FEDERAL EMERGING TECHNOLOGY SUMMIT

APRIL 17, 2018 | MARRIOTT METRO CENTER | WASHINGTON, DC

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Emerging Technology Collaboration Symposium held on April 17, 2018 in Washington, D.C. in conjunction with the ATARC Federal Emerging Technology Summit.

I would like to take this opportunity to recognize the following session leads for their contributions:

MITRE Chair: John Griffith

Challenge Area 1: Artificial Intelligence and Machine Learning

Government Lead: Stephen Dennis DHS S&T
Industry Lead: Bhavish Madurai, IBM
MITRE Lead: Chuck Howell

Challenge Area 2: Blockchain and Other Emerging Technologies

Government Lead: Michelle White, GSA
Industry Lead: Shamlan Siddiqi, NTT Data
MITRE Lead: David Goldenberg

Challenge Area 3: Internet of Things

Government Lead: Jeff Voas, NIST
Industry Lead: Sri Elaprolu, Amazon Web Services
MITRE Lead: Sophia Applebaum

Challenge Area 4: Using Digital Technology to Enhance Citizen Experience

Government Lead: Gwynne Kostin, GSA
Industry Lead: Brett Swartz, Liferay
MITRE Lead: Daniel Weiss

Challenge Area 5: Content Management in a Digital Government Environment

Government Lead: Clara Hall, DoS
Industry Lead: Lisa Marcus, Nuxeo
MITRE Lead: Beth Pabich

Below is a list of government, academic and industry members who participated in these dialogue sessions:

Challenge Area 1: Artificial Intelligence and Machine Learning

Karl Brimmer, USCIS; Patrick Carrick, DHS; Thomas Chester, SEC; Dr. Russell Davis, DHA; Vicente Flores, DHS; Hannah Jung, IBM; Vivien Lau, EIA; Grant Malmberg, IBM; Jon Manger, USCIS; TJ May, NNSA; Murali Nataraj, DOJ; Thomas Nguyen, DISA; Brian Nordman, DoS; Kelsey O'Neill, IBM; Kalpesh Patel, DHS ICE; Anupami Rai, LOC; Eric Steinberg, DOT; Carl Tallis, MITRE; John Torrence, GSA

Challenge Area 2: Blockchain and Other Emerging Technologies

Mimi Boussouf, DoD-VA IPO; Dara Dastyar, ED; Amgad Fayad, MITRE; Sue Lou, ED; Kyle Nichols, IBM; LeAnn Oliver, DOE; Thomas Reaves, EPA

Challenge Area 3: Internet of Things

Alenka Brown, IDA; Craig Chapman, Center of IoT Security; Michele Cohen, NNSA; Dick Greene, USAID; Stephen Harding, GSA; Regina Harrison, NTIA; Pamela Jackson, DHS CBP; Art Saenz, NSF; Marc Schneider, MITRE; Gaurav Seth, MITRE

Challenge Area 4: Using Digital Technology to Enhance Citizen Experience

Karthik Gopalakrishna, Mulesoft; Fady Hakim, Liferay; Francis Hsu, DHS USCIS; Shad Iman, Mulesoft; Sylvester Smith, GSA

Thank you to everyone who contributed to the MITRE-ATARC Emerging Technology Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)
Host organization of the ATARC Federal Emerging Technology Summit

FEDERAL SUMMITS

APRIL 2018
EMERGING TECHNOLOGY SUMMIT REPORT*

August 13, 2018

John Griffith, Sophia Applebaum, Marc Schneider, David Goldenberg, Chuck Howell, Beth Pabich, Daniel Weiss, Justin F. Brunelle
The MITRE Corporation

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

Contents

1 ABSTRACT

The first Advanced Technology Academic Research Center (ATARC) Federal Emerging Technologies Summit was held on April 17, 2018. The summit included five MITRE-ATARC Collaboration Sessions. These collaboration sessions allowed industry, academic, government, and MITRE representatives the opportunity to collaborate and discuss challenges the government faces in adopting and utilizing emerging technologies such as artificial intelligence and blockchain. The goal of these sessions is to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of emerging technologies and associated best practices within the government.

