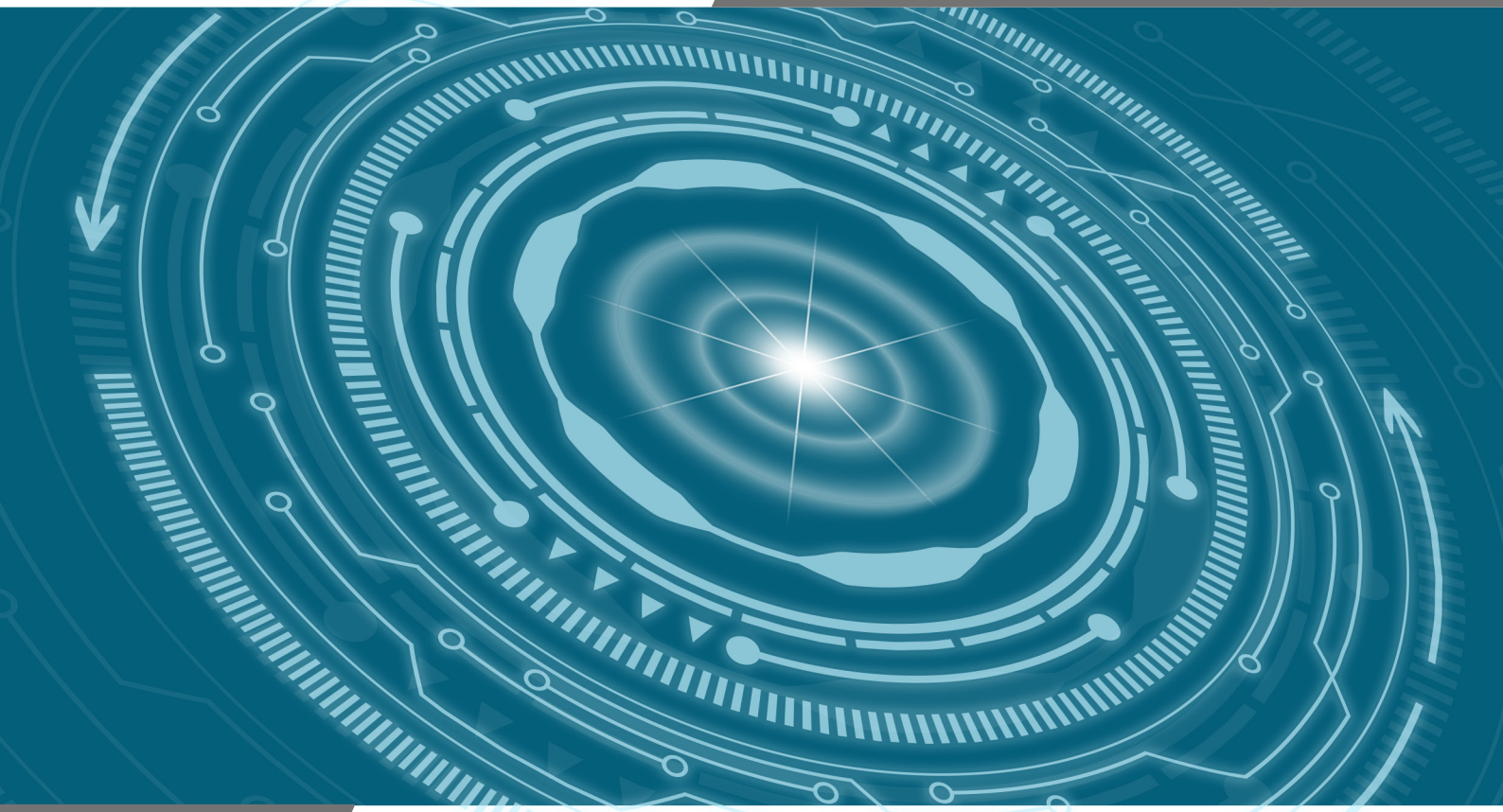
Centre for Economics and Foreign Policy Studies

edam

Cyber Governance and Digital Democracy 2018/9



July 2018

Artificial Intelligence, Authoritarianism and the Future of Political Systems

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University

Artificial Intelligence, Authoritarianism and the Future of Political Systems

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has Üniversitesi

> *Enlightenment is man's emergence from his self-imposed immaturity. Immaturity is the inability to use one's understanding without guidance from another.*"
>
> Immanuel Kant
> (Answering the Question: What is Enlightenment? 1784)

In February 2017 Scientific American featured a special issue, which revolved around the question: 'will democracy survive big data and artificial intelligence.'[1] According to the issue, humanity is undergoing a profound technological transformation, and the advent of large-scale social and behavioral automation would change how human societies will be organized and managed. Later in August 2017, Vyacheslav Polonski, a researcher at Oxford University asserted in a World Economic Forum article, that artificial intelligence 'silently took over democracy,' citing the impact of A.I.-powered digital advertisements, social media platform power and mass communication spoilers (bots and trolls) on political processes.[2] Societies online and offline, mostly against their will and awareness, are increasingly experiencing the effects of large-scale automation. Political systems, elections, decision-making, and citizenship too, are increasingly being driven by aspects or by-products of automation and algorithmic systems at different systemic levels. These systems range from targeted political advertisements to facial recognition, from automated interactions that intensify polarization to Internet-based mass-participation opinion polls that can easily be skewed by factors of automation.

Digital communication is at the epicenter of this critical and historical interaction between politics and automated systems. Political communication professor Andrew Chadwick was the first to coin the term 'hybrid media system,' which referred to the multitude of roles performed by social media platforms.[3] According to the hybrid media system theory, platforms such as Twitter, Facebook or Instagram are not just communication tools, but also perform news-media roles during emergencies, as well as political assembly and protest roles during contested events like elections or key events. The algorithmic structure of these platforms, therefore, increasingly impact and shape political messaging, information-seeking, and citizen engagement. In the words of Jose van Dijck, "Social media are inevitably automated systems that engineer and manipulate connections."[4] In that regard, Facebook is not a passive platform that simply

Robert Bosch Stiftung The research has been made possible by funding obtained from Robert Bosch Stiftung.

1 Dirk Helbing, et al. "Will democracy survive big data and artificial intelligence." Scientific American 25 (2017).

2 Vyacheslav Polonski, "How Artificial Intelligence Silently Took over Democracy," World Economic Forum, August 9, 2017, https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/.

3 Andrew Chadwick, The Hybrid Media System: Politics and Power (New York, NY: Oxford University Press, 2017).

4 Jose van Dijck, The Culture of Connectivity: A Critical History of Social Media (New York, NY: Oxford University Press, 2013), 12.

connects friends and relatives. It is a living and breathing political actor that actively harvests personal information from its users and sells it to third parties.[5] Such data can be used for targeted advertisement, micro-profiling, and political behavioral analysis that the world most recently observed during the Cambridge Analytical scandal.[6] Twitter, Amazon, Netflix, and other algorithmic platforms too are structured upon the harvesting and exploitation of similarly vast quantities of granular human data, that are in turn used to profile and catalog behavioral patterns of societies.[7]

Just like media platforms are hybrid, so are data types. 'Hybrid data' refers to the multi-purpose nature of human footprint online; namely, how people's 'like's, retweets and check-in decisions can be harvested to be cross-fed into each other to generate a multi-dimensional snapshot of micro and macro-level determinants of social behavior.[8] A user's personal fitness tracker, check-in location information and Google search histories combined, can yield a very granular set of information from that person's health, purchasing behavior and political preferences. This personal data hybridity, when cross-matched with people with similar search histories, tastes, and online order patterns creates the information infrastructure of mass surveillance and become the largest ever pool of social monitoring and tracking.[9] Such surveillance is no longer as labor-intensive as it used to be; mass profiling infrastructures too, are largely algorithm-driven. Algorithms, programmers and technology companies that are responsible for developing and maintaining these structures of automation, thus form a new source of power that is partially independent of states as well as international political institutions.[10] As Internet connectivity and social platform membership explode globally, the percentage of the world's population living under these new forms of automated power relations increase exponentially, rendering the impact of automated politics historic.

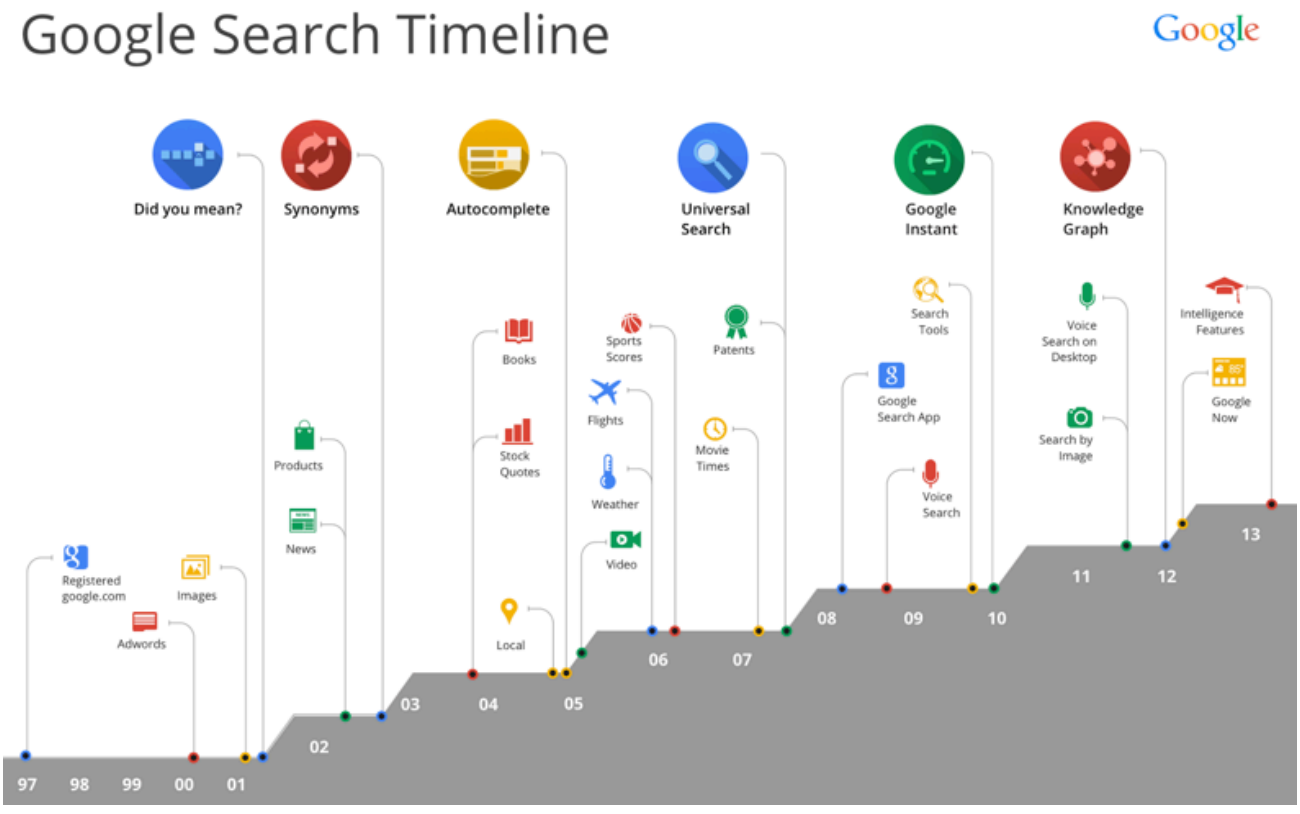


Image 1 - Timeline of the evolution of Google Search algorithms (Source: Google)

5 Trebor Scholz, Digital Labor: The Internet as Playground and Factory (New York, NY: Routledge, 2012), 2.

6 Emma Graham-Harrison, Carole Cadwalladr, and Hilary Osborne, "Cambridge Analytica Boasts of Dirty Tricks to Swing Elections," The Guardian, March 19, 2018, sec. News, http://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections.

