



The existential threat from cyber-enabled information warfare

Herbert Lin

To cite this article: Herbert Lin (2019) The existential threat from cyber-enabled information warfare, Bulletin of the Atomic Scientists, 75:4, 187-196, DOI: [10.1080/00963402.2019.1629574](https://doi.org/10.1080/00963402.2019.1629574)

To link to this article: <https://doi.org/10.1080/00963402.2019.1629574>



Published online: 28 Jun 2019.



Submit your article to this journal [↗](#)



View Crossmark data [↗](#)

OTHER FEATURES



The existential threat from cyber-enabled information warfare

Herbert Lin

ABSTRACT

Corruption of the information ecosystem is not just a multiplier of two long-acknowledged existential threats to the future of humanity – climate change and nuclear weapons. Cyber-enabled information warfare has also become an existential threat in its own right, its increased use posing the possibility of a global information dystopia, in which the pillars of modern democratic self-government – logic, truth, and reality – are shattered, and anti-Enlightenment values undermine civilization as we know it around the world.

KEYWORDS

Cyber-enabled information warfare; information ecosystem; anti-Enlightenment; existential threat; information environment; information dystopia



John F. Kennedy
@TheRealJK



Following

If Pequeno Hombre Cohete (Little Rocket Man) threatens us, we will have no choice but to totally destroy Cuba.



6:30 PM · 16 Oct 1962

The tweet depicted above obviously never happened.¹ But given the ubiquity of social media today, it is interesting to consider what might have occurred if the Cuban Missile Crisis of 1962 had taken place in the global information environment of 2019.²

Nongovernmental open source intelligence organizations could have used commercial satellite imagery to detect the presence of these missiles and publicize them to the world on October 12, four days earlier than the president did. Pictures of Soviet missiles being deployed in Cuba might have found their way to social media, then going viral and alarming millions in the United States and around the world. Imagine that these images were accompanied by disinformation from internet trolls, tailored information leaks, and propaganda from adversaries, all seeking to cast doubt on the facts or to sow confusion among domestic populations and paralyze NATO leadership.

The shooting down of a U-2 spy plane over Cuba might have been news within an hour of its occurrence, soon accompanied by numerous tweets and relentless

commentary on Facebook and other social media platforms, with some posts including realistic (though fake) video clips of what happened. When the Joint Chiefs of Staff recommendation to invade Cuba was overruled by President Kennedy, “alt” social media accounts that served as fronts for disgruntled Pentagon officials might have leaked the proposed invasion plan, hoping to induce the administration to reverse course on the chosen alternative, a blockade.

In the end, President Kennedy might not have had days to deliberate with the Executive Committee of the National Security Council before delivering a measured speech announcing to the world the discovery of Soviet medium- and intermediate-range nuclear-armed missiles in Cuba (see Scott and Smith 1994). Instead, Kennedy might have issued the tweet depicted above.

If the Cuban Missile Crisis, which many experts have characterized as the world’s closest approach to nuclear war, occurred today, the current global information ecosystem might very well have magnified the risk of

CONTACT Herbert Lin  herblin@stanford.edu

¹This hypothetical tweet is taken from a presentation by Sagan, S. “The Cuban Missile Crisis in the Age of Twitter.” Lecture, Center for International Security

²This discussion is adapted from Lin, Jablanski, and Trinkunas, “Retweets to Midnight: Assessing the Effects of the Information Ecosystem on Crisis Decision, Making Between Nuclear Armed States, forthcoming 2020.

war, escalating a high-stakes crisis into all-out nuclear exchange. President Kennedy had estimated that the odds of war were “somewhere between one out of three and even”; former Secretary of Defense William Perry (2015) writes that the odds of nuclear war at the time were even worse than that, because Kennedy did not know at the time that the Soviets already had tactical nuclear weapons on Cuba and authorization to use them in the event of US invasion (which had been the unanimous recommendation of the Joint Chiefs of Staff at the time).

The misuse of social media in the information ecosystem has also made rational responses to the threat of climate change more difficult for national governments to reach, as companies and groups with financial and ideological interest in creating the appearance of doubt sow misinformation about consensus scientific view. That is, cyber-enabled information warfare is a threat multiplier in the climate change arena, just as it is in the nuclear policy area.³

But corruption of the information ecosystem is not just a multiplier of two long-acknowledged existential threats to the future of humanity – climate change and nuclear weapons. Cyber-enabled information warfare has also become an existential threat in its own right, its increased use posing the realistic possibility of a global information dystopia, in which the pillars of modern democratic self-government – logic, truth, and reality – are shattered, and anti-Enlightenment values undermine civilization around the world.

