CUTTER Business Technology Journal

Management, Innovation, Transformation

Vol. 33, No. 1, 2020

2020 Trends and Predictions

CUTTER Business Technology Journal

As business models for creating value continue to shift, new business strategies are constantly emerging and digital innovation has become an ongoing imperative. *Cutter Business Technology Journal* delivers a comprehensive treatment of these strategies to help your organization address and capitalize on the opportunities of this digital age.

Cutter Business Technology Journal is unlike academic journals. Each monthly issue, led by an expert Guest Editor, includes five to seven substantial articles, case studies, research findings, and/or experience-based opinion pieces that provide innovative ideas and solutions to the challenges business technology professionals face right now — and prepares them for those they might face tomorrow. *Cutter Business Technology Journal* doesn't water down or delay its content with lengthy peer reviews. Written by internationally known thought leaders, academics, and practitioners — you can be certain you're getting the uncensored perspectives of global experts.

You'll benefit from strategic insight on how the latest movements in digital innovation and transformation, artificial intelligence/machine learning, Internet of Things, blockchain, analytics, and cloud, to name a few, are changing the business landscape for both new and established organizations and how cutting-edge approaches in technology leadership, enterprise agility, software engineering, and business architecture can help your organization optimize its performance and transition to these new business models.

As a subscriber, you'll also receive the *Cutter Business Technology Advisor* — a weekly bulletin featuring industry updates delivered straight to your inbox. Armed with expert insight, data, and advice, you'll be able to leverage the latest business management thinking to achieve your organization's goals.

No other journal brings together so many thought leaders or lets them speak so bluntly — bringing you frank, honest accounts of what works, what doesn't, and why. Subscribers have even referred to *Cutter Business Technology Journal* as a consultancy in print and likened each month's issue to the impassioned discussions they participate in at the end of a day at a conference!

Get the best in thought leadership and keep pace with the technologies and business models that will give you a competitive edge — subscribe to *Cutter Business Technology Journal* today!

Founding Editor: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Christine Generali
Managing Editor: Cindy Swain
Copy Editors: Jennifer Flaxman, Tara Meads
Production Editor: Linda Dias
Client Services: service@cutter.com

Cutter Business Technology Journal® *is published monthly by Cutter Consortium, an Arthur D. Little Technology company, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA • Tel: +1 781 648 8700 • Fax: +1 781 648 8707 • Email: cbtjeditorial@cutter.com • Website: www.cutter.com • Twitter: @cuttertweets • Facebook: Cutter Consortium. ISSN: 2475-3718 (print); 2475-3742 (online).*

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Consortium. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

□ Start my print subscription to *Cutter Business Technology Journal* ($485/year; US $585 outside North America).

Name Title

Company Address

City State/Province ZIP/Postal Code

Email (Be sure to include for weekly *Cutter Business Technology Advisor*)

Fax to +1 781 648 8707, call +1 781 648 8700, or send email to service@cutter.com.
Mail to Cutter Consortium, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA.

Request Online License Subscription Rates

For subscription rates for online licenses, email or call: **sales@cutter.com** or **+1 781 648 8700.**

CUTTER CONSORTIUM
●●● *Access to the Experts*

Opening Statement

by the *Cutter Business Technology Journal* Team

It's hard to believe that 20 years ago we were barely using cell phones; the Internet — with an extremely slow dial-up connection — was just starting to catch on; and we were saving data on floppy disks. But as we enter the third decade of the 21st century, technological progress is staggering and unrelenting. Smartphones, social media, and the Internet have changed the way we communicate. Enterprises are capitalizing on an array of technologies — artificial intelligence (AI), machine learning (ML), automation, and the Internet of Things (IoT), to name a few — to transform their operations, ultimately hoping to deliver better customer experience and greater value.

With all that is new and changing before our eyes, we asked the Cutter Consortium team of experts to weigh in on the technologies, strategies, and business models that will have the most relevance this year and beyond. Their responses range from the need for more technology regulation to what technologies will be most transformative, from guidelines for keeping our data safe to minimizing the profusion of misinformation. We are sure you'll find value in these observations and we trust that they'll give you the foresight to proceed with optimism, yet vigilance, into this new decade.

In This Issue

In our first article, Cutter Consortium Fellow Steve Andriole discusses the lack of technology regulatory action by the US government. He opens with the assertion that "the proliferation of misinformation on social media, drones flying in protected airspace, and the exploding personal surveillance of Americans are but three examples of the crying need for regulatory action." Andriole details 10 technology areas in need of attention, and the associated guidelines, policies, and regulations that would go a long way in keeping technology misuse in check.

Our next piece moves on to business architecture. According to Cutter Consortium Senior Consultant Whynde Kuehn, "Amid a backdrop of digital transformation and a continually shifting landscape of change, business architecture is gaining momentum and relevance." In her article, she discusses the areas in which business architecture will continue to play a key role and illustrates how three specific scenarios will lead the way to increased relevance and leadership. Kuehn lays out what this might mean to you, along with the steps you need to take to realize these benefits.

> *It's hard to believe that 20 years ago we were barely using cell phones.*

Cybersecurity urgently needs attention from businesses and government, according to Cutter Consortium Senior Consultant Paul Clermont. He highlights how several colliding trends — complexity, AI, and interconnectedness — are compounding long-standing risks. Clermont discusses the tactics necessary to address them but cautions that "compounding the difficulty of these tasks is the need to be able to execute algorithms and procedures in nanoseconds — a tall order that should inspire a bit of conservatism about how much functionality and connectivity we might want versus what we truly need."

Next, Cutter Consortium Senior Consultant Claude Baudoin addresses the issue of trust, or mistrust, in the information we rely on to stay informed or to make decisions. He writes, "This article is not a definitive proposal to achieve the elusive goal of knowing what we can trust, but rather a set of perspectives and considerations to justify the urgency of addressing this issue." Some reasons for our untrusting mindsets include "deep fakes," voting systems breaches, bias in decision algorithms, unknown sources of email, insufficiently secured IoT systems, and robocalls.

> *We live in an exciting time, with technology a catalyst for many of our aspirations.*

Autonomous systems are on the rise and, according to Cutter Consortium Senior Consultant San Murugesan, will "transform many different sectors in unimaginable ways." He describes how technologies such as IoT, drones, robotics, ML, AI, and nano, among others, will extend the capabilities of autonomous systems. Current applications of autonomous systems technology draw attention to the adoption challenges. "For starters," writes Murugesan, "we need to ensure that these systems are built to perform reliably, safely, and sustainably — and are tested and validated satisfactorily. We also need to secure them against hacks and unintentional manipulation and prevent them from being used for unintended harmful purposes or to constitute threats to people and property."

Cutter Consortium Senior Consultant Curt Hall predicts an increase in enterprise adoption of AI and, echoing Andriole's sentiments, emphasizes "calls for new regulations to help guide and ensure the fair use of the technology." He also anticipates a demand for greater transparency, fairness, and "explainability" in AI applications and products from developers and end-user organizations. Moreover, according to Hall, new natural language processing "tools and products … will accelerate enterprise application of the technology, including the use of speech recognition."

Next, Cutter Consortium contributor Barry M. O'Reilly questions the validity of Agile practices. According to him, "The Agile movement's focus on process as the solution to uncertainty has allowed technical quality to fall by the wayside, bringing even more doubt as to the ability of Agile to actually deliver." O'Reilly contends that "only the people working directly with a problem can decide on tools and process in the evolving picture of their project, and their individual talents — not adherence to or avoidance of certain ideas — guide whether they achieve success or not." What is your opinion on Agile versus talent, or is it Agile *and* talent?

Finally, in our concluding piece, Cutter Consortium Senior Consultant Helen Pukszta brings us up to speed on the trends shaping drone usage. She foresees more enactment of regulations and new opportunities for business users of drones as well as for drone technology providers. According to Pukszta, "Regulatory changes, new drone technology, and continuing business adoption will make 2020 an exciting year for all drone users, but many sweeping changes, opportunities, and automation benefits of drones are still ahead of us." How might your organization benefit from drones?

We live in an exciting time, with technology a catalyst for many of our aspirations. We wish you the best of luck in your endeavors in 2020 and hope that the articles in this issue of *Cutter Business Technology Journal* provide you with food for thought and inspiration for action.

Upcoming Topics

Digital Shift
Volker Pfirsching

**Want Happy Customers?
Make Your Employees Happy!**
Robert Scott

Disruptive Agile
Hillel Glazer

Information Trustworthiness/Security
Claude Baudoin

Automation: AI, ML, RPA
San Murugesan

THE FUTURE'S NOT BRIGHT

US Regulators Will Again Fail Technology in 2020

by Steve Andriole

My 2020 prediction: the US federal government will once again ignore its technology regulatory duties.

Let's acknowledge that the US has consistently ignored its technology regulatory duties for decades, and it will likely continue to do so for the foreseeable future. Let's also acknowledge that the need for regulation has never been greater. The proliferation of misinformation on social media, drones flying in protected airspace, and the exploding personal surveillance of Americans are but three examples of the crying need for regulatory action. But federal regulators are nowhere to be found. Other shortcomings abound; the current US technology investment strategy is failing miserably: the US ranks 25th in the world in R&D tax credits,[1] has fallen out of the top 10 in global innovation,[2] is losing the artificial intelligence (AI) arms race,[3] is experiencing falling rankings in computer science and engineering,[4] and is ranked 11 in the world in "technological readiness."[5]

So what should regulators do? What steps should they take? What should be the guiding principles and policies? There are at least 10 areas screaming for regulation and larger federal policies:

1. Privacy
2. Surveillance
3. Misinformation
4. Innovation
5. Robotics
6. STEM (science, technology, engineering, and mathematics)
7. Talent
8. Oligarchy
9. Cybersecurity
10. AI

Let's break them down with a callout of my predictions.

1. Privacy

First and foremost, the US needs to pass an equivalent of the General Data Privacy Regulation (GDPR). Since many private and public corporations are unlikely to help with privacy (since regulations undermine their business models by limiting, protecting, and controlling the information they collect and monetize), the federal government needs to regulate how far corporations can go in their use of individuals' data. The US State of California has already moved in the GDPR direction with its Consumer Privacy Act, which allows Californians to delete their personal data and block the sale of their data to marketers and other vendors. More states are following, which is why, among other reasons, the US needs a federal law to have a consistent privacy policy across the country.

Will any of this happen in 2020? No, though some states — such as Nevada, New York, and Washington — are following California's lead.

> *Will there be any meaningful regulations regarding surveillance in 2020? No.*

2. Surveillance

Regulators need to address the growing surveillance culture, which includes the rapid deployment of facial recognition technologies. This is easily a privacy tipping point. Or at least it should be. The Surveillance Economy[6] is now in full swing. Assuming that you live online and, therefore, provide your personal, professional, location, and behavioral data on a regular basis, there is nothing left that's protected by regulators.

Will there be any meaningful regulations regarding surveillance in 2020? No, primarily because serious regulation here would threaten the monetization of surveilled data, which is a major pillar of the country's economic foundation.

3. Misinformation

The need for regulation in the area of misinformation is screaming from every broadcast tower in the country. The problem, of course — again — is business models that depend upon misinformation, such as public and private media that win by attracting as many participants as possible, even if the participants are loathsome. The regulatory agenda here is complex, to put it mildly, since it involves the First Amendment to the US Constitution. That said, there's a floor upon which "free speech" builds. Hate websites weaken the foundation. The exploitation of media access and the manipulation of content for political advantage require regulation. The dissemination of false content over public networks requires regulation. Recategorizing technology companies as the media companies they clearly are is way overdue.

Prediction? Regulation in this area is not going to happen in 2020, or the foreseeable future.

