The Hyperconnected World
of 2030–2040

ABOUT INSTITUTE FOR THE FUTURE

Institute for the Future is the world's leading futures 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. **www.iftf.org**

ABOUT THIS PROJECT

This report, *The Hyperconnected World of 2030–2040* was made possible by the support of the Office of Director of National Intelligence. The findings are those of the Institute for the Future (IFTF) and do not necessarily represent US Government views.

For more information, contact Alyssa Andersen | aandersen@iftf.org

Table of Contents

Introduction

Much has been written about the advent of 5G in recent years. Press coverage has tended to focus on deployment of the technologies that will enable the new high-speed network, or on which companies are racing to win contracts in key areas of coverage. While these aspects are important, less thought has been devoted to what the world looks like *after* 5G is successfully deployed around the world. What exactly does the hyperconnected world of 2030–2040 look like? *The hyperconnected world* is a future in which 5G networks have been widely and globally deployed, and in which the normal, day-to-day functioning of society depends on billions of connected devices having highly reliable, low-latency connectivity.

Simply put, this world means more data, more devices, and more interactions between the two. A hyperconnected world will support up to 1 million devices per square kilometer of coverage area, orders of magnitude more than the 60,000 devices currently possible with 4G LTE networks. Sensor devices will become omnipresent—20.4 billion devices embedded with connected sensors will be operative this year alone. In this future, the very definition of *scale* itself will change—instead of billions of devices, the world will support hundreds of billions, or possibly trillions. The total amount of data produced in human history, already doubling every two years, is likely to double every six months. While the figures are impressive, less thought has been given to what this world will look like, and what the positive and negative effects of hyperconnection are likely to be—until now. The goal of this report is to forecast the hyperconnected world.

- **A hyperconnected world will be predominantly defined by the social and political effects it engenders—much more so than by its underlying technologies.** The ramifications of hyperconnectivity will affect cybersecurity and privacy and cause power shifts in global financial institutions and labor markets. Further concerns abound. For instance, hyperconnective machine learning and AI may have lasting environmental impacts, and dempocratized synthetic media could destabilize societies at a scale and speed that dwarfs current disinformation challenges. What's more, any types of crime, particularly those enforceable by surveillance of digital devices, will become absolutely enforceable, and offline and online privacy will likely undergo significant erosion. Preparing for these challenges in advance increases the probability we will be able to navigate them more smoothly than current socio-technical challenges.

- **Cybersecurity will be a Herculean challenge in a hyperconnected world**. The increased connectivity of the new millennium has increased vulnerability of connected individuals, institutions, and nations. Hyperconnectivity presents a new challenge—scale itself will be redefined, with hundreds of billions of connected devices vastly increasing the attack surface for nefarious actors. The European Union aptly analyzes that "these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework."

- **Hyperconnectivity offers immense promise for medical advancement.** While important dangers exist, a hyperconnected world is likely to drive progress in medicine. Connected sensor devices—including wearable and internal medical devices—are likely to be a key factor driving such progress.

- **Immersive environments offer new interfaces for human-machine interaction.** Cross reality (XR) and conversational computing are likely to become widespread in a hyperconnected world. Devices and user experience (UX) are likely to undergo great transformations.

- **Present-day, future-oriented research offers unique promise for easing the transition into the hyperconnected world.** Rigorous futures thinking allows us to generate foresight about our hyperconnected future. From that foresight, we can obtain insight about the technological and social forces likely to shape that future, and take action to help mold a desirable and globally beneficial hyperconnected future.

- **Individuals, states, and private companies will all gain greater power in the hyperconnected world, with private companies likely gaining the most.** Several of the trends of the past decade, most notably an increase in individual and state empowerment through technology, are likely to continue in the hyperconnected world. Power is not zero-sum in the hyperconnected world—the same technologies that empower citizens to control their networks of smart devices from afar will also enable great analysis and surveillance power for governments and the private sector. While an individual's ability to communicate and control networks of devices will increase, governments, especially those whose power is unrestricted, will have a historically unprecedented ability to enforce laws, track and de-anonymize citizens, target individuals with autonomous weapons, and paralyze connected societies with cyberwarfare. But the private sector will likely gain the most power in the hyperconnected world—they will challenge citizens' and governments' claims to know their own societies with a near-worldwide ability to surveil citizens and analyze not only individuals, but those individuals' devices. Accordingly, a private corporation's ability to challenge norms of governance and withhold data from governments will increase, leading to more frequent litigation in both open and closed societies.

As highlighted in IFTF's December 2019 expert workshop *Future of the State, Society, and Security in a Hyperconnected World,* it is clear that the advent of 5G, advanced networking, and the spread of hyperconnectivity are likely to drive even more accelerated change than the Internet and automation in past decades. For that reason, knowing how to anticipate the technologies at the heart of this hyperconnective revolution, as well as the social and political changes they are likely to bring in their wake, is key to ensuring a peaceful and prosperous transition into a desirable future.

With this in mind, IFTF has prepared a comprehensive report examining the affordances and dangers of the hyperconnected world of 2030–2040. This report proceeds in two sections: in Part I, *The Social and Political Implications of Hyperconnection,* we explore the main potential social and political areas worthy of further consideration that are likely to present central questions and epoch-making dilemmas in a hyperconnected world. In Part II, *Key Elements of a Hyperconnected World,* we explore and synthesize the main topics covered during the IFTF hyperconnectivity workshop. These two sections build on substantial research and signals from the past and the present day, and aim to cover complementary areas likely to undergo substantial change with the advent of hyperconnectivity. Striving for concision, but loath to sacrifice depth, each section is accompanied by a dedicated appendix, which offers greater detail and presents the wide body of interdisciplinary research from which we have drawn our foresight, insight, and conclusions.

The Social and Political Implications of Hyperconnected Worlds

While the technologies that will enable a hyperconnected world are, at this point, well understood, the social and political implications of these technologies are substantially less clear. Despite this difficulty, anticipating these externalities is crucial to ensuring stability with the hyperconnective revolution, and for ensuring that we are able to reap the greatest benefits from future technologies while minimizing harms. In this section, we aim to explore the main social, political, and cultural issues likely to emerge in a hyperconnected world that remained undiscussed or underexplored during our one-day hyperconnectivity workshop.

In the sections that follow, we consider both *probable* and *possible* areas of social and political disruption in a hyperconnected world. *Probable areas of concern* are those in which near-certain changes can be anticipated. *Possible areas of concern,* by contrast, represent those in which several contingencies, or *hinge factors*, make reliable forecasting of the future difficult. Nonetheless, these areas are likely to precipitate Key Future Research Questions in social and policy realms, and for that reason have been included.

In any possible hyperconnected future, it is certain that cybersecurity will continue to be a critical issue at all levels—from the individual to the nation-state. As *New York Times* national security reporter David Sanger points out in his book *The Perfect Weapon*, the same connectivity that enables developed nations to harness technologies in advanced ways also necessarily increases those same nations' vulnerability to cyberattacks.[1] In this regard, the most connected societies are also those that offer the greatest attack surface for nefarious actors (Sanger, 2019).[2] Cryptographer and cybersecurity expert Bruce Schneier has written compellingly about this topic, declaring that "every part of the [5G] supply chain can be attacked." Fundamental failures of security in the underlying hardware of devices worldwide have reemphasized this dynamic in the past two years alone, with the discovery of Spectre and Meltdown being the most notable example (Newman, 2019).[3]

The paramount importance of securing a hyperconnected world cannot be overstated. We agree that "5G security will need to get commensurately large to scale to meet the multi-dimensional security challenge," and echo scholar Elsa Kania's cautionary note that "security will be more important than speed in establishing a durable foundation for 5G's future" (Kania, 2019; Lomas, 2019). The EU's own assessment of the security risks of 5G found that "these challenges create a new security paradigm, making it necessary to reassess the current policy and security framework."[4] Given the unanimity of

expert judgment on this topic, we will occasionally examine cybersecurity implications within specific domains (such as internal biomedical devices), but have refrained from making cybersecurity a subsection in itself.

Finally, it is important to note that this is not meant to be a comprehensive list of social areas affected by hyperconnectivity—rather, it represents an assessment of what we have judged to be the areas most worthy of attention for anticipation of probable social and policy disruption that will emerge from a hyperconnected world. The hyperconnected world touches on several socio-technical areas that are of course all worthy of further thorough exploration on their own. These domains include smart cities, the Internet of things (IoT), medicine, cloud-enhanced warfare, autonomous weapons, artificial intelligence (AI), privacy, surveillance, cybersecurity, biometrics, the environmental implications of technology usage, the labor market, and many others.

PROBABLE AREAS OF CONCERN

In this section, we consider areas that are highly likely to present new social and political challenges resulting from hyperconnectivity.

Proliferation of Online Crime and the Dawn of Absolute Enforceability

Crime, both online and offline, is likely to change in response to hyperconnectivity. Cybercrime in particular is likely to increase. The vulnerability of hyperconnected institutions to cyberattacks is well-documented—in 2019, more than 100 cities, hospitals, and police stations fell victim to costly ransomware attacks in the United States alone (Kim, 2019; Shi, 2019). Beyond institutional targets, criminal groups are also likely to continue stealing valuable, personally identifiable data.[5] Increased surveillance and distributed communication capabilities will provide more opportunities for eavesdropping and interception of valuable information, facilitating blackmail,[6] and theft of intellectual property (Lourenço & Marinos, 2019).

Gaming and XR technologies will also present new challenges—online gaming[7] has become a major vector for the abuse and exploitation of children, and expanded use of AR and VR media could make children more vulnerable (Bowles & Keller, 2019). Sexual assault has already occurred in VR, and nonconsensual pornographic deepfakes, already frequent and predominantly targeting women, are likely to become far more common (Belamire, 2016; Patrini, 2019). Avatars of real individuals, rendered with "scary accuracy," could be unwittingly victimized in rape and murder simulations.[8] Even between consenting adults, it is not clear how avatar simulations of child abuse ("sexual ageplay"), rape-play, and murder-play will be regarded (Reeves, 2018).[9] Beyond the virtual realm, IoT technologies— ranging from smart home locks and speakers to smart cars' phone applications and GPS tracking devices—are being used to enable domestic abuse (Bowles, 2018; Young & Saxena, 2019).

> Sexual assault has already occurred in VR, and nonconsensual pornographic deepfakes, already frequent and predominantly targeting women, are likely to become far more common.

A diffusion of easy-to-use encryption technologies has implications for criminality as well, particularly online. In 2018, technology companies reported a marked and historic increase in child pornography, reporting 45 million online photos and videos of child sexual abuse[10] (Keller & Dance, 2019a, 2019b). A resurgence of the Crypto Wars of the 1990s is highly likely in this environment, and indeed, signals of this already began to appear in late 2019 and early 2020 (Benner, 2020; McCabe et al., 2019). While the battle for online privacy continues,[11] offline privacy will likely continue to gradually erode (see *privacy* section below).[12] With far more real-time surveillance capabilities possible than ever before, particularly with no latency, the question of how much illegality to allow will become a pressing question in both liberal and autocratic regimes.[13] Societies will for the first time face the question of how absolutely laws should be enforced.

Crimes, particularly those that can be enforced through real-time or retroactive surveillance of digital data, will become absolutely enforceable. Speeding and jaywalking are two easy-to-imagine examples. The absolute power this affords autocratic regimes represents a form of neo-totalitarian control—particularly when coupled with pretextual search and seizure of digital devices, or enforcement of obsolete but unrepealed laws. In liberal societies, it is imaginable that the quantification of enforcement enabled through the same mechanisms may drive revision to laws and enforcement to address these new problems.

KEY FUTURE RESEARCH QUESTIONS:

- How can liberal and autocratic societies decide what level of illegality to allow? Do democratic societies remain free when the law becomes absolutely enforceable?[14]

- What possibilities exist for preserving robust encryption techniques while also stymying an increase in online crime (e.g., identity theft, child pornography, and black market commerce)?

Hyperconnective Medicine—Medical Dreams and Security Nightmares

Hyperconnectivity will enable a much larger number of sensor devices to exist and communicate with low latency in the future. An area in which this fact holds great promise is medicine. Real-time feedback from and monitoring of sensors will be extremely reliable, even in remote areas. Treatments for chronic diseases that require constant monitoring (e.g., glaucoma, diabetes, fertility, and heart diseases) will be transformed as patients and doctors have an unprecedented ability to monitor and log conditions and symptoms in real time, especially with wearable or internal IoT-connected devices. The possibility of real-time monitoring also offers medical alert and prevention possibilities of previously unpredictable diseases—for instance, researchers from the University of Washington recently found that Amazon Echo speakers were able to reliably detect heart attacks in advance by listening for agonal breathing (Brown, 2019; Chan et al., 2019). Brain computer interfaces (BCIs) also offer particular promise and are likely to progress with the advent of hyperconnectivity.[15]

Geographic variations in available healthcare techniques are likely to be extremely stark, particularly given different levels of regulation around the world. China's techno-authoritarian model may result in more advanced medicine,[16] as well as more frequent accidents. The United States is likely to lag behind, with greater regulation on such practices. The EU may lag behind both jurisdictions, given the number of hurdles the General Data Protection Regulation (GDPR) would present to such a system. Complying with the GDPR's stringent requirements on personal data and security would likely only be possible after intimate medical technologies had been widely tested and deployed in other regions.

KEY FUTURE RESEARCH QUESTIONS:

- In both public and private policy realms, how do we ensure the biocompatibility[17] and cybersecurity of wearable/internal medical IoT devices?

- [Global] What variation of quality is likely in hyperconnective medical care given conceivable regulatory differences in diverse countries of implementation (e.g., China, the United States, and the EU)?

- [United States] Do current federal agencies suffice for regulation of wearable and internal IoT devices? What would sensible regulation of such devices look like?

- **What regulations can ensure consumer protection from the granular data afforded by increased wearable/internal medical devices and more frequent genome sequencing?** Data brokers and insurance companies in particular are likely to have a vested interest in procuring intimate data about individuals' health ("Genetic testing threatens the insurance industry," 2017). Shaping sensible policies for these scenarios in advance is necessary for consumer and citizen protection.

Hyperconnective and Digitized Payments Reshape Global Economics and Financial Institutions

Digital payments, already being deployed in India and extremely developed in China, will be a key feature of a hyperconnected world. India has increasingly deployed its Universal Payments Interface (UPI) system in recent years—Facebook has even made digital UPI payments possible as an experimental feature in WhatsApp.[18] Within 18 months of UPI's launch, digital payments in India totaled more than 18 years of credit card payments in the country ("India's digital platforms," 2018). Digital payments are better integrated with the financial system in India than in much of the rest of the world. ("Indians are switching to digital payments in droves," 2019). China in its own right is likely to be the country that implements digital payments most thoroughly and substantially[19]—on Alipay, the most popular form of digital payment service in the country,[20] $25 billion USD were processed in a single day in 2017 ("How mobile money is spreading," 2018). These trends will continue in a hyperconnected world as the usage of cash will continue to dwindle worldwide (Khiaonarong et al., 2019).

In both these countries and throughout the world, hyperconnectivity will enable an infrastructure for commerce that has been lacking historically. This will be a hypercharged form of the "leapfrogging" phenomenon documented in Africa in the early 21st century ("What technology can do for Africa," 2017). Remittances will be easier and more common—and will increasingly cut out banks that have historically extracted costly fees for international transfers. This market, already valued around $500 billion, will continue to grow ("The battle for the remittances market," 2018). Power dynamics of international financial institutions and national central banks are also likely to shift, with countries (such as Venezuela[21] and China) and private companies (like Facebook) moving to launch their own cryptocurrencies (Shuster, 2018; Zhong, 2019). These cryptocurrencies are likely to represent a growing portion of the economy that is not subject to traditional monetary policy and central banks.

KEY FUTURE RESEARCH QUESTIONS:

- **What will power dynamics of the financial and monetary spheres look like in a hyperconnected world?** Digital payments, decreasing use of cash, and increasing use of centralized and decentralized cryptocurrencies will reshape our current global financial system, and possibly usher in a new, post-Keynesian economic era in which central banks have less control over a growing portion of the economy. The geopolitical impact of these changes is a central question to financial and political power in a hyperconnected world.

- **What impacts will the ease of digital payments and decreasing use of cash have on poor citizens around the world?** Impacts will likely be different in various countries, especially if connectivity and infrastructure differ—the United States, EU, India, and China are all likely to offer different scenarios in this regard.

- **As digital payments increase and use of cash diminishes, what are sensible policies for gradually phasing out cash?**[22]

- **What happens to gray and black market commerce in a cashless society?**

Jekyll and Hyde—Offline Privacy Erosion, Online Privacy Erosion, and Enhancement

Arguably the area of greatest concern for a hyperconnected world is privacy. As the era of big data and digital surveillance has arrived, experts have remarked that our former definitions of privacy are ill-equipped in the modern era. This will increasingly be the case in a hyperconnected world, and the social and political implications of eroding privacy will be more salient, urgent, and in greater need of policy remedies. Several signals from past years illustrate this fact. From 2016–2018, humanity generated 90% of the data it had produced in its entire history—this fact is all the more awe-inspiring given that the "digital universe," the amount of data produced by humanity, is doubling every two years (IDC, 2014; Marr, 2018a). The digital universe is projected to grow to 175 zettabytes by 2025 (Reinsel et al., 2018). The Internet of Things (IoT) will be one of the largest drivers of this explosion, and Intel projects that the IoT will comprise 200 billion devices by 2020 alone,[23] an exponential rise since there were 2 billion in 2006 (Intel, 2019). In turn, the installation of hundreds of thousands to millions of small cell sites that underlie 5G will enable even more granular geolocation of devices (Holmes, 2018).[24]

A guarantee of the hyperconnected world is that more data will be generated and collected. Hyperconnection, particularly to remote areas, will enable surveillance of areas that have historically been unsurveillable, given the ease of transmitting video data over hyperconnected networks.[25] Surveillance equipment is also likely to be substantially cheaper—IMSI catchers alone have moved from a retail price of $400,000 to $1,400 in a matter of years (Kolker, 2016; Ooi, 2015). Vice even estimates that one can be made at home for as little as $20 (Cox, 2018). We can accordingly anticipate that surveillance devices will increasingly proliferate in the general public, both officially as a safety commodity[26] and on the black market. The weaponized usage of surveillance by not only governments, but also by private actors (companies, individuals), will increase.[27]

> The weaponized usage of surveillance by not only governments, but also by private actors (companies, individuals), will increase

Offline privacy is likely to face the most significant erosion[28] as facial recognition algorithms[29] become cheaper and easier to use, de-anonymizing machine learning techniques continue to develop and proliferate, and incidental collection increases (Chinoy, 2019; Fox-Brewster, 2018).[30] Online, a dual world is likely to exist—user-friendly encryption and cheap privacy-enhancing techniques are likely to coexist, with neither holding the upper hand permanently.[31] The market for privacy-enhancing technologies, while already robust, will grow significantly as citizen and consumer demands grow—as will a more expansive market for identity spoofing.[32] Digital masking and identity-spoofing services are likely to come into regulatory crosshairs—this is highly likely in autocratic societies, and likely to appear in liberal societies as well. Simultaneously, with the expanding digital universe, the value of open-source intelligence (OSINT) will increase[33]—this logic has already led former acting director of the CIA Michael Morell to call for a new federal agency in the United States devoted to OSINT (Zegart & Morell, 2019). Advances in digital forensics, especially in computational forensic linguistics, are also likely.

Worldwide, several policy questions related to privacy are likely to become unavoidable in a hyperconnected world. In both advertising and campaigning, the question of what constitutes fair delivery of an advertisement/message and what crosses the line into manipulation is a central policy question with which liberal democracies will have to grapple.[34]

KEY FUTURE RESEARCH QUESTIONS:

- **[United States] How can obsolete laws and norms relating to privacy be updated for a hyperconnected world and an expanding digital universe?** It is clear that the third-party doctrine defined in the *United States v. Miller* (1976) case is ill-equipped for the online era,[35] in which virtually no service can be rendered without reliance on a third-party.[36] Similarly, the adoption in 2017 of S.J.Res.34, which allows ISPs to harvest and sell consumer data, guarantees a future of cyber insecurity and opens the floodgates for new possibilities of manipulative microtargeting.[37]

- **[China] What influence will China's neo-authoritarian model of absolute surveillance have on autocratic regimes worldwide?** While autocratic regimes have long used technology to consolidate control of domestic populations, China's current pursuit of totalitarian techno-surveillance represents a new, more absolute form of oppression (Buckley & Mozur, 2019; Rajagopalan, 2017).[38] This model can be conceived of as a soft-power model,[39] particularly when cognizant of the fact that autocratic regimes have long shared technology and surveillance methods (Kalathil & Boas, 2003).[40] With 67% of the world's citizens living in regimes with autocratic Internet censorship, the potential for full or partial adoption of the Chinese model around the world is high (Freedom House, 2016).

- **[China and neo-authoritarian regimes] To what extent will a lack of offline anonymity empower and/or incentivize citizen peer-to-peer surveillance in oppressive regimes?** This would be an online version of offline peer-to-peer surveillance historically seen in China, East Germany, and Iran. It has been reported that the Chinese Communist Party (CCP) already encourages offline surveillance of citizens on American university campuses, both through Chinese Scholar and Student Associations (CSSAs) and pressure on individual students[41] ("The new red scare on American campuses," 2020). This kind of "bottom-up" surveillance is also already present online in China itself, where volunteer censors are flagging content deemed to be "inappropriate" to the Party ("Year of the Rat Fink," 2020).

- **[Global] What regulations can define/prevent digital manipulation? What policies can ensure that digital campaigning and advertising maintain the informative and eschew the manipulative? Similarly, what laws and norms can be crafted to regulate the international spyware market—both in terms of technical tools and human capital?**[42]

- **What models of data ownership empower citizens and consumers while also enabling the private sector to innovate?**[43] IFTF is leading research and convenings in this area, most recently with our December 2019 *Wealth Building in the Digital Economy* summit, co-hosted with the Berggruen Institute, Aspen Institute Financial Security Program, and the Federal Reserve of St. Louis. Possible models here would include data public assets (Collington, 2019; Ternoff, 2018), data as labor (Ibarra et al., 2018), and data ownership (Lanier, 2019).

- **What consequences would the advent of quantum computing have for geopolitics?** While the possibility of at-scale quantum computing remains a wildcard, its consequences must be considered for any circumspect forecast of a hyperconnected world. The automatic decryption of nearly all stored encrypted communications around the world would unquestion-ably have dire consequences for governments, companies, and individuals worldwide (Bushwick, 2019; Emerging Technology from the arXiv, 2019; Mavroeidis et al., 2018; Schneier, 2018).[44] This scenario would also likely play out differently if quantum supremacy were achieved in secret (by a na-tion state) or publicly.

POSSIBLE AREAS OF CONCERN

Areas explored in this section display a higher degree of contingency than those in the *probable areas of concern*. While there is less certainty about how these domains will change and develop in a hyperconnected world, the questions posed by possible developments are worthy of consideration in their own right.

Bots Populi—Synthetic Media Democratizes and Spreads

Synthetic media, or media produced or altered by machines (including pictures, text, and video), presents a possible area of danger in a hyperconnected world. Signaling an awareness that synthetic media presents a real threat on their platforms, Twitter crowdsourced advice on shaping synthetic media on its platform in late 2019, and Facebook banned deepfakes on its platform in 2020 (Bickert, 2020; Harvey, 2019).

The capacity for synthetic media to produce new frontiers in disinformation has already been documented by several experts (Chesney & Citron, 2018). In 2019, social network analysis and threat intelligence company Graphika documented a campaign of nearly 1,000 fake profiles linked to the Epoch Times Media Group that were spreading disinformation on Facebook and Instagram using inauthentic profile photos made by generative adversarial networks (GANs), a form of AI that can produce realistic photos of humans (Alba, 2019; Nimmo et al., 2019). The likelihood of increased

fraud from such techniques is high—a company called Human Longevity developed an algorithm that generates probable faces based on an input genome ("Making faces: Researchers produce images of people's faces from their genomes," 2017). Such techniques offer new methods of identity creation, identity theft, and fraud.

Similarly, OpenAI, an AI-ethics research group, unveiled that it had created a bot, GPT-2, that was able to generate disinformation stories in near perfect English (Hao, 2019a, 2019d; Radford et al., 2019). While the use of Markov chain techniques to generate language is far from new, the possibility of machines generating human-like, targeted messaging at scale would present a new challenge for social media companies and users.

KEY FUTURE RESEARCH QUESTIONS IN SYNTHETIC MEDIA:

- **What rights to free speech do online profiles or algorithms have? What does sensible regulation of bots online look like?**[45]

- **Can techniques be developed to reliably discern between bot-generated text and that written by a human?**[46] **Can the same be done for audio and video?**

- **Will current trends of government and private sector engagement against deepfakes and synthetic media be enough to mitigate the potential harm these technologies pose?**

- **What are the trade-offs of authentication technologies that could be used in a synthetic media context?** How do we empower ordinary citizens, especially in developing countries, to verify the authenticity of videos without also revealing detection methods to malicious actors (Gregory, 2020; Witness.org, 2019, 2020)? Does the Global Internet Forum to Counter Terrorism (GIFCT) offer promise as a potential model for preventing the spread of false, synthetic media online?[47]

- **Hinge factors:** proactive engagement of technology platforms, academics, and civil society to shape synthetic media policies online; public sector regulation of tools

Balkanized Reality—Do You See What I See?

It is clear that technology has the power to shape how we perceive reality. Many of the topics explored in this report, including XR and AI conversational agents, have great potential to silo individuals in enclaves of irreality. In assessing its impact on society, *The Economist* compared the invention of the smartphone to that of the book ("The truly personal computer," 2015). The dangers of information abundance, particularly of an abrupt change in the amount of information available to society, were arguably first encountered after the invention of the printing press in 1440,[48] which some experts contend helped perpetuate the Hundred Years' War in Europe (Green, 2012). While different in its magnitude, a hyperconnected world presents a comparable challenge—hyperconnection will undoubtedly present humanity with a greater volume and frequency of information than ever before.