7 Nick Srnicek, Platform Capitalism (Wiley, 2016), 16.

8 Badraddin Alturki, Stephan Reiff-Marganiec, and Charith Perera, "A Hybrid Approach for Data Analytics for Internet of Things," arXiv:1708.06441 [Cs], August 21, 2017, http://arxiv.org/abs/1708.06441.

9 Zeynep Tufekci, "Engineering the Public: Big Data, Surveillance and Computational Politics," First Monday 19, no. 7 (July 2, 2014), https://doi.org/10.5210/fm.v19i7.4901.

10 Taina Bucher, If...Then: Algorithmic Power and Politics (Oxford University Press, 2018).

Modern algorithmic structures inherit the cybernetic theory, introduced in the late-1940s by mathematician Norbert Wiener. Wiener argued that the behavior of all large systems (bureaucratic, organizational and mechanical) could be adjusted and maintained through regular feedbacks.[11] By 'learning' through constant feedbacks, systems adapt and learn and eventually perform better. It is through the basic premises of the cybernetic theory that some of the most popular forms of automated structures (such as machine learning, blockchain, decentralized data mapping) operate. Since algorithms are trained through live human data, they rapidly act and behave in a way that emulates human behavior. A search algorithm, for example, is designed to provide the most relevant search results based on the query string. When a violinist is searching for a new bow, it is algorithmically more meaningful to curate ads, news feed items and connection suggestions based on violin, or classical music to that user, instead of - say - golf.[12] It saves time and renders online interactions more meaningful and relevant. However, it does more than that. The algorithm improves by studying the search histories of millions of people, their second and third next search strings and page view duration statistics to make a search engine faster and better able to address follow-up queries by users.

How do we, then, contextualize the political implications of these 'automated structures of relevance'? After all, none of these algorithms were initially designed to exert such vast political, economic or social impact. The very code structures that enable a violinist to find more music-related content online are also polarizing societies, intensifying political echo chambers and distorting meaningful political debate in digital space.[13] Whose fault is it? Are societies becoming less tolerant due to technological change? Are governments exploiting these technologies of scale to re-assert their authoritarian dominance? Or is this an evolutionary curve that will settle in time, or are algorithmic structures permanently in place to influence state-society relations for the long haul?

The current debate boils down to the question of whether or not technology companies strategically deploy biased algorithms to reinforce their position of power in 'A.I. arms race'; namely automated information retrieval, engagement maximization, and content curation.[14] The business model environment within which big tech companies operate is dependent on engagement metrics: likes, retweets, comments. To maximize profit, tech companies have to maximize engagement, which inherently suggests content that elicits as much response as possible from as many people as possible.[15] This automatically triggers algorithmic principles that generate extreme or emotional behavior through similarly extreme of emotional content. From an algorithm's point of view, whether users respond to a positive or negative content is irrelevant, since what ultimately matters is the maximization of quantified user statistics. As long as the user response is optimized, an algorithm is doing its job regardless of whether through bloody war videos, or kitten photos. As quantified engagement is cashed in as advertisement revenue, the resultant media environment favors extreme content and media, leading to a toxic interaction culture across all social media platforms. In particular, tense political and social episodes, such as protests, elections or diplomatic escalation, this social media environment exerts a disproportionate effect on misinformation through fake news and automated accounts known as bots.[16]

Although popular, social media is not the only avenue for discussion in exploring A.I. and politics. Another popular debate on A.I.-politics nexus is the issue of automating decisions - namely, day-to-day machinations of the bureaucracy outsourced to machines. Most champions of the 'A.I. bureaucracy' argument favor the outsourcing of low-risk decision-making, rather than policy formulation, to optimize bureaucratic size and depth.[17] In the name of making governments and bureaucratic *apparati* more efficient, algorithmic systems are said to take over the

[11] Norbert Wiener, Cybernetics Or Control and Communication in the Animal and the Machine (Cambridge, MA: MIT Press, 1961).

[12] Ryan Singel, "Analysis: Google's Ad Targeting Turns Algorithms on You," Wired, May 11, 2009, https://www.wired.com/2009/03/google-ad-annou/.

[13] Seth Flaxman, Sharad Goel, and Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," Public Opinion Quarterly 80, no. S1 (January 1, 2016): 298–320, https://doi.org/10.1093/poq/nfw006.

[14] Rob Kitchin, "Thinking Critically about and Researching Algorithms," Information, Communication & Society 20, no. 1 (January 2, 2017): 14–29, https://doi.org/10.1080/1369118X.2016.1154087.

[15] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (March 1, 2015): 75–89, https://doi.org/10.1057/jit.2015.5.

[16] David M. J. Lazer et al., "The Science of Fake News," Science 359, no. 6380 (March 9, 2018): 1094–96, https://doi.org/10.1126/science.aao2998.

[17] Frank Levy, "Computers and Populism: Artificial Intelligence, Jobs, and Politics in the near Term," Oxford Review of Economic Policy 34, no. 3 (July 2, 2018): 393–417, https://doi.org/10.1093/oxrep/gry004.

functions of the rank-and-file bureaucracy gradually.[18] Modern bureaucracy, at least as defined by Max Weber, is the ideal candidate for an algorithm-based, automated habitus: "*Bureaucracy is an organisational structure that is characterised by many rules, standardised processes, procedures and requirements, number of desks, meticulous division of labour and responsibility, clear hierarchies and professional, almost impersonal interactions between employees*".[19] A.I. can indeed solve some of the most chronic dysfunctions of the state, such as corruption, inefficiency, and ego politics. It can offer an efficient centralized response to a multitude of citizen requests, resolve resource allocation problems, remain immune to human fallacies such as fatigue or burnout, and can perform all non-decision tasks such as speech transcription, translation, document drafting and archiving far better and faster than any human-based bureaucracy. However, the erosion of the bureaucratic appartus, transfer of tasks to algorithmic structures bereft of decision-making will nullify one of the most potent sources of authority for the modern state: a rational bureaucratic workforce. With such a significant power source automated and human influence minimized, some states might use A.I. as a guardian of reinforced totalitarianism. Furthermore, pre-existing problems with A.I. transparency and code accountability will be even more relevant in this case, as biases in programming will have a disproportionate effect on administration as mistakes are amplified through the sheer volume and size capacities of algorithmic decision-making.

Automation and Authoritarian Regimes

Although the question of whether A.I. will damage democracy and reinforce authoritarianism has grown popular in the last few years, the empirical answers provided in the literature do not indeed yield either a negative or positive overall impact.[20] The impact of A.I. on human progress is instead expected to be politically neutral, without inherent ideological biases against or in favor of any particular regime type. In that sense, it is better to think of A.I. as a historical enabler of size, scale, distance and volume, rendering its impact closer to that of the engine or electricity (that haven't favored a specific political ideology), rather than communication advances such as the printing press, television or radio (that exerted liberalizing shifts). However, so far, the advent of A.I. has brought about two foremost alarmist futurist traditions that hypothesize different trajectories on how automation will alter existing regime types: algorithmic feudalism,[21] and totalitarianism[22] variants.

There are two main interpretations of how A.I. might create production relations that could generate feudalistic conditions. The first interpretation follows Habermasian notions of the enclosure and distributionary monopoly, that directly explain how non-transparent and non-accountable technology and information systems may lead to discouraged political participation and representation.[23] A.I. as a 'closed technology,' (meaning how algorithms influence political and social life, but cannot be altered or modified by the very users they impact), incurs great biases over human-machine interaction and reinforce centralized structures of control, rather than participation. In addition to the Habermasian interpretation of feudalism, the Marx-Engels interpretation of feudalism focuses on the communal aspects of algorithmic power, where the power rests with those that control modes of production.[24] In this case, communities that are in control of algorithmic structures would be programmers, coders, and companies that control these algorithmic communities.

Although the prevalence of Habermasian and Marx-Engels

[18] Greg Allen and Taniel Chan, "Artificial Intelligence and National Security" (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kenendy School, July 2017), https://www.belfercenter.org/publication/artificial-intelligence-and-national-security.

[19] Max Weber, The Vocation Lectures, ed. David Owen and Tracy B. Strong, trans. Rodney Livingstone (Indianapolis: Hackett Publishing Company, Inc., 2004), 179.

[20] Spyros Makridakis, "The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms," Futures 90 (June 1, 2017): 46–60, https://doi.org/10.1016/j.futures.2017.03.006; Philip N. Howard, Pax Technica: How the Internet of Things May Set Us Free Or Lock Us Up (Yale University Press, 2015); Cass R. Sunstein, #Republic: Divided Democracy in the Age of Social Media (Princeton, NJ: Princeton University Press, 2018).

[21] Thaddeus Howze, "Feudalism and the 'Algorithmic Economy,'" Medium, April 17, 2017, https://medium.com/@ebonstorm/feudalism-and-the-algorithmic-economy-62d6c5d90646; Peter Drahos and John Braithwaite, Information Feudalism: Who Owns the Knowledge Economy? (New Press, 2003).