4. Innovation

The US ranks 25th in the world in R&D tax credits.[7] The federal government needs to dramatically increase R&D tax credits to get the country in the top 10, at a minimum. Information Technology and Innovation Foundation (ITIF) Senior Fellow Joe Kennedy tells us that "Germany, the UK and China are sweetening the pot, while the US slides."[8]

According to Kennedy, "The United States needs to follow the international trend. The [ITIF] has called for increasing the tax credit's Alternative Simplified Credit to at least 20% from its current rate of 14%."[9] How about 25%? While the US dual-use technology investment model has worked to some extent in the past, it's past time for new, single-use investment strategies that bypass the government and go directly to incentivized industries and straight to commercialization.

There are other steps the US should take, as outlined by ITIF President Robert Atkinson:

> The last time the federal government had anything resembling a national innovation strategy was almost 40 years ago.… [T]he federal government takes an ad hoc approach to innovation policy, rather than approach it in a strategic way.… And as a result, it misses significant opportunities. There's also a lack of institutionalization in US innovation policy making; Congress doesn't require any federal agency to be accountable for innovation policymaking, so an administration only produces an innovation strategy if it's inclined to do so.… Few if any federal agencies formally recognize the promotion of innovation (either internally or externally) as part of agency agendas or strategic plans. And this is in part because innovation is not explicitly incorporated in agency missions.[10]

So what will happen in 2020? Will there be a funded innovation strategy instantiated in policies and regulations? Not in 2020, that's for sure.

5. Robotics

How is it possible to fly a drone onto the White House lawn (as occurred a few years ago)? Here's the problem:

> Thanks to their onboard cameras that transmit a visual feed to a pilot's smartphone or tablet, drones can be flown miles from their starting point, making it hard to find a pilot even if their drone is caught in a restricted area. And the FAA [US Federal Aviation Administration] itself has "limited boots on the ground," as a spokesperson put it, often leaving it up to local law enforcement groups to deal with out-of-bounds flyers.[11]

Drones are the least of our problems with (broadly defined) "robotics." Where are the regulations around manufacturing robotics? Farm robotics? Autonomous vehicles? Robotic concierges? What's going on?

> Currently, any regulations of robotics and AI are spread out across many organizations. The Federal Aviation Administration, Securities and Exchange Commission, and the National Highway Traffic Safety Administration have some of the responsibility when it comes to robotics regulations. However, this arrangement doesn't allow for full coverage or expertise in this highly technical and rapidly changing field.
>
> While the US federal government is lagging behind technological advances, many states are struggling to come up with their own solutions. Legislation on autonomous vehicles has been passed [in] Alabama, California, Florida, Louisiana, Michigan, Nevada, North Dakota, Pennsylvania, Tennessee, Utah, and Virginia, as well as in Washington, DC, since 2012. However, when you compare the body of legislation to that of the airline industry, it doesn't even come close. If every department takes on only the robotics issues that affect it directly, there's no across-the-board policy, which can lead to confusion.[12]

Can we expect an integrated set of regulations around robotics? While other countries have begun the regulatory process, the US lags way behind. The year 2020 will not be a catch-up year.

6. STEM

I cannot think of a more important foundational step the US can take to improve the technology infrastructure of the US than supporting STEM in education, which is why the "US Department of Education Fulfills Administration Promise to Invest $200 Million in STEM Education."[13] Sounds good, right? But it's sadly laughable — if not insulting to those who believe wider and deeper STEM education helps everyone. Remember that *one* B-2 Spirit aircraft costs US taxpayers $737 million. One aircraft carrier (without the planes), the USS Gerald R. Ford, cost $13 billion, *or 65 times the government's investment in STEM*. The US just christened the aircraft carrier USS John F. Kennedy, which will eventually cost $11.5 billion. *Federal STEM funding should be increased by at least 50-fold*. Federal STEM educational guidelines should include funding for state-run STEM educational and training programs. Matching federal funding of state-funded programs should also be widely available — and permanent.

Prediction? Not in 2020. Maybe never, which raises questions about US technology policy.

7. Talent

Data reporter Rani Molla succinctly describes how the immigration barriers that the administration of US President Donald Trump has imposed make it increasingly difficult for skilled workers to come to the US:

> Using executive orders, the president has made it more difficult — and expensive — to hire high-skilled tech workers from other countries. The administration has throttled a program that encouraged entrepreneurs to come to the US. It's also ending work permits for spouses of H-1B holders, who are often highly skilled professionals themselves, among other measures to stop immigration. One result has been a net decline in high-skilled visas, known as H-1Bs, which has been bad for tech companies in the US (but good for Canada).[14]

Similarly, a *Wired* headline from early 2019 highlights: "Visa Rejections for Tech Workers Spike Under Trump."[15] What else needs to be said about the race for the best and brightest? Sane technology policy (and resultant regulations) is to incentivize the best and brightest around the world to seek the US as their professional destination. A more recent headline summarizes just how the situation stands today: "The Trump Administration Is Denying H-1B Visas at a Dizzying Rate."[16] This is a dangerous, bizarre strategy whose consequences will be felt for decades. The regulators must reverse these policies; policy must reflect the desire to attract the best and brightest if technological competitiveness is the objective.

Prediction? No changes in 2020. Perhaps there will be changes in 2021, depending on the results of the US presidential election.

8. Oligarchy

In 2018, the five largest companies in the world (by valuation) were Apple, Google, Microsoft, Amazon, and Facebook, followed closely by Alibaba, Berkshire Hathaway, Tencent Holdings, JPMorgan Chase, ExxonMobil, Johnson & Johnson, and Samsung Electronics.[17] Amazon owns around 50% of the e-commerce market, followed by eBay (6.6%), Apple (3.9%), Walmart (3.7%), and Home Depot (1.5%).[18] Four vendors own close to 75% of the cloud infrastructure market (Amazon Web Services [AWS], 33%; Microsoft, 13%; IBM, 8%; Google, 6%; and Alibaba, 4%, as of Q1 2018), and three providers — AWS, Microsoft, and Google — own 55% of the overall cloud market.[19] Google owns over 90% of the Internet search market.[20] Facebook continues to dominate social media, followed by YouTube (Google), WhatsApp (Facebook), Facebook Messenger (Facebook), WeChat (Tencent), and Instagram (Facebook).[21] Microsoft owns 36% of the worldwide operating system market, behind Android at 42% (Google and the Open Handset Alliance).[22] The same market trends are seen in other industries, such as ridesharing, where Uber and Lyft own over 70% of the market.[23]

Policies that reflect a commitment to competition and innovation should yield regulations about what's acceptable and what's not, since it's impossible to compete with oligarchies with decades-long leads. David Wessel, writing in the *Harvard Business Review*, is clear:

> Despite their undeniable popularity, Apple, Amazon, Google, and Facebook are drawing increasing scrutiny from economists, legal scholars, politicians, and policy wonks, who accuse these firms of using their size and strength to crush potential competitors. Technology giants pose unique challenges, but they also represent just one piece of a broader story: a troubling phenomenon of too little competition throughout the US economy.[24]

As many agree, it's time to resurrect antitrust.

Prediction? Technology oligarchies will not be broken up. Instead, they will grow — regardless of 2020 presidential election results.

9. Cybersecurity

The US digital infrastructure is leaky, to put it ridiculously mildly. Just as dangerous, the digital infrastructure and the most popular applications — such as social media — are vulnerable to manipulation by terrorists, hackers, adversaries, and human and software bots. According to the US Department of Homeland Security (DHS), the threats are everywhere and growing. DHS believes that the US should:

> … reduce threats from cyber criminals. In partnership with other law enforcement agencies, DHS must prevent cybercrime and disrupt criminals and criminal organizations who use cyberspace to carry out their illicit activities and leverage identified threat activity and trends to inform national risk management efforts.[25]

The US digital infrastructure is leaky, to put it ridiculously mildly.

In fact, there are lots of plans, objectives, "subobjectives," and goals:

> DHS must continue to strengthen our efforts as part of the law enforcement community to pursue, counter, reduce, and disrupt illicit cyber activity by leveraging, in particular, our specialized expertise and capabilities to target financial and trans-border cybercrimes. The transnational and cross-jurisdictional nature of cyberspace, as well as the sheer size of the challenge, requires closer collaboration with other federal, state, local, and international law enforcement partners.[26]

The problem is enormous and growing faster than anyone can even measure. The proposed 2020 US federal budget for cybersecurity, which includes funding for the Defense and State departments (among other agencies) is up a paltry 4.7%.[27] Note that the "budget proposal asks for more than $9.6 billion for Defense Department cyber operations and just over $1 billion for civilian cybersecurity efforts."[28] *That's $1 billion for civilian cybersecurity efforts, and a 4.7% overall increase in the cybersecurity budget.* One doesn't have to be an expert to conclude that the funding solution is dwarfed by the problem. The federal cybersecurity budget should be increased by 100% across the board every year until the threat is manageable — noting that the problem will never disappear. But it can, with proper funding, become manageable.

Prediction? Underfunding will persist — until there's a major attack on the technology infrastructure that affects millions of people.

10. Artificial Intelligence

The Trump Executive Order on "Maintaining American Leadership in Artificial Intelligence,"[29] issued 11 February 2019, is, one hopes, just an early shot in the AI war; an implementation war the US is arguably already losing, especially in areas such as robotics. As described by *MIT Technology Review* Senior Editor for AI Will Knight:

> The initiative is designed to boost America's AI industry by reallocating funding, creating new resources, and devising ways for the country to shape the technology even as it becomes increasingly global.… However, while the goals are lofty, the details are vague. And it will not include a big lump sum of funding for AI research.[30]

As Knight points out [emphasis added], "*other nations, including China, Canada, and France, have made bigger moves to back and benefit from the technology in recent years.*"[31]

Analysis from Bloomberg Government found that the Pentagon's R&D spending on AI has increased from $1.4 billion to about $1.9 billion between 2017 and 2019.[32] More recently, the proposed 2020 budget has seen more increases in AI R&D. As federal market analyst Chris Cornillie at Bloomberg Government told me:

> The 2020 budget has allocated almost $5B for AI R&D (for the Pentagon and all other US government agencies). From FY 2018 to 2020, the Pentagon's budget request for AI R&D rose from $2.7 billion to $4.0 billion … [but] when you look at what Google or Apple alone are investing in AI, $5 billion doesn't seem that large of a figure. Especially if you put that in the context of the federal government's $1.37 trillion discretionary budget request.[33]

The Chinese are outspending the US by leaps and bounds. Where's the federal government? Where are the policies and regulations that would encourage and incentivize investments in AI?

Prediction? There will be no additional funding or funding requests made for AI.

Summing Up

These 10 areas tell us that policy and regulatory failure is the rule. This year, 2020, will be no different, which is an uncomfortable prediction to make. As regulatory requirements scream for attention, we can expect the federal government to further retreat from its responsibilities. Longer term, if regulatory failures continue, the US will almost certainly continue to fall behind in the global technology arms race. In the meantime, we should just learn to live with all the robocalls we get these days.

References

[1] Kennedy, Joe. "We're No. 25: Why the US Must Increase Its Tax Incentives for R&D." *IndustryWeek*, 14 November 2018.

[2] Jamrisko, Michelle, and Wei Lu. "The US Drops Out of the Top 10 in Innovation Ranking." *Bloomberg Technology*, 22 January 2018.

[3] Andriole, Steve. "Artificial Intelligence, China, and the US: How the US Is Losing the Technology War." *Forbes*, 9 November 2018.

[4] Bothwell, Ellie. "Top US Technology Universities Lose Ground in Computer Science and Engineering." Times Higher Education, 29 November 2018.

[5] Mansfield, Emily. "The Best Countries for Tech Companies: 2018 Rankings." Venture Beat,10 June 2018.

[6] Cocullo, Jenna. "We Need to Talk About the Surveillance Economy. Now." Canadian Centre for Policy Alternatives, 1 May 2019.

[7] "R&D Incentives Continue to Draw Government Favor: Reflections from EY's The Outlook for Global Tax Policy in 2018." Ernst and Young, 2018.

[8] Kennedy (see 1).

[9] Kennedy, Joe. "Countries Continue to Use Tax Incentives to Boost R&D." Information Technology & Innovation Foundation (ITIF), 25 October 2018.

