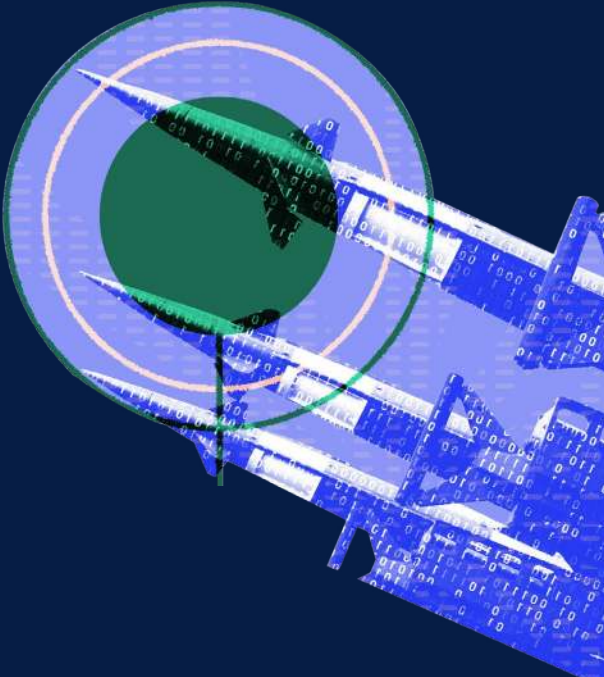




FUTURE DIGITAL THREATS TO DEMOCRACY

Trends and Drivers



Alexa Wehsener
Vera Zakem
M. Nina Miller



This report aims to identify and define 9 driving trends at the intersection of digital systems and democracy. It is part of a broader joint project between the Institute for Security and Technology (IST) and the Center for a New American Security (CNAS) that examines Future Digital Threats to Democracy.

A series of two-pagers examining the different trends can be found [here](#).

This report was designed by Pledger Designs.
Illustrations were provided by CNAS/Melody Cook.

The views expressed in this report do not necessarily reflect the official policy or position of the Institute. Readers should note that IST seeks a diversity of views and opinions on significant topics in order to identify common ground.



CONTENTS

Background	4
Trends in Context	5
Digitally Impaired Cognition	6
Reality Apathy	7
Weaponized Information Environment	8
Fragile Complex Infrastructure	9
Compromised Privacy and Data	10
Weakened Media Institutions	11
Increased Digital Authoritarianism	12
Fractured Ideologies and Identities	13
Intensifying Monetization of Attention	14



INSIGHT

We define a digital threat to democracy as a technological trend that is either facilitating, exacerbating, or instigating the undermining of democratic institutions and norms.



BACKGROUND

Over the last decade, democratic societies have continued to undergo transformational changes. *Demographic shifts, competing narratives, and technological growth have accelerated globalization, urbanization, wealth displacement, and unprecedented access to information.*

While this access has given people a voice, increased their freedom of expression, enhanced human security, and dramatically expanded technological discovery, *it has also given rise to digital threats that have impacted the fundamental security and stability of democratic institutions.*

Based on a comprehensive literature review and conversations with subject matter experts, we have identified nine trends that are likely to pose digital threats to democracy in the future. These trends are:

- Digitally Impaired Cognition
- Reality Apathy
- A Weaponized Information Environment
- Fragile Complex Infrastructure
- Compromised Privacy and Data
- Weakened Media Institutions
- Increased Digital Authoritarianism
- Fractured Ideologies and Identities
- Intensifying Monetization of Attention

For these trends, we have identified drivers that are likely going to contribute to their future development in impacting democratic societies. In addition, while these trends may appear distinct, they are highly interconnected. As such, we have placed them in context and identified cross-cutting challenges that may shape democracy in the future. These trends are derived from currently deployed technologies as well as anticipated advancement and innovation.



INSIGHT

We provide cross-cutting challenges that affect the trends and drivers shaping digital threats to democracy.



TRENDS IN CONTEXT

COMPUTING POWER

As Artificial Intelligence (AI) / Machine Learning (ML), quantum technologies, intelligent machines, and other technologies continue to advance, they will require increased computing power. In order to develop comprehensive AI models, large amounts of computing power, data, and energy will be necessary.