In the past two years, governments and citizens around the world have increasingly shown an interest in mobilizing diasporas and citizens abroad for their own interests.[49] Diasporas are likely to increasingly function as targets and/or propagators of dis- and misinformation[50] in the hyperconnected era. Absent meaningful regulation, disinformation-as-a-service in the form of black PR firms and peer-to-peer persuasion is likely to grow as well (Monaco & Nyst, 2018; Silverman et al., 2020).

KEY FUTURE RESEARCH QUESTIONS:

- **Can a regulatory or technical redline be drawn to distinguish ethical marketing from digital manipulation?** While difficult, the task of distinguishing welcome marketing from digital manipulation is a central question of persuasion profiling in the next decade (Calo, 2014). This question has implications for the private sector (advertising) as well as the public (digital campaigning).[51]

- **What power do current laws have to prevent election interference from the targeting of diaspora populations?** What constitutes foreign interference in diaspora communications is a difficult question for current legal paradigms to answer, and a gray area likely to be exploited in the future.

- **What technical and social methods can be developed for systematic analysis of content on encrypted chat apps?** The increasing importance of encrypted chat apps in democratic communication and dissemination of disinformation[52] is one of the next frontiers of communications research. Quantitative methods for research would benefit companies, governments, and citizens for understanding. To this end, the Digital Intelligence Lab has prototyped software to automate collection of data from particular apps and intends to use this quantitative method to expand on its prior qualitative research projects highlighting the importance of encrypted chat apps (Rebecca Chesney et al., 2018; Digital Intelligence Lab, 2018).

- **What role does WeChat play in shaping the Chinese diaspora's perception of politics in free societies?** As a walled garden application that provides nearly all online needs in one place, the application has remarkable control over how overseas Chinese perceive the societies[53] in which they live, especially if they remain enclaved in unintegrated, isolated communities. While incidents of Islamophobia and disinformation[54] on WeChat have proliferated in recent years, systematic analysis of the presence and impact of these trends is a yawning gap in research.

- **Will peer-to-peer disinformation develop as an industry?** Past years have seen the emergence of veiled peer-to-peer persuasive messaging as a service—most notably with The Spinner, a company that allows individuals to target loved ones with messages encouraging desired behavior (such as weight loss) by inserting cookie profiles on a target device (Olson, 2019; Stoppard, 2018).[55]

- **Hinge factors**: success of the technologies industries' current initiatives to counter disinformation; emergence/success of public regulation to regulate disinformation and define online persuasion/manipulation

Social and Political Ramifications of Hyperconnective AI

Another contingent question in a hyperconnected world is the role of AI, and the resulting social and policy questions that emanate from it. The 2010s saw two notable developments in AI: (1) large advances in AI driven by both hardware and software; and (2) large-scale democratization of AI, through cloud computing, hardware virtualization, free online resources, and easy-to-use packages in programming languages Python and R (Kopf, 2017, 2018). It is, however, important to note that the theory underlying modern AI advancement has existed for more than 60 years, starting with Frank Rosenblatt's perceptron research in the 1950s (Alpaydin, 2016; Rosenblatt, 1958). Whether or not AI advancement will continue at its current pace depends on the development of hardware, specifically semiconductors that are able to enhance computational power. In this regard, we agree with Google's former Global AI Policy Lead Tim Hwang that, while large-scale data sets have played an important role in the AI progress in recent years, the key limiting factor in the future is likely to be hardware (Hwang, 2018). It is also not guaranteed that the role of public enthusiasm for AI will continue to hold its current level—this is nearly as important of a factor in advancement as hardware and software specialization.[56] These contingencies make AI a field worthy of attention in a hyperconnected world, but not a guaranteed disruptor. We find the probability of increasingly specialized AI applications—including specialized hardware—the most probable scenario.

Absent significant progress in computational power, AI advances enabled by hyperconnectivity are likely to be in those applications where AI is primarily bottlenecked by connectivity—real-time machine learning processing of sensor data (in weather, medicine, autonomous vehicles, etc.) will likely see great advances. Adoption of conversational interfaces is also likely to grow substantially, with 31% of American households already owning such a device (Cassagnol, 2019). Benefits of widespread adoption here are evident—great advances in NLP, particularly in natural language understanding and computational dialectology, are highly likely with an explosion of both audio and text linguistic data. On the other hand, the power dynamics of who owns such infrastructure for conversational AI agents is worthy of consideration—open-source initiatives to democratize conversational assistants, such as Stanford's Almond, hold great potential to empower consumers by democratizing development and applications, but also hold peril for abuse (Campagna et al., 2017; Markoff, 2019). The development of malicious "skills"[57] on AI voice assistants is a similar danger that should be planned for.

KEY FUTURE RESEARCH QUESTIONS:

- **What are the benefits and/or dangers of democratized, advanced, open-source AI conversational agents such as Almond?** Early optimism about the benefits of widespread communications technology adoption on social media and the Web 2.0 at large proved to be myopic. Do similar dangers exist for the democratization of advanced conversational agent technologies?

- **[China/United States] In a scenario of Chinese AI supremacy,[58] how do public and private regulations on digital privacy and digital civil liberties change in liberal democracies in order to compete with the Chinese market?** The U.S. National Security Commission on AI (NSCAI) has already considered recommending that the U.S. government pools data with "all democratic nations" to remain competitive[59] (National Security Commission on Artificial Intelligence, 2019; Smith, 2019). The impacts of such changes for liberal democracies and citizens worldwide is worthy of further research.

- **Will trends in the democratization and usability of AI continue as in the 2010s? What factors are most likely to impact this?**

- **Hinge Factors:** Will computational power grow at the same rate as in previous decades, or will it be limited by the diminishing returns of Moore's Law? To what extent will increased cloud computing act as a substitute for enhancing computational power? Will AI applications continue to develop along specialized, specific domains, or will strong/general AI become more feasible?

Automating Inequality—Labor Market Displacement

Another arena in which hyperconnectivity is likely to have an impact is labor. The impact of hyperconnectivity on labor is characterized by (1) the technical expertise necessary to create and maintain hyperconnected technologies and (2) the shifts in nontechnical jobs that result from changes brought about by hyperconnected technologies. AI is anticipated to account for 10% of gross world product in 2030, and technological skills are estimated to comprise 17% of total hours worked (Bughin et al., 2018; OECD, 2018). Technical expertise will be required not only to collect the immense amount of data generated in a hyperconnected world, but also subsequently to store and prepare the data, write and train algorithms, and develop applications (Stanton et al., 2019). Data preparation, which necessitates highly skilled engineers to clean raw data and less-skilled human reviewers[60] to manually classify the data, is especially labor intensive. Far and away, the largest numbers of science, technology, engineering, and mathematics (STEM) graduates are from China and India, while the United States and China lead in terms of monetary investment into machine learning, indicating that these three countries are likely to dominate the highly technical realm (Stanton et al., 2019). It remains to be seen which countries will dominate the less-skilled labor market of data labeling, which in some cases requires digital literacy but not English literacy. Such division of labor is likely to exacerbate socioeconomic inequality, particularly between and within countries.

Increasing socioeconomic inequality through division of highly skilled and less skilled technical labor is not the only worrisome consequence of hyperconnectivity. Roughly one-fifth of time in the workforce is spent completing physical activities or operating machinery in predictable environments (Chui et al., 2016). These jobs, largely in retail, manufacturing, and food services and hospitality, are most susceptible to automation (Chui et al., 2016). Unfortunately, in the United States, job displacement due to automation is borne disproportionately by minority racial groups.[61] Beyond increases in racial inequality, there is also a high likelihood of increased socioeconomic inequality in nontechnical labor—the truck driving industry being a notable example.[62] Given that driverless trucks could save the industry an estimated $168 billion a year, there are pressures to automate, but the future of truck drivers is less clear (Shanker et al., 2013). We note an important caveat highlighted by experts that the technical ability to automate a job is a necessary, but not sufficient, condition to replacing human labor with machine labor. Social and political factors are often equally important in determining whether a job becomes automated (Hwang, 2018).

...a hyperconnected world holds potential to greatly increase inequality.

Finally, a hyperconnected world holds potential to greatly increase inequality. In assessing the dynamics at play in the machine learning value supply chain, the Carnegie Endowment for International Peace notes: *"Taken together [...] impacts suggest increasing inequality between and within countries—a different trend than what took place over the last quarter century, when globalized industrial manufacturing increased inequality within countries but decreased inequality across countries"* (Stanton et al., 2019). We find this assessment to be well-founded and believe it to be a key policy question for the future of global labor and economics.

KEY FUTURE RESEARCH QUESTIONS:

- **How will hyperconnectivity, AI, and automation affect the geopolitics of labor?** The likelihood of a permanent need for short-term contract workers labeling data for at-scale machine learning applications is high. Microsoft Research senior researcher Mary Gray has deemed such work "ghost work" due to its invisibility on the front-end of AI products (Chen, 2019; Gray & Suri, 2019).

- **What policy or technological possibilities exist for mitigating economic and social consequences of an unequal rollout of hyperconnected technologies?** Within a domestic context, staggered or unequally distributed rollout of hyperconnectivity holds potential to exacerbate an already growing urban-rural cultural divide. Internationally, inequality between countries could grow—the possibility of a stratified value chain,[63] particularly for machine learning, would be one scenario likely to exacerbate global inequality.

- **Hinge factors:** potential for social and cultural movements opposing the elimination of automating jobs; whether companies and governments (in China and the United States) will support open diffusion of high-value aspects of the AI value chain to other societies

The Silicon Footprint—Environmental Impact of Hyperconnected Technologies

One relatively under-considered area of a hyperconnected future is the environment. It has recently been discovered that data-intensive algorithms, such as at-scale machine learning training algorithms, are much more energy-intensive than was previously assumed. This fact, coupled with a surge in the number of connected devices worldwide, makes it highly probable that the environmental impact of hyperconnected technologies will be substantial and should be planned for.

The materialization and integration of hyperconnected technologies is extremely energy- and infrastructure-intensive. Not only are requisite components[64] for a 5G network energy-intensive to manufacture and install, but the power consumption of the base stations themselves is estimated to be three times greater than that of 4G LTE base stations (Chen & Ng, 2019; Clark, 2019). In general, it is feared that "higher data rates can only be achieved by consuming more energy" [65] (Energy RealPolitik, 2019; Van Chien et al., 2016). Beyond 5G, hyperconnectivity will likely continue to incorporate machine learning, AI, and blockchain technologies,[66] among other energy-intensive advancements. In 2019, researchers discovered that the process of building and training of one large AI natural language processing model can emit more than "five times the lifetime emissions of the average American car," or 626,000 pounds of carbon dioxide (Hao, 2019b, 2019c). Such immense energy requirements are not only environmentally damaging, but are also financially costly, limiting the number and diversity of researchers who are able to access the necessary computational resources (Hao, 2019b; Schwartz et al., 2019). These facts considered together increase the probability that the net environmental impact of a hyperconnected world will be negative.

KEY FUTURE RESEARCH QUESTIONS:

- **What will the environmental impact of at-scale AI and hyperconnectivity be? What regulations can be crafted to reduce the negative externalities of such technologies, particularly in the context of climate change?**

- **Will the potential for energy optimization of IoT devices offset the energy needs of substantially more devices and at-scale AI applications? What will be the net carbon footprint of these countervailing forces?**

- **[United States/China] What possibilities for climate cooperation exist between the United States and China?** Given dire predictions about the impacts of climate change, how can the world's largest AI powers and carbon dioxide emitters find cooperation opportunities that would reduce climate change's effects? Federal funding for research and development into climate change, particularly in the form of university STEM partnerships between these two countries, would hold great promise for helping mitigate these problems. As the relationship between the United States and China deteriorates and visas for Chinese students decline, solutions in this area would hold promise for U.S.-China relations and the world at large ("The new red scare on American campuses," 2020; Zakaria, 2019).

- **Hinge Factors:** Will the IoT's promise of offering energy-optimized uses of technology offset the clear environmental cost of higher connectivity and increased use of energy-intensive AI applications?

Key Elements of a Hyperconnected World

In the second half of this report, we synthesize discussion topics from the IFTF expert workshop and then further use IFTF's forecasting techniques to capture the experts' discussions of how a hyperconnected world may be differentiated in four different societal scenarios.

TAKEAWAYS FROM THE WORKSHOP

Charged with doing a forecast about the technologies and user experiences of the hyperconnected world in the period from 2030–2040, IFTF approached the topic by considering four key high-level elements:

1. Conversational Computing and AI

2. Immersive User Experiences

3. Robots, Drones, Exoskeletons, and Autonomous Vehicles

4. Extreme Network Capabilities

The hyperconnected world will be a sea change—forever altering how people work, play, learn, eat, shop, get around, get fit, stay healthy, and entertain themselves and each other. Computation will shift from operating with data and abstractions to sensing and manipulating the physical world. Powerful machine learning and AI coupled with conversational computing will fuel new forms of user experiences. Game-changing immersive user experiences will be powered by agile wireless and fixed networks with embedded computation and storage. The workplace will become a hyper-intelligent space where people and intelligent agents convene in network-augmented and virtual spaces, enabling flexible collaboration, seamless sharing, and amplified individual work. Unfortunately, alongside all of these positives, cybersecurity will transition from episodic disruptions to a constant concern, as highlighted in Part I.

One complication with any technology forecast, and that came up repeatedly in the expert workshop, is the fact that major shifts like the hyperconnected world will not play out the same in the myriad conditions seen around the globe. Building on viewpoints and concerns expressed in the workshop, we addressed that problem by applying different lenses—growth, collapse, constrain, transformation—to illuminate how hyperconnectivity will show up and play out under different conditions; hence, we address plural hyperconnected worlds in this report.

1. Conversational Computing Becomes Personalized and Ubiquitous

Conversational computing systems could evolve along several different paths, depending on market forces and other factors. One path could lead to a system in which each user has a single conversational agent that serves as a primary proxy to the hyperconnected world. Another path might result in a system with a wide variety of conversational agents, each dedicated to a specific area (e.g., our personal agent, our apartment/home, our car, or our workplace).

Workshop experts agreed that conversational computing will have a major impact on the user experience in the hyperconnected world of 2030 and beyond. People, in both stationary and mobile interactions, will be depending less on screens [1a] and more on conversing directly with objects in their environment and/or with an intermediary digital agent. [1b]

NLU Systems Resemble Humans

Natural language understanding (NLU) will improve to the extent that utterances will be understood nearly error-free by digital systems in the world's top languages with localization optimizations for dialect and accent. [2a] This will be accomplished partly by better recognition algorithms, but even more so by the development and spread of algorithms that will include conversational context. Instead of depending on understanding spoken language at a word-by-word or utterance-by-utterance level, this new form of interaction will be having natural conversations with users, grasping the subject matter and context of an exchange over minutes, hours, days, or weeks. [2b] Rather than having users completely repeat misunderstood requests, such systems can ask for specific clarifications of particular portions of an exchange, use prior exchanges to make assumptions about what was intended, and even predict what a user is going to request or say.

Conversational computing also will advance to the point of operating naturally and seamlessly with the rest of the hyperconnected world. Not only will applications have the ability to draw upon the resources of cloud computing for reasoning and data about a complex request, they will be able to take a vast assortment of actions with networks of other connected sensors and actuators. [3] In a mature semantic web, systems will discover devices, both local and remote, as well as coordinate with other systems for accomplishing user requests, arranging scheduling and payment for third-party offerings, and orchestrating diverse system capabilities to accomplish complicated outcomes. [4] Dedicated apps to control connected devices will no longer be necessary, and if interactions need a screen or other modality to best communicate details with a user, whatever is required (e.g., an available display surface) will be identified and commandeered for the duration of the interaction.

On-Device Processing as Potential Means to Enhance Privacy in Conversational Systems

A major privacy concern with conversational computing is the amount of speech analysis currently done on cloud computing infrastructure. This situation will be improved in the forecast time frame by moving more and more of the compute processes necessary for conversational computing to terminal devices. [5a] Our personal devices will run the algorithms for many of these conversational interactions, so that fewer recordings of our voices are going to the cloud for analysis, with a further benefit of making the systems respond faster. [5b] Parents will not need to be concerned about who or what is listening in on the child's play, or about a doll or toy truck slyly trying to market to their kids (any more so than they innately do already). In fact, computational computing systems may actually become tailored to the value systems of a household and nudge users to options consistent with those values, like providing educational responses, making sustainable suggestions, or even responding in ways that are aligned with religious beliefs (or deferring sensitive issues to parents or the family priest/pastor/rabbi). [6]

Conversational Agents Adapt to Users' Lives and Personalities

Conversational computing will also become attentive to user moods and proclivities. [7] [8] Affective computing will use the fusion of information from a wide variety of sensors, including vocal cues and biometrics, to appropriately respond to a user's emotional state. [9] If agitation is detected, a conversational computing agent may become more patient and understanding and try to simplify choices, as well as deferring particular topics until later. These advanced affective computing systems also contribute their data to help assess overall health and wellness. Wearables and possibly even implantables in the hyperconnected ecosystem will be providing medical-grade health monitoring for determining various precision-health interventions and continuous-health nudges (which will likely be communicated via the conversational agents). [10]

Conversational agents will fill many practical roles in users' lives, from the obvious ones like personal assistant, secretary, or butler, to lawyer, accountant, nutritionist, nurse, teacher, or personal trainer. How this will play out from a user experience perspective, and how it will be monetized, is yet to be seen, but there is little doubt that this is an unmet need, particularly in communities where such resources are scarce or prohibitively expensive. [11] These systems will even help alleviate loneliness and depression, acting as a silly or dear pet, a confidant, one's confessor, or a close friend, by developing sophisticated behaviors and personas that are tailored to their end users. [12]

Expert opinions were mixed about how the various conversational computing systems will manifest, in terms of whether a typical user will be interacting with a single conversational agent who becomes their primary proxy to myriad other such systems, or whether market forces and other factors will have us interacting with a variety of conversational systems (e.g., our personal agent, our apartment/home, our car, or our workplace). [13]

All of this will be fueled by an extensive underpinning of machine learning and AI that will be modeling our behaviors and preferences, anticipating our needs and wants, and working to deliver improved day-to-day experiences. Digital twins, and perhaps more than one, of many people around the world will be simulating our possible futures, working to relieve us of mundane tasks, and helping us make wise choices. [14]

> These systems will even help alleviate loneliness and depression, acting as a silly or dear pet, a confidant, one's confessor, or a close friend, by developing sophisticated behaviors and personas that are tailored to their end users.

Hyperconnection Enables the Semantic Web in Professional and Educational Settings

Many professions will experience this melding with the digital world. [15] [16] Typical work will involve working in concert with digital intelligences that have the capability to perform instant analysis and simulation, as well as initiate entailments of business decisions. [17] [18] [19] [20] These tightly knit person-machine pairs, coined "centaurs," will proliferate, with the human halves providing swift judgment, general intelligence, and intuition that algorithms are still developing. [21] [22]

Taking the creative discipline of design as an example, there are myriad roles that applied machine intelligence can take, although the current inscrutability of AI results is hindering adoption. [23] [24] Need or trend identification can be culled from the vast amounts of data being gathered about peoples' behavior by devices and sensors in the hyperconnected world. At the low end (although perhaps a poor use of resources), social media can be mined for memes that can be used to create the next day's clever-saying coffee mug (which hopefully gets recycled for the day after). But, just as fads and fashions can be identified early, so can these deeper trends, critical strategies, and emerging technologies that the centaur workforce can help implement and deploy.

AI and machine learning will also allow designers to pursue higher goals, like strategies for sustainability or humane materials. Designers (and many other fields) will benefit from both better interdisciplinary collaborations and centaur relationships with machine intelligence to optimize designs for production, determine the best materials and processes, select geometry and palette for a given demographic, initiate distributed production by a well-treated workforce, minimize lifetime carbon footprint, prioritize effective distribution channels, and more. [25] [26] [27] The pace at which changes in these capabilities happen in the 2030–2040 time frame will necessitate human-machine collaboration. In a hyperconnected world, powered by vast amounts of data that allows for life-cycle accounting and impact analysis, we can aim for a satisfying *and* sustainable relationship with products that have minimal negative impacts on the planet. [28]

2. Immersive User Experiences—VR/MR/AR, Holograms, Projection Mapping, and More

In addition to conversational computing, the convened experts at IFTF discussed how the hyperconnected world will be characterized by myriad immersive user experiences. Whether at work, at school, while shopping, during transportation, in our homes, or at play—every setting will offer opportunities for personalized digital experiences. Sometimes as isolated visual experiences, but often in combination with conversational computing, immersion will transform daily life and potentially replace a large percentage of the interactions we currently experience on external screens and handhelds. And those screens will have transformed too, into compact folding and rolling OLED and micro-LED surfaces and brilliant projections that we deploy only when needed. [29]

...the hyperconnected world will be characterized by myriad immersive user experiences.

Many computational interactions are currently dependent on visual stimuli, typically presented on pixel-mapped screens. A variety of VR/MR/AR delivery techniques will reach technical maturity and replace these external screens, presenting visual stimuli more directly to our eyes. Close-proximity screens (unattractive boxes worn on faces) currently dominate this field and curtail widespread adoption, but other methods will be included in the mix during the forecast period (e.g., holographic waveguide glasses [30], direct retinal projection [31], and even contact lenses [32]).

Immersive XR Proliferates on Sleek, Wireless Devices

The distinctions between virtual reality, augmented reality, and mixed reality, already blurred, will likely vaporize completely by 2030. Again, the early days of virtual reality were characterized by awkward, unattractive, and heavy display goggles worn on the head, often tethered to external computers and power sources, but by 2030 these will rapidly give way to more agile and convenient developments with a radically improved appearance and UX. Moreover, once a cosmetically acceptable solution appears, we predict a rapid adoption, with broader proliferation in the 2030–2040 period. [33]

Limitations in field of view and pixel count will be replaced by high-resolution and wide field-of-view experiences that are largely indistinguishable from our current view of the real world. High frame rates, improved sensing, and faster computation will eliminate distracting lag and reduce discomfort that plagued early virtual and augmented reality experiences and limited the sense of immersion. As we head to 2040, further improvements in functionality and cosmetics, as well as practicalities like power consumption and weight, will make everyday wear of the devices an option for many (and a necessity for some professionals). Initial inroads, likely in enterprise applications, will rapidly be overtaken by a surge from widespread consumer adoption. [34] [35]

Expect a wide variety of mixed reality modalities to emerge, with bone conduction binaural sound [36a] for audio localization and pinnae-shape and environmental cues [36b] providing more of the psychoacoustics required for effective in-world sources. Other sensory outputs will be deployed for specialized settings, with haptic chairs [37] and suits being widely used by gamers, [38] and olfactory and taste output gaining a foothold in the display space. [39] A plethora of input and output modes will battle for market share for interactivity [40], ranging from whole-body engagement to subtle muscle activity that can be used in public without detection. Massive battles will be fought for attention, from entertainment to gaming to virtual travel to celebrity ghosting to wayfinding and on-the-move shopping.

Environmental Immersion Arrives in AR

On the augmented reality end of the spectrum, rapid advances in environmental databases and SLAM (simultaneous localization and mapping) will bring pixel-perfect overlays onto the real world into fruition. [41] A vast improvement over the vague place labels and virtual pushpins of early applications, these advances will allow users to experience a seamless blend of real-world and synthetic objects everywhere. Augmented and mixed reality experiences will amplify distracted behaviors in public to unprecedented heights, and further complicate municipalities' struggles to deal with the balance of device use and public safety (remember the early days of Pokémon GO). [42]

> Augmented and mixed reality experiences will amplify distracted behaviors in public to unprecedented heights.

These personalized experiences will not be limited to those with special eyewear. [43] Advances in multiview displays will direct different content to different people looking at the same screens in public locations, based on tracking algorithms as well as individual identification or demographic characterization via facial recognition algorithms. Personalized experiences will extend into other forms of public displays, with projection mapping and (later) holograms fighting for attention and market share.

Transportation environments, especially as more users become passengers in hyperconnected mobility services and as autonomous vehicles enter the mix, provide a perfect moment for immersive user experiences. Vendors can create highly curated experiences in the enclosed and controlled interior of vehicles, optimally suited for consuming curated content, perfectly outfitted with props for participating in particular e-games or professional sports, or utilizing the unpredictability of the outside environment as inputs for serendipitous gaming. [44]

"Disconnecting" Becomes a Value In Itself

There is a growing sentiment, forecast here as an outlier, that the most valuable user experience in the 2030–2040 time frame will actually be a *lack* of stimulation. People will pay to have their worlds simplified and quieted, and to be free of the hyperstimulation of targeted advertising and ever-present entertainment offerings. Far beyond the device-free time of the Unplug Days of the 2010s, this can be seen as a revolt against the intrusions and unwelcome control that digital technologies (and the companies that create them) have come to represent in users' lives. The irony is that additional technology is among the ways being used to accomplish this.

As highlighted in Part I, the diversity of new experiences offered by XR, particularly in tandem with AI, are also likely to present new challenges for democratic communication, particularly in the realm of synthetic media.

3. Robots, Autonomous Vehicles, and Drones

The transportation system, for people and goods, will see major transitions leading up to and throughout the years 2030–2040. Fleets will electrify and shift away from privately-owned vehicles to a gradual introduction of autonomous vehicles. [45] [46] [47] [48] New vehicle types will continue to enter the mix, especially in urban areas where congestion concerns will pressure cities into encouraging mass- and midi-transport. [49] [50] Electric bikes will continue to be joined by new forms of personal last-mile options (e.g., electric scooters and skateboards), and will be augmented by novel forms of enclosed personal transport for the less adventurous. [51] The overall vehicle mix will continue to see a higher degree of specialization, including more nimble human and computer-controlled package delivery vehicles.