The importance of information to nations and societies

Founded in 1945, the *Bulletin* first focused on the existential threat from nuclear war. The atomic scientists of the Manhattan Project did not believe that the miniature suns let loose on Hiroshima and Nagasaki in themselves posed an existential threat to human existence. (In the project’s early days, some of its physicists raised the possibility that the detonation of an atomic bomb might indeed incinerate the earth’s atmosphere. This concern was taken seriously only in the sense that they performed a variety of calculations that indicated such an outcome was impossible for all practical purposes. See Horgan 2015 for an authoritative account in an interview with Hans Bethe.) However, most of the Manhattan Project’s scientists recognized that atomic bombings of Hiroshima and Nagasaki were omens of a future in which nuclear weapons, used on a large scale, could indeed

threaten human existence, and even used on a smaller scale could threaten modern human civilization.

After sporadically reporting on climate change for decades, in 2007 the *Bulletin* formally expanded its concept of existential threat to include climate change and nuclear war. (Ironically, the possibility of significant global cooling as the result of nuclear war was first raised in the scientific literature in the early 1980’s. See, for example, NRC (1985)) Where large-scale nuclear war threatens to snuff out hundreds of millions of lives in a matter of hours, climate change threatens to alter the planetary ecosystem. Here the effects are more subtle and less easily noticed because they are cumulative over decades. There is no single cataclysmic event in the offing, and yet myriad smaller regional disasters will result in more intense and more frequent forest fires, heat waves, and storms; vastly increased coastal flooding and rising sea levels; loss of arable land; severe shortages of food and water; and mass migrations and relocations.

Nuclear war and climate change threaten the physical infrastructure of human civilization as well as the underlying geochemical processes and the ecology of the planet. Because most people depend on both physical infrastructure and our global ecology for food, energy, and other necessities of existence, nuclear war and climate change put the lives of the great mass of humanity at risk. Because nuclear war and climate change threaten massive changes in cultural identity and the loss of historical resources, our civilization and our legacy are at stake, too. In those ways, both nuclear war and climate change pose existential threats to humanity. But these are not the only such threats to civilization as we know it.

The infrastructure for human civilization is undeniably tangible (that is, physical, chemical, and biological), but it is increasingly virtual as well, and the virtual aspects of that infrastructure – the information ecosystem (or, equivalently, environment) – in many ways has become central and often critical to the way people now live all over the world.

As Balkin (2012) describes, “it is not an exaggeration to say that modern states are informational states: states that recognize and solve problems of governance by collecting, analyzing, and distributing information.” Consider that nations require good information to allocate benefits and social services to the populace; to administer mechanisms for public safety (e.g. law enforcement, court systems, fire-fighting); to provide for national security; to gather revenue to support national expenditures; and to engage with other nations in ways that support national interests.

³Cyber-enabled information warfare is distinct from cyber warfare; the former targets human minds, whereas the latter targets computer and communications systems.

Businesses and nonprofit entities in turn are also highly dependent on information. They use it to develop products and services for customers and clients; to understand markets and audiences for their products and services; to inform customers and clients about their products and services; to comply with laws and regulations applicable to their products and services; and to maintain their accounting and finances. Construction and manufacturing projects entail the coordination of dozens, hundreds, or thousands of parties – all of whom must have a justifiable confidence in the information they are sharing and relying upon.

Contextualized, reliable, trustworthy information is as important to the thinking of human beings as clean air is to human breathing. Human beings depend on good information for making informed decisions about political candidates standing in elections; to know as consumers which specific products and services will best serve their needs; for managing their finances; in making health-related decisions about themselves and their loved ones; in learning to perform their jobs more effectively or efficiently; and in truly countless other ways.

Nations also engage extensively in information production. They provide education for young people; support scientific research that undergirds economic growth and prosperity; and collect, curate, and disseminate large-scale statistical data that influence decisions at every level of society.