[22] Emiliano Treré, "The Dark Side of Digital Politics: Understanding the Algorithmic Manufacturing of Consent and the Hindering of Online Dissidence," IDS Bulletin 47, no. 1 (January 11, 2016), https://doi.org/10.19088/1968-2016.111; Merlyna Lim, "Freedom to Hate: Social Media, Algorithmic Enclaves, and the Rise of Tribal Nationalism in Indonesia," Critical Asian Studies 49, no. 3 (July 3, 2017): 411–27, https://doi.org/10.1080/14672715.2017.1341188.

[23] Jürgen Habermas, The Philosophical Discourse of Modernity: Twelve Lectures (Cambridge, UK: John Wiley & Sons, 2018).

[24] Karl Marx and Friedrich Engels, The Communist Manifesto (Minneapolis, MN: First Avenue Editions, 2018).

schools of algorithmic feudalism in the mainstream debate, a more accurate definition of feudalism goes beyond mere centralized control structures. Feudalism, in its direct practice, is structured upon a military logic: establishment of a warrior caste that operates at the intersection of three nodes of power: lords, vassals, and fiefs. This system emerged as a response to a growing need for protection and order in an inherently anarchic political system, where long-term security could only be established by linking security provision with material service. Those that are able to supply the material factors of protection (ability to produce weapons and armor, train and feed armies), or religious authority (excommunication, shaming, blessing) ruled over an extensive network of vassals and fiefs that in turn provided service in the form of food (serfdom), or monetary compensation (taxation).[25] Therefore, a proper understanding of 'algorithmic feudalism' in today's context would first entail an anarchic system, in which security provision would be in a symbiotic relationship with modes of financial and human capital production. This hypothesizes that the digital space in wholly anarchic (i.e. absence of an overarching government and law) and protection in cyberspace is wholly dependent on how well actors can merge rich financial structures (ad revenue and rent generation) with the ability to train large numbers of highly skilled digital labour (specialists in cybersecurity, data science, or engineering).

In a public discussion with Arkady Vorozh, the CEO of Yandex, Russian President Vladimir Putin asserted that whichever country would master the A.I. in the short-term, 'will be the ruler of the world.' Elon Musk later shared Putin's words on Twitter, who added 'Competition for AI superiority at the national level most likely cause of WW3'.[26] Both Putin and Musk statements constitute high-level affirmations of algorithmic feudalism, given how they both locate the A.I.'s immediate role within political anarchy and global leadership to circumvent its effects. Both, furthermore, view A.I. mastery as an inherently zero-sum game, in which one power has to dominate and others, become dominated. Although Putin's statement referred to both military and non-military applications of A.I., the rest of his statement specifically referred to threats originating from the automation of security tools (drones, cybersecurity, 3D printing), instead of finance, healthcare or other non-military applications of A.I. Both Putin and Musk deviate significantly from Emmanuel Macron, for example, who gave an exclusive interview to Wired on France's A.I. strategy, where he focused exclusively on healthcare, finance and political participation aspects of algorithmic structures, rather than their military applications.[27] 'A.I. feudalism' then, has to imply a political regime, primarily geared towards eliminating systemic anarchy and revolves directly around security provision, both domestically and internationally, in exchange for financial and human capital provision. In domestic politics, it implies riot control and surveillance industries, whereas internationally it concerns cybersecurity, unmanned systems and a wide array of communication-related fronts.

The most immediate impact of A.I. that might reinforce the feudalistic tendencies of the digital space is to create a production system mimicking corporatism - namely, the reconfiguration of power relations through sectoral alliances between coder syndicates and guilds. This would entail the control of algorithm-building and maintaining structures that both state and private actors rely on, and the foundation of the future economic system. The corporatization of A.I. could reinforce power-centralization through the combination of corporations that monopolize modes of code and coder production that will disproportionately influence politics, military and science affairs. This will effectively generate a feudal network that minimizes political participation and representation, leading to the eradication of democracy. The Habermasian 'algorithmic enclosures' that are obscure and inaccessible will establish robust control mechanisms on the society and in turn, empower coder oligarchies and corporations in charge of them.

The second alarmist trend in the popular mainstream is the idea that the A.I. will create a 'fascist system'[28] - where the

[25] François Louis Ganshof, Feudalism (Toronto: University of Toronto Press, 1996).

[26] Paul Ratner, "Putin Weighs in on Artificial Intelligence and Elon Musk Is Alarmed," Big Think, September 24, 2017, https://bigthink.com/paul-ratner/putin-weighs-in-on-artificial-intelligence-and-elon-musk-is-alarmed.

[27] Nicholas Thompson, "Emmanuel Macron Talks to WIRED About France's AI Strategy," Wired, March 31, 2018, https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/.

[28] Timothy Snyder, "Fascism Is Back. Blame the Internet.," Washington Post, May 21, 2018, https://www.washingtonpost.com/news/posteverything/wp/2018/05/21/fascism-is-back-blame-the-internet/; Anthony J. Bell, "Levels and Loops: The Future of Artificial Intelligence and Neuroscience," Philosophical Transactions of the Royal Society of London B: Biological Sciences 354, no. 1392 (December 29, 1999): 2013–20, https://doi.org/10.1098/rstb.1999.0540; Jan Nagler, Jeroen van den Hoven, and Dirk Helbing, "An Extension of Asimov's Robotics Laws," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 26, 2018), https://papers.ssrn.com/abstract=3110582.

over-centralized A.I.-based decision-making will create a hierarchy of repression in which control-oriented, top-down practices will restrict expression, engagement, oversight and political information-seeking behavior. These fears have been intensified with the rise of the far-right groups in the US and Europe in the last years, bolstered by Internet trolls, fake news, and bots. According to the conceptualization of Foucault[29] and Canguilhem[30], the way technology and science are deployed by fascist regimes snowball into a social force, bursting their initial utilitarian origins and take on a life of their own. Technologism then determines the bounds of rights and freedoms in a society, becoming the real political ideology in fascist regimes. In 'techno-fascism,' all aspects of social life are controlled with the purpose of maximizing scientific progress and technological advances that are in turn, used to exert newer forms of sectoral control over social life. Views that don't conform or fully converge to the hegemonic ideology are taken out of the equation through imprisonment and death. Totalitarianism is different from authoritarianism in this context since the latter denotes the centralization of political power without the need to control thoughts and actions of all citizens through a revolutionary mechanism to change the human nature or the world at whole. An 'A.I. fascism' or totalitarianism, therefore, has to entail a bid to change human relations and social interactions; merely political control and centralization are not enough on their own.

One argument in the literature that hypothesizes how A.I. might create the conditions of totalitarianism builds upon what Herbert Marcuse dubbed 'the one-dimensional man'[31]. Marcuse's definition referred to a consumer society where 'humans become an extension of the commodities that they buy,' which inflates their self-worth through their ownership of technologies. This is why, according to Marcuse, capitalist techno-centric societies are more likely to succumb to micro-totalitarianisms, as their technology purchases are driven by a sense of ego-centrism, which in turn shifts the societal order. The resultant bid for techno-centric self-fulfillment makes societies easier to monitor and control through newer forms of digital surveillance, network monitoring, and big data profiling, creating a willing form of direct repression. By making more aspects of their lives available to data harvesting, societies also endanger states or corporations to control and change human relations and interactions, both of which, are pre-requisites of a totalitarian transition. In addition, A.I. does bring in size and scale multipliers to already-problematic state surveillance tools. Automated and highly-refined forms of censorship, real-time tracking, profiling and communication surveillance, A.I-powered tools of speech and pattern recognition, information spoilers such as state-sponsored fake news, bots and trolls indeed empower authoritarian and totalitarian regimes. In building these oppression structures, A.I. lies at the intersection of the surveillance-industrial complex[32], where the financial relationship between the governments and technology companies create a vicious circle that reinforces another form of totalitarianism. A.I. and machine learning architectures are built on the hypothesis that human actions and behavior can be predicted through politically, economically and socially identifiable and recognizable characteristics, that can, in turn, be quantified. Such quantification of social interactions lies at the heart of techno-fascism as citizens become increasingly subjected to profiling through algorithms that are virtually inaccessible and technically difficult to oversee.

However, should we blame A.I. or algorithms? Are algorithms inherently 'totalitarian,' or are there systemic influences that render these neutral code structures more conducive to it? The prevalent trend in the mainstream industry debate is to offer A.I. or algorithms as a sacrificial lamb of sorts, especially by the governments or tech companies, to cover coder biases and mistaken decisions. When algorithms make a mistake, they are usually expressed as independent entities that make mistakes on their own, as if human bias or prerogatives are not fed into the code structure. Rather, the business structure that has produced the code export the authority of their handling of the tool to the tool itself, diverting attention away from the power relations that generate, maintain and alter the algorithm. This neglect and diversion are the modus operandi of veiled authoritarianism, given the fact that neither the code nor the business model behind it can be accounted for, verified or altered by the society that they influence. For example, social media algorithms that were put into place in the last few years to combat terrorism and jihadi content online, have been only slightly readjusted

[29] Michel Foucault, Discipline & Punish: The Birth of the Prison, trans. Alan Sheridan (New York: Vintage Books, 1995).

[30] Ian Hacking, "Canguilhem amid the Cyborgs," Economy and Society 27, no. 2–3 (May 1, 1998): 202–16, https://doi.org/10.1080/03085149800000014.

[31] Herbert Marcuse, One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society (New York, NY: Routledge, 2013).