[10] Atkinson, Robert D. "How the US Government Falters on Support for Innovation." Information Technology & Innovation Foundation (ITIF), 28 August 2019.

[11] Ducharme, Jamie. "How 'No-Drone Zones' Are Being Enforced with Software, Gadgets, and Shotguns." *Time*, 22 May 2018.

[12] Marquart, Kelsey R. "If We Don't Regulate Automation, It Could Decimate the US Economy." Futurism, 14 April 2017.

[13] "US Department of Education Fulfills Administration Promise to Invest $200 Million in STEM Education." Press release, US Department of Education, 8 November 2018.

[14] Molla, Rani. "Visa Approvals for Tech Workers Are on the Decline. That Won't Just Hurt Silicon Valley." Vox, 28 February 2019.

[15] Lapowsky, Issie. "Visa Rejections for Tech Workers Spike Under Trump." *Wired*, 25 April 2019.

[16] Rangarajan, Sinduja. "The Trump Administration Is Denying H-1B Visas at a Dizzying Rate, But It's Hit a Snag." *Mother Jones*, 17 October 2019.

[17] "The 100 Largest Companies in the World by Market Value in 2019." Statista, 2019.

[18] Lunden, Ingrid. "Amazon's Share of the US E-Commerce Market Is Now 49%, or 5% of All Retail Spend." TechCrunch, 13 July 2018.

[19] Stalcup, Katy. "AWS vs. Azure vs. Google Cloud Market Share 2019: What the Latest Data Shows." ParkMyCloud, 30 April 2019.

[20] Desjardins, Jeff. "How Google Retains More than 90% of Market Share." Business Insider, 23 April 2018.

[21] "Most Popular Social Networks Worldwide as of October 2019, Ranked by Number of Active Users." Statista, 2019.

[22] "Operating System Market Share Worldwide, December 2018-December 2019." Statcounter, December 2019.

[23] Richter, Wolf. "Uber and Lyft Are Gaining Even More Market Share over Taxis and Rentals." Business Insider, 30 July 2018.

[24] Wessel, David. "Is Lack of Competition Strangling the US Economy?" *Harvard Business Review*, March-April 2018.

[25] "Cybersecurity Strategy." US Department of Homeland Security (DHS), 15 May 2018.

[26] DHS (see 25).

[27] Hensch, Mark. "Understanding Trump's 2020 Budget Requests for Cyber, IT." GovLoop, 19 March 2019.

[28] Boyd, Aaron. "Trump's 2020 Budget Requests About $11 Billion For Cyber Defense and Operations." Nextgov, 11 March 2019.

[29] Trump, Donald J. "Executive Order on Maintaining American Leadership in Artificial Intelligence." The White House, Executive Orders, 11 February 2019.

[30] Knight, Will. "Trump Has a Plan to Keep America First in Artificial Intelligence." *MIT Technology Review*, 10 February 2019.

[31] Knight (see 30).

[32] Cornillie, Chris. "Can Pentagon Bridge Artificial Intelligence's 'Valley of Death'?" Bloomberg Government, 14 September 2018.

[33] Cornillie, Chris. Conversation with author, 2019.

Stephen J. Andriole is a Fellow with Cutter Consortium's Business Technology & Digital Transformation Strategies and Data Analytics & Digital Technologies practices and the Thomas G. Labrecque Professor of Business Technology at Villanova University. Dr. Andriole was the Director of the Cybernetics Technology Office of the Defense Advanced Research Projects Agency (DARPA); the CTO and Senior VP of Safeguard Scientifics, Inc.; and the CTO and Senior VP for Technology Strategy at Cigna Corporation. His most recent books include Ready Technology: Fast Tracking New Business Technologies *and* The Innovator's Imperative: Emerging Technology for Digital Transformation. *He has published articles in* MIT Sloan Management Review, Communications of the ACM, IEEE IT Professional, *and* European Business Review, *among others. He can be reached at sandriole@cutter.com.*

Leveraging Business Architecture: 3 Predictions Pointing to New Relevance and Leadership

by Whynde Kuehn

Business architecture is here and here to stay. It has taken shape and is being formalized as a true global discipline. Amid a backdrop of digital transformation and a continually shifting landscape of change, business architecture is gaining momentum and relevance within a continually increasing number of organizations, regardless of industry or geography. This is not to say that we do not have much work ahead, but our challenges are clear; with continued adoption, expansion, and maturation, business architecture can play a key role to inform, shape, scale, and realize the constant transformation and improvement of organizations — even societies.[1]

> *Amid a backdrop of digital transformation and a continually shifting landscape of change, business architecture is gaining momentum and relevance.*

Business architecture teams within organizations continue to build their practices, establishing the prerequisite business architecture baseline and knowledgebase expansion as well as intentionally maturing other foundational aspects to prepare the team, integrate the discipline into the organizational fabric, and build advocacy. As a result, there is now an increased focus on the usage of business architecture. The various scenarios in which business architecture has been used to deliver business value constitute an impressive and growing list.[2] For example, organizations have leveraged business architecture for: strategy translation; business and digital transformation; shifting from a product-centric organization to a customer-centric one; business model evaluation and redesign; innovation; mergers and acquisitions; divestitures; startups; joint ventures; cross-organization ecosystem architecting; cross-sector social initiatives; portfolio investment decision making; driving prioritization for Agile teams; organizational design; regulatory compliance; cost transparency and reduction; business and technology simplification and efficiency; application portfolio management; leveraging emerging technologies; IT architecture transformation; legacy modernization; cloud migration; framing requirements and solution design; and more.

Organizations will continue to use business architecture in all these scenarios, but three key scenarios — based on emerging trends and predictions — will lead the way to increasing relevance and leadership. Let’s now turn to each of these trends/predictions for 2020 and beyond, along with what it means to you.

1. Business Architecture Will Become Foundational Enabler and Connector of End-to-End Strategy Execution

Today

While the idea of business architecture as a bridge between strategy and execution is not new, we are now seeing more new business architecture teams positioned up front within the strategy execution path, as well as existing teams actively trying to “shift left” where applicable. Increased strategy execution messaging and positioning is also starting to occur among industry associations and universities. Some organizations have established a cohesive, business-driven, end-to-end approach to strategy execution enabled by business and enterprise architecture, but most are on the journey and are leveraging business architecture where they initially have traction, such as within the portfolio investment decision-making process.

Tomorrow

Organizations should cast a vision for end-to-end strategy execution as the overall framework to achieve organizational agility — closely integrated with innovation and Agile approaches and teams — and actively work toward making it a reality. We must leverage business architecture (coupled closely with enterprise architecture) as a key enabler for decision making and the translation of business direction into a cohesive set of actions. Business architecture should also serve as a connector across teams and across the strategy execution path, both in terms of the traceability it provides and the natural abilities of business architects to serve as connectors. How we leverage both business architecture and the business architects who practice it will likely continue to evolve. For example, some organizations may integrate the business architect role into a broader, cohesive business design team, while others will explore new ways to democratize and automate portions of the role.

What It Means

As more organizations join the journey, it is even more important to invest in your own strategy execution capability to adapt to change and remain competitive. Key steps include:

- Work with key leaders in your organization to assess your strategy execution maturity. Set goals and direction to build end-to-end organizational agility.
- Position and empower your business architecture team as a key enabler of strategy execution, up front of initiatives.
- Invest in deliberately maturing your business architecture practice to be effective, sustainable, and scalable.

2. Business Architecture Will Become Facilitator and Enabler of Cross-Organization/Cross-Ecosystem Collaboration and Integration

Today

While it is not yet a widespread usage scenario, some organizations have used or are planning to use business architecture to help them collaborate with other partners in their ecosystem. For example, business architecture has been leveraged across organizational boundaries to define and execute upon changes for joint ventures and for mergers and acquisitions (M&As) and even for the creation of brand new ecosystems that do not yet exist, where many organizations deliver new value together that is greater than what they can achieve individually. In addition, we can observe cross-government department architecting and collaboration (within a country, though cross-country collaboration is being considered) in a number of places.

> *How we leverage both business architecture and the business architects who practice it will likely continue to evolve.*

Tomorrow

Organizations should think in terms of ecosystems and should leverage business models and business architecture to identify new opportunities and co-architect them together with other organizations. Business architects from all organizations involved should be at the table with leaders, strategists, and other roles to inform decisions, shape and represent the future state, and translate it into a cohesive set of actions to be executed by each individual organization and all organizations collectively. For-profit organizations should consider opportunities such as architecting their ecosystem comprehensively across legal entities (e.g., to architect the scope of a full healthcare system or create a comprehensive view across operating companies), leveraging business architecture for M&As, architecting new ventures involving two or more organizations, and architecting full-scale new ecosystems with many players that exchange value. Governmental organizations should consider opportunities such as creating a shared business architecture across departments within a country (or even across countries where broader regional collaboration makes sense) and leveraging it to deliver cohesive citizen experiences and reusable services across departments. Nonprofit organizations should consider similar opportunities across both these spectrums depending on their nonprofit business model and structure.

What It Means

In our globally connected, digitally enabled world, the ecosystem is the new organization. The opportunity and necessity to work across organizational boundaries is becoming increasingly important. Embodying this mindset and strategizing around what it means should be on the minds of leaders as well as business architects. Key steps include:

- Educate yourself and your organization on the art of the possible with ecosystems. Work with leaders to assess your business model for new opportunities, determine the role your organization will play in the ecosystem, and move into action on defined business direction.
- Leverage the Business Architecture Guild's *Guide to the Business Architecture Body of Knowledge®* (*BIZBOK® Guide*) reference models for value streams, capabilities, and information concepts as together they are becoming the "Rosetta Stone" to connect business architectures across organizations.[3]
- Invest in your business architecture team's personal growth because the business architect role will become less focused on modeling and increasingly focused on delivering value, strategic thinking, and problem solving, which requires new hard and soft skills.

> *Organizations should reflect and reimagine how they operate in our new digital world.*

3. Business Architecture Will Enable Transparency and Governance of Policies, Ethics, and Objectives

Today

The business architecture domain structure per the *BIZBOK Guide* is robust and allows for the association of various extended business domains with the core business architecture domains of value streams and capabilities. Two of these extended domains — in particular, strategy and policy — can play an expanded role beyond how organizations use them today, especially considering new pressures related to transparency, policy compliance, and corporate social responsibility.

Tomorrow

Organizations should reflect and reimagine how they operate in our new digital world. This includes concerns such as how to provide transparency and governance for artificial intelligence algorithms and how to quickly respond to continual shifts in regulation. They should also reflect and reimagine their responsibilities in light of recent shifts in the role of corporations (from shareholder-focused to stakeholder-focused), contributions to achievement of the United Nations' Sustainable Development Goals (SDGs), and creation of necessary climate action plans.[4] Organizations should leverage business architecture as the central framework to capture content such as policies and ethics, which can relate to their applicable capabilities and the systems (even down to the algorithm) that implement them. They should also capture key objectives and metrics, not only from a strategic business perspective, but also as contributions to SDGs or other sustainability goals. These objectives and metrics can also be tied to capabilities and other aspects within the business and technology environment for full traceability. Leveraging business architecture as a central framework will enable more effective and repeatable compliance, transparency, and visibility for some of the most critical concerns of our time.

What It Means

Organizations should take accountability and action to ensure transparency and governance of the products and services they deliver and how they go about doing it. This is not only important to stay ahead of, and in compliance with, forthcoming regulations, but also to meet the expectations of key stakeholders and contribute to a sustainable, meaningful world that we all want to live in. Key steps include:

- Identify the people in your organization responsible for ethics, governance, and compliance related to digital technology, regulations, corporate social responsibility, and other relevant topics. Articulate how your organization can use business architecture to make the jobs of these individuals easier and more repeatable, integrated, and scalable. Establish concrete plans to help them.

- Where efforts do not already exist, lead your organization to a vision of what governance and ethics accountability could look like in the future.

- If you have not done so already, start getting some experience with capturing policies and objectives in your business architecture knowledgebase, along with cross-mappings to value streams and capabilities.