Imagine what life would be like if citizens could not count on the validity and trustworthiness of the information underlying any of these activities. In some cases, the result would be no more than minor annoyance. In others, however, the result could be life-threatening. Nations could be crippled, as they could and likely would make bad or at least sub-optimal decisions about war and peace, the economy, law enforcement, housing, food production, energy, and the many other important matters for which governments have some responsibility.

On the existential threat from cyber-enabled information warfare

Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reliable, trustworthy information when and where it is needed. Information is as much a part of human ecology and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems.

Today, chaos reigns in much of the information ecosystem on which societies depend. In many forums for political and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps “truthful hyperbole.” Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminishing confidence in elections and democratic institutions. Using unsupported anecdotes and sketchy rhetoric, denialists undermine well-established science about climate change and other urgent issues. Established institutions of the government, journalism, and education – institutions that have traditionally provided stability – are under attack precisely because they have provided stability.

The founding of the *Bulletin* predates by several decades the widespread availability of computers, the Internet, smart phones, search engines, and social media. Few could imagine in 1945 a technological environment that affords today’s high-speed and widespread connectivity, high degrees of anonymity, insensitivity to distance and national borders, easy and customized information searches, democratized access to publishing capabilities, inexpensive production and consumption of information content (including and increasingly importantly emotionally evocative video and audio content), disintermediation of established information sources, and ubiquitous, always-on, always-available access to information sources through mobile devices.

Such advances in information technology have heralded the arrival of the information age, a world in which taking near-immediate advantage of information opens up enormous opportunities in both the private and public sectors for improved delivery of existing products and services and, perhaps more important, the creation of entirely new products and services. Products and services can be customized to individual needs and preferences on a large scale and at more affordable costs. Transactional friction can be tremendously reduced. Through the Internet of Things, actuators and sensors can be connected to process control computers to optimize the behavior and function of physical systems. Everywhere that information can be used to create and improve new and existing functionality (that is, essentially everywhere), one can find or imagine new information technologies to do so.

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment

of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive burden that such an environment places on their thinking.

In recent years, we have seen how the Internet, social media, and mobile devices (and other technologies) can be used by foreign adversaries to interfere in elections and to disrupt the democratic process. We have seen:

- Social media exploitation of cognitive biases to increase their impact and reach – short messages of 280 characters and emotionally evocative video/audio clips are nearly ubiquitous and much more the norm than they ever were two decades ago.
- Disintermediation of established information sources that reduces the role and influence of those previously responsible for providing factual information and proliferates information sources. The US Supreme Court noted in *Associated Press v. US* (1945) that “the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society.” Today, modern information technology has enabled the creation of a larger number of information sources than the 1945 US Supreme Court could possibly have imagined.
- Search engines that return highly visible results for queries based in large part on the popularity of those results and the inferred desires of the user for specific information rather than their actual importance to those queries. Such functionality also makes it easier than ever for people to find information online “by doing their own research,” thus indulging in their confirmation biases by selectively finding and attending only to information that confirms one’s beliefs. Search engine optimization techniques enable gaming of search algorithms to promote the visibility of false, misleading, or worthless information.
- Many-to-many connectivity that enables the formation of echo chambers and media bubbles that reinforce pre-existing beliefs.
- Large-scale data mining that allows adversaries to sift huge amounts of personal data on individuals to identify and target those most susceptible to customized, inflammatory, false, malign, or misleading messages – and also to keep such messages away from public view.
- Near-immediate data transfer, which enables propaganda and other malign information to spread far and wide quickly, while efforts to correct false information are more expensive, often fall short, and frequently fail altogether.
- Inauthentic voices that are largely indistinguishable from authentic ones. Macedonian entrepreneurs

discovered ways to monetize an affinity of Trump voters for fake news (Subramanian 2017). Paid human employees of the Internet Research Agency created and spread false information on behalf of the Russian government prior to the 2016 U.S. election (MacFarquhar 2018). And automated “bots”–accounts purportedly associated with human users but in fact managed entirely or mostly by machines – add further chaos to the information environment.

Is this state of information affairs really new? Haven’t adversaries of all stripes always employed propaganda and lies – otherwise known as information warfare (or at least a big part of it) – to advance their interests?