[32] Kirstie Ball and Laureen Snider, The Surveillance-Industrial Complex: A Political Economy of Surveillance (New York: Routledge, 2013).

to be applied to monitor purchasing behavior, urban commute patterns and student attendance at school. When an algorithm is deployed by a school to follow a student's attendance, the algorithm does so in a way that mimics its previous task: harvest and organize patterns of human behavior to maximize an outcome (in this case, attendance). The problem is, most such algorithms come from a military or law enforcement background. These algorithms, when applied to civilian contexts become socially invasive in a way that brings a large number of legal and human rights-related problems. China is one example, where the military is brought into the China Brain Project where deep learning is applied to Baidu (main Chinese search engine) search results, to collect information about user behavior.[33] This project is closely linked to the 'citizen score' - a system where Chinese citizens are graded according to their online and offline behavior and interactions, influencing their loan, job and visa status.[34] The program harvests and orders digital human behavior in a way similar to its past versions that were trained on criminal and national security threat data. Snowden revelations revealed that the United Kingdom used a similar program called the 'Karma Police,' where mass user IP data was cross-referenced with SMS metadata, as well as social media history to lay the foundations of one of the most comprehensive and problematic surveillance programs in European law enforcement.[35]

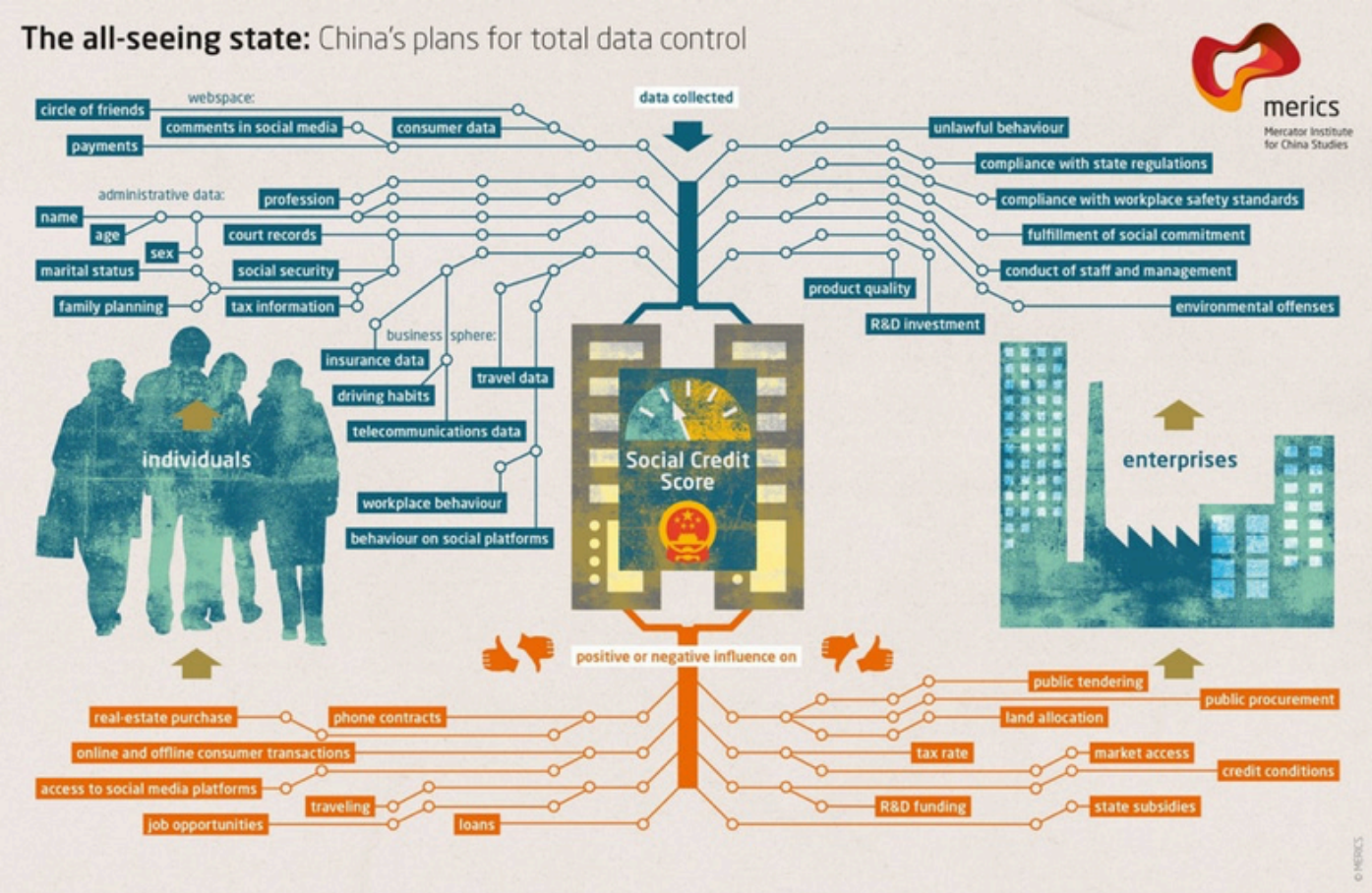


Image 2 - An overview of China's data centralization strategy through Social Credit Score (Source: Mercator Institute for China Studies)

[33] David Cyranoski, "Beijing Launches Pioneering Brain-Science Centre," News, Nature, April 5, 2018, https://doi.org/10.1038/d41586-018-04122-3.

[34] Adam Greenfield, "China's Dystopian Tech Could Be Contagious," The Atlantic, February 14, 2018, https://www.theatlantic.com/technology/archive/2018/02/chinas-dangerous-dream-of-urban-control/553097/.

[35] Nigel Morris, "GCHQ Was Harvesting Metadata on Everybody, Says Edward Snowden," The Independent, September 25, 2015, http://www.independent.co.uk/news/uk/home-news/edward-snowden-gchq-collected-information-from-every-visible-user-on-the-internet-10517356.html.

Another troubling form of A.I. authoritarianism is the advent of persuasive algorithms. A persuasive algorithm directs user behavior without explicit directions or orders, but rather 'nudges' the user into the desired choice or outcome through indirect and covert conditioning. Cambridge Analytica has already shown us how large-scale political engineering can be undertaken by under-the-radar data harvesting and profiling techniques.[36] The way persuasive algorithms influence human behavior directly relates to the concept of 'nudging' as defined by the Nobel Prize winner Richard Thaler and Cass Sunstein's 'nudge theory'[37]. Nudging is a behavioral concept imported from sociology, where indirect suggestions and hints impact the decisions of institutions and individuals without a direct threat or persuasion. A robust nudge is not a threat, or coercion, as it does not appear binding and most of the time guides the target into the desired set of behavior in a way that such decision looks like the target's own choice, among the alternatives. Due to their ability to harvest large amounts of user decision and choice, algorithmic architectures are ideally-designed for automated nudges because they can automatically learn from user data to make successive choices conducive for a nudge. With a large live dataset of user behavior, A.I.-based systems will have an extensive repertoire of possible nudges that can steer individuals into the desired choices and behavior without them realizing it, and worse, appear as if they have agency in the decision required. These problems are particularly more probable in countries where a single search engine or a social media outlet (or a company owning them) establishes the sole monopoly in harvesting and processing digital user data. The state's relationship to the A.I. monopoly is mostly irrelevant, as algorithmic authoritarianism can apply equally in countries where a symbiotic relationship exists and where it does not. This nudging ability of persuasive algorithms can create the foundations of authoritarianism if code oversight is neglected both through legislative and judicial organs. To be able to understand algorithmic subtleties, however, both of these organs have to develop a technical expertise base to assist in such oversight tasks.

Algorithmic Decision-Making and Political Legitimacy

In May 2017, the American writer Joshua Davis has authored one of the most shared articles on the Wired: 'Let's Elect an A.I. President'[38]. Davis' arguments revolved around rapid decisions, proper and accountable response to citizen needs and the ultimate elimination of corruption from the political process. According to the piece, the A.I. President will happen in time, after years of gradual outsourcing of more complex and critical tasks to the machines, eventually culminating with the full take-over of all political decisions by algorithmic structures. However, this narrative omits perhaps the most important source of authority in politics: legitimacy. Once algorithmic decision-making systems are put in place and begin making political decisions, where does the authority to make such binding decisions come from? Will the citizens vote for an algorithm, or a series of algorithms, or a human decision-making team presiding over algorithmic structures that make most of the critical decisions? When an algorithm makes an automated decision to go to war or increase the military budget for example after it weighs possible scenarios and decision trees, how do we assess the legitimacy of this decision? Once human beings are isolated from the bulk of the political decision processes and sleep-walk into a state of alienation (*Entfremdung*) described by Karl Marx[39], which mechanism will animate or take the place of political legitimacy? To understand how A.I. will influence the most fundamental source of authority in politics, we need to look at the actual decision process. Traditional decision-making theory divides the political decision process into five main components. These are agenda setting (how leaders decide which issues are important and urgent), policy formulation (creating most efficient, as well as alternative scenarios to address the agenda), decision-making (weighing alternative approaches and scenarios and designating one option as primary), implementation (execution of policy) and oversight (how executed policy meets the requirements of the problem at hand).[40]

---

36 Gillian Tett, "Trump, Cambridge Analytica and How Big Data Is Reshaping Politics," Financial Times, September 29, 2017, https://www.ft.com/content/e66232e4-a30e-11e7-9e4f-7f5e6a7c98a2.

37 Richard H. Thaler and Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness, Revised & Expanded edition (New York: Penguin Books, 2009).

38 Joshua Davis, "Is There an AI President in Our Future? That Might Be an Upgrade," Wired, May 18, 2017, https://www.wired.com/2017/05/hear-lets-elect-ai-president/.

39 Karl Marx, Economic and Philosophic Manuscripts of 1844 (Mineola, NY: Courier Corporation, 2012).

40 Roland W. Scholz, Decision Making under Uncertainty: Cognitive Decision Research, Social Interaction, Development and Epistemology (Amsterdam: Elsevier, 1983).

As far as agenda-setting (designating important versus redundant issues) is concerned, the most direct application of the A.I. would be to sense the emotions and sentiments of the population through big data analytics. This task would resemble some of the current automated text-mining and entity-extraction tasks that we often see in marketing, advertising, and political campaigns, where word frequency and sentiment sorting are deployed to generated a general snapshot of a large population. It is easy to see A.I. refine its mining algorithms in the near future further to allow policy-makers high-fidelity and granular observations on the citizens' main problems, issue demands and policy opinions. China has been experimenting on a different form of this, by closely monitoring the social media space and relying on A.I. decisions to decide which type of content critical of the government constituted criminal behavior or 'acceptable criticism.' As the famous King (et al.) study shows, the Chinese government has been using algorithmic structures to separate between critical content that in unimportant and those that have the potential to generate physical mobilization[41]. In the UK 2015 general elections too, sentiment analysis studies assumed an essential role for all parties and candidates, most of which set up contracts with seven tech companies and social media platforms to monitor public domain sentiments[42]. Today, political parties, governments, and leaders across the world employ some versions of text mining algorithms to keep up-to-date with citizen and voter sentiments and issues that they want to be raised. In the near-future, sentiment data available on the Internet, communication and social media platforms, will multiply, allowing A.I.-based recognition systems to learn and designate critical issues much faster and more reliably, enabling real-time and fluid agenda-setting capability for politicians.[43]

