BUILDING A HEALTHY

COGNITIVE IMMUNE SYSTEM

defending democracy in the disinformation age

INSTITUTE FOR THE FUTURE

BUILDING A HEALTHY

COGNITIVE IMMUNE SYSTEM

defending democracy in the disinformation age

Evolutionary biologists observe that complex biological and ecological systems are under constant attack from parasites—invaders on the lookout for weaknesses in the system to use as entry points to grow and propagate, in the process undermining the healthy functioning of the host. Under static conditions, these systems have established mechanisms for warding off such attackers. But under conditions of change, these mechanisms are no longer effective, allowing parasites to thrive and weaken the host.

The metaphor is particularly apt in describing the state of our body politic today. Dramatic changes in our media and information technology landscapes are weakening our individual and collective cognitive immune systems, opening us up to disinformation attacks and many new forms of manipulation. And the defenses we've built over decades is ill suited to ward off these new attackers, which include bots, trolls, and much more.

The cognition of individuals and of the larger body politic has always been a target for manipulation. Many are attempting to persuade others in many different directions, and in a democratic society we tolerate and even invite many voices. In today's highly networked world, however, attacks against democracy have the potential to be more devastating than ever before. For better and worse, networked communications tools and technologies have altered existing power dynamics by re-defining who has the power of voice, the power to shape our dominant narratives, and the power to influence our cognition. An individual with a $500 laptop, a $30 a month Internet service plan, and a YouTube account has a greater potential audience than a 1990s television station with a newsroom, cameras, a staff, transmitting equipment, and an FCC license, all of which totaled millions of dollars. Social media platforms have unprecedented insight into the desires, fears, and behaviors of billions of their users. And yet, we still are at the early stages of this transformation, with old structures, regulatory systems, and cultural norms straining to respond to the rapid changes in our information environment.

To preserve democracy, we need to develop new immune mechanisms, a new immune system, suited to today's realities. We need to uprade our "cognitive immune systems" at individual and community levels.

HOW TO USE THIS MAP

This map presents the dilemmas, drivers, and future forces that will play important roles in the battle between disinformation tactics and healthy immune responses. Start with the map side for a visual overview of the cognitive immune system and the attack methods bad actors use to exploit our cognitive biases. The map also reveals seven strategies to improve our defenses. Then, flip the map over to gain a deeper understanding of the trends driving compromised cognitive immunity, as well as the difficult choices we must grapple with in our effort to combat disinformation.

WHAT IS COGNITIVE IMMUNITY?

This is a precarious time in which democracy—our widely shared set of values for responding to social, environmental, and economic challenges—is being undermined by groups that excel in the creation and distribution of infectious social-media-ready viruses. The **Attack Vectors** they employ (described in detail on the other side of this map) are designed to exploit network dynamics as well as one or more of the dozens of **Cognitive Biases** in humans that psychologists and behavioral scientists have identified and cataloged over the years. While cognitive biases may convey certain benefits, such as small group solidarity, they can also compromise our ability to think rationally or judge fairly, making us susceptible to misinformation that raises prejudices, fears, and beliefs that work against flourishing within a functioning democracy.

For democracy to thrive we must develop **Immunity Activators** for healthy cognition. These boosters are tools, laws, regulations, cultural norms, and skills that work in combination to form a socio-technical infrastructure that protects our networked society against malicious or unwanted intrusions that threaten the body politic.

Building a cognitive immune system will require a systemic view of our networked society. We must understand the forces—technological, cultural, economic—on the horizon that could erode, or help sustain, democracy.

COGNITIVE IMMUNE SYSTEM DILEMMAS

It is important to note that a healthy cognitive immune system isn't a cure-all for wiping out disinformation. In the same way that a biological immune system can backfire or over-react, a cognitive immune system can sometimes damage the system it's designed to protect. We must accept that there are challenges we cannot find solutions to. We call these dilemmas. Like parasites in an ecosystem, dilemmas are things we have to live with and learn to manage, in the process balancing difficult choices.

Free Speech vs. Censorship

What are the boundaries of free expression? Who decides where to draw the lines?

Platforms vs. Publishers

How much responsibility does a social media platform bear for the content its users publish? To what extent is a platform a common carrier, like a phone company or an email service, and to what extent is it a publisher, like a newspaper or a magazine?

Innovation vs. Deliberation

How can a media business stay competitive, while also taking time and resources to develop mechanisms that mitigate adverse consequences? In other words, how does an ethical business compete with a business that espouses a credo of "move fast, break things?"

Economic Returns vs. Social Returns

How do we move beyond profit maximization in our media ecosystem? How do we encourage capital investment in media platforms that put their users above sponsors and advertisers?