Dawn of the Robo-tariat—Drones and Robots Become Pervasive in Industrial Settings

The role and import of drones in the overall transportation ecosystem are uncertain, but given their high degree of mobility and immunity to traffic congestion, the presence of drones will certainly expand. Delivery drones will make inroads in many industrial settings, but noise and safety concerns will likely initially limit their adoption in residential settings. The forecast period will most certainly see the adoption and spread of passenger drones, highly influenced and regimented by different legislative restrictions (both at state and local levels), safety concerns, and economic disparities. [52]

The hyperconnected world will see a radical influx of robots in a variety of forms. The industrial deployment of robots will continue to relieve workers of the most tedious and exacting tasks in manufacturing settings, and will do so with increasing autonomy enabled by a hyperconnected world that integrates design, manufacturing planning, supply chain management, and fulfillment. [53] People will increasingly be working in concert with *cobots*—machines designed to function safely alongside and among people—partly because humans still outperform dedicated automation for many assembly tasks. [54] [55] Early deployments in assembly work will expand into more unstructured settings like auto service, surgery, and dentistry, and finally move down into food preparation, retail settings, delivery of goods, health care, and more. These developments are likely to have impacts on the labor market, both domestically in the United States and worldwide, discussed later.

> People will increasingly be working in concert with *cobots*—machines designed to function safely alongside and among people—partly because humans still outperform dedicated automation for many assembly tasks.

Robots and Robo-Human Hardware Enhance Everyday Life

Robots in the hyperconnected world will not be limited to work settings. Our homes, restaurants, and entertainment will be populated by robots doing myriad tasks, commanded and orchestrated by our conversational computing infrastructure, communicating amongst each other and collaborating to accomplish tasks that require multiple skills and capabilities, and making people's lives simpler and easier—at least for those with the means to afford them. [56] Our aging population will be aided by robots for health care and daily life, extending independent living, reducing depression and isolation, and easing demands on the medical and assisted-living sectors. [57] Social robots become an integral part of a more engaging and involving educational system for all ages, and will entertain the youth in all of us. [58]

In some cases, the functionality of robotics will become even more closely coupled to people on a physical level. Exoskeletons will be deployed in industrial work to aid humans in tasks and settings that involve heavy lifting (e.g., vehicle assembly or luggage handling). [59] [60] People with limited mobility, neurological impairments, and even the aged will also be assisted by exoskeletons. During 2030–2040 we will see an explicit blending of humans and technology to augment and bring out the strengths of humans and machines alike.

4. Networks—Fast, Quick, Adaptive, Versatile

A hyperconnected world must be…well…connected. While data rates and latencies vary greatly by application, all of the devices that are participating in a hyperconnected world will require some level of communication link to other confederating devices, and often to the outside world, for retrieving required data, offloading advanced computation, orchestrating with other devices, and, of course, streaming content (admittedly a data stream, but worth highlighting as a special sort).

High-speed networks will certainly open a whole host of new applications around traditional and immersive streaming and storytelling content. Vast collections of high-bandwidth streams of traditional entertainment and other demanding applications like virtual travel will be available on any device, but that's just the tip of the iceberg. Myriad livestreams between individuals and voyeuristic curated streams from settings and celebrities of all stripes will be possible without clogging the system. [61a] Gaming content for mobile VR and AR will be enabled, using the powerful computation and graphic performance of terminal devices, but also utilizing the low latency of the network to support collaborative gameplay and content that is pixel-registered to the real world. To accomplish this, storage of relevant data will be moved closer to edge, to the places where it's needed, facilitating SLAM algorithms and supporting offloading of compute loads to distributed servers. [61b]

Diversity of Hyperconnective Experience, Especially in Urban and Rural Environments

The proliferation of 5G services will allow vastly improved network performance in situations that present severe connectivity challenges, like dense urban centers, sports and entertainment stadiums, and other concentrated communication situations. Such settings will continue to generate increasing numbers of high-bandwidth feeds, delivering them to millions of users, both local and remote. Sports fans will be able to ride along with their favorite cyclist in the Tour de France, take in an exhilarating 360-degree vista from someone climbing El Cap, ride along with a car in the Indy 500, or experience the real-time challenges of their favorite quarterback in the Super Bowl. [62]

The speediest 5G networks bring new challenges for deployment, particularly because they demand line of sight from transmitting antenna to the receiver, but will be augmented by fixed wireless technology (think rooftop routers to bring the signals into buildings), and an increasingly pervasive carpet of seamlessly available Wi-Fi services. Users will largely be freed from the burden of locating and joining hotspots by new flavors of Wi-Fi, including while in transit.

Not every hyperconnected experience requires high bandwidth or low latency. Others simply require complete coverage and inexpensive ways of being on the network. [MO 64] Alongside the development of flagship high-performance networks will be a top-to-bottom stack of appropriate services that will let every device, for every range of required network traffic, participate in the hyperconnected world. While cellular will be a major player, new types of Wi-Fi (e.g., 802.11ah "HaLow" and 802.11af "White-Fi") are also coming online that are more targeted toward longer-distance connectivity than traditional Wi-Fi.

Cybersecurity Becomes a Greater Concern with Larger, More Densely Connected Networks

This hyperconnected world, however, with its proliferation of devices and services (especially with the APIs required to operate as intended and bug fixes and capabilities added from afar), will be a cybersecurity nightmare. [63] [64] Vast databases will continue to be breached on a regular basis, with legislative measures and courts continuing to be ineffective measures for forcing corporations to really take cybersecurity seriously. [65] [66]

Not that taking things seriously is an obvious technical direction. Cybersecurity is essentially a technological war being fought by everybody—ordinary individuals, hackers, corporations, civic institutions, terrorists, and more. New exploits arise as quickly as old ones get addressed. [67]

End users have a real need for security, especially when their hyperconnected world is rife with cameras and microphones. But the hyperconnected world is bringing more and more pieces of high-stakes infrastructure and high-impact systems into the mix. Refineries and water systems. Banking and trading. Transit and shipping. Towns and factories. The range of what can go wrong varies, but the commonality is that no system can be considered totally secure any longer, and the smarter strategies *assume* that an incursion will happen. [68]

Both sides of this war are using more and more sophisticated machine learning tools to discover and patch vulnerabilities. [69] Some of the tools actually use algorithms to create and breed code to find new avenues to use for attacks. The hyperconnected world offers so many new opportunities for exploits, though, and these smaller devices, often hurriedly developed and seldom patched, can be exploited directly or enlisted to perform devious tasks for hackers of all stripes.

Growth of Personal Privacy Products, Increase in Personal Data Breaches

End-to-end security fabrics and widely deployed cryptography will help parties survive the slow transition to a more secure foundation, and blockchain technology shows promise for addressing some security concerns, while quantum computing lurks as a potential disruption to traditional compute-intensive protections. [70] [71] [72] [73] [74]

A related issue that will play out over the coming decade and well into the 2030–2040 time frame is leaks of private data and misuses of collected data, especially when such data is pooled. As a recent security camera breach showed, the sanctity of our homes can easily be breached by careless software implementations, default and/or insecure passwords, and other exploits. Pooled data can become overly intrusive as well. For example, when automotive license plate image collection (by meter maids, police cruisers, and for bridge tolls) is amassed, it can clearly put together the comings and goings of individuals.

Many workshop attendees were of the opinion that the privacy worm had irrevocably turned, and the public's expectations and earlier rights to privacy were forever surrendered. Others believed that a backlash is still coming, but even they thought that operationalizing any major changes might be impossible. Later in this document we take a deeper look at privacy, both online and offline, as well as cybersecurity concerns within specific areas of interest, such as synthetic media and hyperconnective medicine.

By 2030, the 5G rollout and dissemination will largely be complete. Urban areas will be well-serviced, and rural areas will be doing as well as they ever will, in terms of coverage and bandwidth, given the limitations of the technology. Note that it isn't just network coverage and bandwidth that

> By 2030, the 5G rollout and dissemination will largely be complete.

are reduced in rural settings, but the low-latency computing and storage capabilities of the 5G rollout will be absent or severely curtailed as well. This phenomena will likely only aggravate the increasing digital gap between rural and urban populations.

The hyperconnected world will not only be driven by long-lasting, high-bandwidth, and low-latency connections. It will also be marked by billions of low-speed, low-bandwidth, and very low cost connections. A chirp of a data point here, a quick status change there, a burst of data to keep everybody synchronized—all for a fraction of a cent, in a fraction of a second. Not only are these kinds of services not going away, they will become an increasingly critical part of the cellular data mix.

HYPERCONNECTIVITY IN ALTERNATIVE FUTURES

From the discussion above, it should be clear that the hyperconnected world holds vast potential and embodies significant extensions and departures from current technology. Embedded throughout the forecasts, though, are caveats—the hyperconnected future will play out different ways in differing local conditions. For example, it may stall in places where the required investment doesn't make economic sense. Or the activities it enables may not be embraced by some communities, or by some leaders. To examine these sorts of variations, this report uses an IFTF customization of a forecasting tool initially developed by Dr. Jim Dator at the Manoa School of Future Studies at the University of Hawaii.

Based on his years of forecasting work and his founding of the first futures forecasting curriculum in the world, Professor Dator observed that every forecast could get lumped in one of four general categories of possibilities. In turn, these four categories allowed forecasts to discuss general characteristics of futures in those conditions. In our particular case, laying out these canonical futures will allow us to forecast how the hyperconnected world will play out differently in the four variants of the future. The canonical future scenarios are:

1. **Continued Growth**—A future in which current conditions persist, including continued historical exponential growth in economic development, science and technology, cultural complexity, etc. Examples of this might be cities like Istanbul or Dhaka.

2. **Collapse and Decline—**A future in which conditions deteriorate from their present levels, and some critical systems fail, due to a confluence of probable, possible, and wildcard factors (e.g., economic, political, environmental, and social). Examples of this might be Venezuela, São Paulo or Johannesburg.

3. **Constraint and Limits—**A future in which we encounter resource-based limits to GROWTH, such as if a sustainability regime emerges, slowing previous growth and organizing around values that are ancient, traditional, natural, ideologically-correct, or God-given. An example here might be Beijing.

4. **Transformation—**A future of disruptive emergence "high tech" or "high spirit," with the conclusion of some current patterns/values (again, economic, political, environmental, social, etc.) and the development of new ones, rather than the return to older, traditional ways. This innovation-based regime may actually exhibit new and even steeper growth, or may taper to more sustainable levels. Examples here might be London or Stockholm.

While these canonical scenarios can be used to discuss how hyperconnected technology will tend to unfold in particular places, the findings here should be interpreted as general guidelines. In every scenario there will be exceptions, and the geographies of these canonical scenarios are not fixed. A large municipality—take London, for instance—will have people and places that operate in differing canonical scenarios. Further, these canonical scenarios are somewhat localized, and appear in parallel (although a global catastrophe could conceivably put the entire planet into a Collapse scenario, and some entire countries may operate within a Constraint scenario).

These scenarios should not necessarily be ranked in any way. Each one can exhibit advantages and disadvantages for users and for technology alike. Examining major hyperconnected world sectors through the four scenario lenses will illuminate how futures that fit these patterns will manifest.

1. Growth—Islands of Things

Growth scenarios will be distinguished by an assortment of major commercial players aggressively vying for market share. Limited incentives for collaboration and cooperation will result in a fragmented and confusing user experience in many sectors.

For example, a growth scenario for conversational agents pits major tech companies against one another, each working on their own conversational computing technology. Advances in natural language understanding, context aware conversational exchanges, the range of languages supported, and even the actions that can be taken in response to the interactions will largely be driven by privately-held ecosystems. The currently dominant players like Alexa and Google are likely to continue to advance, but they will be met by other players (e.g., Samsung's Nemo [75]) hoping to capitalize on some angle to gain market share in either a general-purpose or sector-specific setting. While this strategy makes commercial sense, it can result in a confusing, fragmented user experience that doesn't fully exploit the possibilities of a more integrated ecosystem.

AI in a growth scenario will similarly exhibit proprietary tendencies that, while being highly advanced, will be hampered by fragmentation and "islands of things" implementation strategies. That said, some of the players may extend their market dominance by licensing or even releasing key portions of their code base to smaller players who wouldn't have the resources necessary to pursue cutting-edge technology on their own (e.g., embedding Alexa, or using Google's TensorFlow). This would be a logical extension of the present day, where companies—big and small—must depend in some way on one of the "frightful five" technology conglomerates (Apple, Amazon, Facebook, Google, and Microsoft) to be successful (Manjoo, 2017).

Paradoxically, this Islands of Things form of market-share driven development will extend across much of the realm of the growth-scenario hyperconnected world. The field of immersive experiences, both in terms of technologies and content, will tend to appear in compelling but poorly-integrated forms. Platforms and delivery systems will partner with corporations and studios to deliver particular shows, characters, and worlds, promote brands, and differentiate themselves to claim market share. A plethora of similar hardware will proliferate, which often proves incompatible in obscure and mysterious ways. Consumers wanting an experience may have to procure content-specific hardware and subscribe to a particular network or platform to participate.

This pattern so significantly plagues growth-scenarios that products and services arise to address it. The early days of IoT saw device control hubs. As a more historical example, think of the universal remote control. Kayak aggregated airlines and rental cars. TripAdvisor mines its reviews to offer single-touchpoint travel planning. Conversational agents in a growth scenario will undoubtedly strive to offer goods and services that require not just aggregation across brands and interfaces, but also manage the complexity of piecing together the hyperconnected world's myriad offerings. Using a quick business trip as an example, a single request could book ridesharing services, airline reservations, more ridesharing services, a hotel, dining and entertainment, more rideshares, etc. Corporations will likely have to further abandon their stranglehold on portions of brand experience in order to compete in this aggregated world (How long has it been since you bought an airline ticket from an airline?).

Network services will continue to be a competition among the major players able to afford the build-out costs for 5G. As computing and storage moves to the edge (i.e., into cell towers and base stations), carriers like Verizon, Sprint, and AT&T will have integrated services like AWS and Azure that can migrate from Cloud to Edge as needed.

In sum, the growth scenario landscape tends to spawn *"purpose-built"* systems from well-resourced forms of development, designed and deployed to provide a particular functionality, in a specific setting, for a given set of stakeholder interests. Developers are motivated to utilize a certain set of system components, develop and deploy said system rapidly and economically, and make decisions and constrain functionality in order to make rapid headway. Little attention is given to sharing and/or re-use with other stakeholder systems within the ecosystem. Very similar systems are typically developed by multiple stakeholders, and ecosystem differentiation arises from minor functional differences and/or strategic partnering. This form of development, however, presents users with a confusing array of very similar offerings. It will give rise to Islands of Things, although this topology may eventually realize the missed opportunities (functional and economic) of additional sharing and cross-pollination.

2. Collapse—Asteroid Belt of Things

Collapse scenarios experience social and economic stresses on both the public and private sectors. They will typically result in insufficient capitalization for the major infrastructure and technology commitments to fully realize a hyperconnected world, as well as a lack of private sector resources, which limits the motivation for corporations to capitalize projects. Pockets of hyperconnectivity will likely exist, but there will be other areas where the user experience of this vision will be spotty and unreliable.

The higher-end products and services of a hyperconnected future are dependent on a highly distributed infrastructure. In a collapse scenario, it is unlikely that government or industry will have the means or will to supply this infrastructure, and only a portion of the citizenry may have the resources needed to fully participate. Collapse scenarios are frequently marked by extreme disparities in wealth, so pockets of hyperconnectivity are likely, but they will often be surrounded by a mix of infrastructure deserts (some complete, like a lack of cell towers, and some relative, like 3G vs. 5G coverage).

Basic versions of hyperconnectivity will likely exist, however. Some of them may be impoverished or slowed by inadequate networks or older handsets. Others may not have the datasets to realize their potential because of the missing sensors or servers (e.g., AR without a detailed map database for SLAM).

Collapse scenarios often see the rise of enterprising individuals and small businesses to offer goods and especially services that fill the voids left by the absence of public and private entities. For example, if a municipality is not collecting garbage, somebody might offer a local hauling service. Hyperconnectivity is harder, though, with many moving parts, interdependent services, and a ubiquitous and reliable network required to deliver a convincing and valuable user experience.

Substandard hyperconnectivity is a compounding situation. Lower bandwidth, less available edge computing and storage, and less advanced terminal devices of all sorts erode the potential user experience. It is possible that finer-grained approximations of the hyperconnected world can be devised, for instance by carpeting a neighborhood with mesh wireless—and these efforts may provide an economical and functional substitute for some residents.

One reality of a collapse scenario is that this variant of the hyperconnected world is likely to be only lightly regulated, as compared to others. Interventions that are prohibited in other regions due to privacy concerns or even safety may be permitted. This can result in innovations that might not arise in other scenarios, but it may also put the public or environment at risk.

Unfortunately, though, many facets of hyperconnectivity boil down to money. Deploying sensors for smart infrastructure. Gathering data for mapping and other local algorithms. Creating speech models for local dialects and accents. Purchasing sophisticated terminal devices for immersive experiences. Deploying and maintaining robots and drones. Installing equipment for vehicle-to-everything connectivity. Creating an infrastructure for autonomous vehicles. It is likely that collapse scenarios will lag significantly and not fully participate in the hyperconnected world.

A collapse scenario, then, will likely foster greater incidents of *"fragmented ad-hoc"* hyperconnected projects, resulting from a resource-limited form of development where system elements contribute to accomplish a local task without depending upon or influencing the larger ecosystem. These systems are highly pragmatic and developed on an as-needed basis, without resources for nor attention to possibilities for sharing and/or re-use. Developers are motivated to utilize that which is ready at hand, and may not be interested or able to integrate or share the fruits of their efforts for more systemic benefits at the ecosystem level. This gives rise to the **Asteroid Belt of Things**, although the resulting systems may, with sufficient enthusiasm and additional resources, scale into larger and less limited opportunities.

3. Constraint—Walled Gardens of Things

Constraint scenarios are characterized by imposed limitations in both the technological and content realms, which can result in restricted user experiences. Particularly in the content arena, fully unrestricted content may conflict with the priorities and goals of powerful interests.

Many constraint scenarios exhibit a characteristic of having highly centralized and sophisticated technologies, often concentrated in a few companies (some state-sponsored) having strong relationships with research institutions and government. These centralized and/or unified systems can be highly capable, sometimes exceeding the functionality of more laissez-faire systems development scenarios, but they can also have a single point of failure or exhibit a "brittle" quality and be harder to migrate when it becomes necessary.

Beijing, for example, recently began using their Face++ technology in the subway system, in an attempt to relieve congestion. The system also includes a social credit score, based on rider behavior (both on the subway and beyond), to determine the level of security checks a passenger would be subjected to. This dependence on a single facial recognition system is an example of where technical issues and faulty training datasets could create a single point of failure. An increasingly annoyed populace could target a specific company and potentially impact the whole system, or a hacker might find a vulnerability and bring down a large quantity of critical infrastructure.

This pattern can play out across the entire social, technical, and economic ecosystem. Stakeholders are not beholden to their consumer base, and may not have their best interests at heart. If, as another for instance, the government wants to discourage the use of a particular dialect or accent (and, one would presume, discourage those who speak it), they need only to make large portions of their infrastructure unresponsive to that language in conversational interactions. Even massive technological vectors like machine learning and AI are subject to these sorts of potholes—while Europe demands greater privacy and the United States struggles with fair training sets and explainable algorithms, China may get miles ahead in deployments where those concerns are swept under the rug.

Constraint-based scenarios, nonetheless, can have fantastic advantages. Massive infrastructure can be deployed at great speeds, with reduced attention paid to safety, privacy, and environmental concerns, often while being directly subsidized by governmental stakeholders. At the ODNI workshop, one attendee was adamant that the constraints of China would put the whole country (and especially the cities) ahead of the rest of the world in this time frame, at least in the technological space. He argued that privacy hand-wringing and parallel build-outs of massive infrastructure would cripple the rest of the world. He agreed that other scenarios might result in more resilient or more just solutions, but that China, on the face of many of these unfolding technological battles, was going to gain the upper hand.

Content, though, can take a back seat in constraint scenarios. Oftentimes, a restrictive government wants to control the narrative, normalize its bad behaviors, and shape the behaviors of society. Foreign news is curtailed. Cinema that depicts alternate ways that society could be structured are censored. Immersive user experiences are certainly among the media that may be restricted and controlled in a constraint scenario. Limits on the amount of time that a given technology (e.g., gaming consoles) can be used and what kind of content is appropriate for it are both forms of control that can be expected. [76]

On the flip side of the content coin, a constraint scenario can result in *mandated* engagement with propaganda and other forms of persuasive content. One recent example is China's "Study the Great Nation" app that is a required download for government employees. They must engage with the app daily to be eligible for jobs and promotions, and was recently revealed to be implemented in such a way that it may be spying on its users. [77]

> Dependence on a single facial recognition system is an example of where technical issues and faulty training datasets could create a single point of failure.

In sum, the constraint scenario breeds a *"strict hierarchical"* form of system architecture and deployment topology, stemming from a highly-designed, mono-functional form of development where all system elements contribute to accomplish a clearly-defined task for a very limited number of stakeholders, typically a government. The gathered data and/or resulting functions are often available only to said agency, despite its obvious utility to others in the broader ecosystem. Examples include rooftop urban pollution monitoring in China (which could be collated to inform officials about pollution patterns), or countless in-city traffic-monitoring systems for congestion control (that don't pool data for a more systemic understanding). It will give rise to **Walled Gardens of Things**, with many forbidden opportunities for utilizing these data for other purposes. This topology can also result in brittle systems that are susceptible to single-point failures, hacking, and other forms of mischief.

4. Transformation—Spiderweb of Things

Transformation scenarios embrace a diverse and expansive set of technological and content possibilities, undertaken by a wider range of stakeholders, creating what could be called an "open ecosystem." This is enabled by a vibrant community that includes the major technology players, but also comprises many startups and individual contributors who are working with open standards, versatile APIs, new modes of producing and distributing digital and physical goods, and powerful development tools and libraries.

Hyperconnectivity in transformation results in, even more so than in other scenarios, a spiderweb of connections and interactions. At an ecosystem level, this results in a constant influx of innovative goods and services, developed in an agile way that nurtures successes and doesn't punish failures too severely.

New design tools and production systems will fuel the feasibility of transformation scenarios. Digital twin technology will close the loop after products and services make it to market, but will perhaps make an equally strong contribution to model-based product design and simulation. Vast databases of components and subsystems will allow entrepreneurs to subject their ideas to simulated operation and use various conditions.

The resulting user experience can be jarring for end users, with frequent changes and innovations being introduced. However, this is sometimes balanced by APIs that allow fine-grained changes to be absorbed into a bigger ecosystem. Early signals of these sorts of innovations include the rapid incorporation of novel transport modalities like e-scooters into map/direction systems.

In summary, transformation scenarios cultivate *"open ecosystems."* These are based on a loosely confederated and highly interconnected form of development where system elements, while possibly deployed for a particular purpose, make their data and/or resulting functions available to others in the overall ecosystem for sharing and/or re-use. Developers often utilize shared resources throughout the prototyping and development process, and may be able to aggregate quite novel functionality from a mix of existing resources with only moderate amounts (typically costly, so it must be minimized) of additional technology deployment (which, in turn, is made available for others). Such scenarios give rise to the **Spiderweb of Things**, with many stakeholders empowered to develop and utilize the unfolding possibilities of these new technological forms.

Conclusion and Future Research Questions

This report has explored what the hyperconnected world of 2030–2040 will look like. In Part I, we synthesized and elaborated on the main themes explored during IFTF and ODNI's December 2019 expert workshop, *Future of the State, Society, and Security in a Hyperconnected World.* In Part II, our team delved into topics that were underexplored in our one-day workshop, including the future of crime, hyperconnective medicine, digital payment systems, offline and online privacy, synthetic media, balkanized reality, AI advancement, labor, and the environmental impact of hyperconnected technologies. This report aims to describe the technologies that will be central to a hyperconnected world, and trace the contours of the most important social and political issues likely to emerge from them. Our hope is that through rigorous futures thinking, we can help develop the foresight to help ensure that a hyperconnected world is a positive-sum game for all stakeholders.

As much of this report has highlighted, while hyperconnectivity offers much promise for advancing society, many scenarios present unprecedented challenges, and many questions still remain. In our expert opinion, further research is recommended, particularly for the *Key Future Research Questions* outlined in Part I. Backlash against both public and private abuses of technology in the past decade have highlighted the importance of advance planning for the unintended, negative consequences that technology can bring with its arrival.

In his book, *Machines of Loving Grace,* on the future of human-robot interaction, *New York Times* technology reporter John Markoff emphasizes that "how we design our [...] machines will determine the nature of our society and our economy." (Markoff, 2015). IFTF believes this principle is central to crafting both policies and technologies that will help hyperconnectivity become a principle that applies not only to the technologies discussed in this report, but to the relationships between individuals and societies that use them.

Endnotes for Part I
The Social and Political Implications of Hyperconnected Worlds

1. Sanger remarks: "*We* [the United States] *have to adjust our strategy to reflect that we will be far more vulnerable than almost any other major nation for years to come*" (Sanger, 2019, p. 326).

2. On this note, former Director for Plans and Operations for Cyber Policy in the Office of the Secretary of Defense Michael Sulmeyer writes: "*When it comes to cyberspace, however, the United States has more to lose than its adversaries because it has gone further in embracing innovation and connectivity without security*"(Sulmeyer, 2019).