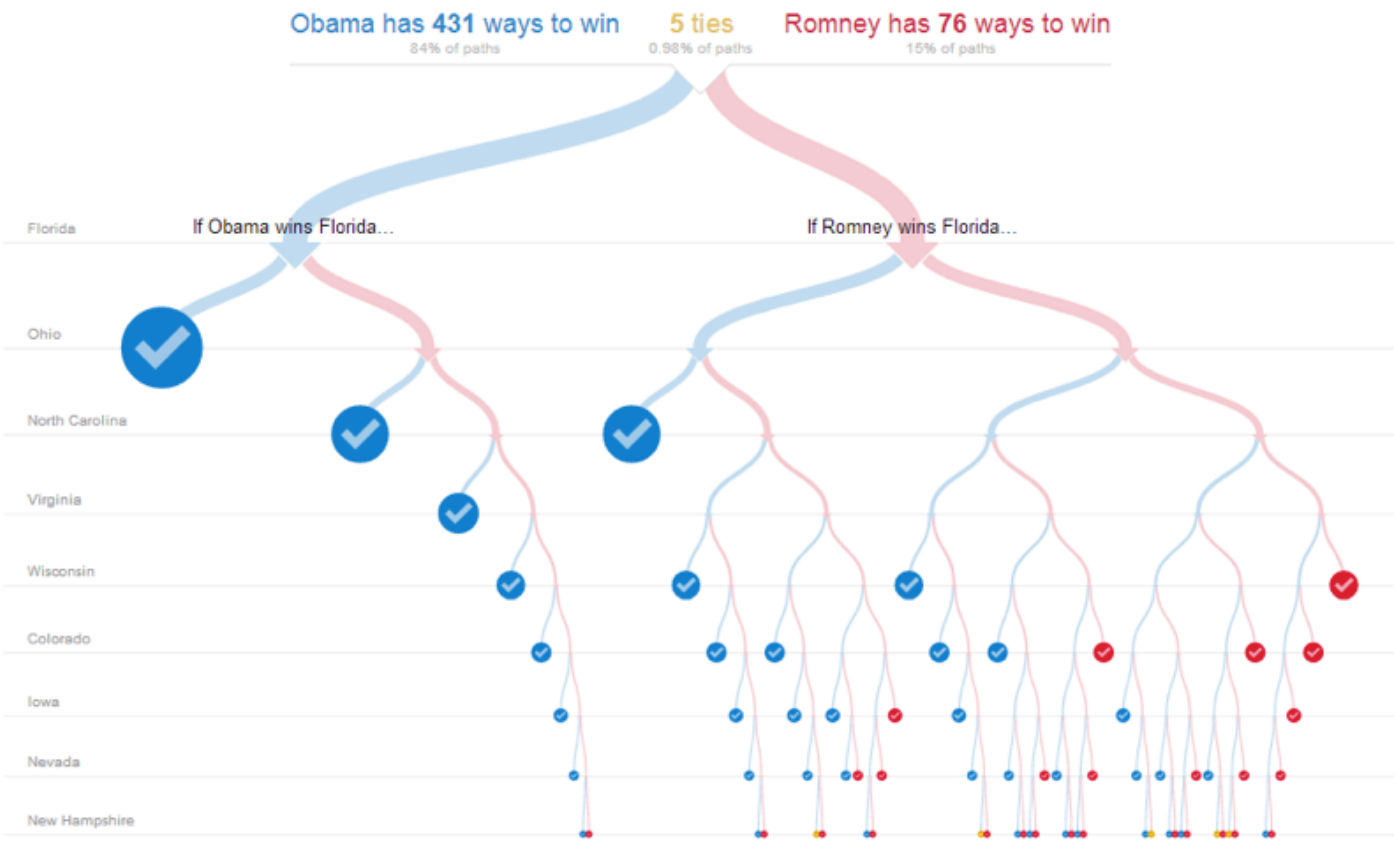


Image 3 – A simple decision-tree showing multiple ways in which the 2012 US Presidential Elections could result, based on past electoral data. (Source: '512 Paths to the White House' New York Times. 2 November 2012. http://archive.nytimes.com/www.nytimes.com/interactive/2012/11/02/us/politics/paths-to-the-white-house.html)

41 Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," American Political Science Review 107, no. 2 (May 2013): 326–43, https://doi.org/10.1017/S0003055413000014.

42 David Bond, "Facebook Key to Winning UK General Election, Political Parties Say," Financial Times, May 14, 2017, https://www.ft.com/content/c78c3bd0-36f8-11e7-99bd-13beb0903fa3.

43 David W. Nickerson and Todd Rogers, "Political Campaigns and Big Data," Faculty Research Working Paper Series (Cambridge, MA: Harvard Kennedy School, February 2014).

In the second step in decision-making - policy formulation - A.I. can help in optimizing scenarios by running multiple tandem processes of outcome and resource distributions, as well as forecasting possible types of public reaction against these outcomes. The most significant help of the A.I. in generating realistic policy scenarios will be cost-efficiency, as its rapid processing capabilities will be able to provide better estimates of material and labor costs of alternative decisions. Chicago Department of Public Health, for example, has used machine-learning tools to optimize its approaches to the lead poisoning incident in the state[44]. Through mapping houses and workplaces with the highest exposure to lead, the administration was able to effectively allocate its resources to maximize effectiveness in combating the epidemic. Algorithms, however, cannot model or forecast policy variables that cannot be quantified. Such unquantifiable variable types will be behavioral, cognitive and psychological data, as well as ego and rent-driven aspects of politics, such as rentierism, corruption, and cronyism. While the most liberal democracies will be somewhat immune to these effects, most of the countries in the world (as well as developed countries) will eventually find it more preferable to sideline algorithmic policy formulation approaches, due to the importance of personal politics in decisions. To that end, the prospect of an 'algorithmic policy formulation' looks more realistic for the highest quality democracies due to the abundance of unquantifiable political variables in more authoritarian systems. Another vital task the A.I. can handle in the policy-formulation phase will be to help create a database of standard operating procedures and employ the most relevant one in times of crises. Especially in scenarios that involve high-risk and danger, such as natural disasters, riots or terrorism, algorithmic structures can work well in mobilizing resources, directing large groups of people and disseminating critical information regarding the emergency at hand.

The third, actual decision-making phase is the most crucial step of the decision process from the perspective of how A.I. will impair or bolster democracy. This is because the actual political decision requires a form of authority and legitimacy to have a binding power and to be put into law. In democracies, such legitimacy comes from representation and voting, and the political capital required to make decisions are acquired through public support. In authoritarian settings, on the other hand, legitimacy comes from a consensus among the ranks of a close-circuit oligarchy, while political capital (albeit always less than democracies) is acquired through repression and order. Algorithms blur the separation between the decision and the process by which that option prevailed over others. Once decision-making is automated, the policy crafting process, as well as the decision itself becomes detached from political legitimacy and sovereignty considerably, and thereby weaken political institutions in both democracies and autocracies. If the actual decision-making process is overwhelmingly automated, without setting legal and legislative oversight mechanisms in place, both respective governments and their societies will be alienated from the decisions produced by the algorithms that are put in place. This will cause long-term structural problems on accountability, checks, and balances, as well as democratic representation, all of which will generate public pressures in favor of scaling back from automation. Currently, it is unlikely that neither democracies, not autocracies will allow A.I. encroachment into decision-making, but as the size and scale of automated decisions proliferate, countries will have to resort to algorithmic policy-making to keep up with the speed trends. Therefore, neither keeping A.I. out, not overwhelmingly depending on it in actual decision-making seems plausible. The most likely outcome will be culture and country-dependent, as different political systems will find the balance between algorithmic-versus-human driven decisions over time.

In the final, execution phase, A.I.-based approaches have significant potential in modeling implementation strategies, designing resource allocation and supply chain structures. Once a decision is made, algorithms can communicate with the relevant agencies and ground assets, check stock in warehouses, transfer finances and establish a working supply chain much faster and across geographically much more distant areas compared to humans. Most recently, the US Army has adopted an 'A.I. Logistics Strategy,' which aims to establish a real-time tracking of the unit, brigade, and company-level needs, establishing quick supply chains to deliver arms, ammunition and other material necessities to the bases and frontline faster[45]. Besides, A.I. can make a significant contribution to the policy communication phase,

[44] Mohana Ravindranath, "In Chicago, Food Inspectors Are Guided by Big Data," Washington Post, September 28, 2014, https://www.washingtonpost.com/business/on-it/in-chicago-food-inspectors-are-guided-by-big-data/2014/09/27/96be8c68-44e0-11e4-b47c-f5889e061e5f_story.html.

[45] Sydney J. Freedberg, "AI Logistics Let Combat Units Move Faster: Uptake's DIUX Contract," Breaking Defense (blog), June 27, 2018, https://breakingdefense.com/2018/06/ai-logistics-can-speed-up-army-tanks-uptakes-diux-contract/.

where it can present and communicate the implementation process to different audiences based on their harvested words and phrases, and in a tone and lexicon that resonate with them. Tailored political advertisements based on gender, age, race and socio-economic background are already being deployed in business and management with good impact[46]. Automated policy communication is not yet perfect, however, as bot-driven public relations attempts (chatbots) are still very much in their infancy phase and usually come off as either tone-deaf or unable to understand questions and commands beyond their immediate code structure. Finally, in the policy evaluation phase, AI can monitor and measure the effects of new policy through pre-set success markers and provide regular feedback to decision-makers on the short-to-medium-term outcome of the policy in question. Further ahead, the policy implementation phase will be significantly influenced by the advent of neural networks that test policy effectiveness and public reaction in real-time, providing decision-makers with near-instant feedbacks to improve and alter policy.

The above breakdown of the political decision-making process is essential because it is this structure that renders the system ultimately vulnerable to A.I. over-reliance. Such over-reliance, in time, can impair two primary sources of statehood - legitimacy, and sovereignty - by over-centralizing and over-complicating the decision-making process. Especially when proper oversight and accountability mechanisms, as well as technically-proficient and binding institutions, are not put in place, the resultant process will inevitably lead to some form of totalitarian regime. The inherently complex and technically confusing nature of the A.I. code structure may render it immune to proper accountability if these institutions and oversight mechanisms lag behind the rapid progress in computer science. Technology companies and coder castes can always draw a wedge between the leaders and the society through code backdoors or rendering the code deliberately over-complicated to deter oversight[47]. Once political and legal institutions relinquish the oversight authority to the technically proficient technology companies or coder syndicates, algorithmic oversight will be monopolized by these companies or syndicates, which will lead to a fundamental shift in political authority and power[48].