Cognitive Cohesion vs. Cognitive Diversity

How do we maintain healthy diversity while maintaining shared worldviews essential to a healthy society?

Media Literacy vs. Media Manipulation

How do we educate people in the workings of technology and media tools without engendering greater distrust?

WHAT'S DRIVING COGNITIVE VULNERABILITY?

A broad array of **technological and social drivers** affect the disinformation tactics and efforts to inoculate democracies against them. Although each driver in itself is important, they are not independent of one another. Their real impact comes from their combinatorial efficacy.

Reality Mining

Every click, purchase, view, and action we make online is a data point that machine learning algorithms use to gain insight into who we are, how we live, and what motivates us.

Internet of Actions

A network of connected smart objects and systems will negotiate, initiate, delegate, and complete tasks based on our patterns of behavior and implicit wishes. IoT devices are notoriously insecure and their behavioral data can be hijacked and used for political intelligence.

Coding For Virality

A deep understanding of how ideas spread through a particular medium, not solely due to their content, but how their wrappers (e.g. memes, gifs, tweets, celebrity endorsements) facilitate propagation through the cultural environment, making media easier to weaponize.

Digital Noise

Information overload, perpetual distraction, and cognitive exhaustion has become our steady state.

Decrypting the Brain

At the intersection of neuroscience, behavioral economics, cognitive psychology, and big data, researchers are uncovering the mysteries of how the mind works, resulting in a real science of persuasion.

VUCA World

First introduced by the Army War College, the acronym refers to the volatility, uncertainty, complexity, and ambiguity of the present day, creating a sense of disorientation that's ripe for exploitation.

Wealth Inequality

Economic inequality undermines overall levels of trust within the population by increasing social distance between members of the society, making people believe that their compatriots are different from them.

Monopolization

Concentration of economic and technological power in the hands of a few information and social media platforms leads to emergence and hardening of class divisions.

FUTURE FORCES

Future forces describe the technological, social, economic, environmental, and political factors likely to have an effect on a given domain. Future forces are important to consider in combination because they form complex systems of interconnected drivers of change. Here we have applied a future forces analysis to the domain of cognitive immunity as a first step towards designing the tools we'll need to create a more resilient and democratic society.

VULNERABLE DEMOCRATIC STATE

Trust in the State is Being Undermined by 21st Century Innovations

"Twentieth century political structures are drowning in a twenty-first century ocean of deregulated finance, autonomous technology, religious militancy and great-power rivalry," writes Rana Dasgupta, author of *After Nations*. The nation state still has substantial power to shape people's lives and global conditions but its powers are increasingly being tested by several forces, key among them free flow of capital, global connectivity, and climate disruptions where actions and policy choices outside of the control of individual states and localities have profound national and local consequences. The state still exercises control over the movements of people, but the costs of maintaining such controls are rising under the strain of climate migration and as disparities in living conditions become more visible.

Rise of Global Plutocrats and Oligarchies

According to Oxfam, in 2018, 26 people owned as much wealth as the 3.8 billion people who make up the poorest half of humanity. Their success is not connected to the fortunes of their fellow national citizens and their goal is to defund public goods, thus undermining the state as they see it as a threat to their successful operation.

Global Criminal Economy

The international criminal economy and global plutocrats are merging to form a new governance system that employs a criminal services industry of lawyers, accountants, and offshore asset managers and other enablers. They also use sophisticated surveillance and propaganda techniques to shape opinions and information flows to sway popular sentiment.

Climate Change Refugees

By 2050, according to scientists, there will be some 200 million environmental refugees. Climate change will become the cause of most wars and political upheavals. At the same time, global environmental youth movements are likely to put pressure on multinational organizations and local governments to act independently of nation state policies.

CULTURE OF EXTREMES

New Media Amplifies Emotional Extremes to Maximize Revenue

Machine learning, artificial intelligence, and insights from neuroscience are driving the development of our media infrastructure. These tools present unparalleled opportunities for expression and access to knowledge. They bring together people across geographic and institutional boundaries, but they also increase polarization, empower marginal extremes, and promote narrow-interest filter-bubble groups. Democratic societies that value freedom of choice and expression can become overwhelmed with an overabundance of noise that obscures and distracts from quality information. Authoritarian societies can constrain access to information and people's abilities to coordinate activities.These technologies can surreptitiously provoke extremes of human emotion and implicitly manipulate behavior.

Fragmented Identities

Familiar institutional markers of identity—work, family, education, religion, politics, and citizenship—are splintering. New information tools enable the creation of affinities around narrow sets of values, opening opportunities for bad actors to destabilize societies and shift established norms.