Participants representing government, industry, and academia addressed five challenge areas in the federal emerging technologies domains: Artificial Intelligence and Machine Learning; Blockchain and Other Emerging Technologies; Internet of Things; Using Digital Technology to Enhance Citizen Experience; and Content Management in a Digital Government Environment.

This white paper summarizes the discussions in the collaboration sessions and presents recommendations for government, academia, and industry while identifying intersecting points among challenge areas. The sessions identified actionable recommendations for the government, academia, and industry which are summarized below:

> Emerging technologies are often misunderstood. Leadership needs to maintain appropriate education on emerging technologies to identify reality from buzzword and media hype. The potential benefits and challenges of emerging technologies need to be communicated throughout the enterprise.
>
> Effective research is important. Agencies and adopters should start small with pilots and proof-of-concept efforts to gain experience and understanding of how emerging technologies apply to a domain.
>
> Artificial Intelligence (AI) is becoming pervasive across all domains. Of particular importance is understanding how AI will impact emerging technology usage and the appropriate usage of AI and Machine Learning (ML) tools.

2 INTRODUCTION

During this first Federal Emerging Technologies Summit, held on April 17, 2018, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in adopting and utilizing emerging technologies. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of emerging technologies use and research in the government. Participants ranged from the CTO, CIO, and other executive levels from industry and government to practitioners from government, industry, and federally funded research and development centers (FFRDCs) to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple FFRDCs [12]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology. MITRE works in partnership with ATARC to host the collaboration session portion of the ATARC Federal Technology Summit Series. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in various emerging technologies domains, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curriculum development, and to help produce graduates ready to join the work force and advance the state of their research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 COLLABORATION SESSION OVERVIEW

Each of the five MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed:

- Artificial Intelligence and Machine Learning;
- Blockchain and Other Emerging Technologies;
- Internet of Things;

- Using Digital Technology to Enhance Citizen Experience; and
- Content Management in a Digital Government Environment.

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 Artificial Intelligence and Machine Learning

The *Artificial Intelligence and Machine Learning* session focused on the increasing emphasis on Artificial Intelligence (AI) and Machine Learning (ML) as an aid to decision making. With government agencies having a greater reliance on data and analytics, how can these technologies be utilized to accelerate and transform the usage of this information? This session examined how AI and ML can be utilized to enhance an agency's mission.

3.1.1 Challenges

The collaboration session discussions identified the following challenges with applying AI and ML in the government:

- Workforce hiring and retention;
- Evaluation of technologies and products; and
- Evaluation and understanding of ML models – this is particularly challenging as government organizations are being continuously asked to do more with less.

3.1.2 Discussion Summary

The session had good participation from across government and industry. The discussion was very broad but focused more on ML and the aspects of systems that learn than the more general topic of AI.

The initial discussions touched on challenges with properly appling ML. Users expect it to be easier to use ML than it is. Deciding what hardware and software to use for ML applications is also challenging. Practitioners should have experience solving relevant problems using real data to help them understand the performance requirements. Practitioners creating ML models need proper training and decision makers need to understand the process for developing and applying ML, as well.

Recruiting, (continuous) training, and retaining experts are important aspects of creating an organization capable of leveraging AI and ML. Typically, private industry can generally

pay more than government, so motivation for remaining in public service positions has to be linked to mission. Even if AI and ML work is outsourced, in-house expertise is still needed to oversee, guide, and assess ongoing efforts.

Government use of AI and ML introduces significant – and often unique – risks. Unintended and unrecognized bias in ML models can arise from biases in the data and processes used for training. There are numerous well-known examples from biased predictive policing models that perpetuate inequalities [10] to chatbots that learn bigotry from malicious users [13]. Commercial companies, such as Google, employ large numbers of humans to check the quality of their models. Government organizations may not have the same ability to hire staff for quality control even though the importance of quality may be higher in government applications than in commercial applications. Careful consideration is also needed to determine if a potential application of AI or ML is legal, ethical, and in the best interests of those affected by its use. For instance, there are reports of China using facial recognition to identify jaywalkers and publicly shame them [3].