Final Thoughts

These are exciting times. The role of business architecture and the talents of business architects have never been more relevant or necessary — not just to enable and influence but to lead our organizations and societies through transformation and to continually create a world in which we all want to live.

References

[1] For a relevant backdrop to this article, see: Kuehn, Whynde. "The Global State of Business Architecture: Where We Are and Where We're Going." Cutter Consortium Business & Enterprise Architecture *Executive Update*, Vol. 22, No. 7, 2019.

[2] Kuehn (see 1).

[3] "About a *Guide to the Business Architecture Body of Knowledge® (BIZBOK Guide®)*." The Business Architecture Guild, 2020.

[4] "About the Sustainable Development Goals." The United Nations, 2020.

Whynde Kuehn is a Senior Consultant with Cutter Consortium's Business & Enterprise Architecture practice and Managing Director of S2E Transformation Inc. She is also Partner at Business Architecture Associates and was selected as an Institute Fellow at the Institute for Digital Transformation. Ms. Kuehn is passionate about bridging the gap between strategy and execution. She is a long-time business architecture practitioner, educator, and industry thought leader, who takes a business-focused and results-oriented approach to business architecture.

Ms. Kuehn has extensive experience in enterprise transformation and planning and was a key player in one of the largest business transformations in the world. She has a track record of creating successful teams that become embedded into their organizations. Ms. Kuehn has developed and taught comprehensive, large-scale business architecture training programs via in-person and online formats, both for the public and inhouse for clients. She is a recognized thought leader in business architecture, regularly speaking, writing, and chairing/cochairing conferences and events that advance best practices and facilitate community across the world. Ms. Kuehn is cofounder and board member of the Business Architecture Guild, a not-for-profit organization that is advancing the discipline, and serves as its Editorial Board Chair. She is a passionate advocate for using business as a force for good and applying solid business approaches to enable nonprofits, social enterprises, and cross-sector social initiatives to successfully start, scale, replicate, and sustain. This has led to an Architecting For Good (A4G) initiative within S2E to create opportunities for business professionals to share their talents with others through transformative experiences. She can be reached at wkuehn@cutter.com.

WHEN FORCES COLLIDE

Cybersecurity in 2020

by Paul Clermont

Over the past few years, I have avoided predicting specific technological innovations, focusing instead on issues around privacy and security and the evolving perceptions of technology and big tech in the public sphere. I believed these issues would become increasingly critical in the emerging era of artificial intelligence (AI). They have. One prominent effect has been the speed with which tech's long honeymoon with the public has come to a sobering end, with lots of tough questions from governments and pundits that have not been very well answered by industry leaders.

It's hard to imagine 2020 not intensifying this trend, with almost every large tech company and even some lesser ones in the crosshairs of one or another government agency in both the US and the European Union (EU). Indeed, in the US, the notion of reining in big tech looms large in some political campaigns. The form that "reining in" may take is still hazy; is it merely about size? About scope of activities? About the appropriateness and societal value (or lack thereof) of some extraordinary profitable business models? We don't know. Europe is taking the lead, but the actions of the US (or lack thereof) will be critical.

> *Tech's long honeymoon with the public has come to a sobering end, with lots of tough questions from governments and pundits.*

I'll skip the obvious about the rapid progress in AI and the fears that it will continue to engender. Most of the threats — like the loss of jobs and privacy, the "surveillance state," intentionally or unintentionally biased algorithms entrusted with too much power over our lives, and, not least, the ability to microtarget lies and disinformation that have already cast shadows over elections — are not going away. Dealing with these justified fears requires attention from the best and brightest; not just technical people but the full range of social scientists: sociologists, political scientists, economists, psychologists, educators, and so on. We should expect 2020 to bring at least a bit of progress in this area.

However, there is, in my opinion, one dragon that can be slain: the fear of imminent artificial *general* intelligence (AGI) — capabilities pretty much like human intelligence, which of course we really don't understand — lurking just around the corner[1] and then morphing rapidly into artificial superintelligence that could, like HAL in Stanley Kubrick's *2001: A Space Odyssey*, decide that some or all of us humans are expendable. We need to note that it took 54 years for a computer to go from mastering checkers to mastering *Go*, even though the games differ only in scale and complexity. Both games offer the advantages of 100% available information and unambiguous goals and rules (just like real life, eh?) — so any worry about the quantum leap to AGI is a counterproductive distraction from the very real threats mentioned above.

One concern that businesses and governments need to address with much more urgency (and we hope they will do so in 2020) is cybersecurity. Attacks can come from hostile governments, criminals, and mischief-makers. Their targets can be companies, governments at all levels, and critical infrastructure. Several trends are colliding in a way that compounds long-standing risks:

- **Complexity.** The more versatile a computer system is, the more complex it must inevitably be. Persuading a computer to do what it's supposed to do and only that (i.e., debugging) is mind-bogglingly difficult. (If it were easy, we would not be getting the frequent mid-release updates addressing "bug fixes" and "security hole" patches from such software powerhouses as Apple and Microsoft.) This suggests that adding functionality just because we can is not a good design approach.

- **Artificial intelligence.** A debugged traditional computer system doesn't do anything we didn't program it to do. AI is different; it learns to do things we didn't tell it how to do. Sometimes it's brilliant, like the unorthodox but legal and devastating move that felled the world *Go* champion. But that's a game; the overarching rules — the guardrails — are built in. Without explicit guardrails, a machine could learn to do something that defies common sense. Are we confident that our teaching software will be flawless enough to prevent its electronic "students" coming up with harebrained ideas that even Dilbert's dimmest colleagues would have more sense than to devise? As the users of AI become ever less conversant with what's inside the black boxes, how well will they recognize something crazy — in time?

- **Interconnectedness.** The Internet, particularly the Internet of Things, keeps opening up ever more surface area for penetration by thieves and mischief-makers. It is hard enough — probably impossible in an absolute sense — to secure even an isolated network from intrusion. Now connect it to thousands or millions of other networks, remembering that a chain is only as strong as its weakest link. For a sobering overview of the kind of mischief that has already occurred, an essay entitled "The Drums of Cyberwar" by Sue Halpern reviews the recently published *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* by Andy Greenberg.[2] The blithe assumption that more interconnection is per se beneficial is not only unjustified, it's downright dangerous.

It will take some very clever technical work to address these issues; the required disciplines and techniques need as much or more priority than basic testing, which assumes that spurious input is simply inadvertent rather than deliberately designed by very smart people to create problems. We need to give priority to:

- **Recognizing intrusions.** Recognizing suspicious inputs will require subtle and sophisticated algorithms. These algorithms are not easy to design and build (AI can help), and they must be continuously improved to stay a step ahead of the would-be intruders. It is not easy to find the sweet spot between excessive and insufficient caution.

- **Isolating intrusions.** Systems need the equivalent of white blood cells to isolate and neutralize spurious input. In cases where the intrusion has gone beyond the entry point and compromised the system, we need mechanisms to provide the equivalent of a containment vessel to isolate the compromised system from all its connections.

Compounding the difficulty of these tasks is the need to be able to execute algorithms and procedures in nanoseconds — a tall order that should inspire a bit of conservatism about how much functionality and connectivity we might want versus what we truly need.

A piece of possibly encouraging news, if much more interconnectedness is inevitable, is that Apple, Amazon, and Google have agreed to join other companies to set up a working group that will (they hope) agree on a set of standards for Internet-connected home products in order to make them compatible with each other and ensure a certain level of security.[3] Let's hope for more such news in 2020.

On the discouraging side, a recent op-ed column by Josephine Wolff, a Tufts University Fletcher School professor of cybersecurity policy, catalogued the wholesale departure of US government experts concentrating on election security.[4]

As ever, a mixed bag.

References

[1] I recently read a report from a scholarly symposium that blithely assumed AGI would arrive in the 2030s; see: Casey, Kevin. "5 AI Fears and How to Address Them." The Enterprisers Project, 30 September 2019.

[2] Halpern, Sue. "The Drums of Cyberwar." *The New York Review of Books*, 19 December 2019.

[3] "Amazon, Apple, and Google Joining Forces Could Be What Makes Smart Homes Happen." *MIT Technology Review*, 19 December 2019.

[4] Wolff, Josephine. "Cybersecurity Experts Are Leaving the Federal Government. That's a Problem." *The New York Times*, 19 December 2019.

Paul Clermont is a Senior Consultant with Cutter Consortium's Business Technology & Digital Transformation Strategies practice. He has been a consultant in IT strategy, governance, and management for 30 years. His clients have been primarily in the financial and manufacturing industries, as well as the US government. Mr. Clermont's major practice areas include directing, managing, and organizing IT; reengineering business processes to take full advantage of technology; and developing economic models and business plans. He is known for successfully communicating IT issues to general managers in a comprehensible, jargon-free way that frames decisions and describes their consequences in business terms. In his consulting engagements, he follows a pragmatic approach to the specific situation and players at hand and is not wedded to particular models, methodologies, or textbook solutions. Mr. Clermont has spoken and written about the challenges of getting significant and predictable value from IT investments and has taught executive MBA courses on the topic. His undergraduate and graduate education at MIT's Sloan School of Management was heavily oriented toward operations research. He can be reached at pclermont@cutter.com.

IMAGINE A WORLD ...

Trustworthiness: A Mouthful That Shouldn't Leave a Bad Taste

by Claude Baudoin

"What can you believe?" has recently become a visible social issue, one that is critical to the proper functioning of our societies. Establishing a degree of confidence in information has also become a complex technical issue, one that may drive a number of changes in the fabric of IT. This article is not a definitive proposal to achieve the elusive goal of knowing what we can trust, but rather a set of perspectives and considerations to justify the urgency of addressing this issue.

> *The latest scary scenarios come from the proliferation of insufficiently secured IoT systems.*

Trustworthiness is defined as "the ability to be relied on as honest or truthful."[1] The word appeared in English in 1820, reached its first peak of popularity in 1890, declined until 1960, then went up the charts, and is now still increasing in frequency,[2] for reasons with which readers should be all too familiar:

- Technology allows the almost undetectable falsification of information, including "deep fakes" that place people and things within a textual, graphical, or video context of which they were never part.

- The most pessimist among us fear that there are essentially no longer any channels of information that can be trusted for their honesty and objectivity. Most in mass media are accused by one side or another of having become biased or virtual instruments of propaganda, even in democratic countries.

- Social media outlets have replaced newspapers, radio, and television as the main sources of news for many of us, but this further weakens the notion of trust. Some of us live in echo chambers that thrive on the "confirmation bias"[3] well known to psychologists.

- We are losing faith in the idea of election results representing the true will of the majority "thanks" to a combination of cyberattacks, the influence of fake news on the electorate, instances of voter suppression, and antiquated voting systems.

- We often do not know the source of the data used to make momentous decisions. In the medical world, for example, we know that certain populations are underrepresented in research studies, including women and ethnic minorities, which risks leading to standards of care that are inappropriate for those populations.

- We do not know if artificial intelligence algorithms have been trained using unbiased data. We know, for example, that when using facial recognition to identify crime suspects, the rate of false positives is much higher for people of color than for white people.

- We can no longer trust the origin of an email, since the Internet protocols, which date back 50 years, do not ensure the authenticity of that information. Hence the plagues of spamming and phishing, and the occasional overreaction that causes us to ignore legitimate messages that were incorrectly filtered out as spam or junk.

- Many of us no longer answer phone calls from unknown numbers, since robocalls often represent over 50% of the calls we receive. Some are just annoying, while others are criminal attempts to extort money from naive recipients, including the elderly or simply uninformed people.

The latest scary scenarios come from the proliferation of insufficiently secured Internet of Things (IoT) systems. According to the director of the US Cybersecurity and Infrastructure Security Agency (CISA), "CISA is currently aware of a system that controls water pumps, one controlling an oil and natural gas facility, and one controlling emergency management equipment that can be accessed without a password and modified by anyone with an internet connection."[4] Now, consider this:

- The agency is unable to locate the owners of those systems without issuing a subpoena to the ISPs responsible for the IP addresses where those systems were detected.