PALEOLITHIC EMOTIONS

Humans are more vulnerable to digital misinformation due to cognitive biases. As a result, individuals have an irrational predisposition to accept new information as true, particularly when it comes from their social circles and confirms prior beliefs.

ENERGY

Large neural networks, supercomputers, and other emerging technologies will have an increasing environmental cost, with potential solutions such as fusion and plasma capabilities still well off in the distant future.

INTELLIGENT MACHINES

Autonomous systems will augment or replace humans by automating jobs, analyzing data, surveilling and policing citizens, and fighting wars. Human interaction with intelligent machines raises legal and ethical questions, causing democracies to examine new risks of bias and international conflict.

CLIMATE CRISIS

The climate crisis will exacerbate existing socio-economic problems in democracies. Current democratic systems are not equipped to address incremental but catastrophic threats.

DEMOGRAPHIC TRENDS IN DEMOCRACIES

Include an aging population and uneven access to higher education, contributing to polarization, lack of critical thinking, and understanding civic institutions. These demographic shifts will likely impact digital threats to democracy.



INSIGHT

Human cognition and capacity is increasingly constrained and even undermined by a growing reliance on and the influence of digital systems. Individuals are more and more incapable of remembering facts, struggle to maintain focus, and lack critical thinking.

DIGITALLY IMPAIRED COGNITION

DRIVERS

Attention addiction makes it difficult to distinguish between validation and rejection in the real or digital worlds.

Technology platforms and social media content algorithms are engineered for virality, sensationalism, provocation, and increased attention.

Microtargeting identifies targeted areas of interest to consumers and undermines consumers' ability to think critically about any given issue.

Viral videos capture and hold human attention better, because motion captivates the eyes and brain.

Brain machine interface technology and AI augment and anticipate our needs.

Augmented Reality/ Virtual Reality combine multiple sensory inputs, thus, increasing the potential for attention addiction and inability to discern real from fake content.

Increasing virality of communication and information results in constant attention-switching and multitasking, thus, further impairing human ability to digest information and make decisions.

Information overload outcompetes both internal memory and decision-making processes.

Widely ubiquitous devices have integrated multiple screens into the lives of individuals globally.

Digitization of everyday life through data management in the workplace, integration of digital tools into education, and the majority of leisure time being spent in front of TV and computer screens.

Research in neuroscience and human psychology enables better targeting and persuasion.

Complex technological advancements make it difficult for the general population to understand how novel technologies interact.



INSIGHT

Reality apathy is characterized by citizens discounting the world around them due to an overload of negative content and false information - resulting in the perception that making a positive impact in the world is simply too hard.

REALITY APATHY

DRIVERS

Information overload makes it difficult to delineate between what is salient and what is not.

Virality of information diffusion identifies the general populations' constant access to horrific information (24hr news cycle) without the training to handle it.

Diffusion of deep fakes is furthered by virality of communication.

Diffusion of information via 'share' button on social media platforms points to a tendency to 're-share' negative content, resulting negative information on the 'news feed'.

Dis/Misinformation operations drive a public perception of political corruption, resulting in apathy during political cycles.

Information flooding incentivized by the tension between the democratic right to free speech and the utilization of speech platforms to distract and/or rally support for political competition.

Competition in the news industry

requires a 24/7 cycle prioritizing negative content, breaking news, and making each disaster seem worse than the last to hold consumer attention to gain advertising revenue.

Increased awareness of international crises

perpetuate a feeling of being unable to help when something goes wrong on the other side of the world.

Learned helplessness

results from increased awareness of global humanitarian challenges without equally powerful tools to address them.

Compassion fatigue

results from viewing a multitude of negative content, but being unable to help — leaving one feeling useless.



INSIGHT

Digital communication spreads viral information across the information environment at such speed that online effects transfer into the physical world. Malign actors can weaponize digital communications to manipulate public opinion and erode the distinction between truth and lie.

WEAPONIZED INFORMATION ENVIRONMENT

DRIVERS

Advanced Persistent Manipulator (APM) kill chain mobilizes a target through a multi-platform attack incorporating staging, reconnaissance, mimicry of 'popular' accounts, and narrative amplification in order to mobilize a specific entity.