Yes. Information warfare indeed has a long pedigree that reaches into the past for at least the three millennia since the Trojan Horse enabled Greek warriors to breach the walls around the city of Troy. Much more recently, the rise of the Nazi regime in Germany relied on propaganda. As Hitler (1925, 155–56) wrote:

[I]ts purpose must be ... to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opinion on things or who wish to form such an opinion on grounds of objective study – because that is not the purpose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers. ... The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feelings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses. ... The receptive powers of the masses are very restricted, and their understanding is feeble.

But more so today than at any earlier point in human history, human beings are vulnerable to information warfare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magnitude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia.

On human cognition

Research in the fields of cognitive and social psychology has formalized what Hitler knew intuitively. We now understand that human cognitive processing capability is not unlimited; humans have finite cognitive resources that can be “used up” under mentally stressful circumstances. Findings from the same cognitive psychology that has transformed neoclassical economics into behavioral economics (and resulted in three Nobel Prizes in economics) have made clear the “bounded rationality” of human thought and the

simultaneous existence in every individual of the capability to engage in two types of cognitive processing.

Specifically, heuristic dual-system cognitive theory posits that human beings have two systems for cognitive processing – an intuitive, reflexive, and emotionally driven mode of thought (often designated as System 1) and a slower, more deliberate, analytical mode of thought (often designated as System 2). Kahneman (2011) provides a primer on System 1 and System 2 thinking. (See Petty and Cacioppo 1986; Chaiken 1987 for other variants of dual-system cognitive theory; see Kruglanski and Thompson 1999 for a contrary view on dual-system cognitive theory.)

System 1 is designed to operate rapidly, but it can do so because it does not take account of all available information and is thus more prone to error (also called bias). System 2 operates more slowly but is more likely to take into account the available information and is less prone to error. People engaging in System 1 information processing respond more emotionally and less rationally or critically than in System 2 processing.

Most important, System 1 thinking is the default mode of thought for human beings – it uses smaller amounts of cognitive resources, relies on simple gut-based judgments, and is used more often when humans are under stress. For most situations encountered in everyday life, System 1 thinking is adequate and produces mostly valid and useful outcomes, but it often fails when a situation requires complex inferences for understanding. For such situations, System 2 thinking, which is effortful and consumptive of cognitive resources, is more often appropriate – and when individuals fail to use System 2 when it is appropriate to do so, they are easily misled.

Most individuals are capable of both System 1 and System 2 thinking; thus, the important operative question is the circumstances under which they select one or the other type of thinking. Psychology has accumulated considerable evidence relevant to this question.

For example, Taber and Lodge (2006) show that an individual tends to be less critical of information that is favorable to his or her position than of information that is not favorable – that is, he or she is more likely to engage in System 1 thinking for favorable information. People have a confirmation bias in their information seeking and processing behavior – they preferentially seek out information that is consistent with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs. In a meta-analysis of 91 studies, Hart et al. (2009) considered two motivations for how an individual might select information to consume – the

desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one's beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al. concluded that both motivations drive human information-seeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. People are also subject to belief perseverance (a.k.a. a continuing influence effect) – a cognitive bias through which individuals do not revise beliefs based on erroneous information even when they know for sure that such information is erroneous (Lewandowsky et al. 2012).

Maintenance of an individual's social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that individuals tend to adopt the views of the peer groups that are most salient to them, even if the "objective" or "factual" information available to them contradicts those views. (Asch 1951 performed the classic "conformity experiments" that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing information that is dissonant to those groups' beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001).

Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (suggestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conversely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of information incongruent with a person's prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that information (Goel and Vartanian 2011).

In the new information environment, exploitation of human cognitive architecture and capabilities – which are largely unchanged from what existed millennia ago –

provides the 21st century information warrior with cyber-enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cognitive limitations, the perpetrators of cyber-enabled information warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed “alternative facts” in advancing their political positions.

Russian interference in the 2016 US presidential election has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states – as undesirable and threatening as it may be – is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed parties on all sides share a basic understanding and knowledge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems.

But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holocaust or to make good decisions about nuclear weapons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in corresponding increases in global temperature and climatic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

Climate change denialism

Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to mitigate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the likelihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events.

Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluctuations in local weather conditions. For example, public

concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as “evidence” that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as information about global climate change).

People are also subject to a loss-aversion bias, in which they place greater weight on losses than gains of equal value. In 1992, the United States committed itself to the United Nations Framework Convention on Climate Change, although President George HW Bush also stated that “the American way of life is not up for negotiation” – and in 2018, the United States withdrew from the Paris Agreement (which was based on the convention). The argument? That the United States would have to give up too much if it kept to the agreement.