- Open source software development is a great thing; it has made millions of lines of code, largely developed and donated by organizations and improved by volunteer experts, available to others for free. But it is also a huge opportunity to inject malware into hundreds of critical systems. This vulnerability led the National Telecommunications and Information Administration (NTIA), a branch of the US Department of Commerce, to launch, in 2019, an effort to develop an approach to document the pedigree of software — a Software Bill of Materials (SBOM) that would allow for the traceability of a security vulnerability up and down the genealogy tree for the code.

By now, you should get the idea that trustworthiness is a key challenge to the integrity of just about everything that happens around us and to us — of the systems we use, of our electricity supply, of our forms of government, of our financial security, of the decisions that lead to war or peace, and of our reactions to worldwide existential threats such as climate change or epidemics.

So, what's next? Unfortunately, if history repeats itself, the situation will get worse before it gets better. But that isn't reassuring.

Part of the answer must lie in the traceability of information as it propagates, as hinted at in the proposed SBOM, discussed above. Let's now imagine a world in which:

- When the phone rings, I can be certain of who is calling me. No more "Michael" with a thick South Asian accent calling me from the "Windows Security Center" to demand access to my laptop. Telecom companies could make it happen; we need to force them to do so.

- When an email arrives, I can be certain of the identity of the author. Goodbye, Nigerian customs officials.

  Now, this would pose a risk for people in countries where freedom of expression is not guaranteed. So, there also needs to be a reliable and optional anonymization method that can only be used among consenting parties and cannot be (easily) subverted by scammers. Tor[5] (the anonymity network project) on steroids, so to speak.

> *Trustworthiness is a key challenge to the integrity of just about everything that happens around us and to us.*

- When I see an image or video, I can query its provenance or pedigree. When was the image taken or the video made? Was it edited, and by whom? What was the chain of custody between the camera and me? Goodbye, fake news about world leaders cozying up with enemies. Again, in some cases we need to protect anonymous sources, and therein will lie a key technical difficulty.

- When I see a quote attributed to a person, I can click on it and find the original source as well as corroborating evidence.

- When I vote, I can trust that my ballot is correctly counted, as well as those of my fellow citizens, perhaps using a blockchain-enabled voting system. Again, we need to ensure that this doesn't allow people to buy votes. If a voter's choices can be verified after the fact, the linking of voter and vote enables bribery. That's another contradiction to be addressed.

- Standards are developed to test machine learning algorithms for the absence of bias, especially gender, racial, and other demographic or sociological bias.

- Identification, authorization, and access control mechanisms are systematically used to know where IoT data comes from, including measurements from sensors and commands sent to actuators.

- All software is delivered with a bill of materials, so that when a vulnerability is identified, the owners and users of all affected systems can be alerted. Not all vulnerabilities are executable in a given system, but they are, at minimum, a time bomb that must be defused.

What will it take to get to this ideal world? Probably a multipronged approach, which will require several years, if not the entire decade that is now opening:

- Suppliers of systems must be more responsible about their products. Market forces as well as regulation may be needed to apply the necessary pressure.
- Buyers need to ask tough questions before something blows up in their hands (figuratively and, in the worst case, literally).
- Legislators must educate themselves about security technology.
- Democratic governments need to take the rebuilding of public trust in information seriously.
- The "fourth estate" — the media — must self-regulate or face regulation.

Technology will play a role — including public key infrastructure, blockchain, a redesign of Internet protocols, and more. But this is not just a technology challenge. It is a fundamental reexamination of an age-old question: "Can I trust you?"

References

[1]"Trustworthiness." Lexico, 2020.

[2]"Trustworthiness, 1800-2008." Google Books Ngram Viewer, 2013.

[3]Cherry, Kendra. "How Confirmation Bias Works." Verywell Mind, 27 November 2019.

[4]"Senate Bill Would Give CISA Limited Subpoena Power." MeriTalk, 17 December 2019.

[5]"Tor Project: History." Tor Project, 2020.

Claude Baudoin is a Senior Consultant with Cutter Consortium's Business & Enterprise Architecture and Data Analytics & Digital Technologies practices. He has been owner and Principal Consultant of cébé IT and Knowledge Management, a boutique consulting practice, since 2009. Prior to that, Mr. Baudoin spent 35 years in IT and software management roles in industry, including 26 years at Schlumberger, the global oilfield services company, in France and the US. Since 2015, he has served as an energy domain advisor to the OMG and the Industrial Internet Consortium and has sat on the steering committee of the Cloud Standards Customer Council. Mr. Baudoin has published two books on software engineering, Méthodes de Programmation *and* Realizing the Object-Oriented Lifecycle, *and numerous papers and conference presentations. He holds two patents related to IT infrastructure and security. Mr. Baudoin's undergraduate engineering degree is from École Polytechnique in Paris, and he holds a master of science degree in computer science from Stanford University. He can be reached at cbaudoin@cutter.com.*

WHAT'S HERE? WHAT'S COMING?

Autonomous Systems Are Rising; Seize the Opportunities!

by San Murugesan

As they make the transition away from stories of science fiction, autonomous systems are becoming a practical reality. Though not yet a popular or household term like self-driving cars, robots, and artificial intelligence (AI), autonomous systems are on the rise. Several such systems are already in use performing different tasks in diverse areas and yielding several benefits. Poised to evolve further, they will surely find widespread adoption. Autonomous systems will be a game changer and will propel new research, development, and business opportunities. It's no wonder they are attracting the interest of researchers, manufacturers, and users alike. Let's examine what autonomous systems are and why they matter.

What Is an Autonomous System?

"Autonomous system" is a relatively new term in modern day usage, though previously used in mathematics and networking. In automation, robotics, and other application domains, the term "autonomous" describes self-governing systems. Specifically, an autonomous system is a machine or system capable of "performing a series of operations where the sequence is determined by the outcome of the previous operation or by reference to external circumstances that are monitored and measured within the system itself."[1] Such a system must be able to sense the environment within which it operates and interact with that environment. A system is autonomous, with respect to a set of goals and while operating under a set of uncertainties, if it achieves the goals under those uncertainties without human external intervention.[2]

Unlike other machines or common automatic control systems that have a single purpose or whose range of activities is predefined, an autonomous system:

> Tailors its behaviour and operations in accordance with the circumstances that it finds: it is "smart" or "intelligent." It "discovers" what is going on in its sphere of operation, and adapts its course of action in accordance with what it finds.[3]

Key features of an autonomous system are self-operation/governance without human or external intervention, independence, a wide operating range, adaptation to uncertainty, and ability to achieve set goals. Several technologies — robotics, drones, various types of sensors, the Internet of Things, high-speed communication networks (including 4G and 5G), AI and machine learning, data analytics, augmented/virtual reality, high-performance processors, nano technologies, and smart signage — are coming together to extend the scope and range of operations of autonomous systems. Ongoing advances in these and other related technologies make practical applications of autonomous systems viable, setting the climate up for a new trend.

Applications on the Radar

We are already seeing autonomous systems surfacing in practice in several applications ranging from fighter jets, air taxis, self-driving vehicles, physical customer delivery, inventory management, surveillance, emergency management, and monitoring and recovery in harsh environments to smart homes, assisted care, tutoring systems, and more. The implications of these systems on business and society are enormous. Let's take a brief look at a few of the current applications.

Autonomous Aircraft

The Royal Australian Air Force and Boeing Australia are building an autonomous fighter jet for possible operational use in the mid-2020s.[4] In addition, German-based urban air mobility provider Volocopter has built the world's first autonomous flying taxi (air taxi), which users will hail with their smartphones. The Volocopter taxi had its official urban flight debut at the Mercedes-Benz Museum in Stuttgart, Germany, on 14 September 2019.[5] Last year, Audi created an autonomous off-roader vehicle that utilizes flying drones to illuminate the road instead of regular headlights.[6]

Autonomous Inventory Management and Delivery Robots

Retail stores and warehouses will increasingly install autonomous robots for inventory management. Walmart, for instance, is set to introduce inventory management robots from tech startup Bossa Nova Robotics at 650 more stores this year.[7] These robots roam a store's aisles and scan shelves to identify products out of stock, mislabeled, or incorrectly priced. They reduce the number of labor hours needed for inventory checking and improve stores' operations. More providers of autonomous inventory management solutions are coming to market. For example, Zebra Technology recently launched a similar solution ("SmartSight"[8]), and Simbe Robotics has an autonomous robot ("Tally"[9]). Last year, Ford showcased a two-legged delivery robot ("Digit"[10]).

Personal and Service Robots

Autonomous robots are now serving as concierges, doormen, baggage checkers, luggage transporters, and bartenders. For instance, Oakland International Airport has deployed a robot named "Pepper"[11] that greets passengers and helps them find their way around the airport. Travelers can talk to the robot to obtain information such as what is available in the food court and directions to shops, restrooms, and other facilities. The robot "Gita"[12] from Vesper can automatically follow you and carry your luggage, leaving you hands-free. We may soon see a fleet of such robots in airports and bus stations to help travelers in the same way that a human assistant might. Personal services can even extend to toilet paper; at the 2020 *Consumer Electronics Show*, Charmin demonstrated its autonomous robot "Rollbot,"[13] which brings a roll of toilet paper to the restroom in response to a request sent from a mobile phone.

Assistance to the Elderly

Autonomous equipment and gadgets assist older people in several ways with day-to-day activities, helping them retain their independence and improving their quality of life. Besides being smart assistants, these devices can also continuously monitor people's health and movement, alerting them to dangers and, when the situation warrants, notifying paramedics and family members. This technology can, for instance, prevent an elderly person from falling and lessen the injury from a fall if the person does fall.[14]

Monitoring and Recovery in Harsh Environments

Autonomous systems are also taking on jobs that are dangerous or unpleasant for humans to perform. They are able to go into places and situations that humans cannot or do not want to enter. For example, autonomous systems inspect inside nuclear reactors to check for faults and provide information on nuclear accidents.[15] These systems can also monitor active volcanos.[16]

Autonomous Vehicles

Driverless cars and trucks are a familiar and much talked about example of an autonomous system. Autonomous trucks could form fleets that travel in the same direction and share information on their surroundings.[17] Automated driving will be the cornerstone of future mobility systems. Autonomous vehicles are expected to make traffic safer, more convenient, and more efficient.

Challenges of Autonomous Systems

Despite their rise and adoption in the last three years, autonomous systems have constraints and concerns. For starters, we need to ensure that these systems are built to perform reliably, safely, and sustainably — and are tested and validated satisfactorily. We also need to secure them against hacks and unintentional manipulation and prevent them from being used for unintended harmful purposes or to constitute threats to people and property.

Trust is a critical factor in autonomous applications used in consumer products, personal robots, industrial and business automation, and automotive automation. Designing trustable systems is a challenge as trust goes well beyond just the technology; it involves people and people's perceptions.[18]

An interesting dilemma is deciding what level of autonomy is appropriate for an application while balancing benefits and risks. Since autonomous systems currently work adequately within well-defined environments only, huge potential exists for R&D in relaxing these constraints. Furthermore, most autonomous systems now operate independently in an isolated manner. However, these systems can work together collaboratively, coordinating with each other as a team and, thereby, extending and enhancing their collective capabilities. Such swarming or teaming of autonomous systems poses different challenges to researchers and developers, yet it is an area that deserves further maturation. Other autonomous system adoption issues that go beyond the technical have societal, regulatory/legal, and ethical implications.

Outlook Ahead

Autonomous systems are at a tipping point and are on an evolutionary growth path. Several technologies are coming together to extend the range and capability of autonomous systems. There is market "push" from both industry big players and startups, and market "pull" from potential users, both industry and individuals. Market pull is driven by a wide range of potential applications where autonomy promises to accomplish what could not be done before, or to carry out existing operations more efficiently and/or safely while offering convenience.