3. Additional examples of at-scale exploitations that have taken the cybersecurity world by surprise in recent years abound. A noteworthy instance is the compromise of nearly half a million Cisco WiFi routers with a form of malware called VPNFilter (Greenberg, 2018a). Such compromises can be expected to become more common, especially with the drastic increase in insecure IoT devices to come in coming years. The weaponization of these devices for historically unprecedented DDoS botnet attacks, such as the Mirai botnet attack in 2016, should also be planned for (Fruhlinger, 2018).

4. As a final introductory note on cybersecurity, we share Sanger's central contention that international cyber norms and treaties must be created to ensure the safety of citizens dependent on connected technologies for nearly every facet of their lives. While we do not underestimate the difficulty of such a task, international norms have previously been crafted areas that seemed to present insurmountable challenges: including nuclear, biological and chemical weapons. The status quo of major powers holding actionable malware "implants" in one another's critical infrastructure is unsustainable—all the more so in a hyperconnected world, in which the United States is more vulnerable than any other country. Until such norms are crafted, scholar Christopher Hitchens' summation of living in the nuclear age rings truer with each passing day: *"You exist at the whim of people whose power does not derive from your own consent and who regard you as expendable, disposable. You merely failed to notice the moment at which you were conscripted"* (Hitchens, 2005).

5. For instance, healthcare data breaches cost an estimated $4 billion for US providers in 2019 (Lagasse, 2019).

6. The exploitation and/or compromise of high-value targets in both the private and public sector is likely to increase as well—a bellwether signal in this domain is the alleged involvement of Saudi Arabian government in the hack and eventual leak of information from Jeff Bezos' phone in 2019 (Srivastava, 2020).

7. According to a 2018 Pew Research Center survey, 97% of boys and 83% of girls aged 13 to 17 play video games (M. Anderson & Jiang, 2018).

8. Law Professor Mary Anne Franks of the University of Miami stated: "We are nearing a situation where inputting a person's body type with scary accuracy into scenarios where they can be raped, assaulted and even killed. You'll never know if the guy in the cubicle next to you or the guy sitting across from you on the train isn't doing exactly that on his phone."(McEvoy, 2019)

9. Professor Carla Reeves investigated the ways in which these incidents have been governed by Community Standards in the online game Second Life (Reeves, 2018).

10. Given that 90% of the reports were made by Facebook, and that many of the largest cloud sharing platforms, such as Amazon Web Services, Google Drive, Dropbox, and Microsoft One, don't scan for abuse when material is uploaded, the number is believed to be a dramatic underestimation. Additionally, there is no unified standard for identifying child abuse videos, so many platforms, including Yahoo and Snapchat, do not scan for them at all. For these reasons, the New York Times reports that these numbers only represent a portion of such content online—Frustration with slow bureaucratic response from law enforcement agencies was also reported to be a limiting factor in this regard.(Keller & Dance, 2019b).

11. In a recent standoff between Apple and Attorney General William Barr, regarding the unlocking of phones used by a terrorist who attacked a naval air station on December 6, 2019, Apple stated: "Americans do not have to choose between weakening encryption and solving investigations" (Benner, 2020).

12. See the Carnegie Endowment for International Peace's AI Global Surveillance Index (Feldstein, 2019).

[13] See Professor Michael Rich's legal framework for weighing the question of whether or not certain crimes or actions should be made impossible (Rich, 2012).

[14] A useful thought experiment here is to think of real-time and retroactive data recorded by telecommunications companies. If evidence exists that a citizen is currently surpassing the speed limit in a given jurisdiction, should he or she be arrested for that? Similarly, if retroactive data proves the same, should such a citizen be apprehended? What level of enforcement constitutes a *pretextual* or *biased* enforcement of the law? Given that most archaic or obsolete laws are simply unenforced and not formally repealed, how do we protect liberal societies from arbitrary enforcement of such laws?

[15] Several cutting-edge breakthroughs in BCIs have occurred in the last two years—such as the production of synthetic speech directly from brain signals (Anumanchipalli et al., 2019; Jeffrey-Willensky, 2019). For a deeper dive on BCI advances and signals from past years, we recommend the Economist's January 2018 Technology Quarterly on Brain Computer Interfaces.

[16] Indeed, China became the first country to conduct brain surgery through a 5G connection in 2019 *(First remote surgery in China conducted using 5G technology,* 2019).

[17] While this is likely to be an easier challenge than cybersecurity, it may prove a non-negligible challenge in this space. Ensuring that internal medical sensors are durable and do not harm their host is a necessary precursor to reliable and safe hyperconnective internal medicine.

[18] India became Facebook's largest market in 2019, in terms of both Facebook and WhatsApp users (Fuscaldo, 2019; Singh, 2019). It is worth remarking that existing UPI infrastructure in India likely helped drive Facebook to deploy an experimental playments feature in the country—an illustration of the fact that countries themselves are able to drive innovation in the private sector when infrastructure allows.

[19] China represents an especially interesting case study for digital payments—the ease of using WeChat pay andAlipay has led many establishments, including roadside noodlestands, to stop accepting cash altogether (R. Chen, 2017; Mozur & Merced, 2016). This system, in addition to having surveillance implications for domestic citizens, increasingly will be necessary for tourists in China to make purchases of any type.

[20] Several other popular forms of Chinese-owned digital payments also exist, including WeChat pay, QQ Wallet, Union Pay and Baidu Wallet (Buchholz, 2019). WeChat pay has recently begun allowing payment by facial recognition (Lee, 2019).

[21] Time magazine's reporting in 2018 that Russia helped Venezuela with key parts of its plans to launch a cryptocurrency underlines the fact that cryptocurrencies, even those that are controlled by a centralized power, are likely to reshape the power dynamics of the international monetary and financial system (Shuster, 2018). This digital strategy resembles China's movement to establish its own multilateral financial institution, the Asian Infrastructure Investment Bank, shared a similar motivation to allow the country to operate outside of the established international financial order (Zakaria, 2019).

[22] India's sudden demonetization policy in 2016, which eliminated 86% of cash in the country overnight, being a notable example of a rushed policy with several negative consequences. Some estimates put the economic cost of this policy at 1.5 million jobs and 1% of India's GDP (Safi, 2018).

[23] The privacy risks of such a large number of connected devices cannot be overstated. Current models of smartphones alone leak several types of personally identifiable information (PII) at all times, including WiFi network probesets, International Mobile Subscriber Identities (IMSI) and advertising ID numbers (Kolker, 2016; Schechner et al., 2019). Importantly, continuing a trend of recent years, what qualifies as personally identifiable information (PII) is and will increasingly be redefined in a hyperconnected world—as early as 2011 scholars had pointed out that previous, static definitions of PII were anachronistic in the modern era (P. M. Schwartz & Solove, 2011). Lawyer Paul Ohm has noted that almost all data can become "personal" when combined with supplementary datasets (Ohm, 2009). This is all the more important given that to-date, nearly all attempts to anonymize datasets have been failures. De-anonymization and re-identification of subjects in "anonymized" datasets dates back to at least the mid-90s, when Dr. Latanya Sweeney famously identified Massachusetts Governor Bill Weld in an anonymized dataset of health visits from state employees released by the Massachusetts Group Insurance Commission (N. Anderson, 2009). Since then, de-anonymization of "anonymized" datasets has occurred frequently—examples include AOL (2006), Netflix (2007), and Twitter (2009) (Bangeman, 2006; Narayanan & Shmatikov, 2007, 2009; Schneier, 2007). These cases all emphasize the fact that de-anonymization becomes easier as time goes on and more data is created and available. The implications of these facts within the context of a hyperconnected world and an ever-expanding digital universe deserve particular attention.

[24] This fact has direct implications for consumers and citizens given recent revelations that major telecoms companies (including T-Mobile, AT&T and Sprint) and third-party businesses in the United States are selling real-time location data of cell phones (Cox, 2019a, 2019b; Hollister, 2019; Thompson & Warzel, 2019).

[25] As discussed in *Computational Power and the Social Impact of Artificial Intelligence* (Hwang, 2018), hyperconnection is only one possibility for bringing greater surveillance to remote areas. With a great enough increase in hardware capabilities, on-device machine learning could enable the processing of video data with sophisticated machine learning and facial recognition algorithms. This possibility is an interesting paradox, since on-device machine learning is most traditionally thought of as a privacy-enhancing development due to decentralization of data processing. For more details on the promise of on-device machine learning techniques, see *Federated Learning: Collaborative Machine Learning without Centralized Training Data* (McMahan & Ramage, 2017) or *Federated Optimization: Distributed Optimization Beyond the Datacenter* (Konečný et al., 2015).

[26] Examples here being baby monitors or smart home surveillance devices, such as the Amazon Ring doorbell.

[27] For an examination of weaponized surveillance by governments, see *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns* (Nicholas Monaco & Nyst, 2018; Riley et al., 2018). For an examination of weaponized surveillance in the private sector, Israeli firm Blackcube's hacking and subsequent physical and digital surveillance of journalist Ronan Farrow is an informative case study (Farrow, 2019).

[28] Importantly, the erosion of offline privacy has significant implications for not only individuals, but also for corporations and governments themselves. The unintentional unveiling of top secret US military bases from the fitness app Strava illustrated the impact a lack of individual privacy can have for nation-states (Hsu, 2018). A lucid, if blithely optimistic, examination of other possible consequences for governments in a world of "ubiquitous surveillance" can be read in *The Age of Transparency* (Larkin, 2016).

[29] In late 2019 and early 2020, *The New York Times* compellingly profiled the use of facial recognition in real time to de-anonymize pedestrians in both China and the United States (Hill, 2020; Mozur & Krolik, 2019).

[30] By "incidental collection", we refer to images, video and other data containing PII of people collected unintentionally. We anticipate that police body cameras, semi-automated and automated driving systems, and smart home devices such as the Amazon Ring doorbell will be but a few of the devices whose bulk of collection will, paradoxically, be incidental collection.

[31] In this regard, we anticipate the future will largely resemble the present day. While sophisticated data collections such as browser fingerprinting currently exist, companies such as Mozilla are automating the hard work of remaining untrackable (Englehardt, 2020). Apple's implementation of easy-to-use full disk encryption, as well as the open-source and easily adaptable Signal encryption protocol are further examples of once complex, privacy-enhancing technologies that have become trivial to use and implement.

[32] The use of synthetic media, such as AI-generated photos and video, to convincingly act under a false identity, will become increasingly common for activity online in which users' wish to maintain anonymity. Signals in this area have already appeared in recent disinformation campaigns such as #OperationFFS (Nimmo et al., 2019). Companies such as the Silicon Valley-based Human Longevity are also developing techniques to generate faces from an input DNA sequence ("Making faces Researchers produce images of people's faces from their genomes," 2017). Possibilities for fraudulent abuse of such technologies in a hyperconnected world is very high.

[33] This fact has already been illustrated by several investigations from Bellingcat, a team of open-source investigators active since 2014. Several of these investigations have had geopolitical implications, including proving Russian involvement in the downing of flight MH-17 (Bellingcat Investigation Team, 2018, 2019; Schwirtz & Barry, 2018). In 2019, our team has also used open-source investigation techniques to discover unfound Chinese government assets active on Twitter and Facebook after official takedowns (Monaco, 2019).

[34] The term *"persuasion profiling"* refers to the fact that "companies can discover what motivates a given consumer and dynamically change the advertisement in real time" (Kaptein et al., 2011). Defining a "red line" between fair advertising and behavioral manipulation is a central question for both private sector advertising and digital campaigning—this topic has been explored compellingly by technology expert and lawyer Ryan Calo (Calo, 2014).

[35] While lower courts have often ruled against the third-party doctrine constituting a reasonable expectation to privacy, a Supreme Court-level ruling or legislative resolution has still not come to pass. Notable cases here include *US v. Warshak* (2010) and *State v. Petino* (2014). Other recent cases that address the physical tracking of individuals through GPS devices (including cell phones) are *United States v. Jones* (2012) and *Carpenter v. United States* (2018).

[36] Even ignoring third-party cookies and online trackers that have become ubiquitous on the web, Farhad Manjoo has compellingly described the virtual impossibility of having a successful business without relying on one of the "frightful five" technology companies (Amazon, Apple, Facebook, Google and Microsoft), which would constitute third-parties in such cases (Libert, 2019; Manjoo, 2017).

[37] This is particularly true given that Emerdata, a new company formed by former employees of Cambridge Analytica and Bell Pottinger, has been explicit about its intent to use all publicly procurable data, including search histories and information purchased from data brokers, to microtarget voters in increasingly sophisticated ways in countries around the world (Ram & O'Murchu, 2018).

[38] The Chinese "social credit system" offers a striking example of this. Expert Shazeda Ahmed has rightfully noted that many Western reactions and reports of the capabilities of the social credit system to-date have been exaggerated, given that it is mostly being used to shame public debtors (*laolai,* 老賴) for the time being. All the same, Ahmen notes that the potential for the system to grow into a coercive tool for controlling social behavior in the future certainly exists (Ahmed, 2019; Daum, 2018; Ohlberg et al., 2017).

[39] This can notably be seen in China's export of surveillance technology to countries such as Ecuador and the United States (Strumpf et al., 2017; Kessel, 2019; Mozur et al., 2019) (Strumpf et al., 2017; Kessel, 2019). China is also attempting to influence surveillance policy in more formal ways, such as driving facial recognition policy at the United Nations (Yang et al., 2019).

[40] For instance, Egypt's telecoms giant Orascom helped North Korea build its domestic telecommunications network, Koryolink; Huawei helped Iranian security forces stifle dissent at home through installation of surveillance-friendly telecommunications in 2011 (Monaco & Woolley, 2017; Schmidt & Cohen, 2014; Stecklow et al., 2011).

41 In recent weeks this dynamic has also reached new levels, with China moving to imprison one of its students who anonymously tweeted cartoons that were critical of CCP Chairman Xi Jinping while studying abroad in the US (Allen-Ebrahimian, 2020). Such incidents highlight the increasing success of the CCP in encroaching on freedom of speech, even in liberal societies (Kokalitcheva & Fischer, 2019; Monaco & Woolley, 2017).

42 By "human capital" here we mean to designate former spies or defense contractors with rare knowledge about signals intelligence. For a reference of the development of aftermarkets of such assets, see *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments* (Mazzetti et al., 2019).

43 IFTF is leading research and convenings in this area, most recently with our December 2019 *Wealth Building in the Digital Economy* summit, co-hosted with the Berggruen Institute, Aspen Institute Financial Security Program, and the Federal Reserve of St. Louis.

44 While secure, post-quantum encryption protocols already exist, it is sure a rollout of techniques would be gradual and staggered. If left unregulated, it is likely that many private entities would lag behind for decades, despite the risks. Out-of-date software that played particularly poignant roles in the 2017 NotPetya attack and the ransomware targeting of US municipal governments in 2019 with leaked NSA's malware EternalBlue (Greenberg, 2018b; Perlroth & Shane, 2019; Wakefield, 2017). These examples illustrate a fraction of the danger presented by a quantum supercomputer capable of decrypting classically encrypted documents.

45 For an insightful exploration of this topic with respect to current bot technologies, we recommend *Regulating Bot Speech* (Lamo & Calo, 2018).

46 To date, one paper has been written on this subject, *Sifting Robotic from Organic Text: A Natural Language Approach for Detecting Automation on Twitter* (E. M. Clark et al., 2016). This paper is limited to Twitter, and rests on the assailable assumption that humans are able to discern bots from humans (as do all modern bot detection techniques outside of platforms and companies). In that sense, it is a limited application, but useful as a springboard for future research efforts.

47 GIFCT has had notable successes, particularly in the development and maintenance of an image and video-hashing database that enables Twitter, Facebook and other social media companies to quickly de-platform content deemed to promote terrorism or extremism (Macdonald, 2018). WITNESS, a non-profit dedicated to using video technology to help empower citizens to protect human rights, has documented several of the failures of GIFCT, including the difficulty of assessing what qualifies as terrorist content and incidents of false-positives (Kayyali, 2018, 2020). The Digital Intelligence Lab at IFTF is particularly interested in exploring the feasibility of adapting this model to a disinformation and synthetic media context.

48 Nate Silver, data journalist and founder of FiveThirtyEight, writes compellingly about this scenario in his book *The Signal and the Noise:* "The amount of information was increasing much more rapidly than our understanding of what to do with it," writes Silver, "Paradoxically, the result of having so much more shared knowledge was increasing isolation along national and religious lines." (Silver, 2012)

49 Several examples of this have occurred since 2017. Turkey mobilized masses in the Netherlands and Germany ahead of a domestic 2017 referendum on presidential power (Escritt & Deutsch, 2017). Ahead of parliamentary elections in late 2019, India targeted Indian-heritage citizens of the UK to vote against the Labour party, in part because of their stance on Kashmir (John, 2019; Khan, 2019). Conversely, diasporas themselves have also begun to attempt influence in their countries of origin: an online astroturfing campaign calling on citizens to boycott the Macedonia's September 2018 name change referendum was in large part driven by diaspora residing outside the country (Karan, 2018).

50 We defer to Data & Society's extremely useful report *Lexicon of Lies* for defining these terms—disinformation being false information knowingly disseminated with malicious intent, and misinformation being false information spread without knowledge of its falsehood. This report is also a singularly useful reference for analyzing the diverse connotations and, in some cases, denotations of the word "propaganda" in languages around the world (Jack, 2017).

51 These questions are particularly important when considering the sense of outrage from the American electorate in 2018 after the Cambridge Analytica scandal. Even after the company's eventual dissolution, many former employees from the company and Bell Pottinger were explicit about their intent to continue microtargeting voters in the future (Ram & O'Murchu, 2018).

52 Particularly pernicious examples include the coordination of attacks on journalists and lynchings resulting from disinformation on WhatsApp in India, and the spread of anti-vaccination disinformation in Brazil (Chaturvedi, 2016; Molteni, 2018; "Why India wants to track WhatsApp messages," 2019).

53 This is particularly pernicious given China's role as the least free internet atmosphere in the world for four years running *(Freedom on the Net 2019|China,* 2019). In a sense, the CCP arguably is attempting to impose this control on its citizens even when they reside abroad in more open societies.

54 Numerous popular press outlets have documented this phenomenon in recent years (CBC News, 2019; Guo, 2017; Huang, 2018; Nuttall, 2019; Peng & Chiu, 2018; Zhang, 2019).

55 Another interesting case study occurred when an apostate Mormon ran a secretive Facebook campaign to attempt to persuade other Mormons to leave the faith (Poulsen, 2019).

56 A notable case study here is the history of machine translation, where a lack of funding and enthusiasm after a critical 1966 report form the US Automatic Language Processing Advisory Committee (ALPAC) largely kneecapped development in the field from 1966-1990 (Hutchins, 1996; Poibeau, 2017).

57 "Skills" have become the preferred term for third-party applications developed for conversational assistants such as Google Home and Amazon Echo.

58 Achieving dominance in AI research and development by 2030 is an explicit goal of the Chinese government (Mozur, 2017; Robles, 2018).

59 Eric Schmidt, the former CEO of Alphabet and current chief of the NSCAI, has been frank in his assessment that the US may have to change its views on AI to compete with China: "There's somebody on the horizon who is different in values from us who is quite capable," Schmidt said. "We should do whatever it takes to make sure that the U.S. wins in this space" (Smith, 2019).

60 While this is a characterization that is often used in popular media, we do care to add the caveat that some forms of labeling require skilled expertise—for instance, part-of-speech (PoS) tagging for NLP applications can only be performed by trained linguists.

61 For instance, by 2030, it is forecast that 25.5 percent of Hispanic/Latino jobs and 23.1 percent of African American jobs will be replaced, compared to 22.4 percent of white jobs and 21.7 percent of Asian jobs (Cook et al., 2019).

62 The potential for unequal demographic displacement if automation is deployed throughout the trucking industry is high. In the United States, 3.5 million people work as truck drivers, 90% of whom are men, making it one of the most common occupations (Cheeseman Day & Hait, 2019). They are on average older than other workers (median age 46 vs. 41) and have lower than average educational attainment (7 percent have a bachelor's degree vs. 35 percent) (Cheeseman Day & Hait, 2019).

63 The Carnegie Endowment for International Peace (CEIP) has compellingly made the case AI and the machine learning value chain contain significant risks for increasing inequality between countries. We find CEIP's tripartite conception of "fast movers", "moderate movers" and "slow starters" particularly useful for envisioning possibilities for what this sort of unequal stratification would look like (Stanton et

al., 2019). In essence, this would resemble a form of what social scientists have deemed the "Matthew effect" of accumulated advantage. This principle is based on the saying "the rich get richer and the poor get poorer", and refers to the ease of accumulating disproportionate advantage as an incumbent power (Merton, 1968). In this context, "fast movers", such as the US and China, would likely continue to be the main innovative economies in AI and reap most of the economic benefits, while countries seen as "slow starters" would likely only contribute low-skilled labor, such as data labelling, to the AI value chain, and do it largely on a contractual basis.

64 Here we refer specifically to two essential investments for 5G networks: base stations and massive multiple-input multiple-output (MIMO) antennas. Network densification, which will involve millions of small cells and macro base stations spaced roughly every 250 meters, is required to handle traffic and to maintain high speed connection (CommScope, 2018; Johnson, 2018; Nordrum & Clark, 2017). Additionally, 5G will require many antennas, in part because millimeter wave communications can be disrupted by walls, plants, weather, and other environmental factors (Energy RealPolitik, 2019).

65 The full quotation we aree referring to here is: "higher data rates can only be achieved by consuming more energy; if the EE [energy efficiency] is constant, then 100× higher data rate in 5G is associated with a 100× higher energy consumption" (Energy RealPolitik, 2019; Van Chien et al., 2016).

66 Like machine learning training algorithms discussed in this paragraph, blockchain technologies are also extremely energy-intensive—Bitcoin has been estimated to consume more energy than the entire country of Switzerland (Vincent, 2019). There are less energy-intensive modes of verification, such as "Proof of Stake," but it is a matter of incentives and policy to change the behavior of companies (Truby, 2018).

Signals for Part II
Key Elements of a Hyperconnected World

2. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Conversational Computing spreads and gets smarter

Conversational Computing companies are striving for global reach to bring in more customers, and they're improving the user experience by moving from word and utterance level understanding to conversational competence and contextual awareness.

SIGNAL | Global spread with more natural exchanges.

WHAT: The biggest speech recognition systems are adding languages all of the time..

SO WHAT: Speech recognition is gaining global reach, although less-resourced regions, accents, and dialects still lag behind..

WHAT: Language recognition researchers and companies are starting to introduce contextual awareness into their offerings..

SO WHAT: The next level of speech interaction needs to move beyond utterance-level comprehension, because their recognizers are already well into the 90% level on a word-by-word level...but that's not how "natural" give-and-take conversation works.

https://www.globalme.net/blog/language-support-voice-assistants-compared
https://www.ibm.com/watson/advantage-reports/future-of-artificial-intelligence/ai-conversation.html
https://www.digitalistmag.com/digital-economy/2017/05/10/perception-vs-reality-conversational-computing-05035366

2

3. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Capabilities of CC expand, but cooperation lags

The "skills" that conversational computing has, in terms of how many outside systems it can interface with and what it can do (e.g., tell stories, help with cooking, etc.) are as important as being able to understand what we say. Coalitions between offerings are needed to reduce duplicated efforts and offer a consistent user experience.
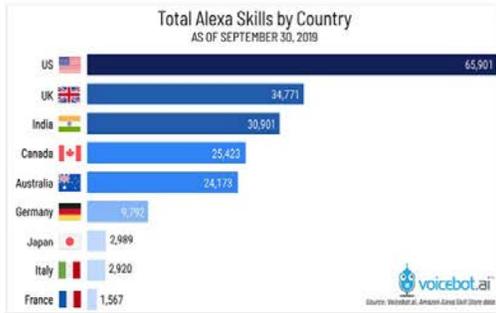
SIGNAL | Many capabilities, but limited overlap.

WHAT: Alexa now has over 100,000 skills, although they are no globally offered..

SO WHAT: The ability to interface with the world is critical, and systems are rapidly expanding these capabilities, although coverage differs drastically.

WHAT: Amazon has created an initiative to share skills, with over 30 participating companies.

SO WHAT: Alliances have the potential to reduce the duplicated effort and make the Conversational Computing arena more consistent, but the other major players (e.g., IBM, Apple, Google) are playing along...yet.

Voice Interoperability Initiative participants

https://voicebot.ai/2019/10/01/amazon-alexa-has-100k-skills-but-momentum-slows-globally-here-is-the-breakdown-by-country/
https://www.theverge.com/2019/9/24/20881321/amazon-voice-interoperability-initiative-alexa-microsoft-baidu-intel-qualcomm-spotify-assistants

3

4. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
Open Personal Assistants and skills are developed

One alternative to the stranglehold that the major players have on the Conversational Computing market is to develop open-source alternatives, both for the assistants themselves, but also the massive number of skills needed to create the ecosystem.

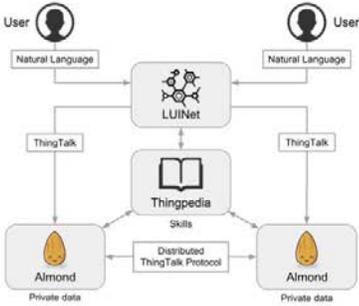### SIGNAL | Emerging open-source alternatives for Assistants

WHAT: Almond is a Stanford-based effort to create an open-source Assistant that preserves privacy.

SO WHAT: Without viable alternatives, the Conversational Computing ecosystems will be driven purely by market forces. Almond offers a system with different priorities.

WHAT: Thingpedia offers a repository for skills, coupled with the ThingTalk protocol for invoking them.

SO WHAT: A Conversational Computing ecosystem is impoverished without a rich and powerful set of skills alongside. The Almond team is creating the whole ecosystem, but without an installed base, commercial players are unlikely to play.

https://almond.stanford.edu/
https://mobisocial.stanford.edu/papers/thingtalk.pdf
https://almond.stanford.edu/doc/thingpedia-intro.md

Almond
The Open, Privacy-Preserving Virtual Assistant

Almond translates your commands into a personalized program.