Intentional manipulation is a risk for every government agency. Both criminal and adversarial purposes may be behind such attacks. Government data and applications are deeply connected to those of other government and commercial organizations. Attacks can occur where not expected or where there is little oversight. ML applications present emerging threats beyond traditional cyber threats. Attacks can be targeted at both the learning data and process aspects as well as at exploiting weaknesses in ML models. For instance, so called adversarial imagery techniques can be used fool a ML model that a picture of one thing is really a picture of something else by imperceptibly (to a human's eye) altering a few pixels in the image [11].

3.1.3 Recommendations

The participants in the *Artificial Intelligence and Machine Learning* collaboration session identified the following important findings and recommendations:

- The government needs to develop a more general way to describe maturity levels for AI similar to the levels of autonomy for autonomous vehicles [15]. Such levels might include the following:

    1. Human decision making;
    2. Computer-assisted decision making;
    3. Automated decision making with human intervention; or

4. Fully automated.

- With respect to workforce, education, training, hiring, and retention are important.
- In the decision to buy or build a service – not all agencies can select "build". Organizations need to identify a process to decide when and how to make that decision.
- Organizations should understand and document data provenance, metadata, and strive for high quality data.
- Organizations should compare new ML models to existing baselines whenever possible.
- Governance is important; government agencies should make an effort to find an internal champion.

3.2 Blockchain and Other Emerging Technologies

The *Blockchain and Other Emerging Technologies* session discussed blockchain technologies and the anticipated impact and utilization of blockchain on other areas of government. Blockchain is a buzzword, but this session aimed to identify the current and potential impact it has on the Federal Government. This discussion examined the state of blockchain within government agencies and discussed the current and future impact of this and other associated emerging technologies.

This session had three goals:

- Engage in level-setting to disambiguate myths and misconceptions around blockchain technology;
- Learn about existing pilot and proof-of-concept blockchain implementations that exist across the government; and
- Discuss current and upcoming issues with blockchain development and applying blockchain technology to tasks across the governmental space.

3.2.1 Challenges

The collaboration session discussions identified the following challenges with implementing blockchain for government adopters:

- The benefits of immutability and federation with blockchain are currently unknown and
- Blockchain is not yet ready for enterprise-wide adoption in the Federal Government

3.2.2 Discussion Summary

The collaboration session began with a conversation with two main goals: level-setting (i.e., understanding the level of understanding about blockchain in the room) and dispelling any myths and misconceptions about blockchain. While blockchain has a lot of hype surrounding it, it is a very complicated topic that is constantly changing, making level-setting important. The participants settled on the idea that blockchains involve a few distinct but interlinked pieces of technology: a shared cryptographic ledger, a peer-to-peer ledger, and a consensus algorithm.

Once the participants finished the level-setting conversation, they began talking about different blockchain pilots and proof-of-concepts that already exist or a being developed in the governmental space. These included projects such as:

- Identity Access Management (IdAM);
- Acquisition;
- Investigation into blockchain for enhanced student transcripts;
- Airport security; and
- Global financial services.

Talking about these projects led to two different topics: types of blockchains and implications of using these types of blockchain technology.

When the participants spoke about types of blockchains, they divided blockchains into two major types.

1. Public blockchains (e.g., Ethereum, Bitcoin) are are easily accessed, easily developed on, and can be pseudonymous but often have slow transaction speeds due to common use of proof-of-work algorithms. In addition, information on public blockchains is easily accessible which may be good or bad depending on application.

2. Private blockchains (e.g., certain versions of Ethereum, Tendermint, Ripple) are blockchains with access controls which means that access to the blockchain is limited in some fashion. These blockchains can be very efficient, and utilize a wide variety of consensus algorithms.

We also briefly spoke about other blockchain types such as KSI[1] (a blockchain that stores metadata and signatures about data) [4], [5], [7].

Speaking about the benefits or detriments of blockchain technology took up a majority of the session time. Spring boarding from the government blockchain pilot discussion and the questions asked in the ACT-IAC Blockchain Playbook [1], the participants talked about a wide variety of pros and cons with regards to blockchain.