Deep fakes and video manipulation make false or manipulated political content more believable and influential.

Content algorithms are manipulated by malign actors in order to spread mis/disinformation.

AI enables intelligent bots and higher quality audiovisual manipulations.

Augmented Reality/ Virtual Reality worsens digital propaganda problems.

Influence Campaigns utilize digital platforms and a trending means of communication to influence civil society by way of inoculation, infection, or treatment.

Reliance on digital communications by civil society and governments creates a vulnerability of weaponization of information.

Exploitation of democratic values to disseminate misinformation and influence campaigns. Traditional unfettered flow of information utilized by malign actors for 'information flooding,' a technique of filling public debate with disinformation and distraction.

Automated laser phishing occurs when AI mines social media to gather information on friends and family and then impersonates them to extract important information.

Proliferation of open source material allows individuals to access code and information that can be used for disinformation campaigns.



INSIGHT

Infrastructures in democratic societies are vulnerable to asymmetric digital warfare that may have physical effects and target societal resilience. Malign actors may exploit weakness in infrastructure in order to target populations and democratic institutions.

FRAGILE COMPLEX INFRASTRUCTURE

DRIVERS

Proliferation of technology and minimum required expertise to carry out a cyber-attack permits non-state actors, “hacktivists,” and individuals to target digital systems.

The cyber offense-defense balance favors the attacker over cybersecurity.

Interconnectedness of physical infrastructure with digital systems means disruption or damage can rapidly spread across elements of the system.

Protocols and systems in infrastructure are often outdated.

5G systems are software-based and in some ways more vulnerable than hardware, because there are no ‘choke points’ and multiple points of entry.

Foreign software for Mobile Cloud Computing introduces vulnerabilities even to systems with domestic-sourced hardware and equipment.

Proliferation of Internet of Things (IoT) increases infrastructure vulnerability, because more online devices have more potential attack pathways.

Countries source critical infrastructure and telecommunications equipment abroad, despite potential vulnerabilities, motivated by low product prices.

Countering gray-zone threats requires a unified approach from government, industry, and civil society, yet Western society typically views these stakeholders as separate.

Strengthening social resilience through localized support infrastructure, social connectedness, and bottom-up support, which can be enabled by new technologies.



INSIGHT

Governments and corporations collect and analyze massive quantities of data to identify individuals' physical and digital activities, along with psychological and physical characteristics. These data sets come from video and drone surveillance, data imprints online, geolocation data, and biometrics.

COMPROMISED PRIVACY AND DATA

DRIVERS

Data regulation is absent, non-comprehensive, or unstandardized, which confuses consumer rights and privacy.

Surveillance technologies are ubiquitous, specifically the use of facial recognition technologies.

AI/ML can be used to analyze huge datasets of consumer information, enabling facial recognition or augmenting virtual reality.

Continuously evolving technologies are difficult for every day citizens to fully understand. Lack of understanding contributes to limited consumer pressure for increase in regulation.

Compromise of secure data sets by hackers further degrades privacy.

Rapid DNA sequencing drives the consumer biometric market, exposing data to theft and sale.

Data and privacy regulation are insufficient to prevent corporate, government, and lone actor abuse. Corporations obfuscate data policies so consumers avoid thinking critically about privacy.

Digital asymmetric warfare by illicit actors to access personally-identifying information for profit or geostrategic aims.

Income inequality motivates consumers to use free apps, despite compromising data privacy.

VR/AR video games provides a data bank of all movements unique to each player.

Lack of access to higher education makes citizens less aware of individual privacy.

Lack of understanding of privacy as a value for individuals and consumers.

Extractive Information Economics is a new form of economics driven by data mining, personalized advertising, and a lucrative data market.



INSIGHT

Traditional media organizations are weakened due to limited funding, lack of trust, monopolization, and corruption. This decline is compounded by social media becoming the medium of choice for many consumers.

WEAKENED MEDIA INSTITUTIONS

DRIVERS

Consumers receive news from social media platforms, which rank stories algorithmically.

Computational propaganda erodes public confidence in accurate information -- deepfakes, AI, bots, manipulation of content algorithms.