Emotion-Driven Media

Platforms use neuroscience and behavioral economics to keep users engaged for as long as possible. Fact-challenged news that stimulates high-arousal emotions is shared more than accurate articles that stimulate low-arousal emotions. Emotion is the main fuel of the new media ecosystem.

Transparency Downsides

Extreme transparency increases levels of accountability but might actually widen the Overton Window—the range of ideas tolerated by the public. When we are confronted with a steady stream of shocking revelations or pronouncements, we reset our normative expectations.

A WORLD OF BLACK BOXES

Decisions About Our Lives are Increasingly Being Made By Opaque Algorithms

Today, the Web serves content to us via various devices. Tomorrow, it will be an overlay on physical reality. Already, high-resolution data about all aspects of our lives feed myriad machine learning algorithms that conduct an orchestra of AI agents to deliver custom content and act on our behalf. As the algorithms deepen in complexity, they'll increasingly become black boxes—systems in which the inputs and outputs are understood but the internal workings are a mystery to the users and, frequently, the creators. This lack of algorithmic accountability and transparency will dramatically increase the risk of failure and make it easier to obscure deceptive, unethical, and malicious practices behind inscrutable code.

Everything is Media

We're entering a world of mixed reality in which digital content is extending well beyond televisions, smartphones, and computer displays to include our homes, vehicles, buildings, and bodies. As the always-on interactions become increasingly algorithmically mediated, reality itself will becomes malleable, sparking an AI arms race between deepfake generation and detection technology.

Algorithmic Bias

Algorithms help humans decide who to hire, who to loan money, and who to send to prison. They also determine what appears at the top of online search results and the headlines in your news feed. Addressing the biases in algorithms is often difficult because of their black box nature.

Surveillance as a Feature

A simple, spoken language request to an AI-powered device triggers a cascade of interactions and activities involving digital and physical objects. The intelligent, connected devices around us are personal panopticons, always happy to help but potentially serving as portals for undesired influence and surveillance.

CULT OF INNOVATION

Shadow Side of the Move Fast, Break Things Ethos

The long-held desire for stable employment has given way to lionization of entrepreneurship. Silicon Valley's singular focus on innovation and easy access to capital has resulted in the rapid growth of tech companies whose ethos is "move fast, break things." They prioritize innovation, rapid growth, and investor returns with little consideration of shadow sides of their products and services. In the process, they are disrupting traditional media and other trusted sources of information before we have a chance to put in place appropriate regulatory mechanisms to mitigate negative impacts.

Business Model Based on Addiction and Data Capture

Social media platforms are engineered to keep users on the site as long as possible, collect data on everything they do, and sell it to advertisers. Treating advertisers as their clients, rather than users, has led to deceptive practices that exploit tactics of propaganda at the expense of the public.

Tech Discovers Ethics

Silicon Valley's ethos of "build and ship" has resulted in social media platforms that fail to consider how their products are used and abused. Tech firms are just now reckoning with how to address potential misuses of their products with a number of ethics and technology initiatives and university courses skyrocketing.

Follow the Money

The death of journalism as we once knew it is due in large part to Advertising models in social media that deprive professional media operations of needed funding. While venture capitalists put their money into for-profit social media firms, there is a dearth of investments in public interest, non-profit, and commons-based media platforms and businesses.

NEW EVIDENCE & NEW AUTHORITIES

People are Placing Their Trust in New, Untested Forms of Authority

Surveys reveal a widespread decline in trust of institutions of all kinds—governments, media outlets, corporations, multilaterals, and philanthropic organizations. Even academic and science experts no longer enjoy the level of prestige they once had. People instead are turning to new sources of evidence and authority. Enabled by massive amounts of data and analytics technologies, we are creating new pillars of trust. For instance, digital reputation systems allow us to trust strangers in ways we've never done before. With the rise of ride-share services like Uber and Lyft, parents are now comfortable allowing their children to get into cars driven by people they've never met.

A Shift Toward Autocracy

People who don't trust the globalist, technocratic establishment, under whose leadership they have been disenfranchised, are inclined to trust those who appeal to their resentments. The result is a worldwide movement toward populist and autocratic "authorities."

Replication Crisis

The ability to repeat experiments with consistent results is the cornerstone of science. In recent years, however, some fundamental studies in social sciences have failed the replication test, leading to a proliferation of anti-science conspiracies.

Personal Trust Networks

Our personal network moderates our worldview. Today, global connectivity enables us to connect with millions like us, amplifying our beliefs and anxieties. This fragmentation will challenge widely shared notions of reality, truth, and evidence.