We can expect amazing advances and innovations in autonomous systems and their features. We will see autonomous systems transform many different sectors in unimaginable ways. As Daniel Burrus wrote in a 2012 *Huffington Post* blog, "It's not about whether technology is good or bad; it's about what we decide to do with technology that matters."[19]

The domain of autonomous systems is fertile, with substantial opportunity for researchers, developers, and industry, and now is the time to act. The impact of autonomous systems will be diverse and significant. In 2020, we will see further advancement of autonomous systems and their applications. Be prepared for the disruptive transformations and changes ahead.

References

[1] Antsaklis, Panos J., Kevin M. Passino, and Shyh Jong Wang. "An Introduction to Autonomous Control Systems." *IEEE Control Systems*, Vol. 11, No. 4, 1991.

[2] Antsaklis, Panos J., and Arash Rahnama. "Control and Machine Intelligence for System Autonomy." *Journal of Intelligent Robotic Systems*, Vol. 91, No. 1, 2018.

[3] "Innovation in Autonomous Systems." Royal Academy of Engineering, September 2015.

[4] Levick, Ewen. "Boeing's Autonomous Fighter Jet Will Fly Over the Australian Outback." *IEEE Spectrum*, 2 January 2020.

[5] Chang, Brittany. "Volocopter Has Created an Autonomous Flying Taxi You Can Hail with Your Smartphone." *Business Insider*, 18 September 2019.

[6] Chang, Brittany. "Audi Created an Autonomous Off-Roader That Uses Flying Drones to Illuminate the Road Instead of Headlights." *Business Insider*, 17 September 2019.

[7] Keyes, Daniel. "Walmart Is Bringing Autonomous Inventory Management Robots to 650 More Stores by This Summer." *Business Insider*, 15 January 2020.

[8] "Zebra Technologies Unveils New Intelligent Automation Solution at NRF 2020." Business Wire, 13 January 2020.

[9] "Say Hello to Tally." Simbe Robotics, 2020.

[10] Ackerman, Evan, and Erico Guizzo. "Ford Self-Driving Vans Will Use Legged Robots to Make Deliveries." *IEEE Spectrum*, 22 May 2019.

[11] Heater, Brian. "Pepper the Robot Gets a Gig at the Oakland Airport." TechCrunch, 25 January 2017.

[12] Sykes, Nathan. "AI Goes Beyond Autonomous Cars When It Comes to Transportation." TechTalks, 6 April 2018.

[13] Titcomb, James. "Charmin Unveils a Robot Built to Bring You Toilet Paper at CES 2020." *The Telegraph*, 6 January 2020.

[14] Adams, Shelly. "Smart Technology and Tracking Devices to Prevent Falls and Injuries." SeniorsLifestylesMag.com, 1 November 2018.

[15] Tsitsimpelis, Ioannis, et al. "A Review of Ground-Based Robotic Systems for the Characterization of Nuclear Environments." *Progress in Nuclear Energy*, Vol. 111, March 2019.

[16] Davies, Ashley, et al. "Rapid Response to Volcanic Eruptions with an Autonomous Sensor Web: The Nyamulagira Eruption of 2006." *Proceedings of the IEEE Aerospace Conference*, IEEE, 2008.

[17] Clevenger, Seth. "How Drivers and Autonomous Trucks Could Work Together to Move Freight." Transport Topics, 8 June 2018.

[18] Siau, Keng, and Weiyu Wang. "Building Trust in Artificial Intelligence, Machine Learning, and Robotics." *Cutter Business Technology Journal*, Vol. 31, No. 2, 2018.

[19] Burrus, Daniel. "Is Technology Good or Evil?" *HuffPost Business*, 24 August 2012.

San Murugesan (BE [Hons], MTech, PhD; FACS) is a Senior Consultant with Cutter Consortium's Data Analytics & Digital Technologies practice, Director of BRITE Professional Services, and an Adjunct Professor in the School of Computing and Mathematics at Western Sydney University, Australia. He is Editor-in-Chief Emeritus of the IEEE's IT Professional. *Dr. Murugesan has four decades of experience in both industry and academia, and his expertise and interests include artificial intelligence, the Internet of Everything, cloud computing, green computing, and IT applications. He offers certificate training programs on key emerging topics and keynotes. Dr. Murugesan is coeditor of a few books, including* Encyclopedia of Cloud Computing *and* Harnessing Green IT: Principles and Practices. *He is a member of the COMPSAC Standing Committee, and a fellow of the Australian Computer Society. Dr. Murugesan held various senior positions at Southern Cross University, Australia; Western Sydney University; the Indian Space Research Organization, Bangalore, India; and also served as Senior Research Fellow of the US National Research Council at the NASA Ames Research Center. He can be reached at smurugesan@cutter.com.*

WHAT'S ON THE HORIZON?

AI and Natural Language 2020: New Regulations and New Developments

by Curt Hall

Enterprise adoption of artificial intelligence (AI) is sure to increase in 2020, but so will calls for new regulations to help guide and ensure the fair use of the technology, which could prove restrictive. Additionally, new and existing consumer data privacy laws could potentially affect commercial development of new AI products and the application of the technology in business.

Moreover, we can expect to see increasing demands from developers and end-user organizations for greater transparency, fairness, and "explainability" in AI applications and products. Such demands have resulted in the new field of "explainable AI" and a new approach to AI modeling and development called "neural-symbolic AI."

Finally, a recent breakthrough in natural language processing (NLP) model building is leading to new NLP tools and products that will accelerate enterprise application of the technology, including the use of speech recognition.

> *In 2019, the media was filled with stories about how almost every industry was applying AI to optimize their operations.*

Regulations, Data Privacy, and Demands for Transparency

Enterprise use of AI will increase, particularly for optimizing customer engagement and customer experience (CX) via the use of machine learning (ML), NLP, and speech recognition. That said, two related issues have the potential to hinder AI implementation: (1) consumer data privacy and other AI regulations and (2) demands by end-user organizations and consumer watchdog groups for greater transparency and bias prevention in AI systems.

Data Privacy Acts and Calls for Increased AI Regulation

In 2019, the media was filled with stories about how almost every industry was applying AI to optimize their operations — ranging from new credit and loan platforms designed to serve the "under-banked" to the ability for ML systems to save lives through early detection and diagnosis of cancer and other diseases.

But AI also received a lot of negative publicity last year, especially concerning the use of facial recognition. With the recent revelation that facial recognition startup Clearview AI developed its technology by screen-scraping images of people posted on Facebook without their permission (or, according to Facebook, Facebook's permission), 2020 has not started off well for AI from a PR standpoint.[1] According to a report in *The New York Times*, over 600 law enforcement agencies have adopted Clearview AI's facial recognition technology.[2]

According to a survey of 800 tech leaders by KPMG back in 2018, technology leaders ranked restrictive regulations at the top of innovation limiters.[3] But times have changed and so have tech leaders' views. Now we are seeing calls by Big Tech — including CEOs from Google, IBM, and Microsoft, among others — for new government regulations to help guide the safe application of AI.

Some countries are further ahead of the US in considering AI regulations. For instance, the European Commission plans to release a white paper on AI, which will shepherd the use of the technology over the next five years. (And it is rumored that it will call for limitations on the use of facial recognition in public settings.) However, being an election year and with the impeachment trial of US President Donald Trump still fresh in mind, any chance of serious federal regulations governing the use of AI in the US happening in 2020 appears slim.

On the other hand, US states and municipalities aren't waiting to enact their own regulations, which are already restricting the manner in which to utilize AI. California has implemented a three-year ban on the use of facial recognition systems in body cameras worn by police,[4] while cities such as San Francisco and Oakland, California, and Somerville, Massachusetts, have enacted legislation banning or restricting the use of facial recognition.[5] It's not just facial recognition that states and local governments are regulating. For example, in Illinois, the Artificial Intelligence Video Interview Act, which took effect 1 January 2020, requires companies to notify job applicants when AI will be used for applicant screening.[6] Applicants can also request that submitted videos are destroyed, and companies must comply within 30 days.

Existing and new consumer data privacy laws, such as the General Data Protection Regulation (GDPR) from the European Union (EU) and the recently enacted California Consumer Protection Act (CCPA), have the further potential to hinder greater development and adoption of AI. For example, the CCPA places restrictions on the use of California residents' data without their permission, including on inferences made by systems using such data.[7] This raises an important question: just how does the CCPA affect a company like Clearview AI if images of California citizens were used (without their knowledge, let alone their permission) to train the facial recognition models used in Clearview AI's product? For instance, if a California resident were to ask Clearview AI to delete his personal data, would the company also be required to retrain its models to comply with the CCPA? Today, this is unclear. Lawyers will eventually need to work out many of these issues.

Growing Demand for Transparency and Explainability in AI Systems

Certainly, we are seeing increasing demand by end-user organizations (and their customers) for more transparency and explainability in AI applications and products. If AI is really going to achieve widespread adoption, it is essential that systems be able to (adequately) explain the reasoning behind their decisions in order to remove the trust and bias issues associated with today's applications. It not only makes good business sense, but for many, if not most business applications, systems are required to explain the basis of their findings for compliance, ethical, legal, and other reasons.

> *If AI is really going to achieve widespread adoption, it is essential that systems be able to explain the reasoning behind their decisions in order to remove the trust and bias issues associated with today's applications.*

The Field of Explainable AI and the Role of Neural-Symbolic AI

The demand for transparency and fairness in AI systems has resulted in considerable interest in explainable AI — a growing field that seeks to create new tools, methods, and models with the ability to peer into the opaque inner workings of deep learning–based AI algorithms and expose their decision-making processes in a way that humans can understand, thereby facilitating greater transparency, traceability, and trust in outcomes, while maintaining a high degree of accuracy.

Although explainable AI is an ongoing research effort that is just now getting underway, in 2019 we saw a number of developments. These included open source tools, commercial products, and cloud-based services available to assist AI researchers, developers, and end-user organizations in probing the inner workings of their ML models and algorithms.[8]

Another development is that of neural-symbolic AI, an approach that combines the pattern recognition and pattern-matching capabilities of neural networks with the symbolic-reasoning functionality and transparency features of rule-based and knowledge-based systems (KBSs). The rule-based and KBSs that prevailed during the first round of commercial AI in the mid-1980s and early 1990s successfully handled explainability and fairness issues because they were based on rules written in a natural (human) language format, as well as on decision trees, confidence factors, and other techniques to explain the logic behind the reasoning (i.e., rule-based inferencing) of their outcomes. In contrast, neural nets do not provide such human-friendly syntax explaining their decisions because they are based on complex mathematical models. Consequently, by marrying the two approaches, neural-symbolic AI offers hybrid AI systems with the ability to explain their reasoning in detail using human language. Moreover, the inclusion of NLP techniques in neural-symbolic approaches will eventually lead to advanced hybrid AI systems that could explain their reasoning using spoken human language output.[9]

Transformer Models for NLP and Speech Recognition

One of the most important recent breakthroughs in AI was the development of transformer-based NLP models in 2018-2019. Transformer-based NLP models are deep learning neural nets that have been pretrained on large corpora of data. This has been shown to lead to increased accuracy in NLP systems, and, in some cases, has reduced significantly the time required to train NLP models for operational use.

> *In 2020, we should see more commercial applications and other products employing transformer-based NLP models.*

Transformer-based NLP models allow developers to create NLP systems that can perform more sophisticated NLP tasks than were previously possible. For example, when it comes to natural language generation (NLG), transformer-based models have been shown to support more coherent, paragraph-length text generation. Transformer-based NLP models have serious implications for the entire discipline of NLP — from speech recognition systems to NLG, natural language understanding (NLU), machine translation, and text analysis applications (including sentiment analysis and emotion recognition). Consequently, tools for developing transformer-based models have become popular among researchers and developers implementing NLP applications.

