disinformation efforts, such as information warfare operations.

Sometimes neither full internalisation of a coherent narrative nor sowing confusion but affecting the perception of one's standing in the society might be the aim. In this case, establishment of immediate associations (positive or negative) attached to certain political and societal actors would likely end up affecting citizen modes of participation as well as perceptions of government policies, ethnic or other groups, general sense of societal development, etc. [56]. The preceding often relies on generating a sense of marginalisation. Here, it is crucial to keep in mind that one of the drivers that motivate resorting to factually false narratives is powerlessness and lack of control, either actual or perceived [50]. This typically involves groups that are societally underprivileged and lack a subjectively convincing possibility for emancipation or groups that had previously been privileged but have since been displaced or are being pushed aside by new, more progressive, groups, meaning that their concerns are also likely to be ignored or dismissed. Of course, in some cases such underprivileged status might be grounded in objective reality, but perceptions of such state of affairs could equally be manufactured as well. Likewise, groups that are disproportionately affected by ongoing crises (economic, health, military, etc.) can be more susceptible to disinformation and attempts to mislead. Strategically manufactured narratives would then

be aimed at providing perceived solutions by offering a sense of belonging to a community of those allegedly in the know, thereby bringing about a sense of subjective empowerment [51]. The latter, then, also brings inter-group dynamics into the mix as individuals are inclined to think that they and their group are firmly rooted in reality, making biases and false assumptions particularly difficult to spot (if they pertain to in-group views) and fostering polarisation by way of externalising the blame to non-like-minded others [59]. Hence, falling for fake news, disinformation, and information warfare operations tends to be understood by individuals and their peer groups as something that 'others' do, leading to the perception that others are vulnerable; the preceding then leads to another dichotomy: the self/we as seemingly rational and critically minded, and of the other as, allegedly, less intellectually gifted [60]. Such contrast can also lead to a false sense of security, whereby the intellectually superior self is seen as resilient by default and in a lesser need to care about the premises of one's own thinking.

It must also be kept in mind that proliferation of false narratives has been made possible by the general drive towards datafication, characteristic of contemporary societies: as populations are rendered fundamentally knowable by way of ubiquitous data collection, their pain points, biases, and preconceptions become relatively easy to identify [61]. The preceding has also significantly transformed the way in which political and opinion leadership is commonly understood: from being at the forefront of audience thought processes to following and voicing them [61]. Audience expectations are also not immune to such transformations as audiences simply expect to be satisfied, rather than challenged. Notably, there is an important international dimension here as well since crisis situations, particularly global ones, also imply the need for a sense of direction, community values, and shared identities, all of which are typical targets of information warfare [56]. Likewise, a key aim on either side of information warfare operations is to create positive habitual perceptions and a sense of shared concerns/values with one's own side in the minds of strategically targeted global audiences while fostering a sense of dissociation with one's adversary, either on a global or regional level [56]. Again, it is not only full convincing but sowing distrust and doubt within an adversary's support network that could be seen as a strategic goal.

Crucially, though, it is important to keep in mind that the effects of information warfare operations tend to be cumulative, meaning that they only become evident over time, once disintegration of a state's informational public (and, consequently, public order) or

global support network becomes manifest – that is, when the harm has already been done [56] and achievement of strategic goals, both domestically and abroad, has been impeded [55]. In this way, protection from such operations becomes particularly problematic. While much of the response has thus far concentrated on proactive defence measures, such as media and information literacy, their effectiveness has thus far faced only very limited empirical testing and lacks reliability due to the absence of a control group. Therefore, the offence should be seen as continuing to maintain an advantage within the domain of information warfare.

## 6.  Conclusions

Overall, it must be noted that the changes in contemporary information environment, particularly overabundance of content and its algorithmic management, has led to a transformation of the role of veracity. In many ways, what is taken as truth and, therefore, as actionable, has become contingent upon attention management strategies employed by individuals, group dynamics, and, most importantly, data-based automated matching of individuals and content that the former are predisposed to like. To this effect, humans must be seen as sharing information agency with an increasing array of digital tools. Such structural conditions are also favourable to information warfare operations that can exploit the new patterns of content dissemination and consumption in order to inject strategically carved narratives into the minds of selected audiences. Moreover, the rapid spread of synthetic media is beginning to initiate yet another change – the emergence of epistemic confusion, whereby everything and anything could potentially be manipulated. Under such conditions, demand for seemingly stable and coherent explanatory narratives can be seen as a coping strategy, with information warfare operations being geared towards offering such alleged solutions. Moreover, deliberate erosion of trust (with the consequent retreat from mainstream information and increased need for explanatory narratives) often happens to be the first stage of information warfare, creating the conditions to nudge target audiences towards pre-crafted narratives – which is all the easier within the present technological context. Overall, then, it transpires that technological change and the ensuing transformations in the information domain have created a new strategic environment in which states targeted by information warfare operations are constantly on the back foot, with limited solutions to ameliorate this situation.