Automated decision-making structures will also test the traditional link between the voters and the government. In a hypothetical political system where the substantial majority of the policy decisions are automated through algorithmic structures, what exactly are the voters voting for? Are the voters voting for a government or an algorithm? If the former, are they voting for a government that will change the algorithms, exert more oversight, or use them preferentially - on specific issues and not others? Will the voter choice be limited to the 'how's of algorithmic governance or the degrees to which competing parties will use algorithmic systems? Let's think of two further scenarios: If we assume that A.I. will ultimately reach the level of singularity, in which the advent of 'superintelligence[49]' will make decisions that are largely viewed as 'objective' by the large majority of the human population, will this cause the gradual abolishment of the very function of the government? When voters vote in a system run by a superintelligence, are they voting for the degrees in which superintelligence will be consulted, or are they voting in favor of policy areas (healthcare, defense, economy) in which they want the intervention of the algorithms? Alternatively, should we think of a totalitarian system in which the full range of tasks and policies are transferred to algorithms, and voting is abolished altogether? If we, however, go with the second scenario, where superintelligence will never materialize, and A.I. structures will always be inherently flawed and remain unable to make better political decisions that humans, what then, is the function of a vote? In a system of 'imperfect intelligence,' where code structures will have the potential to make degrees of mistakes, what exactly will the voters vote for? How will we reconcile the fact that code structures will have an immense influence on political processes, but in turn, cannot be verified or edited by the citizens, but will still become a part of an electoral system?

Regardless of how much A.I. can improve in quantifiable tasks, there is one constant by which all future projections of A.I. politics must be hypothesized: algorithmic structures can never make the unicorn 'perfect decision' in policy

46 Seb Joseph, "How Volkswagen Is Using Artificial Intelligence for Ad Buying Decisions," Digiday (blog), January 8, 2018, https://digiday.com/marketing/volkswagen-using-artificial-intelligence-ad-buying-decisions/.

47 Kim Zetter, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA," Wired, September 24, 2013, https://www.wired.com/2013/09/nsa-backdoor/.

48 Mariarosaria Taddeo and Luciano Floridi, "Regulate Artificial Intelligence to Avert Cyber Arms Race," Nature 556, no. 7701 (April 2018): 296, https://doi.org/10.1038/d41586-018-04602-6.

49 Christof Koch, "When Computers Surpass Us," Scientific American Mind 26, no. 5 (2015): 26–29, https://doi.org/10.1038/scientificamericanmind0915-26.

areas that deal with human complexity. First, because the very concept of a 'perfect' or 'objective decision,' in politics, doesn't exist[50] and second, because systemic data complexity is increasing at a faster rate than the machines' ability to learn them[51]. Once an algorithm is trained on, say, a search engine data, it can reasonably predict short-term search scenarios, but cannot predict human uncertainty or make long-term forecasts on how human search preferences will shape ten years from now. Given the fact that, A.I. decision-making structures try to find a 'one size fits all' solution to most problems, and second, are overwhelmingly built by non-social scientists, they usually reach an optimal result without taking into consideration local and cultural factors and purely on quantifiable, or arbitrarily quantified data[52]. Even after extended iterations of the same decision-making process, any machine-learning cycle learns through quantification, and it is such quantification as the basis of all A.I. functions, which renders the elusive 'optimal decision' impossible in politics.

However, how should politics deal with this kind of automated imperfection? Given the broad spectrum of benefits A.I. brings into the political process, regimes are unlikely to discard algorithms as a decision component. So what is the best practice in algorithmic politics and how can it be appropriately integrated into the decision-making cycle? The democratic approach to A.I. decision-making would be to retain the diversity of the 'information marketplace' with a balanced human-machine interaction, without allowing algorithmic structures to dominate the field altogether[53]. Although seemingly less efficient and more prone to personal politics, this diversification will prevent A.I. over-centralization in the long-run and will be better situated to address the drawbacks of wrong A.I. decisions. Given some of the oversight problems mentioned in this report, the accountability gap can be remedied by deliberately backtracking the A.I. from its true potential by rendering all of its decisions comprehensible to the humans in the decision-making group. In addition, code transparency has to be emphasized at the public level, with a number of non-governmental and citizen-led efforts make up a wide network of oversight. This has to include citizen-led journalism, open-access code culture, crowdsourcing, and free public discussion to diversify ideas, rather than attempt to create a single superintelligent 'benign hegemon.' One of the more recently popular ideas - blockchain voting - could theoretically improve voter turnout as well as rendering elections more secure[54], but making the voting process more secure doesn't fix more pressing problems of algorithmic accountability once algorithms are put in charge of decision-making. Any sort of extreme power centralization, as evidenced by the long history of totalitarian regimes, ends up entering into more conflicts and locks itself into a perpetual cycle of militarized disputes, often with its own population[55]. To that end, A.I.-based power centralization will also generate more recurrent conflicts, rather than creating a global 'super-intelligence' that will bring about peace.

'Politicality' is another important measure when evaluating the impact of A.I. on legitimacy. 'Politicality' refers to the role of political capital and political influence in determining the outcome of a decision[56]. In politics, it is not always the most 'rational' choice that gets implemented, but the one that has the highest degree politicality - meaning political capital and influence. Influence is usually determined by the power relations between major political actors and institutions, as a result of successful or further political capital-generating decisions. More specifically, the politicality of a decision is determined between four systems of power: legitimate (elected), expert (technocratic), ideological, and interest-based. The balance of power among these fundamental aspects of influence determines the stability and institutionalization of a political system. A decision with the highest degree of politicality is the one that meets

50 James W. Dean and Mark P. Sharfman, "Does Decision Process Matter? A Study Of Strategic Decision-Making Effectiveness," Academy of Management Journal 39, no. 2 (April 1, 1996): 368–92, https://doi.org/10.5465/256784.

51 Koch, "When Computers Surpass Us."

52 Laura Spinney, "Can Robots Make Art?," News, Nature, April 27, 2018, https://doi.org/10.1038/d41586-018-04989-2.

53 Haridimos Tsoukas, "The Tyranny of Light: The Temptations and the Paradoxes of the Information Society," Futures 29, no. 9 (November 1, 1997): 827–43, https://doi.org/10.1016/S0016-3287(97)00035-9.

54 Kevin Desouza and Kiran Kabtta Somvanshi, "How Blockchain Could Improve Election Transparency," Brookings Institution, May 30, 2018, https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/.

55 John Henry Holland, Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence (Cambridge, MA: MIT Press, 1992).

56 Paul C. Nutt and David C. Wilson, Handbook of Decision Making (London: John Wiley & Sons, 2010).

the expectations of elected, technocratic, ideological and interest-based political actors. Most political decisions - perhaps with the exception of the fundamental clauses of constitutions - don't enjoy backing from all four sources of political capital. Constant, daily push and pull, bargaining and competition between these sources form the very practice of politics and political life. A.I. will significantly alter this balance of power between influence actors because algorithmic decisions bring their own political power into the equation.

Once decisions are gradually outsourced to algorithms, A.I. will either create its own influence space that will eventually swallow other actors, or strengthen one of these four sources. This will inevitably be the one that is closest to the technical pre-requisites of managing code structures and one that is most likely to be the technocratic source of influence: the expert (technocratic) influence. This will prevent algorithmic decisions to have sufficient politicality, given the fact that such decisions will have to be disconnected from ideological and interest-based sources of authority. Moreover, algorithmic decisions have no visible, public face. Visibility is one of the strongest pre-requisites of legitimacy. Leaders and politicians have to be visible, in public and on media outlets. Since politics is the management of power relations between human beings, it is primarily structured on actors' behavior, charisma, and presence in the eyes of their constituencies. Once A.I. emerges as the predominant form of political decision, it will have to assume a public face and some form of visibility. How this visibility will be attained, in what form and through which actor(s) will also be significantly important for the sake of political legitimacy and political capital.

In June 2018, a widely shared BBC report asked: 'Can we trust AI if we do not know how it works?[57]'. The news report summarized some of the current advances in artificial intelligence and neural networks, emphasizing how machines were now able to handle a wide array of complex tasks. The problem is, machines ability to handle complex tasks does not immediately mean that they are performing these tasks correctly. These performance problems originate from the fact that highly complicated machine-learning methods such as neural networks or deep learning work on such large sets of internal parameters that they were now becoming too difficult to reverse engineer or explain, even by their coders. This growing complication of the A.I. methods has necessitated the creation of DARPA's 'Explainable A.I.' project[58], or the OpenAI, a non-governmental research group that attempts to render A.I. progress safer and more accountable. Adrian Weller, the A.I. Programme Director at the Alan Turing Institute in London was quoted in the same report: "*If an algorithm recommended I be imprisoned for six years, I would want an explanation which would enable me to know if it had followed appropriate process, and allow a meaningful ability to challenge the algorithm if I disagree*[59]." Not only that the current progress with A.I. renders its decisions highly opaque and complex for most political and legal oversight mechanisms, but with regard to more experimental methods such as deep reinforcement learning, even the companies and research groups in charge of the algorithm cannot understand and explain how the machine learned by interacting with its environment and through which iterative processes.

[57] Marianne Lehnis, "Can We Trust AI If We Don't Know How It Works?," BBC News, June 15, 2018, sec. Business, https://www.bbc.co.uk/news/business-44466213.

[58] "Explainable Artificial Intelligence," DARPA, 2018, https://www.darpa.mil/program/explainable-artificial-intelligence.

[59] Lehnis, "Can We Trust AI If We Don't Know How It Works?"

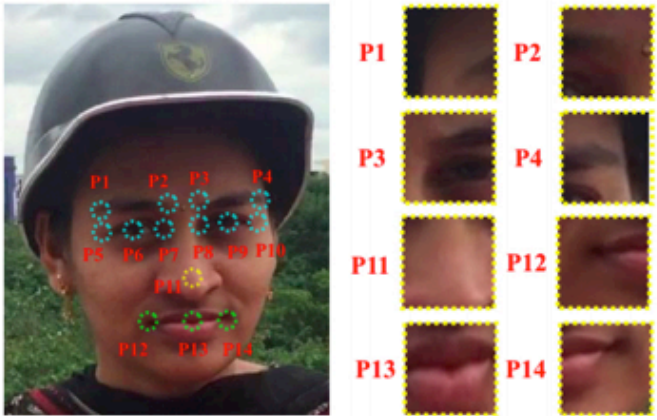


Figure 1: The figure (left) illustrates the 14 facial key-points annotated for both the introduced datasets. The description of the facial points is as: Eyes region (cyan): P1-left eyebrow outer corner, P2-left eyebrow inner corner, P3-right eyebrow inner corner, P4-right eyebroe outer corner, P5-left eye outer corner, P6-left eye center, P7 left eye innner corner, P8-right eye inner corner, P9-right eye center, P10-right eye outer corner; Nose region (yellow): P11-nose; Lipregion (green) P12-lip left corner, P-13-lip centre, P14-lip right corner. Few key points have been shown on the right.