Decentralization (Pro) – In any circumstance where either for logistical, legal, or political reasons one cannot have centralization of authority or a central authority managing the data, blockchains can be of great utility.

Moving across different data silos (Pro) – Blockchains – being decentralized – can more easily move across different and previously incompatible data silos.

Cost (Pro) – In certain circumstances, blockchain technology can be cheaper than going to distributed database functionality.

Transparency (Pro) – In most cases, the transparency of blockchain technology and access to blockchain data was seen as a positive by participants.

Federation (Uncertain) – While blockchain technology may indeed help reduce the problems with federation, it is not a given. It is possible to have mutually incompatible blockchains, so one may have a situation where multiple incompatible blockchains require a separate aggregator service.

Immutability (Pro and Con) – Immutability can be both a pro and a con with regards to blockchain technology. On the one hand, immutability offers secure cryptographic protection of the integrity of the data. Blockchain immutability can mean that it is extremely hard to recover from a mistake; whether this is a bad transaction or a badly written smart contract. In addition, it can be difficult (though not impossible) to utilize blockchains in an application that is required to "forget" data in some respect.

After talking about the pros and cons of blockchain technology, the participants discussed blockchain performance and different types of entities inside a blockchain application. They mentioned that while blockchain size can be an issue, not every entity in a blockchain application need hold onto the whole blockchain database. This led to dividing entities in the blockchain space into a few types.

[1] `https://guardtime.com/technology`

- **Users**: These are the end users; depending on the implementation, they may (and perhaps should not) be aware of the blockchain itself.
- **Nodes**: These are the computers on the peer-to-peer network; nodes are responsible for sending information back and forth on the network and can serve to validate some transactions due to the validation criteria of a particular blockchain; while some nodes should hold the entire blockchain data set, it is not strictly necessary.
- **Validators**: These have all the properties of nodes with the additional property that they run the consensus algorithm of the network; these are required to hold the entire blockchain data set.

3.2.3 Recommendations

The participants in the *Blockchain and Other Emerging Technologies* concluded that while blockchain may be immensely useful in the right situation(s), the blockchain domain is a highly dynamic and changing space, changing as fast as month by month. A wide variety of blockchain technologies exist and new technologies are created every day. As such, the blockchain communities within and associated with the Federal Government should focus on the following areas:

- Exploring the blockchain space through research, proof of concept and pilot work is highly recommended and
- It may be premature to immediately work to build an enterprise level blockchain capability.

3.3 Internet of Things

The large scale and heterogeneity of the Internet of Things (IoT) is an obstacle in the engineering of a system using IoT devices. It is challenging for an organization of any size to assess the security of their IoT systems without an architectural framework or standard for reference. This session examined current standards related to IoT, how they can potentially promote interoperability of IoT devices, and trust in systems containing these devices.

3.3.1 Challenges

The following challenges to the use of IoT were identified:

- There is no universally accepted definition of IoT;
- The properties of IoT devices are typically unknown;
- The security capabilities of IoT devices are limited or difficult to configure;
- Reference architectures for IoT systems currently do not exist; and
- There is no standardized vetting procedure of IoT devices and systems.

3.3.2 Discussion Summary

The session opened with a discussion of the definition of IoT. Unfortunately, the participants were unable to reach consensus on the definition, highlighting the need for a common language to be used across the various IoT domains. That said, the participants discussed multiple IoT domains, such as building automation, health care, and smart cities [8].

Moreover, the participants identified key facets of IoT such as reliability, privacy, performance, quality, and security. Because of the rapid evolution of features and technology, they posited that companies are pressured to focus on time to market rather than reliability and security of their devices.

In spite of its ubiquity, IoT faces many significant challenges. Most pertinently, there is no formal and accepted definition of IoT. This makes it difficult for vendors, researchers, and consumers to fully understand the issues facing IoT environments and can also stifle discussion. Without proper definitions, it can be challenging to construct accurate and realistic threat models.