Of course, similar tools and techniques can be used not only to proliferate disinformation but also by strategic communications and

Post-Truth and Information Warfare in their Technological Context

ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

other counter-disinformation agents. However, in terms of epistemic confusion, it is by no means clear yet, what the end societal effect would be (reduction of potentially harmful beliefs vs further increased epistemic confusion). It is a matter for future research to establish the balance between, for example, mere uncertainty-inducing epistemic confusion versus disinformation-weakening epistemic confusion.

## Funding

## References

[1]     I. Kalpokas, *A political theory of post-truth*. London: Palgrave Macmillan, 2018.

[2]     I. Kalpokas, J. Kalpokiene, "Synthetic media and information warfare: Assessing Potential Threats," in *The Russian Federation in the global knowledge warfare*, H. Mölder et al. (eds.), Cham: Springer Nature, 2021, pp. 33–50.

[3]     L. Diamond, "Liberation technology," *Journal of Democracy*, vol. 21, no. 3, pp. 69–83, 2010, doi: 10.1353/jod.0.0190.

[4]     P. Dahlgren, "Media, knowledge and trust: The deepening epistemic crisis of democracy," *Javnost – The Public*, vol. 25, no. 1, pp. 20–27, 2018, doi: 10.1080/13183222.2018.1418819.

[5]     K. Munger, "All the news that's fit to click: The economics of Clickbait Media," *Political Communication*, vol. 37, no. 3, pp. 376–397, 2020, doi: 10.1080/10584609.2019.1687626.

[6]     R. McDermott, "Psychological underpinnings of post-truth in political beliefs," *PS: Political Science & Politics*, vol. 52, no. 2, pp. 218–222, 2019, doi: 10.1017/S104909651800207X.

[7]     N. Couldry, A. Hepp, *The mediated construction of reality*. Cambridge: Polity, 2017.

[8]     S. Vaidhyanathan, *Anti-social media: How Facebook disconnects us and undermines democracy*. Oxford: Oxford University Press, 2018.

[9]     H. Gil de Zúñiga, B. Weeks, A. Ardèvol-Abreu, "Effects of the news-finds-me perception in communication: Social media use implications for news seeking and learning about politics," *Journal of Computer-Mediated Communication*, vol. 22, no. 3, pp. 102–123, 2017, doi: 10.1111/jcc4.12185

[10]    B. Toff, R.K. Nielsen, "How news feels: Anticipated anxiety as a factor in news avoidance and a barrier to political engagement," *Political Communication*, vol. 39, no. 6, pp. 697–714, 2022, doi: 10.1080/10584609.2022.2123073.

[11]    K. Valaskivi, "Circulation of conspiracy theories in the attention factory," *Public Communication*, vol. 20, no. 3, pp. 162–177, 2022, doi: 10.1080/15405702.2022.2045996.

[12]    M. Seeliger, S. Sevignani, "A new structural transformation of the public sphere? An introduction," *Theory, Culture & Society*, vol. 39, no. 4, pp. 3–16, 2022, doi: 10.1177/02632764221109439.

[13]    A. Chadwick, J. Stanyer, "Deception as a bridging concept in the study of disinformation, misinformation, and misperceptions: Toward a holistic framework," *Communication Theory*, vol. 32, no. 1, pp. 1–24, 2022, doi: 10.1093/ct/qtab019.

[14]    A. Wanless, M. Berk, "The audience is the amplifier: Participatory propaganda," in *The Sage handbook of propaganda*, P. Baines, N. O'Shaughnessy, N. Snow (eds.), Los Angeles: SAGE, 2020, pp. 85–104.

[15]    N. Just, M. Latzer, "Governance by algorithms: Reality construction by algorithmic selection in the Internet," *Media, Culture & Society*, vol. 39, no. 2, pp. 238–258, 2017, doi: 10.1177/0163443716643157.

[16]    H. Song, H. Gil de Zúñiga, H.G. Boomgarden, "Social media news use and political cynicism: Differential pathways through 'news finds me' perception," *Mass Communication and Society*, vol. 23, no. 1, pp. 47–70, 2017, doi: 10.1080/15205436.2019.1651867.

[17]    J. Harambam, K. Grusauskaite, L. de Wildt, "Poly-truth, or the limits of pluralism: Popular debates on conspiracy theories in a post-truth era," *Public Understanding of Science*, vol. 31, no. 6, pp. 784–798, 2022, doi: 10.1177/09636625221092145.