REGULATORY PARALYSIS

Rapid Advances in Technology are Difficult to Understand and Regulate

The global rise of digital disinformation and user data abuse creates an urgent need for regulation. But policies to address them are lagging. Congress has failed to move on curbing deceptive practices in social media ad buying and preventing automated profiles on social media from amplifying particular individuals and information while simultaneously suppressing others. A few European nations are taking steps to curb malicious data practices—but most democratic countries around the world are unable or unwilling to identify and block efforts.

Regulatory Capture

According to the *New York Times*, "four of the biggest technology companies are amassing an army of lobbyists as they prepare for what could be an epic fight over their futures." Armed with money and deep knowledge of advanced technology, they are powerful foes to any who challenge their business models.

Technological Ignorance

Without intimate knowledge of new technologies, it is nearly impossible for policy makers to generate effective regulation in the digital space. Regulators and legislators are in a position of constant catch up—trying to solve problems after the fact rather than anticipating them.

Fear of Being Left Behind

AI is the new competitive battleground for companies and governments. Many believe that whoever builds and deploys most advanced AI will be a global economic leader. The fear of stifling innovation is often as the reason for not curbing the power of largest players.

BUILDING A HEALTHY

COGNITIVE IMMUNE SYSTEM

A GUIDE

Disinformation attack vectors that exploit cognitive biases and immunity activators for defending democracy

Dark Advertising

Use of psychometric data to specifically target individuals online with advertisements that are not shown to all users. These advertisements can be used to sway individuals' behaviors during elections or push individuals towards extremism, amongst other goals.

Nudging/ Recommending

Reinforcement incentives and indirect suggestion tactics to influence thoughts and behavior.

Censorship

The removal of content or users promoting content. Content can be removed manually through takedowns, content containing certain keywords or from certain users can be made unpublishable.

ATTACK

STRUCTURAL MANIPULATIONS

Search Engine Optimization

Manipulating search engine results to promote certain content and control the narrative. Can be used to spread disinformation and steer people towards extremism.

Shadow Banning

A user's content is downregulated, not shown in other users' feeds, and/or does not appear in searches. Then users are not informed that they have been shadow banned, and often remain unaware of the action taken. against them.

IMMUNITY ACTIVATOR

PUBLIC MEDIA PLATFORMS

Private social media platforms are built upon similar core Internet technologies as commons-based ventures like Wikipedia. However, commons-based platforms do not have access to the same levels of funding, and must rely on donations, grants, and other philanthropic investments. An alternative is capital pools that support platforms more beneficial to the social fabric.

Disinformation

False information, such as conspiracy theories and fake news, that is purposefully intended to mislead, confuse, and exhaust our powers of cognition.

Misleading Narratives

Stories that appear to be plausible, but skew facts and context to distort the reality of news events to fit a particular agenda or ideology.

Hyper-partisan Media

News that is not necessarily false but is sensationalized through a partisan lens.

ATTACK

FALSE INFORMATION

AR/VR

Multisensory immersive media can be designed to fabricate convincing but false reality.

Astroturfing

Human users that appear to be grassroots activists and organizers but are in fact coordinated by, and sometimes paid by, political groups, corporations, and individuals.

Deepfakes

Realistic videos and voice recordings, that are difficult to ascertain as fake, created by algorithms.

IMMUNITY ACTIVATOR

DATA OWNERSHIP RULES

Tech giants use data generated by people to create multi-billion dollar businesses. What if you could own, trade, or donate your personal data? What if the data were a public good? Treating data as a personal or public asset significantly changes the economics and operating principles of current social media businesses, removing some of the capabilities for media manipulation.

IMMUNITY ACTIVATOR

REALISTIC TECH APPROACHES

Algorithm-based solutions designed to identify, filter, and fight various forms of digital deception, will result in an arms race between bad actors and the platform engineers, and add black boxes to the space of public discourse. Any technological tools deployed must involve human-machine partnership that combine computational power with qualitative insight.

IMMUNITY ACTIVATOR

EARLY WARNING SYSTEMS

With a wide knowledge gap between rapidly innovating tech companies and government agencies struggling to keep up, it's clear that policy makers and legislators could benefit by having tools and processes for understanding and identifying implications of new technologies on the horizon before they diffuse widely, and implementing early warning systems to signal when regulatory interventions are needed.

Confirmation Bias

Tendency to selectively seek and interpret information so as to confirm existing beliefs, often disregarding contradictory data.