Coupled with a lack of definitions, there are very few publicly available and commonly used reference architectures for IoT systems. This is due in part to the fragmentation within the vendor ecosystem; many vendors offer their own architectures geared towards their products, while others assume that their products will serve a role, leaving the ecosystem provider or the consumer to define how it fits into the larger architecture. Given this fragmentation, it may be hard for industry to, on its own, center around a single reference architecture and definition (though NIST's recent effort to define and standardize IoT shows promise [14]).

The lack of formalisms extends to the IoT devices themselves; the specific properties and features of IoT devices are typically unknown. This is both a definitions problem and an implementation problem. First, when bringing a new device into an IoT system, there is no way to know precisely how – if at all – it will interact with the other devices. Second, on the device itself, there is no way to communicate its implementation capabilities. Does it push data to the cloud, and if so, does it do so with a hardcoded server address, or a dynamic DNS

one? Does it use HTTP or HTTPS? To what ports does it need access? Lacking these details can make it difficult to deploy, secure, and use IoT systems.

Security is a large concern for IoT systems, as they are pervasive, can access intimate and sensitive data, and can control many aspects of consumers' lives. Despite this, security capabilities of IoT devices are often lacking and – when available – are difficult to configure. As an example, the recent Mirai botnet [9] exploited default credentials that were widespread across consumer devices.

Many of these problems have also been faced in the mobile ecosystem and, in response, services offering device or app vetting have emerged. These services will analyze either apps or devices themselves to identify security vulnerabilities and, in some cases, certify that they meet some minimum security standard. Unfortunately, the lack of formalisms in IoT makes this challenging to do for IoT devices, as many of the devices and properties are unenumerated. Nonetheless, formal vetting could help alleviate many of the concerns that can challenge wider-spread IoT deployment.

3.3.3 Recommendations

The participants in the *Internet of Things* collaboration session identified the following important findings and recommendations:

- They recommend a language for IoT that is portable across multiple domains;
- The groups developing IoT standards should involve all stakeholders: government, manufacturers, non-governmental organizations (NGOs), and end-users;
- There is a gap in the enumeration of the fundamental building blocks common to all IoT that standards should fill; and
- Too many groups working on standards are overlapping effort and sometimes have gaps in the same areas; groups need to work in coordinated manner to cover gaps in IoT standards as well as reduced duplicated effort.

3.4 Using Digital Technology to Enhance Citizen Experience

Collaboration Session 4 was entitled *Using Digital Technology to Enhance Citizen Experience*. The focus of the session was on discussing the challenges with the digital experience for the citizen and what government can do to address these challenges as new technologies are introduced. The data in the latest Foresee e-government report shows that when citizens

interact with an excellent federal website, they are 87% more likely to use the website as a primary resource, 101% more likely to recommend the website, 51% more likely to return, and 58% more likely to trust in the government [6]. However, the McKinsey Citizen Satisfaction Score for private sector services was 2.5 times higher than public sector services, showing a large gap in public sector services in the expectations of citizens [2].

This session had two goals:

- Discuss how the government can improve the citizen experience on government sites so they are more in line with commercial experiences; and
- Discuss which modern methods can be applied as the government goes forward.

3.4.1 Discussion Summary

The session focused on three main topics:

- Private vs public citizen experience;
- Trust/ethics; and
- Future emerging technologies.

3.4.1.1 Private Vs Public Sector Experience During the morning Visionary Keynote Briefing, Congressman Rohit Khanna (17th Congressional District, California) stated that he does not think that a single person would say that the user experience of government sites is equal to the commercial sector. Yet citizens do expect their experience to be on par with the rest of their experience of technology.

Some differences in the private sector vs. the public may contribute to this experience. There is a motivational difference. Private sector experience is driven by monetary incentives. No one needs to convince the commercial sector to make their product user-friendly; this is vital to their success. However, in the public sector – which is frequently short on funding – there is rarely monetary incentive to improve the experience. To the government employee for which improving a site may pose additional work, there is more of a need to convince those implementing the site on the "why".