Figure 2: The illustration shows samples images with different disguis-esfrom both the Simple and Complex face disguise (FG) datasets. As seen from the image, the samples from the complex background dataset have a relatively complicated background as opposed as opposed to the simple dataset.

Image 4 – New studies in visual recognition algorithms can detect faces behind masks and veils. (Source: Singh, Amarjot, et al. "Disguised face identification (DFI) with facial keypoints using spatial fusion convolutional network." Computer Vision Workshop (ICCVW), 2017 IEEE International Conference on. IEEE, 2017.)

The above discussion outlines some of the main challenges of A.I. on political decision-making that can blur the lines of legitimacy and sovereignty in statehood. It is ultimately critical to understand that all algorithms reflect the biases of their coders and despite the prevalent view among these programmers, they are not unbiased and most certainly not 'objective' from a political point of view. Most of the time, algorithms systematize existing human biases and wrap them in overwhelming layers of automated code structures, rendering such biases inherently unaccountable, sometimes even to coders themselves. Besides, like all quantitative methods of inquiry, A.I., and machine learning too, can easily suffer from poor decisions that originate from low data quality. Low data quality is a common problem in machine learning methods and causes these algorithms to learn through unverified or error-abundant datasets. Bad quality may, in turn, generate measurement errors or spurious results, further reinforcing systematized inequality.

Embedded biases in political decision algorithms, when unchecked for pre-existing racial, ethnic, religious or socio-economic inequalities, will significantly impair the fairness of the implementation of some of the core duties of statehood, taxation, infrastructure development and disaster relief. Communication scientist Safiya Noble conceptualizes these inherent biases as 'technological redlining'; namely, how identity-related differences can be discriminated against in resource technologies, such as banking, investment, and insurance[60]. An example of embedded technological redlining is how Google's search algorithms yield different racial biases in its auto-complete results when different ethnic identities are typed into the search box. Since Google search data is one of the primary training pools of most A.I. decision-making projects, biases embedded in Google data will impact the near future of algorithmic decision-making in politics.

[60] Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism, 1 edition (New York: NYU Press, 2018).

Conclusion

On 23 June, 12 members of a youth football club, along with their coach, ended up trapped in a deep cave in rural Chiang Rai, Thailand. The entrapped crew were found by chance, although the elaborate, dangerous and labyrinthine twists and turns of the cave structure prevented an easy rescue. Thai military, police and emergency responders gradually rushed to the cave entrance, setting up a large base of operations there. By 28 June, first international rescuers and specialist cave divers began arriving at the Tham Luang mountain, only to discover the difficulty of the task at hand. The cave structure consisted of tiny passages that barred the entry of scuba teams, and heavy rainfall meant that the water level in the cave rose up at certain times, flooding in passageways and isolated chambers. The difficulty of the rescue operation attracted international attention, and Elon Musk was one of the first advocates of a technology-driven suggestion and offered to help by building a makeshift cylinder submarine. Sharing the fast construction and testing process of the submarine through Twitter and Instagram, Musk rallied his followers to generate international support for his intervention in the rescue operation[61]. The problem was, just when Musk completed the tests of his makeshift submarine, the commander of the rescue operation, governor Narongsak Osottanakorn declared that all boys were finally rescued by a large group of volunteers, diving experts, and navy seal units. Furthermore, Osottanakorn claimed that Musk's submarine was not fit for the job at hand, and even scuba divers could not fit through certain passageways in the cave; let alone a submarine - no matter how small. One of the most critical volunteers of the operation, British cave diver Vernon Unsworth, also called Musk's idea as 'PR stunt,' since his submarine 'wouldn't have made the first 50 meters'[62].

The combination of being late to the rescue operation and rejection by the commander and lead cave diver made Musk furious, as he launched a barrage of criticism against the rescuers, including calling Osottanakorn 'not a subject matter expert', and Unsworth a 'pedophile'. Musk insisted that his submarine could have saved the kids, as he so elaborately demonstrated in controlled cave-like contraption in a diving pool in California. Following several simultaneous Twitter war of words and accusations, Musk eventually deleted all of his inflammatory tweets in a couple of days. The Thai cave rescue episode yields important lessons for the future of technology-driven optimism, that 'tech can save them all,' or the prevalent view among engineering circles that innovation by itself can fix all problems of humanity. The biggest trap in techno-optimism is the mistaken belief that all forms of expertise can be translated into other domains; that a skilled engineer can perfectly transfer its set of skills into non-engineering domains. This is the pitfall that most computer scientists fall into when devising algorithms for social purposes: human behavior can be quantifiable, details of human actions can be measured through proxy data and human customs, protocols, and procedures that were shaped across centuries are inherently inferior, or irrelevant to the power of technological progress.

This does not mean that A.I. cannot be a force for good, or render politics more efficient, or more responsive to citizens' needs. If used well, A.I. can broaden the space for democratic representation by decentralizing information systems and communication platforms. It can bolster informational autonomy for citizens and improve the way they collect information about political processes and help them participate in these processes remotely. Just as A.I. can be used to strengthen opaqueness and unaccountability, it can also improve transparency and help establish greater trust between the state and the society and between citizens themselves. It can create information pollution just as much as it can reduce such pollution in communication platforms; it can reinforce echo chambers, just as it can establish new connections between rival political ideologies. Speaking of A.I. as an autonomous force that will 'do something' to human beings is thus a flawed lens with which to evaluate the future of algorithmic structures on political regimes. Given the fact that A.I. systems will continue to reflect coder bias, it will never reach a state of 'perfect superintelligence' that is objective and uniform in its sense of justice, measurement and calculations. Thus, the impact of A.I. on politics will be a direct result of how power relations are coded into the algorithmic platforms and how different code representations of power, legitimacy, and authority will

[61] Laura Yan, "Elon Musk Is Mad His Mini-Submarine Didn't Help in Thai Cave Rescue," Popular Mechanics, July 15, 2018, https://www.popularmechanics.com/technology/a22150734/elon-musks-mad-mini-submarine-didnt-help-thai-cave-rescue/.

[62] Michael Safi and Sam Levin, "British Cave Diver Considering Legal Action over Elon Musk's 'Pedo' Attack," The Guardian, July 16, 2018, sec. Technology, http://www.theguardian.com/uk-news/2018/jul/16/british-diver-in-thai-cave-rescue-stunned-after-attack-by-elon-musk.

influence how different A.I.s will view politics as a means versus an end.

In the words of techno-sociologist Zeynep Tufekci: *'[machine learning] is the worst combination: high enough validity to be hard to resist use; high false and positive negatives and hard to tell which is which'*[63]. False positives and false negatives are binary classification errors in tests results when looking for the presence and absence of certain statistical conditions[64]. The false positive error can be dubbed as a 'false alarm', which signals the presence of a particular condition where there is none. Similarly, a false negative error is a measurement fallacy, which signals that the researched condition does not exist - such as a pregnancy test failing to detect pregnancy while the studied subject is in fact pregnant. All machine learning algorithms work on a classifier structure in which the machine learns to make a set of assumptions about different strands of data. Like all iterative learning processes, machine learning too can suffer from false negative or positive reports. While these reports are common errors in any such study, once such error margin is transferred to political decisions, it can lead to the systematic repression of specific ethnic or social groups, the wrongful implication of suspects or unnecessary systematic profiling of citizens.

Ultimately, a systematic inquiry on the political impact of A.I., or whether algorithms will reinforce democracy or authoritarianism should take into account how decisions are made, regulated and overseen across different regime types. More critically, the role of A.I. in changing the power balance between political institutions, actors, and executive organs needs more structured research. Given the scale of legitimacy and sovereignty problems associated by outsourcing political decisions to algorithms, the role of constitutions, parliaments and the political elite in relation to A.I. need to be studied in-depth with a specific focus on how politicality and political authority should be situated in the age of automated decisions. Furthermore, 'what A.I. will do with politics' is an incomplete question given the fact that this question is structured upon several antecedent questions that originate from the monopolization of information, network control, and data processing. Technology monopolies of Google, Baidu, Alibaba, Amazon, Youtube, Tencent, Facebook and others, coupled with Silicon Valley-style PR brinkmanship culture will likely lead to more dangerous and unnerving developments in algorithmic politics in comparison to what democratic or authoritarian states may or may not do with A.I. In the end, it will be pre-existing human power and rent-generating structures that will have the most significant impact on how algorithms will impact politics, rather than the A.I. itself - as an independent entity, and different big-technology business models, rather than political regime types will have the greatest influence over how algorithms will be deployed in politics.

63 Zeynep Tufekci, We're Building a Dystopia Just to Make People Click on Ads, TEDGlobal (New York, NY, 2017), https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads.

64 D. C. Rao and C. Gu, "False Positives and False Negatives in Genome Scans," Advances in Genetics 42 (2001): 487–98.

References

Allen, Greg, and Taniel Chan. "Artificial Intelligence and National Security." Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kenendy School, July 2017. https://www.belfercenter.org/publication/artificial-intelligence-and-national-security.

Alturki, Badraddin, Stephan Reiff-Marganiec, and Charith Perera. "A Hybrid Approach for Data Analytics for Internet of Things." *arXiv:1708.06441 [Cs]*, August 21, 2017. http://arxiv.org/abs/1708.06441.

Ball, Kirstie, and Laureen Snider. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. New York: Routledge, 2013.

Bell, Anthony J. "Levels and Loops: The Future of Artificial Intelligence and Neuroscience." *Philosophical Transactions of the Royal Society of London B: Biological Sciences* 354, no. 1392 (December 29, 1999): 2013–20. https://doi.org/10.1098/rstb.1999.0540.

Bond, David. "Facebook Key to Winning UK General Election, Political Parties Say." Financial Times, May 14, 2017. https://www.ft.com/content/c78c3bd0-36f8-11e7-99bd-13beb0903fa3.

Bucher, Taina. *If...Then: Algorithmic Power and Politics*. Oxford University Press, 2018.

Chadwick, Andrew. *The Hybrid Media System: Politics and Power*. New York, NY: Oxford University Press, 2017.

Cyranoski, David. "Beijing Launches Pioneering Brain-Science Centre." News. Nature, April 5, 2018. https://doi.org/10.1038/d41586-018-04122-3.

Davis, Joshua. "Is There an AI President in Our Future? That Might Be an Upgrade." *Wired*, May 18, 2017. https://www.wired.com/2017/05/hear-lets-elect-ai-president/.

Dean, James W., and Mark P. Sharfman. "Does Decision Process Matter? A Study Of Strategic Decision-Making Effectiveness." *Academy of Management Journal* 39, no. 2 (April 1, 1996): 368–92. https://doi.org/10.5465/256784.