[18]    T. Harjuniemi, "Post-truth, fake news and the liberal 'regime of truth': The double movement between Lippmann and Hayek," *European Journal of Communication*, vol. 37, no. 3, pp. 269–283, 2022, doi: 10.1177/02673231211046784.

[19]    A. Jungherr, R. Schroeder, "Artificial intelligence and the public arena," *Communication Theory*, vol. 33 no. 1–2, pp. 164–173, 2023, doi: 10.1093/ct/qtad006.

[20]    U. Hasebrink, L. Merten, J. Behre, "Public connection repertoires and communicative figurations of publics: Conceptualizing individuals' contribution to public spheres," *Communication Theory*, vol. 33, no. 2–3, pp. 82–91, 2023, doi: 10.1093/ct/qtad005.

[21]    A. Bruns, "From 'the' public sphere to a network of publics: Towards an empirically founded model of contemporary public communication spaces," *Communication Theory*, vol. 33, no. 2–3, pp. 71–81, 2023, doi: 10.1093/ct/qtad007.

[22]    E. Esposito, *Artificial communication: How algorithms produce social intelligence*. Cambridge, MA: MIT Press, 2022.

[23]    A. Hepp, N. Couldry, "Necessary entanglements: Reflections on the role of a 'materialist phenomenology' in researching deep mediatization and datafication," *Sociologica*, vol. 17, no. 1, pp. 137–153, doi: 10.6092/issn.1971-8853/15793.

[24]    N. Schaetz, E. Gagrčin, R. Toth, M. Emmer "Algorithm dependency in platformized news use," *New Media & Society*, 2023, doi: 10.1177/14614448231193093.

[25]    A. Hepp, *Deep mediatization*. London: Routledge, 2020.

[26]    D. Lupton, A. Watson, "Towards more-than-human digital data studies: Developing research-creation methods," *Qualitative Research*, vol. 21, no, 4, pp. 463–480, 2021, doi: 10.1177/1468794120939235.

[27]     R. Braidotti, *Posthuman knowledge*. Cambridge: Polity, 2019.

[28]     J. Monforte, "What is new for new materialism for a newcomer," *Qualitative Research in Sport, Exercise and Health*, vol. 10, no. 3, pp. 378–390, 2018, doi: 10.1080/2159676X.2018.1428678.

[29]     D. Lupton, *Data selves*. Cambridge: Polity, 2020.

[30]     R. Braidotti, "A theoretical framework for the critical posthumanities," *Theory, Culture & Society*, vol. 36, no. 6, pp. 31–61, 2019, doi: 10.1177/0263276418771486.

[31]     C. Pentzhold, A. Bischof, "Making affordances real: Socio-material prefiguration, performed agency, and coordinated activities in human-robot communication," *Social Media + Society*, 2019, doi: 10.1177/2056305119865472.

[32]     T. Oliver, *The self-delusion: The surprising science of how we are connected and why that matters*. London: Weidenfeld and Nicolson, 2020.

[33]     N. Charter, *The mind is flat: The illusion of mental depth and the improvised mind*. New Haven: Yale University Press, 2019.

[34]     M. Coeckelbergh, *AI ethics*. Cambridge, MA: MIT Press, 2020.

[35]     J. Twomey, D. Ching, M. P. Aylett, M. Quayle, C. Linehan, G. Murphy, "Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine," *PloS ONE*, vol. 18 no. 10, pp. 1–22, 2023, doi: doi.org/10.1371/journal.pone.0291668.

[36]     V. Elliott. (July 27, 2023). *Big AI won't stop election deepfakes with watermarks*, *Wired*. [Online]. Available: https://www.wired.com/story/ai-watermarking-misinformation/. [Accessed: 10 November 2023].

[37]     T. Benson. (June 18, 2023). *Humans aren't mentally ready for an AI-saturated 'post-truth world'*, *Wired*. [Online]. Available: https://www.wired.com/story/generative-ai-deepfakes-disinformation-psychology/. [Accessed: 10 November 2023].

[38]     M. Cantor. (May 8, 2023). *Nearly 50 websites are 'AI-generated'*, *a study says. Would I be able to tell?*, *The Guardian*. [Online]. Available: https://www.theguardian.com/technology/2023/may/08/ai-generated-news-websites-study. [Accessed: 10 November 2023].

[39]     W. Knight. (August 29, 2023). "It costs just $400 to build an AI disinformation machine," *Wired*. [Online]. Available: https://www.wired.com/story/400-dollars-to-build-an-ai-disinformation-machine/. [Accessed: 10 November 2023].

[40]     N. Hagar, N. Diakopoulos, "Algorithmic indifference: The dearth of news recommendations on TikTok," *New Media & Society*, 2023, doi: 10.1177/14614448231192964.