4

5. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
Speech algorithms relocate

Intelligence at the edge and in devices allows for faster response times and can improve privacy. The development of specialized hardware for this purpose (by Qualcomm, Huawei, Samsung, etc.) will simplify the deployment of these sorts of solutions.
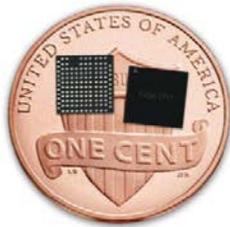
SIGNAL | New hardware for repositioned computing

WHAT: Google's tiny TPU does inference at the edge, and the same sort of chip architecture can aggregate into bigger machines in data centers.

SO WHAT: Specialized architectures are being introduced to efficiently run neural network computing in low-power situations.

WHAT: Companies are introducing stand-alone systems to perform Conversational Computing in smaller and cheaper footprints, like the CNX shield.

SO WHAT: Smaller and faster microprocessors can run the algorithms for speech interfaces, to be more responsive and run disconnected.

ttps://cloud.google.com/edge-tpu/
https://www.zdnet.com/article/huawei-unveils-ai-second-chips/
https://www.cnx-software.com/2019/06/06/movi-shield-offline-speech-recognition-arduino-raspberry-pi/

5

6. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
Speech Recognition factors in privacy concerns

Some applications of speech interfaces bring up big concerns about privacy. The market is responding by bringing out systems that reassure consumers in particular sensitive settings

### SIGNAL | Secure cloud and embedded hyperconnectivity

WHAT: Kidsense offers an alternative particularly aimed at parental concerns about privacy.

SO WHAT: More and more companies are looking at special markets and finding ways to offer advanced functionality without triggering privacy issues..

WHAT: Realink offers security cameras without the cloud.

SO WHAT: Systems that send video to the cloud and do two-way communication to cameras (to, for instance, talk to delivery people from afar) see great security challenges. Operating off the grid without cloud connectivity can alleviate concerns.
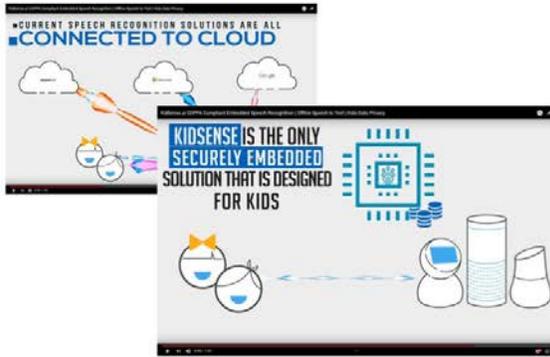
https://kidsense.ai/
https://reolink.com/product/reolink-go/

6

7. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
Affective computing gains traction on devices

Affective computing, which factors the users mood into interactions, is making great strides and is getting folded into our devices. Sensed in myriad ways, such systems can accommodate our emotions into everyday encounters with technology.

SIGNAL | Affective Computing R&D expanding rapidly

WHAT: The affective computing market is exploding.

SO WHAT: While killer apps are yet to be identified, a great deal of interest and activity is present in both the underlying research and initial applications of affective computing.
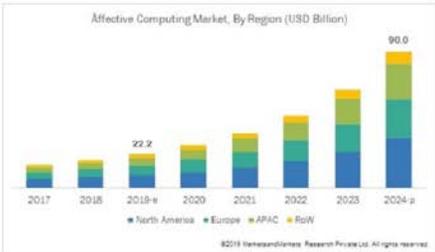
https://medium.com/@focusteamtuni/affective-computing-trends-map-625b554ab0d1
https://finance.yahoo.com/news/worldwide-affective-computing-market-outlook-145408774.html
https://www.marketsandmarkets.com/Market-Reports/affective-computing-market-130730395.html

7

8. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Devices will become affective, responding to user moods

Cars, for instance, will implement affective computing and will be responsive to the emotional states of their drivers and passengers.

:) Affectiva

DISTRACTION	100
DROWSY	80
YAWN	0
EYE CLOSURE	100
JOY	0

SIGNAL | Camera-based systems sense users' mental states

WHAT: Many computational systems will become aware of their users' moods, based on facial expressions, tone of voice, and other factors.

SO WHAT: Knowing the state of mind of users lets devices respond in appropriate ways, and can enhance user experience and improve safety.

http://go.affectiva.com/auto

8

---

9. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Sensors monitor our bodily functions...very closely

Affective computing and precision medicine both need accurate and constant monitoring of vital signs of various sorts. New devices are being developed to monitor us using myriad methods, from cameras to tattoos to implanted devices.

SIGNAL | Recent tools address data sharing with APIs

WHAT: Wireless electronic tattoos have been developed to monitor various signs of emotional state.

SO WHAT: Tattoos offer an unobtrusive and low-maintenance way to monitor our bodies for various hyperconnectivity purposes.

WHAT: Eversense has received FDA approval for an implanted blood glucose sensor.

SO WHAT: Some medical conditions can be better treated with close and constant monitoring of bodily functions. FDA approval of this device for diabetics can help them deal with insulin regimine, or even communicate directly to an insulin pumps so people can lead more normal lives.

https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/19429/IoT-Enabled-Flexible-Sensors-Can-Be-Applied-Like-a-Temporary-Tattoo.aspx
https://www.sciencedaily.com/releases/2019/07/190718112502.htm
https://www.ubergizmo.com/2018/06/fda-approves-first-implantable-continuous-glucose-monitoring-sensor/

9

10. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Health nudges delivered via CC, but displays and actuators, too

Continuous health care and precision medicine are gaining traction as alternatives to the acute and incident-based care of the past. Sensors are tightly coupled to systems that nudge people to healthier eating and other behaviors. This has the potential to deliver better outcomes in a easier, cheaper, and more efficient ecosystem.

SIGNAL | Nudging solutions for better long-term outcomes

WHAT: Upright Go is a sensor that detects slouching and other pain-triggering behaviors.

SO WHAT: Continuous monitoring of unconscious behaviors can stave off acute incidents of chronic conditions like back pain.

WHAT: Recent research is proving the effectiveness of this approach.

SO WHAT: Moving beyond anecdotal evidence, this nudging approach to health outcomes is proving effective in the field.

https://www.engadget.com/2018/03/21/upright-go-posture-trainer/
https://www.researchgate.net/publication/334343934_The_Potential_Role_of_Digital_Nudging_in_the_Digital_Transformation_of_the_Healthcare_Industry

10

---

11. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Your lawyer, your banker, your nurse…they're all CC bots

Many professions' most routine encounters can easily be encoded into scripts and decision trees to provide basic or initial consultations. Law and medicine are seeing an influx of apps with Chatbots (and on-screen variant of Conversational Computing) and Voice-based Assistants. This has the promise of delivering services inexpensively and to communities who might not otherwise be able to afford them.
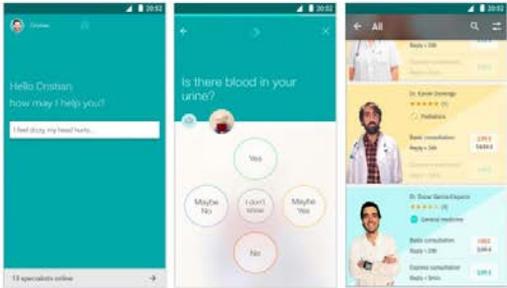
DoNotPay App

SIGNAL | Professional chatbots in numerous fields

WHAT: The DoNotPay helps people fight parking tickets, moving violations and deal with filing and responding to lawsuits.

SO WHAT: While not a complete alternative to hiring a lawyer, DoNotPay can help with the early steps of many legal actions. It encodes the routines of a complicated ecosystem of how to respond to everyday legal actions.

WHAT: MyChart is a recently-introduced health app that aids people in deciding what course of action to take when they're not feeling well.

SO WHAT: Many times, people need to know simple things from a medical consultation, like whether a symptom is worthy of a visit to the ER, and how long can a symptom persist before it's worthy of a doctor's visit. Such systems can do this effectively and inexpensively, and avoid exposure to other disease vectors if they visit a doctor.

https://www.theverge.com/2018/10/10/17959874/donotpay-do-not-pay-robot-lawyer-ios-app-joshua-browder
https://chatbotslife.com/legal-chatbot-chatbots-have-the-potential-to-revolutionize-law-71e304377ffe
https://www.mobihealthnews.com/news/north-america/healthcare-chatbots-are-coming-be-afraid-or-not

11

12. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Your therapist, your rabbi, and your priest are all CC bots, too

Other, more personal encounters with professionals are also being created. Therapy bots, Catholic confession apps, and robot priests are all becoming very real.
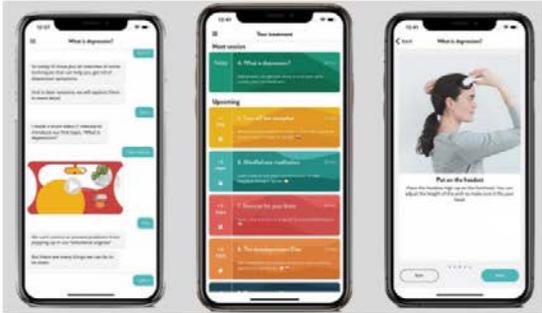
SIGNAL | Apps and robots enter sensitive and sacred territory

WHAT: Flow is a recently-introduced app for personal therapy.

SO WHAT: Therapy is an expensive and daunting step for many who might benefit from it. Apps like Flow can deliver some of those benefits in an inexpensive and convenient format.

WHAT: Mindar is a new robotic priest developed for a Buddhist temple in Kyoto, Japan.

SO WHAT: This robotic clergy can deliver sermons, and interact with worshippers. Modelled after Kannon, the deity of mercy, it currently delivers one sermon over and over, but its capabilities are being expanded with machine learning.

https://www.healtheuropa.eu/chatbot-therapist-to-combat-depression-up/93609/
https://www.theguardian.com/society/2018/apr/25/meet-tess-the-mental-health-chatbot-that-thinks-like-a-therapist
https://www.vox.com/future-perfect/2019/9/9/20851753/ai-religion-robot-priest-mindar-buddhism-christianity

12

---

13. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Conversational agents will be everywhere, cars included

Cars will become conversational, and there will be a major struggle over which conversational agent will reign supreme in consumers' lives (home, handheld, car, etc.). Recent announcements from major automotive players, though, reveal unreasonable expectations about the role that the car-based conversational agents will play in the conversational agent playing field.

http://web.eecs.umich.edu/~yuqqi/pdf/iip2018adasa.pdf

13

14. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
Our personal assistants and twins serve many purposes

Our personal agents will eventually know our preferences very well and will model our behaviors in detailed ways. They will schedule our days, answer our texts and emails, do social media postings, and more. Groups of agents will be able to simulate the behaviors of the people they represent in collective activities, too.

SIGNAL | Digital twins accurate enough to model responses to complex changes to laws and policies

WHAT: An emerging role of personal assistants, being advanced by NTT, is to use groups of the digital twins of use to model and simulate proposed societal changes.

SO WHAT: While not rising to the level of science fiction depictions of our universe actually being a simulation, some researchers are seeing a role for digital twins of people as a way to simulate proposed changes to society…to essentially do a "dry run" of new worlds.

WHAT: Molly uses pattern recognition and natural language processing to figure out an individual's interests and mannerisms and to build an AI version of them.

SO WHAT: Machine learning technology can analyze everything a person has typed or said on the Internet to create an evolving simulacrum for both knowing an individual's preferences and automatically generate responses similar to what they would have written or said.

https://www.smartcitiesworld.net/news/news/digital-twin-initiative-aims-to-model-society-of-the-future-4262
https://www.marketingaiinstitute.com/blog/ai-tools-social-media

14

---
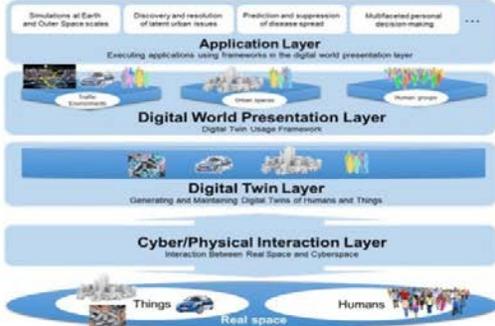
15. HYPERCONNECTED WORLD | Conversational Computing and AI
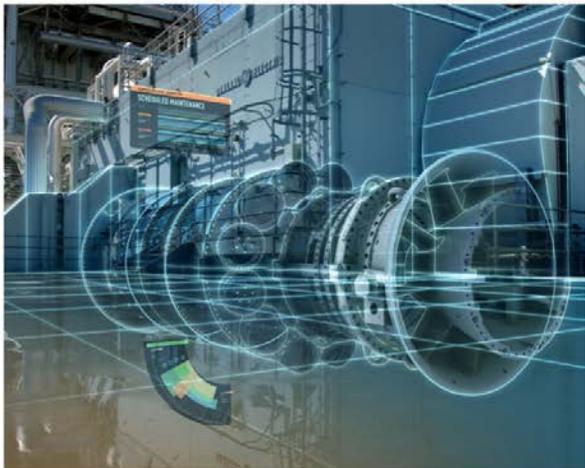
SUB-FORECAST
Spread of digital twins

Digital twins will become an integral element of future factories and enineering work. They will also play a major role in deploying and monitoring complicated electromechanical systems (like aircraft and luxury automobiles). These advanced simulation capabilities will initially be used for fault detection, but they will increasingly be used for quality assurance (in-model testing of real subassemblies), predictive maintenance and will even drive design changes.

SIGNAL | Digital twin consulting services

WHAT: Predix is General Electric's software platform for the collection and analysis of data from industrial machines, and GE has a supporting consulting practice to help enterprises with their deployment.

SO WHAT: Digital twins are an emerging technology for assembly lines and products alike, as well as a set of practices for deploying collecting and sharing data for machine learning models that detect anomalies, recommend maintenance, and optimize performance.

https://www.iot-now.com/2018/07/11/85625-demand-growing-fast-digital-twins-ai-automotive-power-generation-aviation-says-ges-cdo//

15

SUB-FORECAST
Digital twins in the field

Digital twins also can and will be used to increase the reliability of complex products like aircraft, cars, trucks, robots, appliances, and more. Particularly in situations like fleet deployments where there isn't a single owner to report maladies, the digital twin technology should be a huge competitive advantage for keeping time between failures high.

SIGNAL | Field deployment of digital twins proliferates

WHAT: Santa Cruz mountain bike visualization was a convincing early demo of digital twins on deployed machines.

SO WHAT: Sophisticated digital models, linked to sensors on actual hardware, create an insightful perspective on complex machine performance. Privacy issues abound, though, and it isn't clear that the private sector will be swift to allow the data to be collected.

GE interview on jet engine digital twins with Joel Klooster

Bryan Lyles interview on digital twins on the power grid

GE interview on jet engine digital twins and general avionics with Joel Klooster.
Bryan Lyles interview on digital twins on the municipal power grid.

16

SUB-FORECAST
Cloud services for digital twins and big data analytics

Cloud computing will continue to ease the collection and storage of massive collections of data (within—and cross-enterprise, production and operational sensor streams, and usage patterns) ripe for advanced analytics. Some sectors will require secure infrastructure, and hybrid data lake and warehousing solutions will also become commonplace.

SIGNAL | AWS simplifies deployment and scaling

WHAT: AWS has solid support for the data storage architectures and analytic capabilities needed to effectively utilize digital twins, big data, and advanced analytics.

SO WHAT: AWS can be utilized for a secure and virtualized set of data services to support any size enterprise with essentially-infinite on-demand storage and computing resources. Services can be ramped up and cooled down to suit specific application requirements.

https://aws.amazon.com
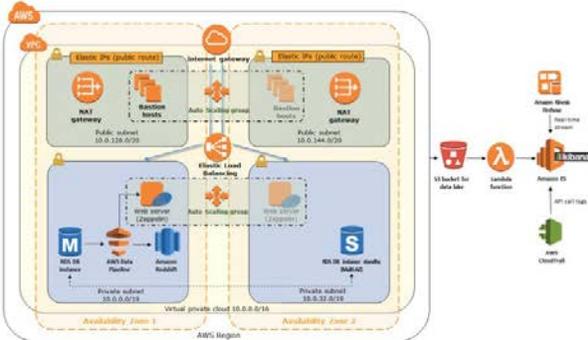
17

18. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Tools to manage complexity

Many of the process improvements argued for future corporations (especially those that make products) require a level of data sharing that few enterprises can deliver upon—not within the corporation and certainly not when the supply chain is integrated into the picture. Systems become too diverse, there are data format and interchange issues. These horizontal and vertical system integration issues will be an ongoing challenge, complicated by legacy systems and cross-enterprise sharing.

**SIGNAL | People and apps collaborate on complex problems**

WHAT: Ironclad is a human-machine hybrid system that helps enterprises create, automate, and track contracts efficiently and accurately.

SO WHAT: Innovative systems are being introduced that use AI to help people manage the increasing complexity of everyday business operations.

WHAT: WorkFusion is process automation software that utilizes AI and other intelligent techniques to take over small chunks of human workflow.

SO WHAT: Pairing people with narrowly intelligent software robots is likely to grow as an approach in the coming decades.

https://ironcladapp.com/
https://www.workfusion.com/company/
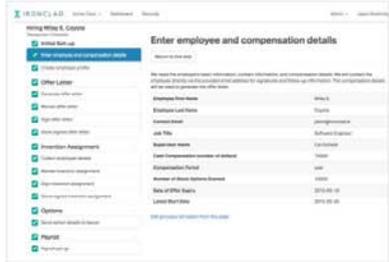
IRONCLAD

WorkFusion

WORKFUSION

18

19. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Massive data sharing issues

Analysis and planning improvements within organizations call for apps that work well together and more data sharing in real time across organizational boundaries and with supply chain partners. Managing vast CAD models, production planning, ordering and shipment, assembly management, and more will require a high degree of fluidity in enterprise data. APIs can be utilized to identify, qualify, filter, and condition data for upstream analysis. Solid and Inrupt is a recent Tim Berners-Lee project that is revolutionizing how to serve up large amounts of decentralized data.

SIGNAL | Apps introduced to ease data sharing

WHAT: Workato integrates disparate apps for workflow optimization.

SO WHAT: Emerging software solutions tie diverse data and analytics together to deliver insights.

WHAT: ELI (by Throughput) is an Automated Data Consultant™ that analyzes supply chain data and recommends areas of improvement to meet unique business goals.

SO WHAT: Applications are being introduced that use analytics to propagate best practices to new business sectors.

https://throughput.world
https://www.workato.com/
https://solid.inrupt.com/

workato
Connect your Apps. Automate your Work.

WORKATO

ELI

19

SUB-FORECAST

Increased supply chain complexities

Supply chains in large enterprises are complex—and often can be delicate when they need to be nimble and robust. Products can disappear from the market from supply chain disruptions (e.g., a natural disaster that causes a component to go EOL), and this situation is exacerbated by spatial distribution of production and increasing protectionism.

SIGNAL | Sophisticated supply chain management tools

WHAT: Axens offers blockchain technology that simplifies SCM.

SO WHAT: Using blockchain can provide more secure and collaborative opportunities for trade finance.

WHAT: Tive's real-time shipment tracking system uses proprietary trackers and cloud-based software to give companies visibility and analysis on inbound and outbound shipments.

SO WHAT: Adding wireless network sensing through existing GPS, Wi-Fi, and cell tower systems enables customers to get more precise location identification. It can be attached to a shipment box or integrated with returnable packaging.

AXENS

TIVE

https://medium.com/applicature/the-latest-blockchain-supply-chain-startups-7b0e5c07548f
https://tive.co/

20

SUB-FORECAST

Humans and AI designing together

They will be steering algorithmically derived results to aesthetically pleasing, integrated, and functional parts. AI assistants will be in production planning, strategic decision-making, supply chain management, and many other traditionally white-collar jobs as well.

SIGNAL | Human-guided generative design

WHAT: Autodesk used Fusion 360 modeling and the Shapeways 3D marketplace to create 3D printed titanium skateboard trucks, and then Braille Skateboarding showcased their impressive functionality.

SO WHAT: People and computers can partner to create parts and processes that neither would have come up with alone.

https://www.shapeways.com/blog/archives/38807-3d-printing-mythbusting-braille-skateboarding.html

21

SUB-FORECAST

Working as a centaur

The employee experience of working in tight or inseparable partnership with machines and software will become commonplace over the next decade. This situation will play out over time, but the workers, the engineers, the programmers, and management are all going to have to evolve for myriad new workplace situations.

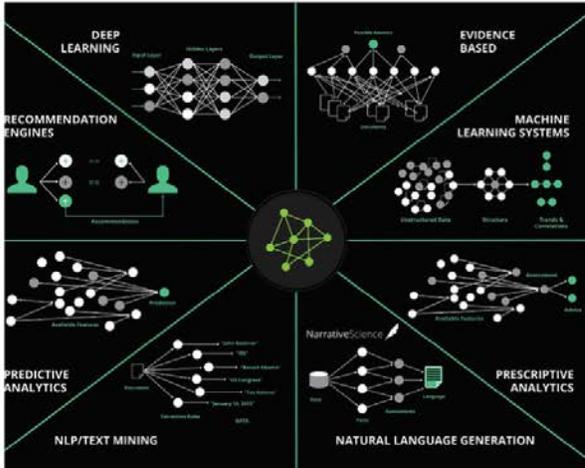| Entity	Advantage	Explanation	However ...
Computer	Speed	Fast generation and testing in big search space of solutions. Fast processing over big data	Solution generator is incomplete in the open world. Data not a full representation of the open world.
Human Team	Knowledge and human perception.	Life experience in the open world. Diverse experience of cross-disciplinary teams in multiple domains.	There are coordination costs.
Human-Computer Team	Highest performance.	Complementary kinds of cognition compensate for each other's failure modes and enhance performance.	We need a better theory and practice for building Human-Computer teams.

http://jods.mitpress.mit.edu/pub/issue3-case
https://www.parc.com/blog/half-human-half-computer-meet-the-modern-centaur/

22

SUB-FORECAST

Deep learning continues to produce brittle AI

An issue that arises at many levels of this topic (and spills into many others in the technology thread, as well) is the brittle nature of many current AI systems. Trained-up deep learning systems can easily be fooled, and sensor systems can be attacked (e.g., laser pointers and LIDAR) or foiled by suboptimal conditions (rain and snow, for many autonomous vehicle systems).
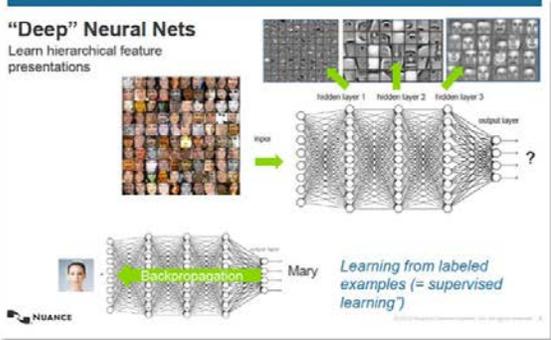

https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/
https://www.popsci.com/hackers-can-trick-lidar-used-in-autonomous-cars-with-laser-pointer

23

SUB-FORECAST

AI via deep learning creates inscrutable algorithms and results

Compounding the issue of AI's brittleness is the fact that typical deep learning systems cannot explain their behaviors in terms that humans can understand. This makes it difficult to debug the systems and makes it even harder for them to be comprehensible to consumers (or, in the case of an accident, to a jury).

"Deep" Neural Nets
Learn hierarchical feature presentations

Learning from labeled examples (= supervised learning")

NUANCE

24

SUB-FORECAST

Cross-enterprise data sharing challenges persist

A major challenge in creating "what if?" tools for large enterprises is getting data into forms that permit collaboration across diverse systems. The approaches used must avoid becoming a least-common-denominator situation that prevents insightful analysis from being performed.

SIGNAL | Tools to address the data sharing challenge

WHAT: Velostrata is an Israeli startup whose software uses live streaming technology to reduce the complexity, risk, and labor costs associated with migrating and running data, apps, and other IT functions in the cloud and across hybrid environments.

SO WHAT: This tool and others (e.g., CDAP, a unified integration platform for big data, designed to reduce the time required to create new analytic applications) are being introduced to meet the challenges of optimizing diverse data resources.


RISC Networks—Discovery/Assessment   Velostrata—Accelerated Cloud Migration

VELOSTRATA

CDAP
CASK DATA APP PLATFORM

Google Cloud

CASK DATA

25

49

26. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
API-based tagged and raw data sharing tools

One approach to data unification is for component systems to export requested information using agreed-upon APIs. The enterprise and supply chain participants must all use programs that implement the APIs, and the APIs must also not suffer from the least-common-denominator issue.
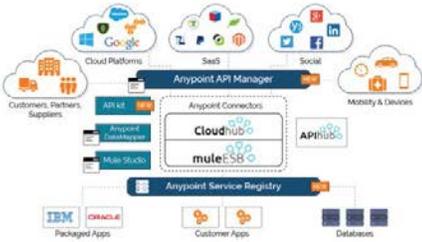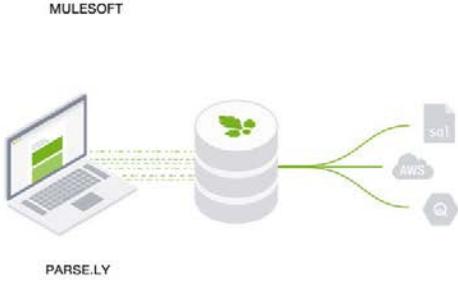
SIGNAL | Recent tools address data sharing with APIs

WHAT: MuleSoft offers the Anypoint Platform to export data using microservice APIs.