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other people, but they won’t happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves – and the misperception that “others may suffer from such problems but I won’t” diminishes the power of personal concern as a driver for rational decision making.

Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and “short-term socio-political context can play a critical role in determining the lenses through which climate change is viewed.” Note especially the importance of “short-term socio-political context” – precisely the context that social media shapes.

Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these arguments to a broad segment of the American public. Fewer in number than, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers

online than in print. Furthermore, subtleties and nuances in their extended written pieces are likely to be lost when they are represented in social media.

Another important element of climate change denialism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by *The Guardian*, a variety of largely secret funding sources distributed \$118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have generated a variety of products for public and policy consumption (but – unsurprisingly – not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their products are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover “both sides” of a controversy that is intellectually equivalent to a “controversy” about whether the earth is round or flat.

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980's and early 1990's rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, compares them, and then acts accordingly.

But the psychologically informed understanding of real-world decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflexive, heuristic System 1 thinking to make decisions, particularly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1

often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today's information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influential participants in one or another of them.

It is thus easy to posit that in this information environment, manipulated information – either artificially constructed or adopted by a strong grassroots base – could be used by interested parties to generate pressure on leaders to act. At the same time, leaders themselves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted information originating from their constituencies.

The coming information dystopia

Nuclear war and climate change are arguably the most important existential challenges today that are compounded by the corruption of the information ecosystem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impossible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyber-enabled information warfare could still lead to an information dystopia. Here are some possible elements:

- Adversaries manufacture numerous graphic videos of American soldiers (complete with sound effects) committing battlefield atrocities, and spread them widely through the Internet. Once upon a time, high-quality video forgeries were difficult and expensive to make. AI-based technologies will bring this so-called deepfake capability to the masses, and anyone with imagination, a modicum of technical skill, and a personal computer will be able to distribute reasonably realistic forgeries. Denials will be issued but of course will also not be believed by large fractions of viewers. Even if proof of inauthenticity can be provided, such evidence will not affect the responses of many viewers.

- Political campaigns conduct similar efforts to discredit political opponents (e.g. “showing” an opponent making controversial or disqualifying remarks before an election). But they also use the existence of deepfake technologies to deflect attention from authentic and real evidence of their own political and personal misdeeds. For example, a real video of a candidate punching an old lady who supports his opponent will be dismissed as “one of those deepfakes that anyone could have produced.”
- Financial markets are disrupted by falsified videos of CEOs making announcements regarding company prospects that are much more pessimistic than expected. Attempts to correct the record are drowned out in a subsequent flood of contradictory information, all of which appear at first glance to be authentic.
- Public safety is compromised by reports of local disasters (e.g. explosions of chemical plants that result in the release large amounts of toxic gases). These reports, along with “authentic” video of people choking amidst locally familiar locations (e.g. well-known fields or sport stadiums), cause spontaneous mass evacuations. Contradictory directions for evacuation broadcast using social media result in chaos on the streets and highways.
- Public health is placed at risk when the safety and efficacy of medical treatments known to be safe and effective are publicly questioned through active disinformation campaigns conducted on the Internet and in bookstores. Attempts to provide valid information are met with responses such as “that’s what the pharmaceutical companies and medical establishment want you to think, but just look at what’s happened to our children.”
- Children in schools are threatened by online campaigns to spread rumor, innuendo, and positive or negative information about various students. Conducting such campaigns for pay becomes the business model of entrepreneurs who advertise that they can guarantee admission to selective colleges, boost the social standing of the children of their clients, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.
- Journalists, political leaders, and judges are compromised by artfully forged emails and alterations to other documents that are mixed with entirely authentic leaked emails and documents and are indistinguishable from them.

A world with these elements – and many more comparable ones – will be the inevitable result if and when deployment and use of the tools of cyber-enabled information warfare become widespread. And even more

troubling is the fact that not every bit of information needs to be corrupted for this dystopian outcome to occur – it will require only a fraction of it to be corrupted for people to lose faith entirely in “objective” and “trustworthy” sources of information, the result of which will be that people will fractionate into their own information realities.