In addition, implementations are not always driven by the needs of the citizen. They may more be driven by regulations, security, culture, or process. Regulations and guidance keep things the same. Companies have lobbyists to shift antiquated laws, whereas government does not have a similar process. Culture also is a barrier. The intelligence community, in

particular, has a risk averse culture. There may also be resistance to change due to fear or jobs being lost as new technology takes its place. Lastly, the focus on outcomes instead of process does not consider the citizen's journey through the system and the inefficiencies and frustration inherent in that process.

There is also a proliferation of technology endpoints in the private sector. Mobile apps and sites are widespread, voice command interfaces are prevalent, and smartwatch access is common. This is not so in the public sector, where technology lags behind and even mobile access is not universal. One cause of this may be the way the two sectors view data. In many cases, government looks at citizen information as content in a form. The public sector, on the other hand, views the information as data that can be manipulated into many forms and used for many uses. In many cases, the public sector data is not transferred between systems even within the same agency and frequently cannot be transferred across services in different parts of government resulting in the citizen having to re-enter data multiple times. This is not so in the private sector where there is frequently a single point of entry and the data is available across different parts of the system.

3.4.1.2 Trust/Security/Ethics There are some more philosophical questions when it comes to trust and ethics. When one is talking about trust in the government, is the government a single entity? It may be the case that the general public views it as one but, in reality, the government is made up of many parts that create a whole. When a citizen is asked whether they can trust the government, it is likely not a "yes" or "no" answer. At a more practical level, how does one balance people's desire for convenience with security and other concerns?

The participants discussed how Social Security numbers are not the best way to keep track of people. They are easily hackable and once there is a breach it can give the hackers access to all a person's accounts. In addition, security happens where citizens cannot see it. There does not seem to be enough incentive for organizations to spend the resources needed to ensure that their stored data is not hacked. There also do not seem to be repercussions when data is stolen for organizations that do not secure citizens information well enough. This is particularly an issue as organizations gather more and more data in a single location.

The conversation then shifted to transparency issues with a number of major issues discussed. First, it needs to be clear to individual what the government is doing with their data. It needs to be clear what data is being collected. It needs to be apparent what is being tracked, as well. In addition, the government should be allowing the citizen to verify their information and the citizen should be able to edit the data collected on them if it is inaccurate. A copy of a citizen's data should also be able to be downloaded by that individual. Another

transparency issue is all the jargon concerning data storage and protection. There needs to be a plain language explanation of what is being done with an individual's data. Lastly, if there is a breach, the government should be alerting people immediately and provide next steps, if possible. Rather than a letter arriving months later disclosing the breach, perhaps an SMS message with next steps to secure one's information would be useful.

3.4.1.3 Future Emerging Technology Lastly, as more complex and futuristic technologies are created, it is important to stay in touch with the direction technology is taking and monitor the effects of these developments. Data input through mobile or voice interfaces is increasingly common. Biometric identification and access to technology through facial, voice or fingerprint markers are present in most new devices. At the same time, more data is being captured than ever before with a proliferation of cheap sensors and the advent of the IoT. In addition, AI and ML are accelerating the possibilities of what can be done with that data.

There are many benefits to such advancements and the government should strive to keep in step with the technologies that citizens expect. However, there are also inherent dangers present in these advances that the government needs to take steps to mitigate. Large collections of stored information provide a single place to hack, putting vast amounts of user data at risk of compromise. New sensors and data sources raise privacy concerns. Results from a ML algorithm are not always transparent and can unintentionally lead to bias.

As these technologies continue to develop, it would be prudent to consider and research their implications to citizens. For example, as mentioned before, there also needs to be more transparency into how AI is making decisions. If someone is, for example, being denied benefits because of a decision an AI system was making, there needs to be insight into that. What data was it using to make that decision? Was care taken to verify that there was no bias in the algorithm or decision making process?

3.4.2 Recommendations

The participants in the *Using Digital Technology to Enhance Citizen Experience* collaboration session identified several important findings and recommendations.

- Do not simply *re-skin*: The government needs to think beyond websites. Instead of just updating the "look and feel" of the site, make sure to think about the process and the citizen experience when going through that process. One example would be focusing on mobile access to government systems since that is a way many citizens currently access internet services.