SO WHAT: Emerging platforms give businesses tools for data migration and the ability to extend their network connectivity across divisions and enterprises using APIs.

WHAT: With the view that raw data is "the ultimate API," Parse.ly developed the Data Pipeline. It provides users with data streams collected from their own sites and apps in real time and gives them a clean, structured data source for analytics.

SO WHAT: New tools will be developed to address how analytics are complicated by systems that change over time (i.e., data are not gathered under the same circumstances or with identical sensors) or are performing edge analysis and only storing data that's already been subjected to algorithmic analysis at collection time (possibly by a black box algorithm or a deep learning system that cannot adequately characterize its behavior).

https://www.mulesoft.com/resources/esb/data-migration-solution
https://blog.parse.ly/post/4006/rawdata

MULESOFT

PARSE.LY

26

---

27. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST
Tools emerge to create more resilient supply chains

It will become critical to connect and manage supply chain ecosystems that are robust and resilient to issues like local content laws, natural disasters, fickle protectionism, and technological advances. The complexity of decision-making and the fluidity required will be aided by AI and sophisticated analytics watching for instabilities and identifying opportunities.

SIGNAL | Supply chain risk management software

WHAT: The GroundTruth Global platform (created by PeaceTech Lab) is a SaaS solution offering risk monitoring tools that provide early warning of social and economic disruption due to volatility in fragile and emerging economies.

SO WHAT: New tools are being developed that rely on a combination of human and machine learning to model risk, recognizing and predicting the likelihood of disruption from days up to several months in advance.

WHAT: SAP Ariba is one of an emerging group of supply chain risk management tools.

SO WHAT: Software can help incorporate industry- and component-specific exposures when analyzing and minimizing chances of disruptions.

http://www.peacetechlab.org/groundtruth-global
https://www.ariba.com
https://www.parse.ly/data-pipeline/

27

---

28. HYPERCONNECTED WORLD | Conversational Computing and AI

SUB-FORECAST

Digital product prototyping flourishes

Seeking to avoid marketing gaffes, manufacturers will use CAD, simulation, as well as VR and AR to test products against simulated real-world conditions and with consumers before making them real.

SIGNAL | Firms do digital prototyping for automotive

WHAT: ZeroLight VR/AR is designed to help automotive companies better test and calibrate their products and get things right before entering production.

SO WHAT: Virtual prototyping, from accurate digital models, allows enterprises to iterate rapidly and try more options for how a product will look and operate. It can be done for less money and will be employed in the design phase as well as during sales.

https://zerolight.com/vr-ar-enterprise

28

---

29. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST

Screen form factors get more interesting

While handsets are on the decline, new form factors will be enabled by screens that fold and roll..

SIGNAL | New screens abound with folds and scrolls

WHAT: Dell Ori is a new folding machine that occupies a niche between PC and tablet.

SO WHAT: Ori is just one example of a host of intriguing new products that will offer new form factors for people who only sometimes need a big screen, .

WHAT: Samsung is showing technology for phones that roll up.

SO WHAT: A rolling screen, as this technology advances and becomes thinner, promises convenient screen size without the bulk.

DELL ORI

SAMSUNG

https://mashable.com/article/all-the-flexible-displays-at-ces-2020/

29

30. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
Better VR and AR glasses

Technology improvements are yielding more practical and cosmetically acceptable eyewear. Resolution and field-of-view improvements are accompanying the lighter weight and battery life gains.

SIGNAL | Waveguide glasses hitting the market

WHAT: DigiLens and Apple are touting AR glasses that use waveguide technology for better performing and attractive eyewear.

SO WHAT: AR and VR adoption for the general public has been plagued by bulky and unattractive form factors, The maturation of waveguide technology is addressing this issue.

DIGILENS

APPLE

30

---

31. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
Better VR and AR glasses

Technology improvements are yielding more practical and cosmetically acceptable eyewear. Resolution and field-of-view improvements are accompanying the lighter weight and battery life gains.

SIGNAL | Direct retinal projection getting closer to reality

WHAT: Intel technology acquired by Vaunt use direct retinal projection to deliver AR experiences.

SO WHAT: Direct retinal projection is one of the most promising ways to deliver augmented content to a viewer's eye. Recent advances suggest that this technology will definitely be available during the forecast period.

VAUNT

North's Focals
Laser Beam Scanning AR Glasses
"Color Intel Vaunt"

31

32. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
VR and AR contact lenses

Possibly the holy grail of VR and AR eyewear for some is to utilize the contact lens form factor. A viewer's retina would have incoming light augmented or replaced with retinal projections from the back of the lens. Battery life, display technology and other factors will likely push this technology out into the latter part of the forecast period, but recent advances are promising.

SIGNAL | Digital contact lenses getting closer to reality

WHAT: Mojo has recently shown a digital contact lens prototype, indicating that the technology might not be as farfetched as previously thought.

SO WHAT: Long considered the stuff of science fiction, the digital contact lens is making strides towards feasibility for some applications.

MOJO Contact Lens

https://www.theverge.com/2020/1/16/21067883/mojo-smart-contact-lens-augmented-reality-startup
https://www.wired.com/story/mojo-vision-smart-contact-lens/

32

---

33. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
AR and VR start paying attention to fashion

A big impediment to mass-market adoption of AR/VR technology is that they've been ugly. Design studios and brands will partner with technology firms to bring a new focus on aesthetics and the lure of name brands to these new technolgies.

SIGNAL | Attractive audio and funky visuals arrive

WHAT: Huawei's partnership with glasses-maker Gentle Monster is showing how fashion and high-tech can yield attractive eyewear with technology integrated.

SO WHAT: Although audio-only, Huawei is acknowledging that fashion and functionality have to go together.

WHAT: Panasonic showed rather steampunk 5K eyewear at CES 2020, showing that high tech needn't always be totally ugly.

SO WHAT: Although hardly for everyone, Panisonic's recent offering shows a growing awareness about how fashion sense needs to be blended with emerging tech.

Huawei and Gentle Monster

Panasonic

https://www.twice.com/industry/ces/panasonic-unveils-5k-hdr-capable-vr-glasses-at-ces-2020
https://consumer.huawei.com/en/wearables/gentle-monster-eyewear/

33

34. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
VR and AR at work

VR is being used for training (e.g., human resources people); AR is being used to acclimate line workers and do real-time assembly and service instruction.

SIGNAL | Firms tackle VR/MR/AR in enterprise settings

WHAT: STRIVR VR offering for sports training has expanded into providing training solutions for enterprises.

SO WHAT: The company based the move on the observation that most training principles in football are applicable in business situations.

WHAT: Atheer is using AR on the factory floor and in service bays to train and guide workers.

SO WHAT: AR has made the leap to practicality for many enterprise applications, offering training, documentation, and real-time process guidance.

https://www.strivr.com/
https://atheerair.com/vr-assembly/

STRIVR

ATHEER

34

---

35. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
Workers immerse in data for decision support

Everyone has a dashboard for immersion in organized data.

SIGNAL | VR tools extend screen-based decision support

WHAT: vSpatial is using VR for improving productivity and enhancing sensemaking.

SO WHAT: VR promises to upgrade information displays to create virtual spaces that immerse users in organized data to intuitively navigate complexity—not only helping people be more productive but also bringing them together in novel ways.

WHAT: The Oculus Dash interface is set to replace traditional desktops with more immersive VR experiences.

SO WHAT: No longer limited by small rectangular screens, VR workspaces embed users in vast seas of pixels that can be used to spatially arrange and represent data.

https://vspatial.com/vision/
https://www.theverge.com/2017/12/6/16743042/oculus-rift-core-dash-home-beta-update-desktop

VSPATIAL

OCULUS DASH

35

36. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
Glasses and algorithms for auditory experiences

Audio that seems to be coming from inside your head, like many headphone and earbud experiences do, are not good for immersion situations where a real space is being depicted. Algorithms that shape the frequency and arrival times of sounds to simulate real places can radically transform personal audio. Delivering audio while not removing oneself from the real world will be increasingly important in AR situations where the real world and the synthetic world coexist.

SIGNAL | New audio developments for AR & VR

WHAT: Sony's new 360 Reality Audio brings a new, spatialized experience to headphone audio.

SO WHAT: Taking ear shape into account, 360 Reality Audio takes headphone audio to where it can render sounds as coming from outside your head, providing location cues and a more natural listening experience.

WHAT: Bose, too, have been working on smart eyewear that people won't immediately associate with geek/nerd culture..

SO WHAT: Bose blends adequate style and high functionality in their advanced audio eyewear.

https://www.engadget.com/2019/09/06/sony-360-reality-audio-headphone-calibration-hands-on/
https://www.theguardian.com/technology/2019/jul/08/bose-frames-review-smart-audio-sunglasses-are-a-blast

36

37. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
VR/MR/AR chairs offer heightened immersion too

Better synesthesia chairs will be introduced to provide full-body motions and other sensory stimulation for VR and AR experiences.

SIGNAL | Consumer-grade VR chairs for work and play

WHAT: Roto VR is one of many chairs that provide other motion and body sensation cues for gamers.

SO WHAT: Offering even more immersive experiences (g-forces, wind, heat/cold, etc.), these technologies are going to work for enhanced immersion during simulations and data visualizations.

https://www.rotovr.com/

37

38. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
Haptic suits will become refined and see gradual adoption

Better synesthesia gloves and suits will be introduced to provide full-body haptic feedback (and motion capture) for VR and AR experiences.

SIGNAL | Haptic suits for gamers, for now

WHAT: The Rez Infinite Synesthesia Suit adds full-body haptic feedback to VR experiences.

SO WHAT: Many experiences can be further enhanced, in situations where a user is willing, by body sensations like touch.

http://rezinfinite.com/synesthesia-suit/

38

39. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST
More senses for immersion

More attention is being paid to how other sensory modalities play into immersion, as well. Olfactory and taste are outliers, but research work is being done and occasional products enter the scene.

SIGNAL | Analyzing and delivering smells is improving

WHAT: Ayrballe has been demonstrating an artificial nose that helps experience designers craft and match olfactory data.

SO WHAT: Working with smell has always been a challenge, but devices are being introduced to help designers deliver appropriate olfactory stimulation for a scene.

WHAT: Artiris Parfum is a recently-introduced five-smell emitting appliance.

SO WHAT: While far from a general-purpose smell emitter, the Parfum is an attractive device that can augment experiences with olfactory stimulation.

AYRBALLE

ATHEER

https://ayrballe.com/
https://www.moodify.today/
https://medium.com/swlh/ces-2020-smell-tech-highlights-7b585057de90

39

40. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST

Additional modalities make AR/MR/VR more involving

MR in static locations allows for more immersive experiences, like haptics and binaural audio.

SIGNAL | Gloveless haptic technology brings touch to users

WHAT: In-air haptics without worn actuators create touchable designs and data.

SO WHAT: Immersive experiences are more involving when more of our senses are engaged, and engaging touch without requiring users to wear gloves is a big advantage.

https://motherboard.vice.com/en_us/article/78xa5x/how-haptics-make-holograms-you-can-touch
http://www.ultrahaptics.com/

40

---

41. HYPERCONNECTED WORLD | Immersive User Experiences

SUB-FORECAST

Vehicle AR becomes a well-registered world overlay

AR will be available on all car surfaces (especially the windows, to overlay onto the world). It will become (alongside audio) the main mechanism for getting driving instructions, and passengers and drivers alike will have augmented views of their surroundings.

SIGNAL | AR delivers enriched vehicle experiences

WHAT: WayRay is one strong example, partnered with Porsche and Hyundai. Automakers will turn to other suppliers for this advanced functionality.

SO WHAT: Many device manufacturers are incorporating AR into their products. Cars are a prime target for these experiences, presenting many appropriate surfaces for the display technology and myriad applications, including vehicle information, wayfinding, and entertainment.

https://wayray.com/

41

SUB-FORECAST

AR brings new risks and legal exposure

AR and VR brings unfamiliar experiences and technology into everyday life and legacy situations. Tuned-out people may wander into danger, not unlike cellphone zombies and earbud deafness. Many more varieties exist, and more to be discovered.

SIGNAL | Extended reality's numerous risks, outlined

WHAT: Just as cellphones and Pokemon Go have brought unanticipated dangers and urban challenges, the cited report touches on new ones that our latest technologies will bring..

SO WHAT: AR has the potential to be a nightmare of public safety concerns as heads-up vision is potentially impaired by distracting overlays.

Liam Walsh/The New Yorker

https://sloanreview.mit.edu/article/preparing-for-the-risky-world-of-extended-reality/

42

SUB-FORECAST

Projected AR helps groups collaborate around data

Projected and collaborative AR for work settings can include group redlining of electromechanical systems and group sensemaking around data visualizations.

SIGNAL | Projection mapping creates shared representations

WHAT: Lightform is a system that can create projected and shared AR tools on ordinary surfaces.

SO WHAT: Current demonstrations focus on entertainment, but future business applications of this projection mapping authoring system are apparent.
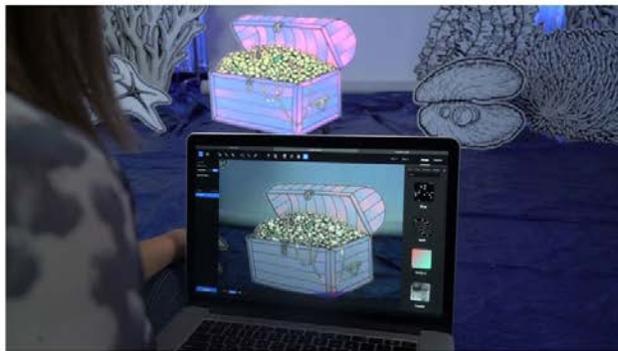
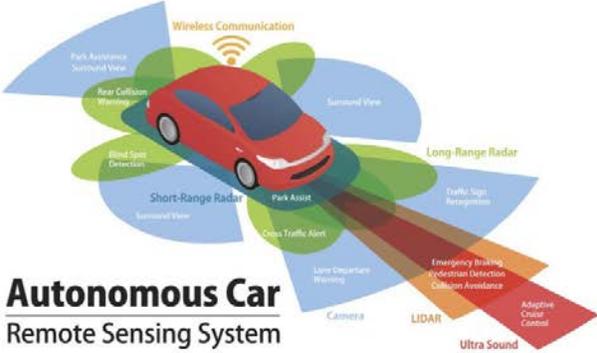Moses Ma case studies with banking customers.
https://lightform.com/

43

58

SUB-FORECAST

Active AR windshield for information presentation

Partial autonomy, like Tesla's Autopilot hardware, will spread to other brands, and AR will display sensor data similar to those needed for autonomy to alert drivers to road safety issues (imagine using an active windshield overlay).

Autonomous Car
Remote Sensing System

Wendy Ju interview
https://www.thedrive.com/tech/17161/think-self-driving-cars-are-around-the-bend-time-for-a-virtual-reality-check

44

---

45. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST

Electrification of the vehicle fleet will grow significantly

The shift to EVs will accelerate in the US in the next decade, and there are indications of them reaching 5% new vehicle market penetration in the US by 2025. There will be larger percentages in some regions or municipalities (e.g., 25% of the overall fleet in California). Global penetration is murkier, but China's enthusiasm should drive prices down rapidly and push adoption up to 10% or so in the same time period (20% in China). Norway has incentivized heavily and is already at 50% electric vehicle sales.

http://mitsloan.mit.edu/ideas-made-to-matter/real-barriers-to-electric-vehicle-adoption
http://evadoption.com/

45

46. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
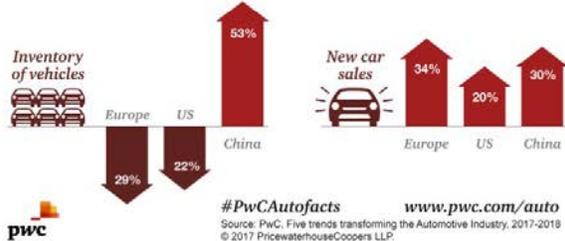# Private car ownership will decline with increased sharing

Most forecasts suggest something on the order of a 50% reduction in private car passenger-miles possible by 2030 in US urban areas. The dominant shift, though, will be in who owns and operates the vehicles rather than a large portion of the vehicle fleet being eliminated. Impediments to higher rates of vehicle sharing include the challenges of rural coverage and the "road trip" problem (i.e., limited range).

SIGNAL | Decreasing ownership doesn't mean fewer cars

WHAT: Vehicle inventory will see a reduction, but the growing number of passenger miles means that new car sales will continue to increase slowly.

SO WHAT: The automobile market is seeing upheaval and changes, but consensus is that no general collapse is on the near horizon.

By 2030, vehicle inventory will drop in some markets but vehicle sales will continue to increase

Inventory of vehicles Europe US China 53% 29% 22%

New car sales Europe 34% US 20% China 30%

#PwCAutofacts   www.pwc.com/auto
Source: PwC. Five trends transforming the Automotive Industry, 2017-2018
© 2017 PricewaterhouseCoopers LLP.

interview with Anthony Townsend
https://press.pwc.com/News-releases/by-2030--the-transport-sector-will-require-138-million-fewer-cars-in-europe-and-the-us/s/a624f0b2-453d-45a0-9615-f4995aaaa6cb

46

---

47. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Urban driver demographics will shift and fleets get larger

Most forecasts suggest something on the order of a 50% reduction in private car passenger-miles possible by 2030 in US urban areas. The dominant shift, though, will be in who owns and operates the vehicles rather than a large portion of the vehicle fleet being eliminated. Licensing rates in the US will continue to wane, especially in the lower age brackets, which contributes to ridesharing growth.

SIGNAL | Sharing shifts drivers, but passenger-miles go up

WHAT: Fewer young people are learning to drive, and those that are learning learn later. Studies reveal that ridesharing actually increases passenger miles for cars and steals riders from other modes like walking and transit.

SO WHAT: Many auto driver demographics are changing, and playing into the shift in vehicle usage patterns. Enterprises will need to carefully track what's happening in strategic markets and major sectors.

interview with Anthony Townsend.
https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/03/03/why-teens-still-dont-want-to-get-a-drivers-license

47

48. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST

Some demographics will resist hyperconnectivity

Portions of the user community may resist hyperconnectivity, citing privacy concerns and complextity An approach some companies will use to appeal to these consumers is to create user experiences that develop a history with a consumer durable or smart device or imbue it with personality to create a special relationship with the user.

SIGNAL | Relationships with objects for desire and loyalty

WHAT: Elder care robot ELLI.Q is designed as an "aging companion" that forms a bond with the user.

SO WHAT: Using machine learning to enable proactive suggestions for entertainment and activities in addition to wellness and environmental monitoring.

WHAT: Social robots aim to become one of the family in order to foster product loyalty. After Jibo's failure, the flag is still being waved by companies like Misty Robotics, who build robots that have personalities and build a history with users.

SO WHAT: While social robots are still struggling, evidence from conversational computing indicates that products with evident personalities can create social bonds.

https://www.techemergence.com/applications-of-ai-in-elderly-care-robotics/
https://www.mistyrobotics.com/

ELLI.Q

JIBO

48

---

49. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST

Other autonomous vehicles see adoption too

Some localities will be willing to develop infrastructure (dedicated lanes, idling lots, inductive charging, etc.) with these new technologies in mind. Since autonomous vans can be deployed in lieu of other extremely expensive transport modes (e.g., light rail), some municipalities will see them as viable alternatives to public works expenditures.

SIGNAL | Autonomous rail-less vehicles developed

WHAT: One alternative is trackless trams for cities and shuttle routes.

SO WHAT: Trackless trams offer more economical alternatives for many transit routes. Fixed routes make them prime targets for automation and electrification.

Interview with Anthony Townsend.
http://theconversation.com/why-trackless-trams-are-ready-to-replace-light-rail-103690

49

50. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST

Changing vehicle mix will bring added efficiencies

Further development of right-sized vehicles will create more variety in the vehicle fleet. This will be especially true in urban areas where appropriate deployment of shared vehicles creates economic benefits from higher fleet utilization. Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication will improve safety and make smaller and lighter vehicles into safe alternatives. Vehicles based on a modular technology core, with bodies customized for particular uses, will become common and may lead to the resurgence of the local coachbuilder that tailors vehicles for buyers. Again, passenger-mile statistics are likely to increase, and opportunities are present for many new and existing players in the market.

Interview with Anthony Townsend.

50

---

51. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST

Last-mile and short-run vehicle options proliferate

Many other last-mile and as-needed transportation modes will show up over the next decade, especially in urban settings. Electrification of the existing fleet will allow consumers to utilize these transport modes in comfort, and will be increasingly attractive in congested cities. Cities are struggling to come up with good regulations, ensure public safety, and generally cope with the pace of these innovations.

SIGNAL | E-scooters deployed widely, but hitches remain

WHAT: Scooters and e-bikes are invading numerous American cities and reshaping the set of options available for last-mile and short-run trips.

SO WHAT: While attractive to some, as a convenient and speedy last-mile mode, lawsuits have been filed in various cities citing service provider negligence, public nuisance, and aiding and abetting assaults, among other infractions.

https://www.vox.com/2018/8/27/17676670/electric-scooter-rental-bird-lime-skip-spin-cities
https://www.curbed.com/2018/10/22/18009492/bird-lime-scooter-lawsuit-los-angeles

51

52. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Passenger drones excite and see fixed-route deployments

Passenger drones will continue to see enthusiastic development as a flexible and futuristic transport mode. Regulations and technology will likely be restricting them to very limited use cases during the next decade (e.g., point-to-point runs in a few cities).

SIGNAL | Passenger drones move past initial feasibility

WHAT: A government-led group in Japan includes businesses to figure out the regulation and infrastructure for passenger drones.

SO WHAT: Major companies and governments are taking a serious look at what it will take to make this mode of transportation practical and safe.

https://www.forbes.com/sites/montymunford/2018/07/13/passenger-drones-are-landing-soon-as-the-race-to-the-skies-heats-up/#599ecc113f9c
https://www.engadget.com/2018/08/24/japan-teams-up-uber-airbus-19-others-flying-taxi-plan/

52

---

53. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Delivery robots and drones everywhere

AGVs and drones are making inroads in delivering the correct parts and pieces to assembly workers in highly-variable and customized production runs. Algorithms can keep track of where a given product is in the production system and make sure it's properly optioned. Many firms are prototyping ways to bring these efficiencies to other delivery challenges, using robots and drones to bring parcels to homes and businesses.

SIGNAL | Drone delivery trials are proving this concept

WHAT: Audi has demonstrated steering wheel in-factory delivery for this often-custom item in luxury vehicle interiors.

SO WHAT: Novel combinations of people and machines can cover the great flexibility needed to deliver parts and pieces along assembly lines.

WHAT: Workhorse Group's Combined Truck and Drone Fleet can cover the same distance as most supply chain vehicles and then send a drone to finish the last leg of the route for greater efficiency.

SO WHAT: Drones will be deployed for expedient first- and last-mile parts deliveries, definitely for businesses, and some form of automated delivery will be used for a subset of homes.

AUDI

WORKHORSE

https://www.allaboutlean.com/project-shop/audi-tech-day-2016/
https://www.rfgen.com/blog/3-companies-successfully-using-drones-in-the-supply-chain

53

SUB-FORECAST
Cobots enter the workforce

Working alongside humans to position parts and to tend machines (e.g., loading and unloading workpieces in a CNC milling workcell), cobots can speed production and improve workplace conditions (e.g., handling moderate lifting, positioning parts for an assembly operation, or reducing worker tedium in repetitive packaging tasks). The deployment of cobots, though, is a complex issue for the human workforce, with interaction design details determining whether workers will embrace or resist the technology. Machine learning is tackling the task of how these machines figure out what to do.

SIGNAL | Cobots on the rise

WHAT: Universal Robots is the rising star in cobot manufacturing with placements in many industrial sectors.
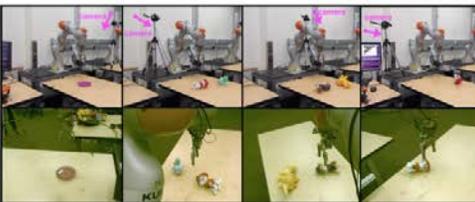
SO WHAT: Cobots take on a "helper" role in industrial tasks, streamlining some tedious operations without the more expensive commitment to full-on automation.

WHAT: Advances in robot learning are replacing the need to program operations, such as grasp strategies for irregular parts in random orientations.

SO WHAT: Programming automation has long been a barrier to adoption, and robotics can require additional workcell accommodations (e.g., for jigs and palletizing). Robot learning is letting robots figure out what to do on their own, through observation and other operations planning strategies.

https://www.youtube.com/watch?v=QBngLFJqEVU
https://ai.googleblog.com/2018/06/teaching-uncalibrated-robots-to_22.html

UNIVERSAL ROBOTS

ADVANCES IN ROBOT LEARNING

54

SUB-FORECAST
Human workers outperform automation

Traditional assembly line robots are proving too "brittle" for many modern assembly settings. Robots are expensive (and must be upgraded and replaced at regular intervals), the programming is tedious, and only in specific places on the production line (e.g., welding body panels, the paint booth) do robots pay off (unless it's a high-volume line, typically with a uniform product). Other industrial applications of robotic automation make more sense, and there will be an ongoing shift to their use, but the flexibility of humans in the final assembly of complex products will be resistant.

https://www.leanblog.org/2017/09/toyotas-people-vs-teslas-robots-battle
https://arstechnica.com/cars/2018/04/experts-say-tesla-has-repeated-car-industry-mistakes-from-the-1960s/

55

56. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Social robots will proliferate

Social robots have seen a rocky road to widespread adoption, with big failures of Jibo and other early players. Manufacturers keep trying, though, and will make inroads during the forecast period. Finding the sweet spot between practicality and fun will be an ongoing challenge, especially when cost and privacy get factored in.