[41]     M. Burgess, M. (May 25, 2023). "The security hole at the heart of ChatGPT and Bing," *Wired.* [Online]. Available: https://www.wired.co.uk/article/chatgpt-prompt-injection-attack-security. [Accessed: 10 November 2023].

[42]     W. Knight. (August 1, 2023). "A new attack impacts major AI Chatbots – and no one knows how to stop it," *Wired.* [Online]. Available: https://www.wired.com/story/ai-adversarial-attacks/. [Accessed: 10 November 2023].

[43]    S. Alemohammad, J. Casco-Rodriguez, L. Luzi, A. I. Humayun, H. Babaei, D. LeJeune, A. Siahkoohi, R. G. Baraniuk, "Self-consuming generative models go MAD," *arXiv*, 2023, doi: 10.48550/arXiv.2307.01850.

[44]    M. Bay, "Arendt in the metaverse: Four properties of extended reality that imperil *factual truth and democracy*," *Convergence*, vol. 29, no. 6, pp. 1698–1712, 2023, doi: 10.1177/13548565231199957.

[45]    M. Hameleers, F. Marquart, "It's nothing but a deepfake! The effects of mis-information and deepfake labels delegitimizing an authentic political speech," *International Journal of Communication*, 17, pp. 6291–6311, 2023.

[46]    M. Holmstrom, "The narrative and social media," *Defence Strategic Communications*, vol. 1, no. 1, pp. 119–133, 2015, doi: 10.30966/2018.RIGA.1.7.

[47]    U.K.H. Ecker, "Why rebuttals may not work: The psychology of misinformation," *Media Asia*, vol. 44, no. 2, pp. 79–87, 2018, doi: 10.1080/01296612.2017.1384145.

[48]    A. de Albuquerque, T. M. Oliveira, M. A. dos Santos Jr, R. Quinan, D. Mazur, "Coronavirus meets the clash of civilizations," *Convergence: The International Journal of Research into New Media Technologies*, vol. 28, no. 4, pp. 1198–1213, 2022, doi: 10.1177/13548565221105789.

[49]    M. Andrejevic, *Automated media*. London: Routledge, 2020.

[50]    M. Butter, *The nature of conspiracy theories*. Cambridge: Polity, 2020.

[51]    G. Cosentino, *Social media and the post-truth world order*. London: Palgrave Macmillan, 2020.

[52]    A. Bruns, S. Harrington, E. Hurcombe, "'Corona? 5G? or both?': The dynamics of COVID-19/5G conspiracy theories on Facebook," *Media International Australia*, vol. 177, no. 1, pp. 12–29, 2020, doi: 10.1177/1329878X20946113.

[53]    N. O'Shaughnessy, "From disinformation to fake news: Forwards into the past," in *The Sage handbook of propaganda*, P. Baines, N. O'Shaughnessy, N. Snow Eds., Los Angeles: SAGE, 2020, pp. 55–70.

[54]    I. Kalpokas, "Influence operations: Challenging the social media–democracy nexus," *SAIS Europe Journal of Global Affairs*, vol. 19, no. 1, pp. 18–29, 2016.

[55]    I. Kalpokas, "Information warfare on social media: A brand management per-spective," *Baltic Journal of Law and Politics*, vol. 10, no. 1, pp. 35–62, 2017, doi: 10.1515/bjlp-2017-0002.

[56]    I. Kalpokas, "Social media: Mimesis and warfare," *Lithuanian Foreign Policy Review*, vol. 35, pp. 116–133, 2016, doi: 10.1515/lfpr-2016-0006.

[57]    L. Schwaiger et al., "Mindsets of conspiracy: A typology of affinities towards conspiracy myths in digital environments," *Convergence: The International Journal of Research into New Media Technologies*, vol. 28, no. 4, pp. 1007–1029, 2022, doi: 10.1177/13548565221106427.

[58]    I. Z. Baron, *How to save politics in a post-truth Era*. Manchester: Manchester University Press, 2018.

[59]    E. Bonetto, T. Arciszewski, "The creativity of conspiracy theories," *Journal of Creative Behavior*, vol. 55, no. 4, pp. 916–924, 2021, doi: 10.1002/jocb.497.

ACIG

APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

[60]     J.E. Uscinski, A.M. Enders, "What is a conspiracy theory and why does it matter?" *Critical Review: A Journal of Politics and Society*, vol. 35, no. 1–2, pp. 148–169, 2023, doi: 10.1080/08913811.2022.2115668.

[61]     S. Altay, A. Acerbi, "People believe misinformation is a threat because they assume others are gullible," *New Media & Society*, 2023, doi: 10.1177/14614448231153379.

[62]     I. Kalpokas, J. Kalpokiene, "Reimagining political competition for the age of data and algorithm," *Giornale di Filosofia*, vol. 2, pp. 33–46, 2022, doi: 10.7413/1827-5834013.