- Interoperability is key: It is important that there is interoperability between government systems and that data flows between them. In addition, it would be helpful if relevant data (e.g. CDC alerts) flowed to private sector technology as well so that a person could find relevant public information embedded in public sites or use other interfaces such as voice access it.

- Centralization of data : Rather than having many sites and logins, there should be a single point of entry where citizens can login that has all their data accessible and where actions can be taken on that data. Where possible, automatically fill fields with data that is already in the system so citizens do not have to fill it in multiple times. Centralization of information will create a better experience for the citizen while allowing for more expedient processing on the government side.

- Personalization: The private sector provides an experience that is personalized to the customer. The government should look to personalize the experience to the citizen so that, for example, a user can get notifications if their license needs to be renewed or their taxes have not yet been filed. This would reduce what can sometimes be an overwhelming experience where government websites have dozens of forms and the citizen does not know what she needs to do at a given moment.

- Control over data: The government should provide citizens with access to their own data, ability to correct information that is incorrect, and alert them in a timely manner when data is lost or stolen.

- Closing the motivation gap: The government should find ways to effectively motivate the public citizen experience to close the gap between the private and public sectors.

3.5 Content Management in a Digital Government Environment

The *Content Management in a Digital Government Environment* session primarily discussed web content management. This included the aspects of the support and migration of legacy systems and the impact on content management.

This session had three goals:

- Discuss the support and migration of legacy systems;

- Identify best practices for metadata management; and

- Discuss the impact of emerging technologies on content management.

3.5.1 Challenges

The collaboration session discussions identified the following challenges facing content management:

- Comfort levels with cloud vary between agencies;
- Collaboration across agencies with varying tools and cultures; and
- Consolidating, integrating, and verifying authoritative sources is a challenge.

3.5.2 Discussion Summary

The participants began with a discussion of legacy systems and migration projects, citing the need to start small and take an iterative approach. They also mentioned that this can be an opportunity to standardize the look and feel of a web resource. However, overcoming local design desires can be a challenge. There is also an emphasis on the need to "create once, publish everywhere." This creates a solution to finding the authoritative version of content. However, consolidating, integrating and verifying authoritative sources is a challenge.

Front-end and back-end web content management involves integrating front-end publishing with back-end processes such as approvals. This can involve multiple different tools. Metadata management is also important in this process, including the following aspects:

- AI and ML are the key to doing this effectively;
- Synonym management; and
- Scaling up to 100s of tags and large volumes of content.

When performing content management, often enterprise or legacy tools conflict with preferred personal industry tools. Many younger workers, in particular, are used to personal tools such as Facebook, Instagram, and the Google suite, and find enterprise tools hard to use or *clunky*. Resolving this challenge requires the need for workers to be agile and embrace emerging technology. Staff must have the mindset to embrace changes and not fear being replaced. However, workforce willingness to adopt new tools varies between organizations, as does collaboration across agencies with varying tools and cultures. Comfort levels with cloud often varies between agencies.

3.5.3 Recommendations

The participants in the *Content Management in a Digital Government Environment* collaboration session identified the following important findings and recommendations:

- Start small, take an iterative approach;
- Leverage AI and ML effectively; and
- Foster a culture that embraces change and toolsets for increased efficiencies.

4 SUMMIT RECOMMENDATIONS

As is common with the MITRE-ATARC Collaboration Symposium discussions, this set of collaboration sessions discussions had a common set of themes:

- There is a clear difference in the user experience of public citizens using government applications and a user's experience using a commercial product;
- Security, trust, and ubiquity are pervasive issues in government use of emerging technologies; and
- AI and ML are becoming increasingly important, but must be used effectively and appropriately.

Overall, the participants in the collaboration sessions made notice of the need to improve the way in which emerging technologies are adopted, used, and implemented for citizens, agencies, and both internal and external partners. While keeping pace with industry is – in most cases – not possible, the government should strive to leverage best practices and principles from industry success in more efficient manners.