REACHY

SIGNAL | Social robots get bigger and more functional

WHAT: Reachy, by Pollen Robotics, is an open source social robotics platform shown at CES 2020..

SO WHAT: Humanoid social robots are a big commitment, and they may currently set the bar too high on expectations for what the machines currently do. Large and too expensive for most, these open-source varieties may appeal to the early adopter hobbyists.

WHAT: Chuangze Intelligent Robot occupies a much different place in the size and functionality dimensions of the social robot design space

SO WHAT: Smaller social robots have struggled for adoption, but many consumers find them cute and approachable.

Chuangze Intelligent Robot

https://www.pollen-robotics.com/
https://www.cnet.com/news/ces-2020-little-robots-are-ready-to-make-the-world-better-in-a-big-way/

56

---

57. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Health- and elder-care robots are widely adopted

A major market for home robots is the healthcare market, with a further focus on caring for the growing numbers of elderly people. Many nations are facing an crisis of caring for elderly, and extending their independent living time by using robots is seen as a great way to reduce that burden.

Mobile Arm Robot System (MARS)   GenkiCam   Robot with Smart Joints

SIGNAL | New and helpful robots enter the scene

WHAT: A wide range of robotic form factors were at CES 2020, all touting new uses of machine learning and AI to make them more functional.

SO WHAT: ML & AI are out of the lab, and helping robots navigate unstructured environments, perform tasks and learn their users' habits, and interact in safe and useful ways.

WHAT: Pria, by Black and Decker, is a pill dispensing robot aimed at the growing AgeTech market.

SO WHAT: Big players are seeing the potential in this market, and believe that their reputations for reliability and trusted brands names will aid in getting people to buy. Robots don't need to move around and lift things to be useful, either.

https://www.businesswire.com/news/home/20191211005271/en/ITRI-Showcases-AI-Robotics-Technologies-CES-2020
https://www.reviewjournal.com/business/conventions/ces/robots-are-coming-to-help-seniors-live-healthy-independent-lives-1932402/

57

58. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Robot companions and pets breed like rabbits

Lonliness and depression are epidemics, and companion robots have been shown to reduce these problems in many populations, including shut-ins. The offerings are taking many forms, from small, vaguely-humanoid machines to adorable robotic pets.

SIGNAL | Companion robots in many shapes and sizes

WHAT: Pibo, out of Samsung's future-looking C-Lab, is a cute social robot that's aimed at being a friendly companion for those who live alone.

SO WHAT: Staying active and stimulated can be a big plus for those with mild depression. Pibo strives to keep its owner engaged by being fun and a little silly.

WHAT: Tombot is an inexpensive robot puppy that takes a different path to keeping people engaged..

SO WHAT: Tombot is a responsive robotic dog that loves to be talked to, petted, and scratched. Sure, it snores a little, but it doesn't fart or need to be taken outside..

https://gizmodo.com/samsungs-incubator-lab-is-making-indoor-sunlight-and-a-1840703248
https://www.cnet.com/news/a-snoring-robot-labrador-puppy-stole-my-whole-heart-at-ces-2020/

58

---

59. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
Amplified humans

Exoskeletons are an automation approach that will gain ground over the next decade. Humans will use their sophisticated dexterity and sensing to properly position parts and thread fasteners, while the exoskeleton helps with the lifting and reduces strain. Widespread worker acceptance will need to be nurtured—most existing exoskeleton technology has been deployed only in pilot studies.

SIGNAL | Progress towards productive cyborgs

WHAT: A mechanical exoskeleton called the Paexo from German artificial limb manufacturer Ottobock is an example of this technology.

SO WHAT: Exoskeletons can ease the physical strain of laborers doing extensive mechanical work in factories, and will soon allow workers to perform tasks otherwise beyond their human capabilities, like heavy lifting.

WHAT: SmartCap is a wearable human performance-sensing technology that measures a person's alertness by measuring brain activity while operating, for instance, heavy machinery or a dangerous workcell.

SO WHAT: SmartCap can make working around and with dangerous machines safer. It may also foreshadow an emerging field of "safety surveillance" across sectors like mining, assembly, transport, and commercial construction.

PAEXO

SMARTCAP

https://www.reuters.com/article/us-ottobock-exoskeletons-focus/ottobock-reaches-for-growth-with-industrial-exoskeletons-idUSKCN1LR0LI
http://www.smartcaptech.com/

59

60. HYPERCONNECTED WORLD | Robots, Autonomy, and Drones

SUB-FORECAST
More amplified humans

Exoskeletons are an automation approach that will gain ground over the next decade. Humans will use their sophisticated dexterity and sensing to properly position parts and thread fasteners, while the exoskeleton helps with the lifting and reduces strain. Widespread worker acceptance will need to be nurtured—most existing exoskeleton technology has been deployed only in pilot studies.

SIGNAL | Exoskeletons on the tarmac

WHAT: Delta Airlines and Sarcos have developed a powerful exoskeleton to reduce workplace injuries..

SO WHAT: At the RoboCop end of the scale, these exoskeletons were designed to give airport baggage handlers a break from heavy lifting. At CES 2020, delighted attendees tried the system and hefted heavy suitcases with ease.

60

61. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
5G deployment and use cases ramp up, globally

A vast number of research teams, alliances, and corporations have sketched out compelling visions of how 5G will play out in the years to come. Approaching the challenge from different perspectives—consumer IoT, industrial IoT, smart cities, and more—and looking at how it will show up differently in various global situations.
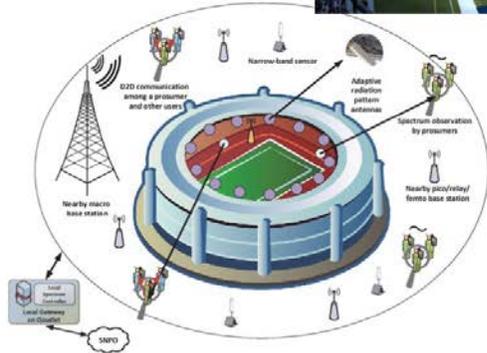
61
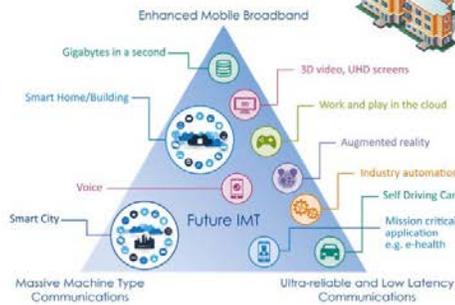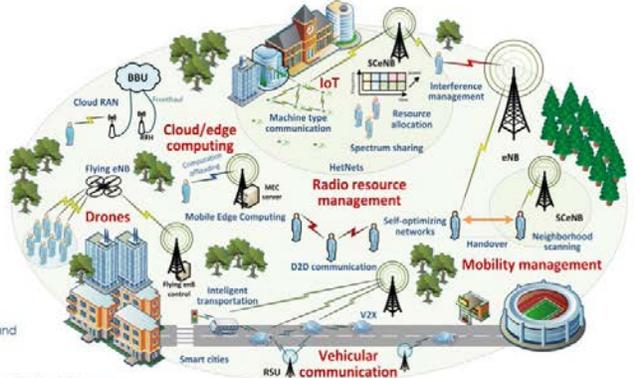
62. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
5G in stadiums and other dense public venues

Current networks are crippled when many devices are concentrated in one location. Signal strength is easy, but capacity is lacking. 5G will address this situation by utilizing the highest frequency bands and line-of-sight connections to the thousands of users who show up at concerts and sporting events. This will likely be one of the earliest success stories of the new technology.

https://es.kearney.com/article/?/a/finding-the-money-in-5g-sports-broadcasting
https://www.raconteur.net/business-innovation/5g-technology-sports

62

63. HYPERCONNECTED WORLD | 5G & Extreme Networks
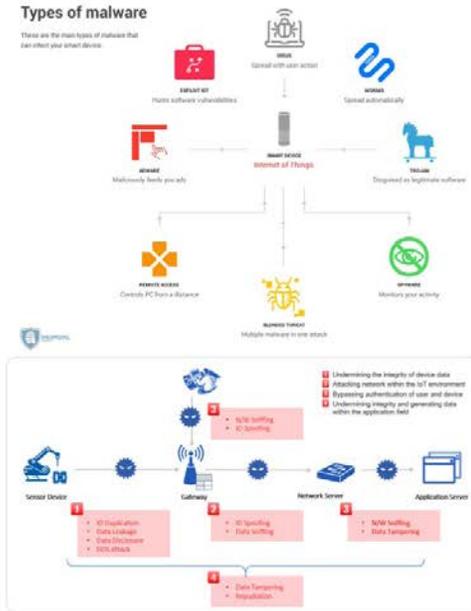
SUB-FORECAST
Distributed exploit opportunities abound

As more products become connected to the Internet and have options for external control and remote updates, they will be increasingly vulnerable to being compromised. This can include having their intended behavior maliciously altered and being used for exploiting other systems.

Bryan Lyles interview.
Bruce Schneier interview.

63

64. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
Vulnerabilities heightened by attack vector landscape

Exploits infiltrate enterprises through myriad paths, including mobile phones, wireless networks, laptops, and tablets, etc. Using AI to recognize the computational signatures of threats can help make the enterprise and individual telecom devices more secure.

SIGNAL | Tools with machine learning address attacks

WHAT: Zimperium offers the latest machine learning in the z9 engine to provide mobile security solutions and mobile threat protection.

SO WHAT: Detecting both known and unknown threats by analyzing device behavior can reduce the effects of hacking and viruses spread via mobile phone apps.

WHAT: Armis offers an agentless IoT security platform with capabilities such as automatic identification and disconnection of unmanaged devices from the network.

SO WHAT: The platform is an example of a new generation of tools to discover all devices in an environment, analyze their behavior to identify risks or attacks, and protect critical business information automatically.

https://www.zimperium.com/
https://www.armis.com/

ZIMPERIUM

ARMIS

64

---

65. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
Laws enacted that force cybersecurity compliance

Legislation and regulations will help force the industry into adopting some of the simple steps that could be taken to address the most blatant vulnerabilities (e.g., default passwords).

SIGNAL | California SB-327 signed

WHAT: California IoT security laws are the nation's first to require that manufacturers implement security measures for IoT hardware.

SO WHAT: Regulations will be one tool to encourage enterprises to adopt better IoT and IIoT security practices.

https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

65

66. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST

Cybersecurity impedes progress on IoT technology

IoT research says our current lack of ability to secure systems that include elements from different vendors is limiting IoT market growth. This issue is even more sharply felt in complex systems with intricate supply chains that include embedded software components. Refer to comprehensive Europa report on this topic.

enisa

Baseline Security Recommendations for IoT
in the context of Critical Information Infrastructures

NOVEMBER 2017

---

67. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST

Best practices are articulated but often ignored

Cybersecurity is a really hard issue to address: it cannot and will not be solved by localized efforts or buzzwords. Best practices do exist, but many products do not follow them, so companies incorporating components from diverse supply chains will need to adopt processes for certifying their supply chain components. These best practices are a broad set that must be incorporated into many phases of development and deployment, for both advanced manufacturing facilities and products with myriad embedded computational systems.

Secure Development Services
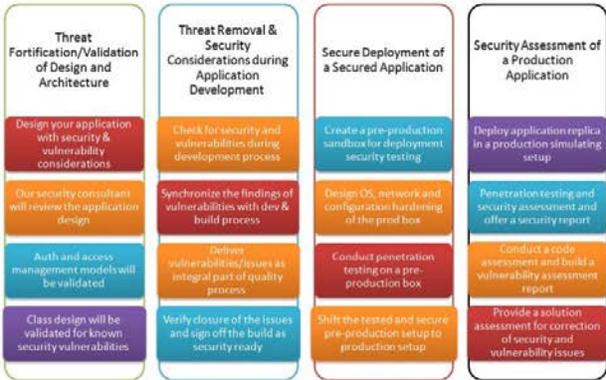
68. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST

Coordinated ransomware attacks spread

Ransomware attacks are getting bigger and more coordinated, with entire companies shutting down in the wake of being locked out of their systems and municipalities being crippled for weeks when their systems are compromised.

CYBER SECURITY | NEWS | 6 MIN READ

Massive Ransomware Attack in Texas Hits 22 Cities and Towns, Hackers Demand Millions in Payment

SCOTT IKEDA · SEPTEMBER 2, 2019

https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault
https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/

68

---

69. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST

Hackers will use machine learning to carry out attacks

Hackers will also be using AI technologies to identify targets and craft their attacks, so both the IIoT and the IoT are shaping up as major battlefields where the upcoming cyberwars will be fought.

https://pureai.com/articles/2018/08/10/ai-hacking.aspx
Bruce Schneier interview.

69

70. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
Blockchain is applied to IIoT

Some IIoT security challenges can potentially be partially addressed using blockchains for data exchange. Advances in blockchain technology (e.g., sharding) will soon get transaction rates up to where this is a viable approach.

SIGNAL | SW and HW help secure device transactions

WHAT: Filament's Blocklet application software and Blocklet Chip hardware solutions enable connected machines and devices to transact and exchange value against a blockchain.

SO WHAT: These emerging technologies will allow enterprises to connect with devices securely and the devices to exchange data autonomously.

https://filament.com

70

---

71. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
Blockchain-agnostic tools address compatibility issues

The rapid expansion of blockchain technology is making it easier for developers to be blockchain agnostic—to create platforms that can use multiple blockchains at the same time and adopt new ones as they arise. The decentralized nature of blockchain solutions has sparked renewed interest in expanding the IoT and seeking ways to address security authentication, mapping, and validation.

SIGNAL | New tools interoperate with many blockchains

WHAT: Korean startup HDAC is building a multiple-chain-based blockchain platform.

SO WHAT: Software platforms can facilitate machine-to-machine transactions, authenticate IoT devices, and create the mappings required for effective applications.

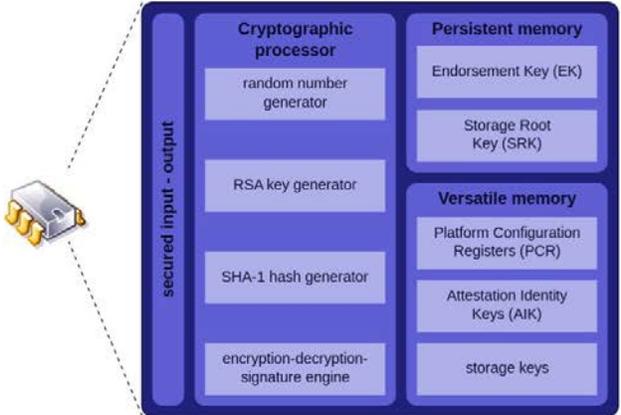https://iao42.com/resources/how-innovative-startups-are-using-blockchain-to-make-iot-more-secure/

71

72. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
Hardware-assisted cyber-security deployed more often

Trusted Platform Modules and other hardware solutions are being used in other sectors to provide assurances that IIoT devices are operating on a secure foundation, but they cannot guarantee the security of the rest of the IIoT software stack.

secured input - output	Cryptographic processor	Persistent memory
	random number generator	Endorsement Key (EK)
		Storage Root Key (SRK)
	RSA key generator	**Versatile memory**
		Platform Configuration Registers (PCR)
	SHA-1 hash generator	Attestation Identity Keys (AIK)
	encryption-decryption-signature engine	storage keys

Bryan Lyles interview

72

73. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST
Quantum computing technology advances, but cryptography survives

Doomsday scenarios about quantum computing defeating all key-based cryptography exist, but numerous approaches are being developed to address the issue.
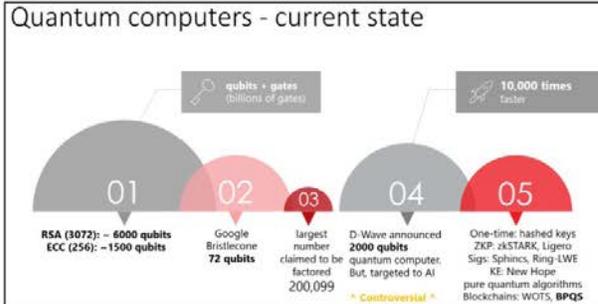
Quantum computers - current state

qubits + gates (billions of gates)   10,000 times faster

01 RSA (3072): ~ 6000 qubits ECC (256): ~1500 qubits

02 Google Bristlecone **72 qubits**

03 largest number claimed to be factored 200,099

04 D-Wave announced **2000 qubits** quantum computer. But, targeted to AI ^ Controversial ^

05 One-time: hashed keys ZKP: zkSTARK, Ligero Sigs: Sphincs, Ring-LWE KE: New Hope pure quantum algorithms Blockchains: WOTS, **BPQS**

Bruce Schneier interview.
Bryan Lyles interview.

73

74. HYPERCONNECTED WORLD | 5G & Extreme Networks

SUB-FORECAST

Quantum computing technology advances, but cryptography survives

NIST has initiated a Post-Quantum Cryptography Standardization process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. It is likely that NIST will select several algorithms at the end of the process, as each of the technologies has its own strengths and weaknesses.

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization
Bruce Schneier interview.
Bryan Lyles interview.

74

---

75. HYPERCONNECTED WORLD | Alternative Futures

SUB-FORECAST

Synthetic characters cannot be distinguished from real

Niche innovations can give particular vendors an inroad into highly-competitive market sectors. Integrating convincing characters, having fantastic language coverage, incorporating real-time translation and other features can open doors to otherwise shut market segments..

SIGNAL | Synthetic characters augment voice interfaces

WHAT: Samsung is showing their synthetic character generator that creates convincing 3D humans that run unscripted, with realistic expressions and body movements.

SO WHAT: Characters of this sort can augment interactions with digital agents, creating heightened engagement and interaction. These sorts of .innovations can help companies break into the crowded market or these technologies.

https://www.theverge.com/circuitbreaker/2020/1/3/21047923/samsung-neon-artificial-human-ces-2020-rumor

75

76. HYPERCONNECTED WORLD | Alternative Futures

SUB-FORECAST
Chinese government allows consoles, but with curfew

Constraint scenarios come with a host of restrictions that can significantly shape how new technologies get both introduced and used. Sometimes these situations are beneficial, like using a state-sponsored company to assure smooth and swift roll-out of a new telecommunication capability. Other times, forces end up altering the usage patterns of a new technology.

SIGNAL | China allows game consoles, but with curfew

WHAT: China has recently relaxed a long-standing ban on gaming consoles, but has now instituted a curfew on youth who play online

SO WHAT: Content and usage restrictions in China shift patterns of network activity. While these rules may benefit the education of students, they sow discontent.

https://fortune.com/2019/11/07/china-gaming-curfew-10-pm-under-age-18/

76

---

77. HYPERCONNECTED WORLD | Alternative Futures

SUB-FORECAST
Required activities spread propaganda & spy on citizens

Control scenarios can result in mandated activities, like apps that are required for government employees or spending time on news feeds that spread propaganda. Some of these activities can be further exploited to track the activities of the citizenry.

SIGNAL | Propaganda app includes a security hole

WHAT: China has mandated the use of the Study the Great Nation app for government employees, tying their engagement and scores to hiring and promotions.

SO WHAT: Beyond the observation of this app's content being government-sponsored propaganda, it was discovered that the app contains a back-door exploit that allows the government to spy on users.

https://www.bbc.com/news/technology-50042329

77

Bibliography

Ahmed, S. (2019, April 22). *The Messy Truth About Social Credit*. ChinaFile. http://www.chinafile.com/reporting-opinion/viewpoint/messy-truth-about-social-credit

Alba, D. (2019, December 20). Facebook Discovers Fakes That Show Evolution of Disinformation. *The New York Times*. https://www.nytimes.com/2019/12/20/business/facebook-ai-generated-profiles.html

Allen-Ebrahimian, B. (2020, January 22). *University of Minnesota student jailed in China for tweets critical of government*. Axios. https://www.axios.com/china-arrests-university-minnesota-twitter-e495cf47-d895-4014-9ac8-8dc76aa6004d.html

Alpaydin, E. (2016). *Machine Learning*. MIT Press.

Anderson, M., & Jiang, J. (2018, May 31). Teens, Social Media & Technology 2018. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

Anderson, N. (2009, September 8). *"Anonymized" data really isn't—And here's why not*. Ars Technica. https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

Anumanchipalli, G. K., Chartier, J., & Chang, E. F. (2019). Speech synthesis from neural decoding of spoken sentences. *Nature*, *568*(7753), 493–498. https://doi.org/10.1038/s41586-019-1119-1

Bangeman, E. (2006, September 26). *AOL subscribers sue over data leak*. Ars Technica. https://arstechnica.com/information-technology/2006/09/7835/

Belamire, J. (2016, October 22). *My First Virtual Reality Groping*. Medium. https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee

Bellingcat Investigation Team. (2018, September 26). *Skripal Suspect Boshirov Identified as GRU Colonel Anatoliy Chepiga*. Bellingcat. https://www.bellingcat.com/news/uk-and-europe/2018/09/26/skripal-suspect-boshirov-identified-gru-colonel-anatoliy-chepiga/

Bellingcat Investigation Team. (2019, June 19). *Identifying the Separatists Linked to the Downing of MH17*. Bellingcat. https://www.bellingcat.com/news/uk-and-europe/2019/06/19/identifying-the-separatists-linked-to-the-downing-of-mh17/

Benner, K. (2020, January 13). Barr Asks Apple to Unlock Pensacola Killer's Phones, Setting Up Clash. *The New York Times*. https://www.nytimes.com/2020/01/13/us/politics/pensacola-shooting-iphones.html

Bickert, M. (2020, January 7). Enforcing Against Manipulated Media. *About Facebook*. https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/

Bowles, N. (2018, June 23). *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*. The New York Times. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Bowles, N., & Keller, M. H. (2019, December 7). Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators. *The New York Times*. https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html

Brown, D. (2019, June 20). *Alexa could detect whether you're having a heart attack, study suggests*. USA Today. https://www.usatoday.com/story/tech/2019/06/20/alexa-could-detect-heart-attack-research/1508460001/

Buchholz, K. (2019, March 19). *Infographic: China's Most Popular Digital Payment Services*. Statista. https://www.statista.com/chart/17409/most-popular-digital-payment-services-in-china/

Buckley, C., & Mozur, P. (2019, May 22). How China Uses High-Tech Surveillance to Subdue Minorities. *The New York Times*. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). *Notes From the AI Fronter: Modeling the Impact of AI on the World Economy*. McKinsey Global Institute.

Bushwick, S. (2019, October 8). *New Encryption System Protects Data from Quantum Computers*. Scientific American. https://www.scientificamerican.com/article/new-encryption-system-protects-data-from-quantum-computers/

Calo, R. (2014). Digital Market Manipulation. *George Washington Law Review*, *82*, 995–1858.

Cassagnol, D. (2019, May 9). *Americans Adopt AI: Smart Speakers See Largest Gain in U.S. Household Ownership, Says CTA Study*. Consumer Technology

Association. https://www.cta.tech/News/Press-Releases/2019/May/Americans-Adopt-AI-Smart-Speakers-See-Largest-Gai.aspx

CBC News. (2019, February 14). *"China is your daddy": Backlash against Tibetan student's election prompts questions about foreign influence*. CBC. https://www.cbc.ca/news/canada/toronto/china-tibet-student-election-1.5019648

Chan, J., Rea, T., Gollakota, S., & Sunshine, J. E. (2019). Contactless cardiac arrest detection using smart devices. *Npj Digital Medicine*, *2*(1), 1–8. https://doi.org/10.1038/s41746-019-0128-7

Chaturvedi, S. (2016). *I am a Troll*. Juggernaut.