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between statement A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empirical data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information warfare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti-Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

Adversaries foreign and domestic that make use of cyber-enabled information warfare turn our internal cognitive processes and our external institutional and legal processes against us. Under the cover of “fair play” rubrics and the First Amendment, they have turned us against ourselves. Desperately needed are ways of countering the insidious tactics of cyber-enabled information warfare for ourselves.

How might we proceed? We need action to develop better ways of identifying adversary cyber-enabled information warfare campaigns in progress; good countermeasures to help human beings resist the use of cyber-enabled information warfare operations targeted against them; and good measures to degrade, disrupt, or expose the adversary’s use of cyber-enabled information warfare operations. All of this is easier said than done, however, as cyber-enabled capabilities for information warfare increase while human cognitive limitations remain the

same. Our work is cut out for us. If we fail, the world is at increasing risk of large-scale and long-term societal fracture, the end of the Enlightenment, and the start of an informational Dark Age.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by the Carnegie Corporation of New York under Grant G-17-55292 (International Program) for research, teaching, international engagement, and outreach in international security.

Notes on contributor

Herbert Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly knowledgeable about the use of offensive operations in cyberspace as instruments of national policy and the security dimensions of information warfare and influence operations on national security. In 2016, he served on President Obama's Commission on Enhancing National Cybersecurity. He has also served as professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues.

References

- Asch, S. E. 1951. "Effects of Group Pressure upon the Modification and Distortion of Judgments." In *Groups, Leadership and Men*. Edited by Harold Guetzkow, 222-236. Pittsburgh, Pennsylvania: Carnegie Press.
- Associated Press v. United States. 1945, 326 1.
- Balkin, J. M. 2012. "The First Amendment Is an Information Policy." *Hofstra Law Review* 41 (1): 1-30. Article 2.
- Bodenhausen, G. V., L. A. Sheppard, and G. P. Kramer. 1994. "Negative Affect and Social Judgment: The Differential Impact of Anger and Sadness." *European Journal of Social Psychology* 24 (1): 45-62. doi:10.1002/ejsp.2420240104.
- Chaiken, S. 1987. "The Heuristic Model of Persuasion." In *Social Influence: The Ontario Symposium*, edited by M. P. Zanna, J. M. Olson, and C. Peter Herman, 3-39. Vol. 5. Hillsdale: Lawrence Erlbaum.
- Elsasser, S. W., and R. E. Dunlap. 2013. "Leading Voices in the Denier Choir: Conservative Columnists' Dismissal of Global Warming and Denigration of Climate Science." *American Behavioral Scientist* 57 (6): 754-776. doi:10.1177/0002764212469800.
- Goel, V., and O. Vartanian. 2011. "Negative Emotions Can Attenuate the Influence of Beliefs on Logical Reasoning."