In 2020, we should see more commercial applications and other products employing transformer-based NLP models. Moreover, we should see a significant uptake in enterprise adoption of NLP and speech recognition technology, especially for customer engagement and CX management scenarios. In a 2018 Cutter Consortium survey examining AI adoption in the enterprise, nearly 50% of responding organizations expressed interested in adopting NLP, in particular, making it third among all AI technologies — just after predictive analytics and ML — organizations say they are most interested in adopting.[10]

Conclusion

Business leaders should prepare for a number of developments that have the potential to impact the use of AI technologies this year and beyond. Probably the hardest to plan for are regulations governing the use of AI and the possible effects of consumer data privacy laws on AI usage because they are so new, or still under consideration as "moving targets." Nonetheless, organizations should carefully consider how any new or existing systems could run afoul of GDPR and CCPA regulations, as well as of those implemented by local governments.

Demands for more transparency and explainability in AI systems is only going to grow — from government agencies, politicians, and consumer watchdog groups to end-user organizations. Business leaders should require that vendors offering AI products guarantee that their systems are not inherently biased and that they are transparent in their reasoning, so as not to have their companies thrown under the bus when it comes to penalties — and bad PR — should it be revealed that their HR, lending, or other AI applications discriminate against some group of consumers. Companies exposed for using biased or discriminatory systems risk having their brands tried in the court of public opinion — always a dicey prospect.

Explainable AI and neural-symbolic AI hold the promise of eventually leading to more transparent and explainable AI systems via the combination of neural and symbolic approaches. Until this is realized, organizations should utilize the open source tools, commercial products, and cloud-based services currently available. Although these offerings are somewhat limited in their capabilities, they are helpful for providing insight into the inner workings of ML models and algorithms.

Finally, breakthroughs in NLP modeling techniques are leading to new NLP and speech recognition products that will spur enterprise applications of the technology. Thus, organizations should examine how they can leverage NLP and speech. Popular application domains include customer engagement and CX management.

References

[1] Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times*, 18 January 2020.

[2] Hill (see 1).

[3] Global Technology Innovation Center. "Managing Technology Innovation: Insights for Technology Companies on Driving, Measuring, Fostering, and Overcoming Barriers to Innovation." KPMG, 2020.

[4] Metz, Rachel. "California Lawmakers Ban Facial-Recognition Software from Police Body Cams." CNN, 13 September 2019.

[5] Conger, Kate, Richard Fausset, and Serge F. Kovaleski. "San Francisco Bans Facial Recognition Technology." *The New York Times*, 14 May 2019.

[6] Waltz, Daniel, Molly DiRago, and Ronald I. Raether, Jr. "Illinois Employers Must Comply with Artificial Intelligence Video Interview Act." Society for Human Resource Management (SHRM), 5 September 2019.

[7] Lomas, Natasha. "California's Privacy Act: What You Need to Know Now." TechCrunch, 12 October 2019.

[8] For more on such offerings, see: Hall, Curt. "Transparency and Fairness in AI Systems, Part II: The Quest for Explainable and Unbiased AI." Cutter Consortium Data Analytics & Digital Technologies *Advisor*, 10 September 2019.

[9] For more on neural-symbolic AI, I recommend checking out: Tenenbaum, Joshua B., and Chuang Gan. "Empowering AI with Symbolic Reasoning." MIT-IBM Watson AI Lab, 2018.

[10] Hall, Curt. "AI & Machine Learning in the Enterprise, Part IV: How Do AI Technologies Rank?" Cutter Consortium Data Analytics and Digital Technologies *Executive Update*, Vol. 18, No. 9, 2018.

Curt Hall is a Senior Consultant with Cutter Consortium's Data Analytics & Digital Technologies and Business & Enterprise Architecture practices. He has extensive experience as an IT analyst covering technology trends, application development trends, markets, software, and services. Mr. Hall's expertise includes artificial intelligence, cognitive systems, machine learning, conversational computing, and advanced analytics. He also focuses on the Internet of Things, including platforms, architectures, and use cases; big data platforms and use cases; blockchain for business; and business intelligence (BI), predictive modeling, and other analytic practices. Mr. Hall's research also includes mobile and social technologies in the enterprise as well as mobile BI and collaboration. He has conducted extensive research on how all these technologies are being applied to develop new advisory, decision support, customer engagement, and other enterprise applications.

Mr. Hall is a frequent contributor to Cutter Consortium's Data Analytics & Digital Technologies research deliverables as well as Cutter Business Technology Journal. *He served as Editor of numerous Cutter Consortium journals, including* Intelligent Software Strategies, Data Management Strategies, *and* Business Intelligence Advisor. *His study on the corporate use of data warehouses and the issues associated with data warehousing projects resulted in the in-depth Cutter Consortium research report* Corporate Use of Data Warehousing and Enterprise Analytic Technologies. *Mr. Hall also coauthored, with Cutter Consortium Senior Consultant Paul Harmon,* Intelligent Software Systems Development: An IS Manager's Guide, *and contributed to James Martin and James Odell's* Object-Oriented Methods: Pragmatic Considerations. *His work has appeared in various technical journals and IT publications, including as a contributing author to PricewaterhouseCoopers* Technology Forecast Yearbooks. *He can be reached at chall@cutter.com.*

AN ARBITRARY STANDARD?

2020: The Year That Agile Gets Found Out

by Barry M. O’Reilly

The bed of Procrustes[1] is a Greek legend that describes a giant — Procustes — who had a bed of a certain size. When entertaining guests, the giant would either stretch them or break off their limbs to make them fit the bed.

As the original creators of the Agile Manifesto recoil in horror at the giant they have created, it is easy to see why the procrustean bed is an apt metaphor.[2, 3] As Agile becomes ever more vapid (and meaningless), it becomes possible to break the limbs of any practice to make it fit the Agile bed, until the behaviors and the practices described as Agile begin to resemble the very practices the original movement sought to be rid of. “Four legs good, two legs better,” says the Agile industrial complex, as it totters around unconvincingly selling two-day certification courses.[4]

> *As the original creators of the Agile Manifesto recoil in horror at the giant they have created, it is easy to see why the procrustean bed is an apt metaphor.*

For those who previously had no problem in asking why the Agile emperor was not only naked but also deranged, 2020 will bring some satisfaction and a changing of the guard. The communist argument — that communism absolutely will work if only it is done right — will no longer hold for Agile as many become acutely aware that the meaningless, certification-driven Agile industrial complex is made up of an increasing percentage of “dark” or ‘”faux” Agile, or Agile “in name only,” practices. “True” Agile unfortunately remains a Procrustean idea, only appearing where things have gone well, with dark Agile suspiciously seeming to occur only in failing projects.[5] And there are many failing projects, if we are to believe the few sources of empirical evidence, such as Chris Porter’s “An Agile Agenda”[6] and the Standish Group’s CHAOS reports.[7]

As Agile makes its way to the boardroom, it will be harder and harder to hide behind procrustean declarations of what is and isn’t Agile, as the key to understanding success or failure will cease to be anecdotal and start to focus on cold, hard results. Cynicism will grow, as with all trends, and answers will need to be forthcoming.

What will change in 2020, however, is our perception of the problem. Developers have long seen change as the enemy, the reason for requirements churn, and something to be either fought, predicted, or embraced. The last few years have seen some digging deeper than the Agile Manifesto’s aphorisms, trying to understand change instead of mastering it via process or prediction. In truth, change represents how developers are forced to view the world because this is traditionally how problems are presented to them. Yet, most of what is presented as change to developers is a result of uncertainty in the business world, and the Agile sticky plaster of process, Post-it Notes, and certifications pretends to solve the problem of change without ever tackling the much more difficult question of uncertainty. Uncertainty is left up to the business, which bizarrely now looks to Agile methods to solve the problem it should have been solving all along.

The reason for change is because businesses present problems as requirements, requirements that are half-truths elaborated in the shadows of uncertainty, and as the truth reveals itself, changing requirements become a second-order effect. Agile therefore fixates on stemming the bleeding without ever stitching the wound, eventually allowing the patient to bleed to death, albeit with working software every two weeks. The truth is that the only true way to cope in modern business environments is to embrace not change, but the uncertain. Agile is, and has been, a response to uncertainty, but the current practices around Agile at scale involve selling certainty to executives. Selling certainty in an uncertain environment is an attractive pitch, but it can be done only so many times. The Agile movement’s focus on process as the solution to uncertainty has allowed technical quality to fall by the wayside, bringing even more doubt as to the ability of Agile to actually deliver. As Agile practices crash and burn, proponents gather to complain about the reasons it's not working, usually focused on the new favorite target of hierarchical management practices. Such excuses will not be endured for long. The Agile movement has served its purpose as a vehicle for driving the needs of developers frustrated by working in complex contexts that neither they nor their task givers understood, but it will soon be time to take stock, to look back at 20 years of hype and ultimately underachievement.

Standish CHAOS reports show that the number of successful projects has barely shifted since the publishing of the Agile Manifesto.[8] Although it shows much higher rates of success in Agile than in waterfall projects, the overall numbers have not shifted enough to suggest that anything has changed significantly, which suggests that the choice of methodology is not the driver of results or that successful teams had already figured things out before the Agile Manifesto. This leads to the conclusion that agility and quality are products of the team, not of the process. The same teams that have had success with Agile would probably have had success if constrained to waterfall processes — but these ideas are dangerous, since they suggest that developer talent is what survives uncertainty and drives results, and no one can sell developer talent with the same margins as certification programs based on simplistic processes and truisms.

In 2020, Agile will reach fever pitch, as it moves on from software development to penetrate the nightmares of naive executives. There will be more hype, more noise, and more religion. But the dam has already sprung a leak. Indeed, the IT industry is starting to embrace the Cynefin framework,[9] which leads to the obvious conclusion that while the Agile Manifesto had the diagnosis right in reacting to the changes caused by underlying uncertainty, it only ever guessed at a potential cure. It will become increasingly obvious that few Agile methodologies stand any form of empirical test, and the dam will eventually break.

Agile will never officially die, of course. Its procrustean bed will always fit everyone; complexity approaches will be absorbed and older methodologies will be quietly swept under the rug, as Agile changes to become something else entirely, something where technical quality, developer talent, and understanding of complexity become paramount to success.

This is a hard argument to make. So convinced are the followers of today's version of Agile that their arguments seem to them obvious truths, anecdotes pass for data, and the loose relationship between cause and effect is always interpreted in favor of a set of fluid principles in a manifesto that no one really seems able to make concrete.

In a world where uncertainty is the rule, there cannot be a process, a set time for meetings, or an exact way to design, break down work, put Post-it Notes on the wall, or handle requirements and change. Only the people working directly with a problem can decide on tools and process in the evolving picture of their project, and their individual talents — not adherence to or avoidance of certain ideas — guide whether they achieve success or not. In 2020, the role of uncertainty and talent will become clear. The proponents of Agile will claim that they always meant to emphasize uncertainty and talent, and some of them truly did, but the Industrial Agile that has evolved beyond their control needs to be put to bed — in whatever size bed we need.

References

[1] "Procrustes." Wikipedia, 2020.

[2] Fowler, Martin. "The State of Agile Software in 2018." martinFowler.com, 25 August 2019.

[3] Jeffries, Ron. "Developers Should Abandon Agile." RonJeffries.com, 10 May 2018.

[4] "Important Quotations Explained: *Animal Farm* — George Orwell." SparkNotes, 2020.

[5] Agile is a Procrustean concept, in that it is made to fit the narrative of success; those Agile projects that fail and don't help the narrative are rejected as not being true Agile.

[6] Porter, Chris. "An Agile Agenda: How CIOs Can Navigate the Post-Agile Era." 6Point6 Technology Services, April 2017.

[7] "Sample Research." The Standish Group International, Inc., 2020.

[8] The Standish Group International (see 7).

[9] Snowden, David J., and Mary E. Boone. "A Leader's Framework for Decision Making." *Harvard Business Review*, November 2007.

Barry M. O'Reilly is the founder of Black Tulip Technology and creator of Antifragile System Design. Previously, he held positions as Chief Architect for Microsoft's Western Europe practice and IDesign, IOT TAP Lead for Microsoft's Western Europe practice, Worldwide Lead for Microsoft's Solution Architecture Community, and startup CTO. He can be reached at barry@blacktulip.se.