Chen, R. (2017, August 22). *Alipay and WeChat Prove That China's Future Is Cashless*. The Sixth Tone. https://sixthtone.com/news/1000731/alipay-and-wechat-prove-that-chinas-future-is-cashless

Chen, S., & Ng, E. (2019, July 20). *Gallium: China tightens grip on wonder metal as uses expand*. South China Morning Post. https://www.scmp.com/business/companies/article/3019299/gallium-china-tightens-grip-wonder-metal-huawei-works-promising

Chesney, Rebecca, Frauenfelder, M., Gentry, E., & Woolley, S. C. (2018). *Chat Apps: Frontiers and Challenges for Journalism*. Institute for the Future and Google News Lab. http://www.iftf.org/partner-with-iftf/research-labs/digital-intelligence-lab/research-archive/chat-apps-frontiers-and-challenges-for-journalism/

Chesney, Robert, & Citron, D. K. (2018). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (SSRN Scholarly Paper ID 3213954). Social Science Research Network. https://papers.ssrn.com/abstract=3213954

Chinoy, S. (2019, April 16). We Built an 'Unbelievable' (but Legal) Facial Recognition Machine. *The New York Times*. https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html

Chui, M., Manyika, J., & Miremadi, M. (2016). *Where machines could replace humans—And where they can't (yet)*. McKinsey Digital. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet

Clark, E. M., Williams, J. R., Jones, C. A., Galbraith, R. A., Danforth, C. M., & Dodds, P. S. (2016). Sifting Robotic from Organic Text: A Natural Language Approach for Detecting Automation on Twitter. *ArXiv:1505.04342 [Cs]*. http://arxiv.org/abs/1505.04342

Clark, R. (2019, October 30). *Operators Starting to Face Up to 5G Power Cost*. Light Reading 5G: A New Generation of Communications. https://www.lightreading.com/asia-pacific/operators-starting-to-face-up-to-5g-power-cost/d/d-id/755255

Collington, R. (2019, November 1). *Digital Public Assets: Rethinking value, access and control of public sector data in the platform age*. Common Wealth. https://www.common-wealth.co.uk/industrial-strategy-gnd.html

CommScope. (2018, October 3). Why is network densification important for 5G success? *RCR Wireless News*. https://www.rcrwireless.com/20181003/5g/5g-demands-more-network-densification

Cook, K., Pinder, D., Stewart III, S., Uchegbu, A., & Wright, J. (2019). *The future of work in black America*. McKinsey. https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-in-black-america

Corry, K. (2018, September 25). *Spotify Is Using DNA Tests to Curate Playlists, Which Is Pretty Creepy—VICE*. Vice. https://www.vice.com/en_us/article/8x7xd5/spotify-playlists-dna-curation-ancestry

Cox, J. (2018, November 16). Here's How Easy It Is to Make Your Own IMSI-Catcher. *Vice*. https://www.vice.com/en_us/article/gy7qm9/how-i-made-imsi-catcher-cheap-amazon-github

Cox, J. (2019a, January 8). I Gave a Bounty Hunter $300. Then He Located Our Phone. *Vice*. https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

Cox, J. (2019b, February 6). Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls. *Vice*. https://www.vice.com/en_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls

Dan Strumpf, Natasha Khan, & Charles Rollet. (2017, November 12). Surveillance Cameras Made by China Are Hanging All Over the U.S. *Wall Street Journal*. https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949

Daum, J. (2018, October 16). Social Credit Articles – A complete list of articles and interviews by Jeremy Daum on Social Credit. *China Law Translate*. https://www.chinalawtranslate.com/social-credit-articles/

Digital Intelligence Lab. (2018). *Journalism and False Information*. Institute for the Future. http://www.iftf.org/journalismandfalseinfo/

Emerging Technology from the arXiv. (2019, May 30). *How a quantum computer could break 2048-bit RSA encryption in 8 hours*. MIT Technology Review. https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

Energy RealPolitik. (2019, May 31). *What 5G Means for Energy*. Council on Foreign Relations. https://www.cfr.org/blog/what-5g-means-energy

Englehardt, S. (2020, January 17). *Firefox 72 blocks third-party fingerprinting resources*. Mozilla Security Blog. https://blog.mozilla.org/security/2020/01/07/firefox-72-fingerprinting/

Escritt, T., & Deutsch, A. (2017, March 11). Turkish protest grows outside consulate in Rotterdam. *Reuters*. https://www.reuters.com/article/us-turkey-referenedum-netherlands-protes-idUSKBN16I0RS

Farrow, R. (2019, October 7). *The Black Cube Chronicles, Part I: The Private Investigators*. https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators

First remote surgery in China conducted using 5G technology. (2019, March 17). Global Times. http://www.globaltimes.cn/content/1142340.shtml

Fox-Brewster, T. (2018, May 22). *Amazon Is Now A "Cheap Mass Surveillance" Dealer—It's Selling Facial Recognition To U.S. Cops*. Forbes. https://

www.forbes.com/sites/thomasbrewster/2018/05/22/amazon-now-sells-facial-recognition-to-american-police/

Freedom House. (2016, November 4). *Freedom on the Net 2016| Silencing the Messenger: Communication Apps Under Pressure*. Freedom House. https://freedomhouse.org/report/freedom-net/freedom-net-2016

Freedom on the Net 2019|China. (2019). Freedom House. https://www.freedomonthenet.org/country/china/freedom-on-the-net/2019

Frenger, P. (2019, September 17). *A technical look at 5G energy consumption and performance*. Ericsson.Com. https://www.ericsson.com/en/blog/2019/9/energy-consumption-5g-nr

Fruhlinger, J. (2018, March 9). *The Mirai botnet explained: How IoT devices almost brought down the internet*. CSO Online. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Genetic testing threatens the insurance industry. (2017, August 3). *The Economist*. https://www.economist.com/finance-and-economics/2017/08/03/genetic-testing-threatens-the-insurance-industry

Green, S. (2012, October). Nate Silver on Predicting the Unpredictable. *Harvard Business Review*. https://hbr.org/2012/10/nate-silver-on-predicting-the

Greenberg, A. (2018a, May 23). Stealthy, Destructive Malware Infects Half a Million Routers. *Wired*. https://www.wired.com/story/vpnfilter-router-malware-outbreak/

Greenberg, A. (2018b, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Guo, E. (2017, April 20). How WeChat Spreads Rumors, Reaffirms Bias, and Helped Elect Trump | Backchannel. *Wired*. https://www.wired.com/2017/04/how-wechat-spreads-rumors-reaffirms-bias-and-helped-elect-trump/

Hao, K. (2019a, February 16). *The technology behind OpenAI's fiction-writing, fake-news-spewing AI, explained*. MIT Technology Review. https://www.technologyreview.com/s/612975/ai-natural-language-processing-explained/

Hao, K. (2019b, June 6). *Training a single AI model can emit as much carbon as five cars in their lifetimes*. MIT Technology Review. https://www.technologyreview.com/s/613630/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/

Hao, K. (2019c, August 2). *AI researchers need to stop hiding the climate toll of their work*. MIT Technology Review. https://www.technologyreview.com/f/614056/ai-research-has-an-environment-climate-toll/

Hao, K. (2019d, August 29). *OpenAI has released the largest version yet of its fake-news-spewing AI*. MIT Technology Review. https://www.technologyreview.com/s/614237/openai-released-its-fake-news-ai-gpt-2/

Harvey, D. (2019, November 11). *Help us shape our approach to synthetic and manipulated media*. Twitter. https://blog.twitter.com/en_us/topics/company/2019/synthetic_manipulated_media_policy_feedback.html

Hassan, A. (2018, September 22). *Spotify and Ancestry can use your real DNA to tell your "musical DNA."* Quartz. https://qz.com/quartzy/1399279/spotify-can-use-your-ancestry-dna-test-to-tell-your-musical-dna/

Herman, P. (2018, March 5). *How renewable energy will power 5G mobile service*. Panasonic USA. https://na.panasonic.com/us/trends/how-renewable-energy-will-power-5g-mobile-service

Hill, K. (2020, January 18). The Secretive Company That Might End Privacy as We Know It. *The New York Times*. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hitchens, C. (2005). *Letters to a Young Contrarian*. Basic Books.

Hollister, S. (2019, February 6). *Carriers selling your location to bounty hunters: It was worse than we thought*. The Verge. https://www.theverge.com/2019/2/6/18214667/att-t-mobile-sprint-location-tracking-data-bounty-hunters

Holmes, A. (2018, March 2). 5G Cell Service Is Coming. Who Decides Where It Goes? *The New York Times*. https://www.nytimes.com/2018/03/02/technology/5g-cellular-service.html

How mobile money is spreading. (2018, May 4). *The Economist*. https://www.economist.com/special-report/2018/05/04/how-mobile-money-is-spreading

Hsu, J. (2018, January 29). The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data. *Wired*. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

Huang, F. (2018, November 27). China's Most Popular App Is Full of Hate. *Foreign Policy*. https://foreignpolicy.com/2018/11/27/chinas-most-popular-app-is-full-of-hate/

Hutchins, J. (1996). *ALPAC: The (In)Famous Report*. 5.

Hwang, T. (2018). Computational Power and the Social Impact of Artificial Intelligence. *ArXiv:1803.08971 [Cs]*. http://arxiv.org/abs/1803.08971

IDC. (2014, April). *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*. https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Indians are switching to digital payments in droves. (2019, June 8). *The Economist*. https://www.economist.com/finance-and-economics/2019/06/08/indians-are-switching-to-digital-payments-in-droves

India's digital platforms. (2018, May 4). *The Economist*. https://www.economist.com/special-report/2018/05/04/indias-digital-platforms

Jefrey-Willensky, J. (2019, April 26). *Scientists turn brain signals into speech with help from AI*. NBC News. https://www.nbcnews.com/mach/science/scientists-turn-brain-signals-speech-help-ai-ncna998551

John, T. (2019, November 26). *Hardline Hindus are pushing the Indian government's agenda on British voters*. CNN. https://www.cnn.com/2019/11/25/uk/bjp-kashmir-tory-uk-election-ge19-intl-gbr/index.html

Johnson, D. (2018, October 3). *The 5G Dilemma: More Base Stations, More Antennas—Less Energy?—IEEE Spectrum*. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/energywise/telecom/wireless/will-increased-energy-consumption-be-the-achilles-heel-of-5g-networks

Kalathil, S., & Boas, T. (2003, January 18). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2003/01/18/open-networks-closed-regimes-impact-of-internet-on-authoritarian-rule-pub-1072

Kania, E. B. (2019). *Securing Our 5G Future*. Center for New American Security. https://www.cnas.org/publications/reports/securing-our-5g-future

Kaptein, M., Duplinsky, S., & Markopoulos, P. (2011). Means based adaptive persuasive systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 335–344.

Karan, K. (2018, September 23). *#ElectionWatch: Boycott Campaign in Macedonia Features Familiar Characters*. Medium. https://medium.com/dfrlab/electionwatch-boycott-campaign-in-macedonia-features-familiar-characters-ef0f1aab52b6

Kessel, J. M. (2019, April 26). In a Secret Bunker in the Andes, a Wall That Was Really a Window. *The New York Times*. https://www.nytimes.com/2019/04/26/reader-center/ecuador-china-surveillance-spying.html

Khan, O. (2019, November 14). The BJP supporters' targeting of British Indian voters is divisive – and it won't work. *The Guardian*. https://www.theguardian.com/commentisfree/2019/nov/14/friends-of-bjp-indian-voters-tories

Khiaonarong, T., Humphrey, D., & Alwazir, J. (2019). Cash Use Across Countries and the Demand for Central Bank Digital Currency. *IMF Working Papers*.

Kim, A. (2019, October 8). *In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks*. CNN. https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html

Kokalitcheva, K., & Fischer, S. (2019, October 9). *American speech puts spotlight on Chinese censorship*. Axios. https://www.axios.com/american-speech-puts-spotlight-on-chinese-censorship-91263dbf-d9ba-44bc-8373-35582a8985df.html

Kolker, R. (2016, March 10). What Happens When the Surveillance State Becomes an Affordable Gadget? *Bloomberg*. https://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget

Konečný, J., McMahan, B., & Ramage, D. (2015). Federated Optimization: Distributed Optimization Beyond the Datacenter. *ArXiv:1511.03575 [Cs, Math]*. http://arxiv.org/abs/1511.03575

Kopf, D. (2017, December 8). *Meet the man behind the most important tool in data science*. Quartz. https://qz.com/1126615/the-story-of-the-most-important-tool-in-data-science/

Kopf, D. (2018, October 2). *The rise of Python, as seen through a decade of Stack Overflow*. Quartz. https://qz.com/1408660/the-rise-of-python-as-seen-through-a-decade-of-stack-overflow/

Lamo, M., & Calo, R. (2018). *Regulating Bot Speech* (SSRN Scholarly Paper ID 3214572). Social Science Research Network. https://papers.ssrn.com/abstract=3214572

Larkin, S. P. (2016, May). The Age of Transparency. *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency

Lee, Y. N. (2019, November 19). *Forget the QR code. Facial recognition could be the next big thing for payments in China*. CNBC. https://www.cnbc.com/2019/11/19/tencents-wechat-china-may-soon-use-facial-recognition-for-payments.html

Libert, T. (2019, September 18). This Article Is Spying on You. *The New York Times*. https://www.nytimes.com/2019/09/18/opinion/data-privacy-tracking.html

Lomas, N. (2019, October 9). European risk report flags 5G security challenges. *TechCrunch*. http://social.techcrunch.com/2019/10/09/european-risk-report-flags-5g-security-challenges/

Lourenço, M., & Marinos, L. (2019). *ENISA threat landscape for 5G Networks* [Report/Study]. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Macdonald, S. (2018, June 26). *How Tech Companies Are Trying to Disrupt Terrorist Social Media Activity*. Scientific American. https://www.scientificamerican.com/article/how-tech-companies-are-trying-to-disrupt-terrorist-social-media-activity/

Making faces Researchers produce images of people's faces from their genomes. (2017, September 9). *The Economist*. https://www.economist.com/science-and-technology/2017/09/09/researchers-produce-images-of-peoples-faces-from-their-genomes

Manjoo, F. (2017, October 18). How the Frightful Five Put Start-Ups in a Lose-Lose Situation. *The New York Times*. https://www.nytimes.com/2017/10/18/technology/frightful-five-start-ups.html

Markoff, J. (2015). *Machines of Loving Grace: The Quest for Common Ground between Humans and Robots*. Ecco.

Marr, B. (2018a, May 21). *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*. Forbes. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/

Marr, B. (2018b, August 13). *The 4th Industrial Revolution Is Here—Are You Ready?* Forbes. https://www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications*, 9(3). https://doi.org/10.14569/IJACSA.2018.090354

Mazzetti, M., Goldman, A., Bergman, R., & Perlroth, N. (2019, March 21). A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments. *The New York Times*. https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html

McCabe, D., Isaac, M., & Benner, K. (2019, December 10). Facebook and Barr Escalate Standoff Over Encrypted Messages. *The New York Times*. https://www.nytimes.com/2019/12/10/technology/whatsapp-barr-encryption.html

McEvoy, F. J. (2019, December 11). *If Virtual Reality Is Reality, Virtual Abuse Is Just Abuse.* Medium. https://towardsdatascience.com/if-virtual-reality-is-reality-virtual-abuse-is-just-abuse-34f09f1007ef

McMahan, B., & Ramage, D. (2017, April 6). Federated Learning: Collaborative Machine Learning without Centralized Training Data. *Google AI Blog*. http://ai.googleblog.com/2017/04/federated-learning-collaborative.html

Merton, R. K. (1968). The Matthew Effect in Science. *Science*, *159*(3810), 56–63.

Molteni, M. (2018, March 9). How WhatsApp Could Worsen Brazil's Yellow Fever Outbreak. *Wired*. https://www.wired.com/story/when-whatsapps-fake-news-problem-threatens-public-health/

Monaco, Nicholas, & Nyst, C. (2018, July). *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Institute for the Future. http://www.iftf.org/statesponsoredtrolling

Monaco, Nick. (2019, November 23). *Welcome to the Party: A Data Analysis of Chinese Information Operations*. Medium. https://medium.com/digintel/welcome-to-the-party-a-data-analysis-of-chinese-information-operations-6d48ee186939

Monaco, Nick, & Woolley, S. (2017, September 6). Tech companies automate autocratic media in China around the world. *TechCrunch*. http://social.techcrunch.com/2017/09/06/tech-companies-automate-autocratic-media-in-china-around-the-world/

Mozur, P. (2017, July 20). Beijing Wants A.I. to Be Made in China by 2030. *The New York Times*. https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

Mozur, P., Kessel, J. M., & Chan, M. (2019, April 24). Made in China, Exported to the World: The Surveillance State. *The New York Times*. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Mozur, P., & Krolik, A. (2019, December 17). *A Surveillance Net Blankets China's Cities, Giving Police Vast Powers*. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html

Mozur, P., & Merced, M. J. de la. (2016, April 26). Alibaba Financial Affiliate Raises $4.5 Billion. *The New York Times*. https://www.nytimes.com/2016/04/27/business/dealbook/jack-ma-alibaba-alipay-ant-financial.html

Nakashima, E., & Mekhennet, S. (2019, April 1). *U.S. officials planning for a future in which Huawei has a major share of 5G global networks*. Washington Post. https://www.washingtonpost.com/world/national-security/us-officials-planning-for-a-future-in-which-huawei-has-a-major-share-of-5g-global-networks/2019/04/01/2bb60446-523c-11e9-a3f7-78b7525a8d5f_story.html

Narayanan, A., & Shmatikov, V. (2007). How To Break Anonymity of the Netflix Prize Dataset. *ArXiv:Cs/0610105*. http://arxiv.org/abs/cs/0610105

Narayanan, A., & Shmatikov, V. (2009). De-anonymizing Social Networks. *2009 30th IEEE Symposium on Security and Privacy*, 173–187. https://doi.org/10.1109/SP.2009.22

National Security Commission on Artificial Intelligence. (2019). *National Security Commission on Artificial Intelligence: Interim report*. National Security Commission on Artificial Intelligence.

Newman, L. H. (2019, January 3). The Elite Intel Team Still Fighting Meltdown and Spectre. *Wired*. https://www.wired.com/story/intel-meltdown-spectre-storm/

Nimmo, B., Eib, C. S., Tamora, L., Johnson, K., Smith, I., Buziashvili, E., Kann, A., Karan, K., Rosas, E. P. de L., & Rizzuto, M. (2019, December 20). *#OperationFFS: Fake Face Swarm*. https://graphika.com/reports/operationffs-fake-face-swarm/

Nordrum, A., & Clark, K. (2017, August 19). *5G Bytes: Small Cells Explained—IEEE Spectrum*. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-small-cells-explained

Nuttall, J. (2019, October 20). *Extreme-right misinformation is flooding Chinese media in Canada—And observers say there's virtually nothing stopping it | The Star*. The Toronto Star. https://www.thestar.com/vancouver/2019/10/20/extreme-right-misinformation-is-flooding-chinese-media-in-canada-and-observers-say-theres-virtually-nothing-stopping-it.html

OECD. (2018). *GDP Long-Term Forecast*. Organization for Economic Cooperation and Development. https://data.oecd.org/gdp/gdp-long-term-forecast.htm

Ohlberg, M., Ahmed, S., & Lang, B. (2017, December 12). *Central Planning, Local Experiments*. ChinaFile. http://www.chinafile.com/library/reports/central-planning-local-experiments

Olson, P. (2019, January 15). *For $29, This Man Will Help Manipulate Your Loved Ones With Targeted Facebook And Browser Links*. Forbes. https://www.forbes.com/sites/parmyolson/2019/01/15/a-shadowy-entrepreneur-claims-his-online-manipulation-business-is-thriving/

Ooi, J. (2015). *IMSI Catchers and Mobile Security*. School of Engineering and Applied Science University of Pennsylvania.

Patrini, G. (2019, October 7). Mapping the Deepfake Landscape. *Deeptrace*. https://deeptracelabs.com/mapping-the-deepfake-landscape/

Peng, J., & Chiu, J. (2018, October 16). *Vancouver society at centre of vote-buying allegations has ties to Chinese government | The Star*. The Toronto Star. https://www.thestar.com/vancouver/2018/10/16/vancouver-society-at-centre-of-vote-buying-allegations-has-ties-to-chinese-government.html

Perlroth, N., & Shane, S. (2019, May 25). In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc. *The New York Times*. https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Poibeau, T. (2017). *Machine Translation*. MIT Press.

Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). *Language Models are Unsupervised Multitask Learners*. OpenAI. https://cdn.openai.com/better-language-models/language_models_are_unsupervised_multitask_learners.pdf

Rajagopalan, M. (2017, October 17). *This Is What A 21st-Century Police State Really Looks Like*. BuzzFeed News. https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here

Reeves, C. (2018). The virtual simulation of child sexual abuse: Online gameworld users' views, understanding and responses to sexual ageplay. *Ethics and Information Technology*, *20*(2), 101–113. https://doi.org/10.1007/s10676-018-9449-5

Regalado, A. (2018, February 12). *2017 was the year consumer DNA testing blew up*. MIT Technology Review. https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/

Regalado, A. (2019, February 11). *More than 26 million people have taken an at-home ancestry test—MIT Technology Review*. MIT Technology Review. https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/

Rich, M. (2012). *Should We Make Crime Impossible?* (SSRN Scholarly Paper ID 2029201). Social Science Research Network. https://papers.ssrn.com/abstract=2029201.204

Riley, M., Etter, L., & Pradhan, B. (2018, July 19). A Global Guide to State-Sponsored Trolling. *Bloomberg*. https://www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/

Robertson, J., & Riley, M. (2018, October 4). China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies. *Bloomberg*. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Robles, P. (2018, October 1). *China plans to be a world leader in Artificial Intelligence by 2030*. South China Morning Post. https://multimedia.scmp.com/news/china/article/2166148/china-2025-artificial-intelligence/index.html

Rosenblatt, F. (1958). The perceptron: A probabilistic model for information storage and organization in the brain. *Psychological Review*, *65*(6), 385–407. https://doi.org/10.1037/h0042519

Safi, M. (2018, August 30). Demonetisation drive that cost India 1.5m jobs fails to uncover "black money." *The Guardian*. https://www.theguardian.com/world/2018/aug/30/india-demonetisation-drive-fails-uncover-black-money

Sanger, D. E. (2019). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Crown.

Schechner, S., Glazer, E., & Haggin, P. (2019, October 10). Political Campaigns Know Where You've Been. They're Tracking Your Phone. *Wall Street Journal*. https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889

Schneier, B. (2007, December 12). *Why "Anonymous" Data Sometimes Isn't*. Wired. https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/

Schneier, B. (2018, September 14). *Quantum Computing and Cryptography*. Schneier on Security. https://www.schneier.com/blog/archives/2018/09/quantum_computi_2.html

Schneier, B. (2019, September 25). *Every Part of the Supply Chain Can Be Attacked*. The New York Times. https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html

Schwartz, P. M., & Solove, D. J. (2011). The PII Problem: Privacy and a new Concept of Personally Identifiable Information. *New York University Law Review*, *86*(8), 1814–1894.

Schwartz, R., Dodge, J., Smith, N. A., & Etzioni, O. (2019). Green AI. *ArXiv:1907.10597 [Cs, Stat]*. http://arxiv.org/abs/1907.10597

Schwirtz, M., & Barry, E. (2018, October 9). Armchair Investigators at Front of British Inquiry Into Spy Poisoning. *The New York Times*. https://www.nytimes.com/2018/10/09/world/europe/bellingcat-skripal-poisoning.html

Shanker, R., Locraft, G., & Flannery, S. (2013). Autonomous Cars: Self-Driving the New Auto Industry Paradigm. *Morgan Stanley*, 109.

Shi, F. (2019, August 28). Threat Spotlight: Government Ransomware Attacks. *Barracuda*. https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/

Silverman, C., Lytvynenko, J., & Kung, W. (2020, January 6). *Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online*. BuzzFeed News. https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms

Smith, C. S. (2019, November 4). *U.S. should consider pooling data with other countries to beat China in artificial intelligence, group says*. The Washington Post. https://www.washingtonpost.com/technology/2019/11/05/us-should-consider-pooling-data-with-other-countries-beat-china-artificial-intelligence-group-says/

Srivastava, M. (2020, January 21). *Saudi's MBS implicated in hacking of Jeff Bezos's phone*. Financial Times. https://www.ft.com/content/83dcdf74-3c9b-11ea-a01a-bae547046735

Stanton, C., Lung, V., Nancy (Hanzhuo) Zhang, Minori Ito, Weber, S., & Charlet, K. (2019, August 5). *What the Machine Learning Value Chain Means for Geopolitics*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/08/05/what-machine-learning-value-chain-means-for-geopolitics-pub-79631

Stoppard, L. (2018, August 3). *Inside The Spinner: A real-life inception project*. Financial Times. https://www.ft.com/content/944d068c-8a99-11e8-affd-da9960227309

Sulmeyer, M. (2019, February 15). *How the U.S. Can Play Cyber-Offense*. https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense

Ternoff, B. (2018, April 1). *The Data Is Ours!* Logic Magazine. https://logicmag.io/scale/the-data-is-ours/

The battle for the remittances market. (2018, May 4). *The Economist*. https://www.economist.com/special-report/2018/05/04/the-battle-for-the-remittances-market

The new red scare on American campuses. (2020, January 2). *The Economist*. https://www.economist.com/briefing/2020/01/02/the-new-red-scare-on-american-campuses

The truly personal computer. (2015, February 26). *The Economist*. https://www.economist.com/briefing/2015/02/26/the-truly-personal-computer

The Year of the Rat Fink Some people in China help the party police the internet. (2020, January 18). *The Economist*. https://www.economist.com/china/2020/01/18/some-people-in-china-help-the-party-police-the-internet?frsc=dg%7Ce

Thompson, S. A., & Warzel, C. (2019, December 19). Twelve Million Phones, One Dataset, Zero Privacy. *The New York Times*. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

Truby, J. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Research & Social Science*, *44*, 399–410. https://doi.org/10.1016/j.erss.2018.06.009

Van Chien, T., Björnson, E., & Larsson, E. G. (2016). Joint Power Allocation and User Association Optimization for Massive MIMO Systems. *IEEE Transactions on Wireless Communications*, *15*(9), 6384–6399. https://doi.org/10.1109/TWC.2016.2583436

Vincent, J. (2019, July 4). *Bitcoin consumes more energy than Switzerland, according to new estimate*. The Verge. https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison

Wakefield, J. (2017, June 28). Tax software blamed for cyber-attack. *BBC News*. https://www.bbc.com/news/technology-40428967

What technology can do for Africa. (2017, November 10). *The Economist*. https://www.economist.com/special-report/2017/11/10/what-technology-can-do-for-africa

Why India wants to track WhatsApp messages. (2019, October 30). *BBC News*. https://www.bbc.com/news/world-asia-india-50167569

Yang, Y., Murgia, M., & Gross, A. (2019, December 1). *Chinese tech groups shaping UN facial recognition standards*. Financial Times. https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67

Young, R., & Saxena, K. (2019, November 27). *Domestic Abusers Are Weaponizing Apps And In-Home Devices To Monitor, Intimidate Victims*. WBUR: Here & Now. https://www.wbur.org/hereandnow/2019/11/27/domestic-abuse-apps-home-devices

Zakaria, F. (2019, December 27). *The New China Scare*. https://www.foreignaffairs.com/articles/china/2019-12-06/new-china-scare

Zegart, A., & Morell, M. (2019, May). Spies, Lies, and Algorithms. *Foreign Affairs*. https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms

Zhang, H. (2019, August 19). *College Daily, the "Post-Truth" Publication Where Chinese Students in America Get Their News*. The New Yorker. https://www.newyorker.com/culture/culture-desk/the-post-truth-publication-where-chinese-students-in-america-get-their-news?verso=true