- Cognition and Emotion* 25 (1): 121-131. doi:10.1080/02699931003593942.
- Goldenberg, S. 2013. "Secret Funding Helped Build Vast Network of Climate Denial Thinktanks." *The Guardian*, February 14, sec. Environment. Accessed. <https://www.theguardian.com/environment/2013/feb/14/funding-climate-change-denial-thinktanks-network>
- Hart, W., A. H. Dolores Albarracín, I. B. Eagly, M. J. Lindberg, and L. Merrill. 2009. "Feeling Validated versus Being Correct: A Meta-Analysis of Selective Exposure to Information." *Psychological Bulletin* 135 (4): 555-588. doi:10.1037/a0015701.
- Hitler, A. 1925. "Mein Kampf." Translated by James Murphy. Accessed. <http://www.greatwar.nl/books/meinkampf/meinkampf.pdf>
- Horgan, J. 2015. "Bethe, Teller, Trinity and the End of Earth." *Scientific American Blog Network*. Accessed. <https://blogs.scientificamerican.com/cross-check/bethe-teller-trinity-and-the-end-of-earth/>
- Kahneman, D. 2011. *Thinking, Fast and Slow*. New York: Farrar: Straus and Giroux.
- Kahneman, D., and S. Frederick. 2002. "Representativeness Revisited: Attribute Substitution in Intuitive Judgment." In *Heuristics and Biases: The Psychology of Intuitive Judgment*, edited by T. Gilovich, D. Griffin, & D. Kahneman, 49-81. New York, NY: Cambridge University Press. doi:10.1017/CBO9780511808098.004.
- Krosnick, J. A., A. L. Holbrook, L. Lowe, and P. S. Visser. 2006. "The Origins and Consequences of Democratic Citizens' Policy Agendas: A Study of Popular Concern about Global Warming." *Climatic Change* 77 (1): 7-43. doi:10.1007/s10584-006-9068-8.
- Kruglanski, A. W., and E. P. Thompson. 1999. "Persuasion by A Single Route: A View from the Unimodel." *Psychological Inquiry* 10 (2): 83-109. doi:10.1207/S15327965PL100201.
- Kunda, Z., and L. Sinclair. 1999. "Motivated Reasoning with Stereotypes: Activation, Application, and Inhibition." *Psychological Inquiry* 10 (1): 12-22. doi:10.1207/s15327965pli1001_2.
- Lewandowsky, S., K. H. Ullrich, C. M. Ecker, N. S. Seifert, and J. Cook. 2012. "Misinformation and Its Correction: Continued Influence and Successful Debiasing." *Psychological Science in the Public Interest* 13 (3): 106-131. doi:10.1177/1529100612451018.
- Lin, H., D. Jablanski, and H. Trinkunas. Forthcoming. "Retweets to Midnight: Assessing the Effects of the Information Ecosystem on Crisis Decision Making between Nuclear Weapons States." In *Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*, edited by H. Trinkunas, H. Lin and B. Loehrke. Stanford, CA: Hoover Institution Press. 2020.
- MacFarquhar, N. 2018. "Inside the Russian Troll Factory: Zombies and a Breakneck Pace." *The New York Times*, October 15, sec. World. Accessed. <https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html>
- Morgan, P. M., edited by. 2003. "Deterrence and Rationality." In *Deterrence Now*, edited by P. Morgan, 42-79. Cambridge Studies in International Relations. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511491573.003.
- NRC (National Research Council). 1985. *The Effects on the Atmosphere of a Major Nuclear Exchange*. Washington: National Academies Press. doi:10.17226/540.

- Oreskes, N., and E. M. Conway. 2011. *Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming*. New York: Bloomsbury Publishing.
- Perry, W. 2015. *My Journey at the Nuclear Brink*. Stanford: Stanford University Press. Accessed. <http://www.sup.org/books/title/?id=25448>
- Petty, R. E., and J. T. Cacioppo. 1986. "The Elaboration Likelihood Model of Persuasion." In *Advances in Experimental Social Psychology*, edited by L. Berkowitz, Vol. 19, 123–205. San Diego, CA: Academic Press. doi:10.1016/S0065-2601(08)60214-2.
- Pfeffer, J., T. Zorbach, and K. M. Carley. 2014. "Understanding Online Firestorms: Negative Word-of-Mouth Dynamics in Social Media Networks." *Journal of Marketing Communications* 20 (1–2): 117–128. doi:10.1080/13527266.2013.797778.
- Postmes, T., R. Spears, K. Sakhel, and D. G. Daphne. 2001. "Social Influence in Computer-Mediated Communication: The Effects of Anonymity on Group Behavior." *Personality and Social Psychology Bulletin* 27 (10): 1243–1254. doi:10.1177/01461672012710001.
- Roxburgh, N., D. Guan, K. J. Shin, W. Rand, S. Managi, R. Lovelace, and J. Meng. 2019. "Characterising Climate Change Discourse on Social Media during Extreme Weather Events." *Global Environmental Change* 54: 50–60. doi:10.1016/j.gloenvcha.2018.11.004.
- Scott, L., and S. Smith. 1994. "Lessons of October: Historians, Political Scientists, Policy-Makers and the Cuban Missile Crisis." *International Affairs* 70 (4): 659–684. doi:10.2307/2624552.
- Subramanian, S. 2017. "Meet the Macedonian Teens Who Mastered Fake News and Corrupted the US Election." *Wired*, February 15. Accessed. <https://www.wired.com/2017/02/veles-macedonia-fake-news/>
- Taber, C. S., and M. Lodge. 2006. "Motivated Skepticism in the Evaluation of Political Beliefs." *American Journal of Political Science* 50 (3): 755–769. doi:10.1111/j.1540-5907.2006.00214.x.
- Zaval, L., and J. F. M. Cornwell. 2016. "Cognitive Biases, Non-Rational Judgments, and Public Perceptions of Climate Change," November. doi:10.1093/acrefore/9780190228620.013.304.