Mere-Exposure Effect

The phenomenon by which repeated exposure to an idea, person, or thing leads individuals to prefer it. Also known as the familiarity principle.

Bandwagon Effect

The desire to adopt the new beliefs and trends of others increases as more people adopt them.

Truth Bias

The assumption that the information one is receiving is true. This bias is central to human communication.

Spiral of Silence

The fear of being excluded from the group leading individuals to remain silent on ideas that they feel are minority opinions, but are actually held by the majority.

Ingroup Bias

The tendency of individuals to treat members of their in-group more favorably than members of the out-group.

Trolling

Engaging in many activities ranging from harassment, meme creation and promotion, and the disruption of discussions with intentionally inflammatory dialogue.

Leaking

Public release of confidential information gathered through illegitimate methods.

Impersonating

Assuming real individuals' identities by attackers.

ATTACK

DIRTY TRICKS

Hacking

Obtaining unauthorized access to a computer or private network.

Doxxing

Publishing an individual's or organization's private information (e.g. home address, cell phone number, and national identity numbers) publicly online.

Phishing

Malicious email, phone calls, or texts designed to give attackers access to private data or login credentials.

IMMUNITY ACTIVATOR

BEYOND MEDIA LITERACY

Media literacy and critical thinking are commonly considered to be the building blocks of a strong cognitive immune system. But the most effective strategies to defend against disinformation are self-awareness of how our filters affect our interpretation of information, promoting social cohesion instead of technological alienation, and strengthening social and cultural resiliency.

IMMUNITY ACTIVATOR

NEW SOCIAL MEDIA NORMS

We can use research from psychology, evolutionary biology, immunology, network dynamics, political and other sciences to not only construct media platforms that safeguard culture against negative influences but that also promote prosocial behaviors online. After all, information spreads because of some combination of cognitive biases and network effects. We need to understand both and apply this understanding to fostering cognitive and cultural immunity.

Sockpuppets/ Cyborgs

Human users that seek to manipulate online discourse, usually with manufactured identities, acting in coordination, and using bot-like methods (automated mass posting, coordinated approval and spamming, etc.).

Botnets

Coordinated, large-scale network of bots.

Sleeper Bots

Automated accounts that engage in all of the aforementioned behaviors, but are distinguished in that they lie dormant for long stretches of time and are activated for mass, coordinated attacks when needed.

ATTACK

BOTS

Social Bots

Bots that are intended to impersonate and/or interact with humans on social media.

Roadblock Bots

Automated accounts that spam hashtags and conversation threads with irrelevant information and gibberish in order to disrupt streams of communication and coordination.

Amplifier Bots

Automated accounts that spread information by sharing, retweeting, and republishing content. Some only interact with other bots in coordinate efforts to manipulate trending algorithms. Often work in conjunction with approval bots.

Approval Bot

Automated accounts that retweet, "like," and comment on specific posts and profiles to enhance their credibility.

IMMUNITY ACTIVATOR

INDEPENDENT PLATFORM REVIEW BODIES

Governments struggle to regulate social media platforms, while the platforms themselves have failed to institute effective self-regulation. There is a need for an independent oversight body to regulate the use of technology for the manipulation of public opinion across platforms and countries. Transparency will be a key mechanism for auditing potential misuses of social media platforms.

INSTITUTE FOR THE FUTURE

ABOUT INSTITUTE FOR THE FUTURE

Institute for the Future is the world's leading futures thinking organization. For over 50 years, businesses, governments, and social impact organizations have depended upon IFTF global forecasts, custom research, and foresight training to navigate complex change and develop world-ready strategies. IFTF methodologies and toolsets yield coherent views of transformative possibilities across all sectors that together support a more sustainable future. Institute for the Future is a registered 501(c)(3) nonprofit organization based in Palo Alto, California.

AUTHORS

Marina Gorbis
Mark Frauenfelder
Katie Joseff
David Pescovitz

DESIGN AND PRODUCTION

Jean Hagan
Robin Bogott
Helen Bruno
Trent Kuhn
Karin Lubeck
Robin Weiss

With special thanks to contributing experts and workshop attendees:

Ed Bice
Jan English-Lueck, Ph.D.
Adriano Farano
Brittan Heller, J.D.
Lyn Jeffery, Ph.D.
Brian Knutson, Ph.D.
Becca Lewis
Nick Monaco
Juliana Schroeder
Drew Sullivan
Lawrence Wilkinson
Tamsin Woolley-Barker, Ph.D.
Samuel Woolley, Ph.D.

INSTITUTE FOR THE FUTURE

201 Hamilton Avenue
Palo Alto, CA 94301
650.854.6322 **www.iftf.org**