ARE WE THERE YET?

Trends Shaping Drone Adoption for 2020 and Beyond

by Helen Pukszta

This year and the next few years will bring more regulatory changes and new opportunities for both business users of drones and drone technology providers. Some of the foundational US Federal Aviation Administration (FAA) regulations focused on integrating small unmanned aircraft systems (UASs), or drones, into the national airspace are briskly moving forward and converging with independent but complementary drone technology advancements. Together, they are moving us closer to the holy grail of the drone industry: scalable, integrated, continuous, long-range operations beyond visual line of site (BVLOS) and with little or no human intervention.

> *Amazon is touting its drone as "independently safe" and capable of delivering packages in less than 30 minutes.*

The Skies Are Now Open for Drone Delivery

With announcements on two regulations, one addressing the certification of unmanned aircraft and the other the certification of carriers using drones for delivery, the FAA revealed the regulatory framework that accommodates commercial package delivery by drones.

Drone Airworthiness Certification

Unlike airplanes or helicopters, unmanned aerial vehicles do not require FAA airworthiness certificates. Nor would such certification be practicable in general for most drone original equipment manufacturers (OEMs). Restrictions now in place under the FAA Part 107 rules are designed to keep drones flying low-risk missions, and drone users benefit from healthy drone tech innovation and availability of a multitude of drone makes and models, none of which are ever (officially) reviewed by the FAA.

Some of this is about to change. The FAA recently announced a proposed rule for the type certification of some drones under special classes of aircraft.[1] Large aircraft makers — such as Boeing, Airbus, or Cessna — apply for type certifications for their aircraft before they are authorized to fly them. Now all the major aspirants in drone package delivery will want that airworthiness certificate for their delivery drones as well.

The FAA had issued a special experimental airworthiness certificate to Amazon Prime Air a few years ago, and the company has now requested a full certificate for its latest iteration of the drone, unveiled at last year's Amazon *re:MARS* conference.[2] Featuring multiple safety and sense-and-avoid technologies aboard the aircraft, Amazon is touting its drone as "independently safe" and capable of delivering packages in less than 30 minutes. It's likely this is the drone we'll be seeing making Amazon package deliveries. And it's likely we will finally see some of those deliveries in 2020.

Carrier Certification for Delivery by Drones

Companies wanting to use drones for package delivery are directed to fly under FAA Part 135,[3] the same rules as air commuter and on-demand air taxis, with that certification process now adopted for drone operations.

A few companies now hold a Standard Part 135 air carrier certificate that effectively makes them drone airlines. They include Alphabet's Wing Aviation and UPS Flight Forward. Amazon Prime Air is in the process of getting its Standard Part 135 air carrier certificate. The FAA is currently working on a handful of additional applications, and there will likely be more.

The Standard Part 135 certificate does not set limits on the size or scope of operations, and Part 107 restrictions no longer apply. The FAA has clarified that this certification is currently the only path for drones to deliver packages and fly BVLOS.

Although the FAA is using the existing regulatory framework to enable package delivery — with both drone air carrier and drone airworthiness certifications required — the agency has recognized that in order for more complex drone operations to become routine, we will need a regulatory framework that is more specific to the needs of complex, high-volume drone operations.

In short, drone deliveries can take off, but there is much more to come.

Drone Remote ID Will Enable Tracking of Drones in the Air

The FAA's recent and long-anticipated notice of proposed rulemaking for the remote identification of drones outlines the framework for broadcasting drone ID and location, which could then be cross-referenced with drone registration data.[4] Virtually all drones produced for operation in the US will be required to comply and broadcast their remote ID information using radio frequency as well as by connecting via the Internet (when service is available) to a UAS service supplier, a private party approved by the FAA.

This is a significant change, and the FAA is allowing three years for it to take full effect. Much of 2020 will likely be spent on the development and collection of standards and technical requirements to meet the proposed rule. The importance of implementing the remote ID is well captured in this FAA statement:

> The remote identification framework would provide UAS-specific data, which could be used in tandem with new technologies and infrastructure to facilitate future, more advanced operational capabilities (such as detect-and-avoid and aircraft-to-aircraft communications that support [BVLOS] operations) and to develop the necessary elements for comprehensive UAS traffic management (UTM).[5]

The remote ID gets us closer to UTM implementation, which is the key enabler of flying BVLOS (now prohibited without an explicit waiver from the FAA) and autonomous operations (now illegal, as a pilot in command is required at all times for every drone in the air).

How does the remote ID rule affect current commercial and public sector users of drones? It has little immediate impact, as the full rollout will come gradually. Most drones now in operation, particularly in the enterprise class, can be made compliant relatively easily with a drone maker's firmware update and the use of yet-to-be defined apps.

The ADS-B Mandate Will Lead to Safer Skies

As of this year, all commercial aircraft and aircraft flying in Class A, B, and C airspace are required to be equipped with transponders having ADS-B (automatic dependent surveillance–broadcast) out capability.[6] ADS-B uses GPS to determine an aircraft's position and broadcasts it at rapid intervals, along with altitude, velocity, and other data. That data can be used by other aircraft and air traffic control equipped with an ADS-B in receiver.

Drone deliveries can take off, but there is much more to come.

This mandate may seem only indirectly related to drone operations. Drones will not be equipped with ADS-B out, as the volume of data from UASs (which are expected to outnumber manned aircraft) will not be useful to air traffic controllers. But data transmitted out from non-drone aircraft can be automatically picked up by a drone to alert it to the presence of other aircraft in the vicinity, causing it to automatically yield and keep a safe distance.[7]

Some drone makers have already implemented ADS-B in, and their drones receive information broadcast from ADS-B out transmitters and alert the pilot to the presence of broadcasting aircraft. Given the relative ease of implementation, more drone makers will likely follow suit. Many drone models also have built-in obstacle and collision avoidance, but the technology isn't perfect, and it is often disabled in the course of inspection work; for example, when a pilot needs a closer look at an object or a structure.

Recent Regulations Present New Opportunities, But Also Questions

With these new regulations, there is an opportunity for drone makers to pursue airworthiness certificates and sell or lease such UASs to drone delivery operators. There is an opportunity for third-party operators to offer drone delivery services as air carriers under Part 135. There is an opportunity for the delivery service to be hired by the consumer or business ordering a product or by the merchant selling it. For those with even deeper pockets, there is an opportunity to have an integrated operation of drone deliveries using their own certificated drones (e.g., the Amazon Air approach).

But there is little room for a corner restaurant to remotely pilot the drone it now owns to deliver a pizza. It's hard to imagine many scenarios where that would be practical under current Part 107 restrictions (no flights BVLOS, over people, or at night). Yet the idea of a small merchant delivering its product to a customer via drone should not be that much different — or, ultimately, less safe — than delivering the same product in a car. The infrastructure and regulations for that entrepreneurial freedom are not yet in place. Here's hoping that the remote ID rule is one step forward in getting us there.

> *The cost of today's FAA drone certifications could stifle innovation and competition in today's drone market and ultimately shift much of that cost to the drone buyers.*

It is also unclear where the new FAA policies leave the much larger, non-certificated part of the commercial drone market or what the path is to lifting BVLOS and other restrictions to open up the economies of scale and significant additional value that drones can bring outside of the headline-grabbing business of drone deliveries.

Will using a drone with an airworthiness certificate make it more likely to be cleared for BVLOS operations, for example, to inspect miles of oil and gas or electrical infrastructure? Is there a happy medium — driven by a framework of safety standards for both technology and operations — perhaps requiring simpler certification through other organizations or only self-certification? The cost of today's FAA drone certifications could stifle innovation and competition in today's drone market and ultimately shift much of that cost to the drone buyers. This challenge applies even if such certifications are not mandated but perceived as the only viable option.

Expect more on the regulatory front for drones in 2020. It's unlikely, though, that any of the rules will impinge on the current business and public sector usage of drones. If anything, they might expand it.

Drone Technology and Its Adoption Continue to March Forward

This year will see deeper experimentation and adoption of drone technology for the use cases already in play — infrastructure and asset inspections; mapping, surveying, and model building; public safety; precision agriculture; and specialized detection missions.

Technology, particularly the integration aspects, will continue to mature as well. You will see it in smaller and more powerful sensors (48MP drone cameras have just debuted), longer flight times, smarter batteries and controllers, communication links with increased coverage and reliability, faster edge processing for faster results, and increasingly sophisticated ecosystems of software for mission planning, mapping, and analytics.

You will see more innovations that make drones not only more useful and powerful but also increasingly safer — whether those innovations are onboard the aircraft, at the controller, or with separate anti-crash add-ons and counter-drone devices. Amazon's MK27 delivery drone hints at such innovations.[8] Moreover, Skydio recently released Skydio 2,[9] a self-flying, obstacle-avoiding drone using artificial intelligence and a host of sensors to stay amazingly crash-proof. It is a consumer drone and can't fly at night, but it gives us a taste of things to come across all segments. More sensor-laden, self-piloting drones will follow, with similar technology likely to cross over to the commercial and enterprise side.

Regulatory changes, new drone technology, and continuing business adoption will make 2020 an exciting year for all drone users, but many sweeping changes, opportunities, and automation benefits of drones are still ahead of us.

References

[1] "Type Certification of Unmanned Aircraft Systems." *Federal Register*, 3 February 2020.

[2] Vincent, James, and Chaim Gartenberg. "Here's Amazon's New Transforming Prime Air Delivery Drone." The Verge, 5 June 2019.

[3] "Package Delivery by Drone (Part 135)." US Federal Aviation Administration (FAA), 1 October 2019.

[4] "UAS Remote Identification." US Federal Aviation Administration (FAA), 21 January 2020.

[5] "Remote Identification of Unmanned Aircraft Systems." *Federal Register*, 31 December 2019.

[6] "Equip ADS-B." US Federal Aviation Administration (FAA), 10 February 2020.

[7] Helicopters and agriculture planes flying at low altitudes can be particularly vulnerable to a collision with a drone.

[8] Garrett-Glaser, Brian. "Amazon Seeks FAA Approval for Prime Air Drone Delivery." Avionics International, 9 August 2019.

[9] "Skydio 2." Skydio, 2020.

Helen Pukszta is a Senior Consultant with Cutter Consortium's Business Technology & Digital Transformation Strategies practice. She is also President and cofounder of Drone Arrival, a company that helps organizations leverage the transformative power of drone-based technologies as the foundation for a new breed of solutions for private and public sectors alike, with the goal of improving businesses and lives. With her more than 20 years helping businesses innovate through technology, Ms. Pukszta has extensive leadership, advisory, and research experience, particularly as it relates to digital strategy, organizational structure, and culture. She is an expert in incorporating technology considerations into business strategies and building and evaluating business cases for technology-based products and services. After beginning her career as a systems engineer, Ms. Pukszta has held positions in IT management and management consulting and has authored numerous articles on a variety of business technology innovation and management topics. Ms. Pukszta earned a bachelor of science degree in computer science from DePaul University and an MBA in strategic management and finance from the University of Chicago. She can be reached at hpukszta@cutter.com.

CUTTER Business Technology Journal

About Cutter Consortium

Cutter Consortium is a unique, global business technology advisory firm dedicated to helping organizations leverage emerging technologies and the latest business management thinking to achieve competitive advantage and mission success. Through its research, training, executive education, and consulting, Cutter Consortium enables digital transformation.

Cutter Consortium helps clients address the spectrum of challenges technology change brings — from disruption of business models and the sustainable innovation, change management, and leadership a new order demands, to the creation, implementation, and optimization of software and systems that power newly holistic enterprise and business unit strategies.

Cutter Consortium pushes the thinking in the field by fostering debate and collaboration among its global community of thought leaders. Coupled with its famously objective "no ties to vendors" policy, Cutter Consortium's *Access to the Experts* approach delivers cutting-edge, objective information and innovative solutions to its clients worldwide.

For more information, visit www.cutter.com or call us at +1 781 648 8700.