Further, as industry continues its adoption of emerging technologies, trust in the government's implementations is a major risk in future adoptions. For (hypothetical) example, citizens may be wary of the government's use of blockchain for accessing or controlling citizen information. The government should assess these impacts and take the appropriate measures and investments to ensure the effectiveness of technology adoption.

Finally, as data is being used for AI and ML, the government should focus on data quality to remove potential bias, ensure AI and ML tools are used in appropriate circumstances, and invest in research that establishes decision provenance for resulting decisions.

5 CONCLUSIONS

While the April 2018 Federal Emerging Technology Summit highlighted areas of continued challenges and barriers to adoption, the Summit also made recommendations regarding the future implementation of emerging technologies. For example, the government should use industry best practices to boost adoption successes and citizen buy-in.

While the Federal Government may lag behind industry in emerging technologies research, there is an opportunity to use this as an advantage and to lower risk.

Government also faces unique challenges, such as the stricter burden on safety, security, and decision provenance. The government has an opportunity to partner with industry and academia to drive the research in these areas based on their unique use cases. As the Federal Government moves forward with emerging technologies adoption, it should consider the impact on its citizens.

ACKNOWLEDGMENTS

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit.

The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the ATARC Emerging Technologies Summit web site[2].

REFERENCES

[1] ACT-IAC white paper: Blockchain playbook for the u.s. federal government. Technical report, ACT-IAC Emerging Technology COI, April 2018. https://www.actiac.org/act-iac-white-paper-blockchain-playbook-us-federal-government.

[2] A. Baig, A. Dua, and V. Riefberg. Putting citizens first: How to improve citizens' experience and satisfaction with government services. Technical report, McKin-

[2] https://www.atarc.org/emerging-tech-summit

sey Center for Government, December 2014. https://www.mckinsey.com/~/media/mckinsey/industries/public%20sector/our%20insights/how%20us%20state%20governments%20can%20improve%20customer%20service/putting%20citizens%20first%20how%20to%20improve%20citizens%20experience%20and%20satisfaction%20with%20government%20services.ashx.

[3] C. Baynes. Chinese police to use facial recognition technology to send jaywalkers instant fines by text. https://www.independent.co.uk/news/world/asia/china-police-facial-recognition-technology-ai-jaywalkers-fines-text-wechat-weibo-cctv-a8279531.html, March 2018.

[4] A. Buldas, A. Kroonmaa, and R. Laanoja. Keyless signatures' infrastructure: How to build global distributed hash-trees. Cryptology ePrint Archive, Report 2013/834, 2013. https://eprint.iacr.org/2013/834.

[5] A. Buldas, A. Kroonmaa, and R. Laanoja. Keyless signatures' infrastructure: How to build global distributed hash-trees. In H. Riis Nielson and D. Gollmann, editors, *Secure IT Systems*, pages 313–320, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. https://guardtime.com/files/BuKL13.pdf.

[6] ForeSee. The foresee experience index (fxi): E-gov – q1 2017. Technical report, ForeSee, May 2017. https://learn.foresee.com/hubfs/eGov_Q1_2017.pdf.

[7] Guardtime federal webpage on keyless signature infrastructure. Accessed July 5, 2018. https://www.guardtime-federal.com/ksi/.

[8] IEEE. Standard for an architectural framework for the internet of things. https://standards.ieee.org/develop/project/2413.html, 2018.

[9] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[10] C. O'Neil. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group, New York, NY, USA, 2016.

[11] Open AI Blog. Attacking machine learning with adversarial examples. https://blog.openai.com/adversarial-example-research/, February 2017.

[12] The MITRE Corporation. FFRDCs – A Primer. http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf, 2015.

[13] D. Victor. Microsoft Created a Twitter Bot to Learn From Users. It Quickly Became a Racist Jerk. https://www.nytimes.com/2016/03/25/technology/microsoft-created-a-twitter-bot-to-learn-from-users-it-quickly-became-a-racist-jerk.html, March 2016.

[14] J. Voas. Networks of 'things'. *NIST Special Publication*, 800(183):800–183, 2016.

[15] Wikipedia article: Autonomous car. https://en.wikipedia.org/wiki/Autonomous_car.