Degradation of trust in media institutions linked to polarization, with a decline in support for political elites with opposing views.

Authoritarian and democratic leaders attack independent media by aligning themselves with certain media sources and de-legitimizing others.

Social media and online platforms have taken advertising revenue, eroding the economic model of traditional newspapers.

Institutional changes in traditional media to update their business model has cut down on institutional knowledge and support.

The interplay between social media algorithms and human psychology causes selective exposure, due to consumers preferring content that confirms prior biases.

Conspiracy theories in mainstream discourse indicates a growing number of individuals who are unable to be convinced by contrary evidence.

Media corruption has weakened media institutions and has given rise to disinformation, polarization etc.

Media monopolization and opaque ownership create a media environment that exacerbates the weaponization of information and polarization.



INSIGHT

Governments are investing significant resources in cutting-edge technologies for surveillance and control. The global sale of these technologies contributes to the rise of authoritarianism.



INCREASED DIGITAL AUTHORITARIANISM

DRIVERS

Surveillance (AI, 5G, genetics, autonomous systems) generates massive datasets for technical research and development.

Increasing computing power facilitates large-scale data analysis with sophisticated AI/ML.

The digitization of everyday life enables surveillance from consumer digital devices. Autonomous policing based in sophisticated AI, robotics, facial recognition, and autonomous decision-making may be used for surveillance and/or crowd control.

The rise in digital communication facilitates new censorship tools such as, automated inauthentic accounts.

Targeting of traditional democratic values and freedoms by closing or censoring internet, and other outlets for speech, press, and assembly.

Countries establish an information wall by limiting which populations have access to sophisticated communications technologies.

The public accepts surveillance because these technologies often do not 'seem' oppressive. Techno-authoritarian synergy between companies and illiberal governments, with authoritarian regimes offering data access without regulation.

States and companies strategically restrict access to technology platforms from subsets of their citizens and consumers.

Governments and industry employ novel types of digital propaganda in order to amplify their narratives, increase polarization, and "us versus them" divisions.



INSIGHT

Content algorithms favor information that confirms user beliefs and amplifies divisions. Together with unequal access to digital communications, this trend worsens geographic, economic, and social divides while eroding trust in public institutions.

FRACTURED IDEOLOGIES AND IDENTITIES

DRIVERS

Content algorithms reinforce user beliefs (confirmation bias), resulting in selective exposure.

AI-enabled 'bots' and deepfakes generate false and inflammatory content aimed at user biases, further fracturing ideologies and identities.

Online anonymity enables malign actors to spread content on social media and mass messaging apps without attribution.

Virality amplifies polarizing voices and misinformation on online platforms, worsening existing social, geographic, and economic divisions.

Digital propaganda exploits societal divisions, erodes trust in media and political institutions, and spreads conspiracy theories.

Online disinformation campaigns, and inauthentic and synthetic accounts target vulnerable populations by impersonating members of targeted groups in order to fracture consensus and increase polarization.

A small group of consumers of disinformation has an outsized impact through voting and amplification.

Mass migration associated with climate change, conflict, urbanization, and demographic shifts will strain limited resources to address digital threats to democracy.



INSIGHT

Extractive information economics is characterized by a massive data market with little regulation, privacy, or transparency. This economy is supported by virality, and the need to capture and hold attention in order to sustain the technology industry.



INTENSIFYING MONETIZATION OF ATTENTION

DRIVERS

Proliferation of systems and platforms that enable data extraction.

Free social media through which consumers provide data and content to companies, while platforms gain revenue from targeted advertising.

AI/ML to analyze collections of data imprints and generate predictions.

Surveillance capitalism is the economic and legal basis for social media and internet handling of consumer data imprints.

Attention addiction drives continued and increasing consumer engagement with platforms.

The attention economy is an advertising business model that exploits the mismatch between technology and human ability to process complex information.

Personalized advertising to consumers uses large-scale data, including 'psychographics' for personality and psychological analysis for political targeting.

Decentralization of news infrastructure leads to 'attention' determining virality and the spread of information.

Product design fosters addiction in order to sustain user engagement and increase advertising revenue.

Limited competition in the technology sector restricts consumer options for private or sustainable platforms.