Desouza, Kevin, and Kiran Kabtta Somvanshi. "How Blockchain Could Improve Election Transparency." Brookings Institution, May 30, 2018. https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/.

Dijck, Jose van. *The Culture of Connectivity: A Critical History of Social Media*. New York, NY: Oxford University Press, 2013.

Drahos, Peter, and John Braithwaite. *Information Feudalism: Who Owns the Knowledge Economy?* New Press, 2003.

"Explainable Artificial Intelligence." DARPA, 2018. https://www.darpa.mil/program/explainable-artificial-intelligence.

Flaxman, Seth, Sharad Goel, and Justin M. Rao. "Filter Bubbles, Echo Chambers, and Online News Consumption." *Public Opinion Quarterly* 80, no. S1 (January 1, 2016): 298–320. https://doi.org/10.1093/poq/nfw006.

Foucault, Michel. *Discipline & Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York: Vintage Books, 1995.

Freedberg, Sydney J. "AI Logistics Let Combat Units Move Faster: Uptake's DIUX Contract." *Breaking Defense* (blog), June 27, 2018. https://breakingdefense.com/2018/06/ai-logistics-can-speed-up-army-tanks-uptakes-diux-contract/.

Ganshof, François Louis. *Feudalism*. Toronto: University of Toronto Press, 1996.

Graham-Harrison, Emma, Carole Cadwalladr, and Hilary Osborne. "Cambridge Analytica Boasts of Dirty Tricks to Swing Elections." *The Guardian*, March 19, 2018, sec. News. http://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections.

Greenfield, Adam. "China's Dystopian Tech Could Be Contagious." The Atlantic, February 14, 2018. https://www.theatlantic.com/technology/archive/2018/02/chinas-dangerous-dream-of-urban-control/553097/.

Habermas, Jürgen. *The Philosophical Discourse of Modernity: Twelve Lectures*. Cambridge, UK: John Wiley & Sons, 2018.

Hacking, Ian. "Canguilhem amid the Cyborgs." *Economy and Society* 27, no. 2–3 (May 1, 1998): 202–16. https://doi.org/10.1080/03085149800000014.

Holland, John Henry. *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*. Cambridge, MA: MIT Press, 1992.

Howard, Philip N. *Pax Technica: How the Internet of Things May Set Us Free Or Lock Us Up*. Yale University Press, 2015.

Howze, Thaddeus. "Feudalism and the 'Algorithmic Economy.'" *Medium*, April 17, 2017. https://medium.com/@ebonstorm/feudalism-and-the-algorithmic-economy-62d6c5d90646.

Joseph, Seb. "How Volkswagen Is Using Artificial Intelligence for Ad Buying Decisions." *Digiday* (blog), January 8, 2018. https://digiday.com/marketing/volkswagen-using-artificial-intelligence-ad-buying-decisions/.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* 107, no. 2 (May 2013): 326–43. https://doi.org/10.1017/S0003055413000014.

Kitchin, Rob. "Thinking Critically about and Researching Algorithms." *Information, Communication & Society* 20, no. 1 (January 2, 2017): 14–29. https://doi.org/10.1080/1369118X.2016.1154087.

Koch, Christof. "When Computers Surpass Us." *Scientific American Mind* 26, no. 5 (2015): 26–29. https://doi.org/10.1038/scientificamericanmind0915-26.

Lazer, David M. J., Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, et al. "The Science of Fake News." *Science* 359, no. 6380 (March 9, 2018): 1094–96. https://doi.org/10.1126/science.aao2998.

Lehnis, Marianne. "Can We Trust AI If We Don't Know How It Works?" *BBC News*, June 15, 2018, sec. Business. https://www.bbc.co.uk/news/business-44466213.

Levy, Frank. "Computers and Populism: Artificial Intelligence, Jobs, and Politics in the near Term." *Oxford Review of Economic Policy* 34, no. 3 (July 2, 2018): 393–417. https://doi.org/10.1093/oxrep/gry004.

Lim, Merlyna. "Freedom to Hate: Social Media, Algorithmic Enclaves, and the Rise of Tribal Nationalism in Indonesia." *Critical Asian Studies* 49, no. 3 (July 3, 2017): 411–27. https://doi.org/10.1080/14672715.2017.1341188.

Makridakis, Spyros. "The Forthcoming Artificial Intelligence (AI) Revolution: Its Impact on Society and Firms." *Futures* 90 (June 1, 2017): 46–60. https://doi.org/10.1016/j.futures.2017.03.006.

Marcuse, Herbert. *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society*. New York, NY: Routledge, 2013.

Marx, Karl. *Economic and Philosophic Manuscripts of 1844*. Mineola, NY: Courier Corporation, 2012.

Marx, Karl, and Friedrich Engels. *The Communist Manifesto*. Minneapolis, MN: First Avenue Editions, 2018.

Morris, Nigel. "GCHQ Was Harvesting Metadata on Everybody, Says Edward Snowden." The Independent, September 25, 2015. http://www.independent.co.uk/news/uk/home-news/edward-snowden-gchq-collected-information-from-every-visible-user-on-the-internet-10517356.html.

Nagler, Jan, Jeroen van den Hoven, and Dirk Helbing. "An Extension of Asimov's Robotics Laws." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 26, 2018. https://papers.ssrn.com/abstract=3110582.

Nickerson, David W., and Todd Rogers. "Political Campaigns and Big Data." Faculty Research Working Paper Series. Cambridge, MA: Harvard Kennedy School, February 2014.

Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. 1 edition. New York: NYU Press, 2018.

Nutt, Paul C., and David C. Wilson. *Handbook of Decision Making*. London: John Wiley & Sons, 2010.

Polonski, Vyacheslav. "How Artificial Intelligence Silently Took over Democracy." World Economic Forum, August 9, 2017. https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first/.

Rao, D. C., and C. Gu. "False Positives and False Negatives in Genome Scans." *Advances in Genetics* 42 (2001): 487–98.

Ratner, Paul. "Putin Weighs in on Artificial Intelligence and Elon Musk Is Alarmed." Big Think, September 24, 2017. https://bigthink.com/paul-ratner/putin-weighs-in-on-artificial-intelligence-and-elon-musk-is-alarmed.

Ravindranath, Mohana. "In Chicago, Food Inspectors Are Guided by Big Data." Washington Post, September 28, 2014. https://www.washingtonpost.com/business/on-it/in-chicago-food-inspectors-are-guided-by-big-data/2014/09/27/96be8c68-44e0-11e4-b47c-f5889e061e5f_story.html.

Safi, Michael, and Sam Levin. "British Cave Diver Considering Legal Action over Elon Musk's 'Pedo' Attack." *The Guardian*, July 16, 2018, sec. Technology. http://www.theguardian.com/uk-news/2018/jul/16/british-diver-in-thai-cave-rescue-stunned-after-attack-by-elon-musk.

Scholz, Roland W. *Decision Making under Uncertainty: Cognitive Decision Research, Social Interaction, Development and Epistemology*. Amsterdam: Elsevier, 1983.

Scholz, Trebor. *Digital Labor: The Internet as Playground and Factory*. New York, NY: Routledge, 2012.

Singel, Ryan. "Analysis: Google's Ad Targeting Turns Algorithms on You." *Wired*, May 11, 2009. https://www.wired.com/2009/03/google-ad-annou/.

Snyder, Timothy. "Fascism Is Back. Blame the Internet." *Washington Post*, May 21, 2018. https://www.washingtonpost.com/news/posteverything/wp/2018/05/21/fascism-is-back-blame-the-internet/.

Spinney, Laura. "Can Robots Make Art?" News. Nature, April 27, 2018. https://doi.org/10.1038/d41586-018-04989-2.

Srnicek, Nick. *Platform Capitalism*. Wiley, 2016.

Sunstein, Cass R. *#Republic: Divided Democracy in the Age of Social Media*. Princeton, NJ: Princeton University Press, 2018.

Taddeo, Mariarosaria, and Luciano Floridi. "Regulate Artificial Intelligence to Avert Cyber Arms Race." *Nature* 556, no. 7701 (April 2018): 296. https://doi.org/10.1038/d41586-018-04602-6.

Tett, Gillian. "Trump, Cambridge Analytica and How Big Data Is Reshaping Politics." Financial Times, September 29, 2017. https://www.ft.com/content/e66232e4-a30e-11e7-9e4f-7f5e6a7c98a2.

Thaler, Richard H., and Cass R. Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Revised & Expanded edition. New York: Penguin Books, 2009.

Thompson, Nicholas. "Emmanuel Macron Talks to WIRED About France's AI Strategy." *Wired*, March 31, 2018. https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/.

Treré, Emiliano. "The Dark Side of Digital Politics: Understanding the Algorithmic Manufacturing of Consent and the Hindering of Online Dissidence." *IDS Bulletin* 47, no. 1 (January 11, 2016). https://doi.org/10.19088/1968-2016.111.

Tsoukas, Haridimos. "The Tyranny of Light: The Temptations and the Paradoxes of the Information Society." *Futures* 29, no. 9 (November 1, 1997): 827–43. https://doi.org/10.1016/S0016-3287(97)00035-9.

Tufekci, Zeynep. "Engineering the Public: Big Data, Surveillance and Computational Politics." *First Monday* 19, no. 7 (July 2, 2014). https://doi.org/10.5210/fm.v19i7.4901.

———. *We're Building a Dystopia Just to Make People Click on Ads*. TEDGlobal. New York, NY, 2017. https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads.

Weber, Max. *The Vocation Lectures*. Edited by David Owen and Tracy B. Strong. Translated by Rodney Livingstone. Indianapolis: Hackett Publishing Company, Inc., 2004.

Wiener, Norbert. *Cybernetics Or Control and Communication in the Animal and the Machine*. Cambridge, MA: MIT Press, 1961.

Yan, Laura. "Elon Musk Is Mad His Mini-Submarine Didn't Help in Thai Cave Rescue." Popular Mechanics, July 15, 2018. https://www.popularmechanics.com/technology/a22150734/elon-musks-mad-mini-submarine-didnt-help-thai-cave-rescue/.

Zetter, Kim. "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA." *Wired*, September 24, 2013. https://www.wired.com/2013/09/nsa-backdoor/.

Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89. https://doi.org/10.1057/jit.2015.5.

Cyber Governance and Digital Democracy 2018/9

July 2018

Artificial Intelligence, Authoritarianism and the Future of Political Systems

H. Akın Ünver | EDAM, Oxford CTGA & Kadir Has University